Operation Safety-Net

Best Practices to Address Online, Mobile, and Telephony Threats

Prepared by the

Messaging, Malware and Mobile Anti-Abuse Working Group

and the

London Action Plan

June 1, 2015

CAUCE

LONDON ACTION PLAN
INTERNATIONAL CYBERSECURITY ENFORCEMENT NETWORK

M³AAWG | MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP

This work is licensed under a Creative Commons Attribution-NoDerivs 3.0 Unported Licence
http://creativecommons.org/licenses/by-nd/3.0/deed.en_US
©2015 LAP and M³AAWG.

This report refers to some commercial products as possible solutions to various electronic threats. Inclusion of these products does not constitute an endorsement by organizations that have endorsed or contributed to this report.

Preamble

In October of 2011, members from the London Action Plan (LAP) and the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG) made a presentation to the OECD Committee on Consumer Policy (CCP) regarding the current prospect for the OECD's anti-spam recommendations to address future online threats.

At the meeting, a Canadian delegate of the LAP noted that while the existing set of OECD spam recommendations were highly successful in mobilizing industry and governments to take action to address spam, a greater understanding of the more sophisticated next generation of online threats would be beneficial. Based on initial follow-up with the Canadian CCP delegate and the Chair of the CCP, the National Anti-Spam Coordinating Body at Industry Canada prepared an outline for a report to be drafted by volunteer members of M³AAWG and LAP. The outline was shared and agreed upon by members of M³AAWG and LAP and was reviewed by the CCP Secretariat.

On June 6, 2012 members of LAP and M³AAWG met in Berlin to begin the process of developing the report which was published in October of that year. Three years later, this report has now been updated to reflect the changing landscape and the new ways cybercriminals are able to profit and avoid detection.

The original report was divided into four key sections:

i) Malware and Botnets,

ii) ISP and DNS,

iii) Phishing and Social Engineering, and

iv) Mobile Threats.

This second version of the report includes updates to the four original sections, and covers new areas including Voice over Internet Protocol (VoIP) and Voice Telephony fraud, Caller ID Spoofing, abuse issues for Hosting and Cloud Services and online harassment.

The process of updating this best practices report involved an invitation being sent to the M³AAWG and LAP membership seeking contributors for the report. Industry experts were chosen as section leads and these leads also sought input and contributions from experts outside of the M³AAWG and LAP membership. A list of contributors can be found at the end of this report.

M³AAWG, the LAP and CAUCE (the Coalition Against Unsolicited Commercial Email) have officially endorsed this report. Additionally, the contributors would appreciate feedback on the report from the OECD CCP, Working Party on Information Security and Privacy (WPISP) and the Committee on Information, Communications and Computer Policy (ICCP). If appropriate, the contributors would also welcome further collaboration on this initiative in other fora.

Table of Contents

Executive Summary 3

Introduction: The Evolution of Online Threats 7

Malware and Botnets 9

The Current Malware and Botnet Threat Landscape 10

The Future of Malware and the Botnet Threat Landscape 10

Best Practices for Addressing Malware 10

Phishing and Social Engineering 17

The Damage for Consumers and Industry. 17

The Phishing Landscape 18

Best Practices to Counter Phishing and Social Engineering 21

Domain Names and IP Addresses 29

Technology Overview 29

Internet Protocol (IP) Addresses. 29

The Domain Name System 29

Malware that targets the DNS. 31

Attacks through abuse of domain name registration services 32

Web and other server DNS attacks 34

IP address attacks 34

Mobile and Voice Threats 37

The Mobile Environment 37

App Markets 37

Mobile Malware 39

Blended Threats 40

Modifying Mobile Devices. 41

Baseband Threats 42

Premium Rate Business Model: 43

Mobile Spam 44

Growth of Cross-border Exploits 46

Voice Telephony Threats 48

Hosting and Cloud Services 53

Types of Hosting 53

The Threat Landscape 55

Major Areas of Concern 56

Best Practices 57

Online Harassment 61
Conclusion 63
Glossary 64
Endnotes 66
Contributors 69

Executive Summary

This report provides readers with a plain language description of the threats facing businesses, network providers and consumers in the online and mobile threat environment. As many of us are aware, Internet and mobile technologies have been key drivers of the global economy over the past twenty years. These technologies impact almost every facet of our day-to-day lives and have also been incorporated into almost every business model and supply chain. As our laptops, smartphones and tablets have become integrated into our daily personal and business lives, our dependence on these devices has grown. We use the devices to connect to family and friends, shop and bank online, engage with civic agencies and elected officials, interact with business colleagues and partners, streamline supply chains and deliver just-in-time products from manufacturing facilities to retail outlets.

With growing consumer and business dependency and rapid migration of commercial transactions to online and mobile platforms come threats from cybercriminals. Cybercriminals profit from sending spam, phishing, injecting malware onto websites, spreading botnets, redirecting Internet traffic to malicious websites, hijacking cloud and hosting services and inserting spyware onto computers and mobile devices.

The economic impact of these endless attacks is not easily measured, be it by country or on a global scale, as losses from cybercrime often go unreported or under reported by victims, financial institutions that cover the expense of the loss, or by businesses that incur everything from defence and remediation costs to service downtime due to attacks.

The primary focus of this report is not only to study the threat to the online, mobile and VoIP environment that threaten consumers, businesses and governments every day, but more importantly, to suggest best practices for industry and governments to address these threats. The focus of the report is on five major areas:

Malware and Botnets

Malware and botnets are among the most serious threats to the Internet economy. Malicious software or "malware" is created or used by criminals to disrupt computer operations, gather sensitive information, or gain access to private computer systems. Botnets are groups of machines infected with malware that communicate (often through a complex network of infected computers) to coordinate their activity and collect the information the individual malware infections yield. Botnets leverage the impressive computing power and bandwidth capabilities that come with being able to control over a million computers.

Criminals are continuously changing or "morphing" their malware to avoid its detection and remediation. Consequently, most Anti-Virus (A/V) software has difficulty identifying emerging and recent threats. A growing proportion of malware can detect that it is being "monitored" while it is running, perhaps by an anti-virus researcher, and will alter its characteristics to make it impossible for malware experts to detect or analyze its functions. Some malware will even respond to attempts to monitor and analyze it by counter-attacking with a Distributed Denial of Service (DDoS) attack.

Because of this, it is becoming increasingly difficult for the online security community to keep pace with the malware threat environment.

Phishing and Social Engineering

Phishing refers to techniques that are used by malicious actors to trick a victim into revealing sensitive personal, corporate, or financial information.

Phishing has been steadily increasing in frequency, sophistication, and damage since it emerged as a threat in the mid-1990s, and it is showing no signs of abating. In fact, phishing has been on the rise since 2011, and almost one quarter of recipients open phishing e-mails and over ten percent click on malicious attachments. As well, the type of data sought through phishing has grown increasingly more valuable, evolving from simple access to e-mail and consumer bank accounts that incur individual losses in the thousands of dollars, to current-day high-value targets.

High-value targets, namely corporate accounts containing trade secrets or those allowing special privileges to banking and financial accounts have been repeatedly and frequently exploited, producing catastrophic single-event intellectual property and financial losses of hundreds of millions of dollars, with an untold number of such events occurring annually.

Although phishing is not new, escalation in the number, targeting, and sophistication of the attacks in recent years represents an ever increasing threat to companies, governments, and consumers, and also erodes overall confidence in the digital economy. Defences must be coordinated to leverage open, transparent, multi-stakeholder solutions to maximize effectiveness, minimize costs, and increase public trust.

Internet Protocol and Domain Name System Exploits

A variety of illegal activities exploit vulnerabilities associated with the Domain Name System (DNS) and Internet Protocol (IP) addresses. The most serious DNS exploits are resolver exploits or cache poisoning, in which bad actors introduce forged data to redirect Internet traffic to fake versions of popular websites.

Every computer on the Internet has an IP address, which is used to identify that computer similar to the way telephones are identified by telephone numbers. Traditional IP addresses, known as IPv4 (Internet Protocol version 4) addresses, are 32-bit binary numbers, written as four decimal numbers, such as 64.57.183.103. The first part of the address, in this case 64.57.183, often identifies the network, and the rest of the address, in this case 103, the particular computer ("host") on the network. The division between the network and host varies depending on the size of the network, so the above example is merely typical. Since IP addresses are hard for humans to remember, and are tied to physical networks, the DNS is a distributed database of names that lets people use names like www.google.com rather than the corresponding IP address 173.194.73.105.

Despite its enormous size, the DNS gets excellent performance by using delegation and caches. That is, different organizations are each responsible for their part of the domain name system, and end-sites remember recent DNS results they've received. Since it would be impractical to store all of the names in the DNS in a single database, it is divided into zones that are stored on different servers, but logically linked together into an immense interoperable distributed database.

IP and DNS exploits cause an elevated risk because in many cases consumers are completely unaware that they have been redirected to a fake site rather than the one they actually wanted to visit.

Mobile, VoIP, and Telephony Threats

With the advent of the smartphone and the application markets for Android, Apple, Windows and Blackberry devices, the e-commerce environment has grown to include mobile devices. As consumers migrate their e-commerce activities to mobile platforms, bad actors seeking to profit and defraud have been quick to follow. In addition, the mobile environment creates unique opportunities for new types of attacks and threats targeting both consumers and businesses.

Mobile devices provide increased functionality and ease of use for consumers. They are often carried by individual users, are typically kept in an active state, and are often GPS enabled and location aware. Because of this, mobile devices are inherently more attractive for malicious attacks.

In the past few years, the mobile environment has seen increased development of malware, the first mobile botnets, an increase in premium rate text message (SMS) scams, and sophisticated exploits that have been associated with the jailbreaking (untethering a device from a designated, trustworthy source of software apps) of mobile devices.

With the growth of mobile-broadband subscriptions, Voice over Internet Protocol (VoIP) and Telephony threats are on the rise. The frequency and severity of robocall scams is growing and new technology that enables bad actors to hide or change their outgoing phone numbers to trick unwary targets makes these frauds more effective. As more telephone services move online, Telephony Denial of Service (TDoS) attacks are also growing in size and frequency. These types of attacks can be devastating when essential services are targeted so that phone systems are overwhelmed and the calls of legitimate individuals trying to reach, for example, the fire department or an ambulance are unable to get through.

Cybercriminals have a strong preference for operating in a transnational environment, further complicating enforcement efforts. For example, an illegal online pill seller living in the US might send spam advertising those drugs from a compromised computer in Brazil, pointing potential purchasers to a website with a Russian domain name, while physically hosting that website in France. Credit card payments for orders might be processed through a bank in Azerbaijan, with orders being drop shipped from a site in India, and proceeds funneled to a bank in Cyprus. Criminals know that by operating in this manner, many factors complicate any official investigation into their online crimes, and reduce their likelihood of being caught. These factors include a lack of cooperation, regulatory differences from one jurisdiction to another, and the cost of international investigations.

Hosting & Cloud

Hosting refers to service providers who provide businesses access to websites, files, intranets, and provide Internet access via multiple connected servers as opposed to one single or virtual server. Hosts are companies that provide space on a server owned or leased for use by clients, and they may also provide data center space and connectivity to the Internet. The scope of web hosting services varies greatly. The most basic is small-scale file hosting and website hosting. Many Internet service providers (ISPs) offer this service free to subscribers. These hosts operate the nuts and bolts that make the Internet work and range in size from sole proprietorships to global Internet businesses.

Cloud Computing is the storing and accessing of data and programs over the Internet instead of using your computer's hard drive. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cloud.

Online and mobile threats exploiting hosting and cloud sources are on the rise and include spam, spamvertising, phishing, hacked websites, DDoS (Distributed Denial of Service attacks), port scanning for exploitable vulnerabilities, defaced webpages, copyright/trademark infringement and malware. This document categorizes types of hosting, and outlines areas of concern. It provides a look at the current threat landscape in the online hosted and cloud environment, and a brief look at the remediation methods being used to address those critical issues.

Conclusion

In order to safeguard the internet, and ensure its promise to the world's citizens, it is essential that we identify efficient and effective responses to these many threats. This report, submitted by an international group of experts from industry and government, summarizes best practice recommendations to address these new and more sophisticated online, mobile, and telephony threats. It is our hope that this report will facilitate effective ongoing collaboration between this group and the international community to address these threats.

Introduction: The Evolution of Online Threats

Since 2006 the global Internet and mobile economy has seen the evolution of online threats and the emergence of novel attacks. The tools used to defraud and steal information in the online and mobile environment today are increasingly sophisticated, providing bad actors and fraudsters with an expanded toolbox.

In this context, as your parents probably intoned more than once, an ounce of prevention is worth a pound of cure. This report not only describes the online, mobile and telephony threat environment in a manner in which most any person can understand, it provides a list of tools for governments and industry to adopt as best practices to prevent these types of threats from turning into successful cyber-attacks.

While much of this illicit online activity is neutralized before it reaches typical end users due to modern-day filtering and blocking techniques, spam remains an important vehicle, often conveying malicious payloads as well as unwanted and often malicious e-mail. Spam is not just an e-mail phenomenon. It continues to expand into various forms of new media. For example, mobile messaging and Voice over Internet Protocol (VoIP) spam are now common, as are spam comments on social media, blogs and websites, and spam entries polluting and degrading the quality of search results in online search engines.

The domain sector (consisting primarily of the Internet Corporation for Assigned Names and Numbers (ICANN), Registrars and Registries can play a critical role in the anti-abuse space, particularly as new Internet protocols (e.g., IPv6) become more prevalent and a massive number of new Top Level Domains (TLDs) has been released. Traditionally there were approximately 24 TLDs, such as .com, .org, .net, .gov, plus two letter country TLDs, like .ca for Canada or .jp for Japan. Recently, ICANN introduced over 500 new generic TLDs, including .bike, .city, and .clothing and has hundreds more in the application process.

It is our suggestion that participants in the OECD and other international organizations strengthen their participation in the main coordinating entity in the domain space, the ICANN Government Advisory Council, working to encourage ICANN to redouble its efforts in the area of contractual compliance work and oversight of registries and registrars.

Much effort has gone into breaking down silos and facilitating cooperative ventures between business entities, NGOs, governments, regulators, and law enforcement agencies. The OECD, LAP, M^{3}AAWG and other international organizations have been effective in the development of existing public-private coordination and cross-organizational collaboration. For example, the DNS Changer Working Group[1], and the Conficker Working Group[2] are amalgams of subject matter experts, law enforcement, and industry representatives that have had notable success based upon a mutual-trust model, putting aside competitive concerns. This collaboration has been extremely successful, and remains vital to continued anti-abuse efforts.

However, there continues to be a need for stronger, more comprehensive, technology-neutral anti-spam and anti-abuse legislation and regulatory regimes facilitating cross-border cooperation. Part of the solution may lie in the diplomatic arena, particularly when it comes to enabling more effective cross-border law enforcement activity. Substantially improved end user education and awareness are other important facets of effective anti-abuse measures.

Malware and Botnets

Malicious software or "malware" is created or used by criminals to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in a variety of forms, from compiled programs to scripts, or bits of code inserted into otherwise legitimate software. "Malware" is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software. Malware generally includes computer viruses, worms, Trojan horses, droppers, spyware, adware, rootkits, spamware and other malicious programs. Malware is generally designed to fulfill one or more functions, ranging from facilitating the introduction of other malware (e.g., droppers/downloaders) to the collection of information (e.g., spyware). Other malware may specialize in the disruption of computers, users, and networks.

Botnets are groups of machines infected with similar malware that communicate (often through a complex intermediate network of infected computers) to coordinate their activity and collect the information the individual malware infections yield. Botnets are most often named for the specific malware that implements and coordinates this communication, for example, Zeus and SpyEye. However, each machine in a botnet may contain a variety of malware components. For example, a Zeus botnet node may contain the Zeus malware itself (handling botnet communication, theft of information and downloading of additional malware), as well as other threats such as spamware (such as Cutwail) or "attack" components (such as Pushdo DDoS malware).

Botnets can be large. Botnets composed of more than a million machines have been observed under the control of a single botmaster. However, a botnet does not have to be this large to be extremely damaging. Even a botnet composed of 1,000 or 2,000 nodes (computers) can wreak massive havoc.

In its beginning, malware was most often developed by "hobbyists", computer savvy people who were looking for a challenge or amusement. Since that time criminals, and increasingly organized crime, have realized that there is a lot of money to be made in malware. An example of this is the WinFixer case[3], where criminals tried to scare victims into making software registration payments. Today, virtually all malware is created and used for criminal purposes. To a lesser extent, malware may also be state sponsored and used by intelligence agencies to carry out covert actions against other states' computer systems or to spy on activists, journalists, and dissidents or it may be used by hacktivists and extremists for ideologically, politically, or socially motivated purposes.

Malware is one of the foremost threats to the Internet economy and is being used to conduct the following activities:

- Capturing personal and business information by:
  - capturing keystrokes
  - collecting logins and passwords
  - copying address books
  - stealing sensitive corporate information, documentation, and/or trade secrets or even capturing sensitive government or military information
  - collecting banking and transactional information
- Facilitating devastating DDoS attacks for nation state purposes, political activism, or as a prelude to extortion, among many other purposes
- Sending spam via e-mail, SMS and other methods

Criminals are continuously changing malware to avoid detection and remediation. Most Anti-Virus (A/V) software has a dismal track-record when it comes to identifying current and recent threats. A growing proportion of malware can detect that it is being "observed" (perhaps by an anti-virus researcher) and alter its behaviour to make it more difficult for researchers and analysts to determine how it works. Some malware will even attempt to discourage monitoring by counter-attacking researchers and analysts with a DDoS. Because of this, it is becoming increasingly difficult for the online security community to keep up with the pace at which the malware threat environment is evolving.

The Current Malware and Botnet Threat Landscape

The landscape has not changed and is unlikely to do so. The general reluctance by governments, banks and corporations to share private or sensitive data, impeded by real or perceived legal and regulatory barriers or a fear of liability, means that the producers of malware continue to retain the upper hand when it comes to being able to accurately deliver their product. Accurately measuring the scale of the issue is not possible given that there are no generally accepted metrics for malware infections, bots or botnets.

In email-carried malware, badly spelled, implausible e-mail has been replaced by new phishing techniques, discussed later in this report. Although global spam volume has dropped in recent years, social media is now increasingly being used with techniques like "clickjacking" or "likejacking" in which a user clicks a website link to watch a tempting video and the attacker uses that click to post a comment to all the user's Facebook friends, enticing them to click on the same malicious link. Facebook has largely countered this attack by asking the user to confirm a "like" before it posts if the user is liking an untrustworthy domain.

In terms of web-carried malware, Symantec found that in 2013, web-based attacks were up 23 percent over 2012 and that 1 in 8 websites had a critical vulnerability.[4] This indicates that attackers are trying to circumvent security countermeasures by using the Web to deliver malware rather than attaching it to e-mail.

Threats against the Apple OSX and iOS operating systems, though relatively few in number, represent the propagation of malware onto platforms that have up to now been relatively free of malware. The means of attack are similar to those seen for Windows and Android platforms. The fact that many attack tools have become cross-platform, making use of Java exploits, for example, is in itself a new method of malware propagation.

The Future of Malware and the Botnet Threat Landscape

According to the McAfee Threat Predictions[5] report, mobile malware will be the driver of growth in both technical innovation and the volume of attacks in the overall malware "market" in 2015. Increasingly, malicious ransomware attacks are also occurring, fueled by the growth in virtual currency. The deployment of a growing number of cloud-based corporate applications is also expected to create new attack surfaces that will be exploited by cybercriminals.

Lastly, it is hard to conceive of many other more significant threats in the next few years than that posed by the Internet of Things. As billions of devices are connected to the Internet there will be an increasing threat to the fundamental infrastructure posed by unpatched or inherently insecure devices. It is likely that many connected devices will not receive regular security patches; some vendors will not regard security as a part of their responsibility as they prioritize the next product release and focus more on aesthetic or practical features.

Consumers may not put pressure on equipment vendors for security patches. If, for example, a device is operating satisfactorily as a fridge, lightbulb or thermostat but has a security issue with its cyber-functionality, consumers may not be motivated to replace it on security grounds alone. Consequently the long tail of insecure devices will continue to grow.

Best Practices for Addressing Malware

While much of what is contained in this section is focused on educating individuals and ISPs it should be recognized that addressing malware is an ecosystem-wide problem that will require a multi-faceted approach and actions from a variety of parties, not limited to ISPs or educating end users.

For governments and educators, this section focuses on the prevention, detection, and remediation of malware. For the ISPs, this section focuses on providing advice regarding what an ISP can do to assist individuals in detecting malware. The section concludes with a discussion of malware forensics in the legal and regulatory areas of governments, as well as industry let practices.

Best Practices for Educators and Users

A) Best Practices: Prevention

These recommendations focus on how individuals can avoid getting infected with malware.

1. **Choose a Secure and Current Operating System**: When choosing an operating system (OS), look for one that has proven capabilities to reduce your exposure to malware. Regardless of what operating system you choose, be sure to run the most recent production version of it. Modern operating systems have built-in mitigations that help protect against exploits used by malware to compromise a system.

2. **Stay Patched and Up-To-Date**: Ensure that operating systems and all applications, including helper applications (such as Acrobat Reader, Flash Player, Java, and QuickTime) are fully patched (meaning all updates have been downloaded as they became available) and up-to-date. Most issues exploited by malware have had patches available for more than a year. On systems running Microsoft Windows, Microsoft has a number of recommended downloads available.[6] Secunia PSI[7] is also a popular tool that can help you keep third party applications up-to-date.

3. **Use Only What You Need**: In general, it's best to only download or use software that's needed to get the job done. Avoid downloading software or files that do not add useful or necessary features or functionality, and delete un-used software.

4. **Seek Expert Help**: Ask the experts what the best choice for your needs is. (The "experts" may answer in different ways, but if they're the ones you rely on for support, going with what they say will almost always be better in your circumstances.)

5. **Run an Antivirus Program**: While antivirus products aren't perfect, they still can help, so pick and use one, and keep it up-to-date by downloading updates when alerted to do so. Schedule a full scan of your system at least once a week. Be sure you select a real antivirus product, and avoid being tricked into installing a fake antivirus product that is, itself, malware! (And if your antivirus program doesn't also protect against spyware, also use an anti-spyware program).

6. **Use a Firewall**: Although firewalls aren't foolproof, a hardware or software firewall will at least potentially add another layer of protection.

7. **Use Strong Passwords**: Passwords should be sufficiently complex to resist guessing or cracking. Some people rely on passwords that are at least eight characters long, and include a mix of upper and lower case letters, numbers, and special symbols. Others prefer a set of three to five unrelated words that are easier to remember but difficult for computer programs to guess. Either way, do not always use the same password on multiple sites. Password applications make this process easier.[8]

8. **Make Regular Backups**: If your system does become infected, having a clean backup can be tremendously helpful when it comes to getting cleaned up and back online.

9. **Clean Up Any Unneeded Temporary Files**: Some malware may hide copies of itself among temporary files, and even if there aren't any infected temporary files, removing those temporary files will speed up system scans and reduce the size of your backups. One widely used tool for cleaning up temporary files under Windows is CCleaner.

10. **Don't Routinely Run As An Administrator**: "Administrator," "root" and other accounts that have special powers should only be used when you're doing something that requires the special privileges associated with those high powered accounts (for example, intentional installation of new software). When you're doing regular tasks, run as a normal user.

11. **Disable JavaScript (Or Use NoScript)**: JavaScript (a scripting language that's not related to Java, name notwithstanding), enables many exciting interactive applications; however, it is also widely abused and used to drop malware on vulnerable systems. If you don't need JavaScript, don't enable it in your Web browser.

12. **Block Known Malicious Domain Names in DNS**: Some malware relies on the ability to successfully translate symbolic domain names to numbers. If you block the translation of those names via your domain name server, that malware may then be unable to successfully run. OpenDNS is an example of a company that offers malware-filtered DNS of this sort.

13. **Filter/Defang Potentially Dangerous E-mail**: Your e-mail administrator should scan e-mail for potentially dangerous e-mail attachments, links, or other content that may be e-mailed to you. One example of such a program that can help with this is MIMEDefang.

14. **Files Downloaded via P2P Applications Are Often Infected**: Be aware that many of the files shared on peer-to-peer (P2P) file sharing services may be intentionally or accidentally infected with malware.

15. **Assume Any USB Thumb Drive Has Been "Booby Trapped"**: If you are given a USB thumb drive, or find a "lost" USB thumb drive, never put it into your computer. It may have been intentionally infected with malware, and then dropped where you might find it in an effort to get malware onto your system.

16. **Avoid Using Unfamiliar Wi-Fi Hotspots**: Some open Wi-Fi hotspots may intercept any unencrypted traffic, thereby potentially violating your privacy. Use of a Virtual Private Network (VPN) may offer some protection. Ensure that any wireless access point you operate is secured with WPA2 (a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks) to limit access.

B) Best Practices: Detection

These recommendations focus on how malware gets detected when prevention efforts fail.

1. **Be aware when a local scan detects something**: One of the most common ways that malware is detected is via an antivirus scan. Another similar option would be to perform a scan using a purpose-built one-time anti-malware tool such as a "cleanup only" tool[9].

2. **Take notice when your system begins to behave strangely**: Another prime indicator that something's amiss is when the system begins to behave "strangely." Strange behaviours may include running slowly or crashing, having unwanted windows pop up (e.g., fake A/V notifications), asking for one Web page only to go to some other one, not being able to go to some sites at all (particularly if those sites are update sites or security-related sites), etc.

3. **Take action if your ISP tells you that your system is doing bad things**: For example, your ISP may notify you that your system has been observed sending spam, or has been seen attacking another system on the Internet.

C) Best Practices: Remediation

These recommendations focus on how malware infected systems can be dealt with.

1. **Clean In Place**: This approach relies on the user (or someone acting on the user's behalf) running one or more antivirus products on the infected system in an effort to clean it up (experts may also manually delete infected files in some cases). This process may be time consuming, and ultimately may or may not work. Even after devoting substantial effort toward cleaning up an infected system, the infection may remain, or the system may be unstable or unusable.

2. **Rollback**: If the user has a clean backup, another option is to roll back to that earlier clean backup. Selecting this option may result in the loss of work since the last clean backup, unless those files are separately preserved and can be restored (note that if this is done, it needs to be done very carefully to ensure that restoring those files doesn't result in re-infection). Generally speaking, a rollback strategy works best when backups are frequent, and multiple backup generations remain available for potential selection.

3. **Complete reinstallation**: In this option, the system is reformatted, and the operating system and applications are re-installed from scratch. This can be a time-consuming process, and will often be frustrated by a lack of original media (many vendors no longer ship a copy of the operating system on physical media when they sell new hardware).

4. **Replace the System**: Finally, at least some fraction of users may decide that they simply want to replace their infected system, rather than trying to clean it up. Or, this may be the only way to safely disinfect a machine. This option may be more palatable if the infected system is old or was not very powerful in the first place, or if the user wants to change operating systems or go from a desktop to a laptop, for instance. The industry parlance for this type of action is 'nuke & pave'.

Best Practices for Industry and Government

A) Best Practices for Detection and Notification (ISP-to-User)

Many ISPs today notify customers if they are infected with malware. ISPs may use a variety of techniques to notify individuals of infection. This section provides a list of some activities different ISPs should take to notify end users, however, it shouldn't be implied that any one technique has been identified as a best practice. There are different benefits and downsides associated with each form of notification. Examples include the following:

1. **E-mail**: When an infected system is noticed, the ISP may notify the user by e-mail. Unfortunately, many times users never check the e-mail the ISP provides for their use, and the user may never provide the ISP with the e-mail address that they do routinely use. Users may also have become wary of trusting e-mail notifications as a result of widespread phishing attacks and tech support scams that mislead consumers about the presence of malware on their PCs.

2. **Telephone**: The ISP can also notify the user by telephone. When contacting customers it is important to consider that while automated calling can be efficient, users may be suspicious of phone-based notifications as a result of voice-based phishing attacks. On the other hand, manned phone notification can be tedious and time consuming if a large number of infected users need to be notified.

3. **Text Message**: In cases where the ISP knows the mobile phone number of the customer, another option would be to push text message notifications to the users.

4. **Regular (Paper) Mail**: An ISP may consider notifying users via traditional postal mail perhaps via an insert to their monthly bill. However, if the ISP is not already mailing the customer, doing *ad hoc* mail notifications may be expensive and of limited effectiveness, particularly if the user is predisposed to discard mail communications unopened due to a perception that they are likely just marketing.

5. **Truck Roll**: In situations where the user has purchased an on-site support contract, another notification approach may be via an in-person "truck roll" to the customer's site. Obviously the ISP technician will need to be able to satisfy the customer of his or her credentials, and we must also note that this can be a very expensive notification option.

6. **In-Band (Web) Notification**: In this approach, an ISP notifies the user by interposing an interstitial message when the user attempts to visit a normal website. This approach can be somewhat disconcerting for users, but is less disruptive than some other approaches, such as the "walled-garden" approach (see below).

7. **Walled-Garden**: If an ISP needs to immediately limit the damage that an infected user can cause, one option is to put them into a so-called "walled garden." When this is done, the user is allowed to access selected sites for remediation and hardening purposes, and may perhaps be allowed to continue to have VoIP access for things like access to emergency services, but typically cannot access most other Internet resources. It should be emphasized that this strategy is not meant to be punitive. Walled Gardens have been extremely effective in diminishing the amount of infection at the consumer ISP level and in fact precipitate a move of malware and botnets to hosting services.

For additional information see also Internet Engineering Task Force RFC6561 'Recommendations for the Remediation of Bots in ISP Networks".[10]

Notification to end users isn't limited to ISPs. Other parties in the Internet ecosystem who have a relationship with end users can, and have, performed notifications. For example, it was widely publicized that both Google and Facebook attempted to alert end users of potential infections associated with the DNS Changer malware.

B) Best Practices for Raising Awareness

1. **One-On-One Teachable Moments**: In the unfortunate event that a customer's system does become infected, that may be a prime "teachable moment" when selected techniques for avoiding re-infection may be particularly salient.

2. **Customer Security Website**: The most basic example of offering customer education and awareness is probably the creation of a customer security website offering advice and access to tools.

3. **Inserts in Bills**: If ISPs routinely send information to customers via regular mail, this may provide another opportunity to share recommendations for securing the customer's system, and is something that can be distributed to all customers, including those that have shown no sign of infection to-date.

4. **Public Service Announcements (PSAs)**: Another opportunity to educate end users about malware would be through public service announcements through televisions and radio. For example, in the US the National Cybersecurity Awareness Campaign, *STOP THINK CONNECT*, has developed numerous PSAs placed into circulation annually since 2010.

5. **Promotional Materials**: There are also a variety of promotional materials such as customized mouse pads, mugs, t-shirts, bottle openers, pens or pencils, or other give-aways that may help raise awareness of malware and botnet threats.

6. **Contests**: Another opportunity for sharing the cybersecurity message may be associated with contests, particularly things like essay contests targeting school age users.

7. **Formal Education**: Another vital part of education and awareness is to incorporate cybersecurity or digital citizenship curriculum into schools. Addressing cybersecurity generally and in particular malware and botnets, is a long term public safety issue, and like other public safety issues, it can be best addressed by establishing societal norms which in many cases may be best instilled as part of an individual's formal education.

Due to the rapidly shifting threat landscape and complexity of malware and botnet threats, education and awareness can only be partially effective at protecting end users. Legal, regulatory, technical and industry efforts will remain at the forefront of dealing with the malware and botnet problem. However, basic education and awareness about online threats remains a necessary ingredient to protecting end users.

Industry, associations and governments should develop and promote communications programs that provide end users with a basic understanding of threats and simple to understand techniques on how to protect themselves.

Many such initiatives already exist and can be used as models or simply as a source for educational material (see below). Several of these resources are broadly based rather than strictly focused on malware and botnet related issues. However, it is usually better to provide end users with a combined message about Internet safety rather than numerous uncoordinated suggestions. In other words, the information should be short and coherent whenever possible.

- National Cybersecurity Alliance - Keep A Clean Machine - http://www.stopthinkconnect.org/campaigns/keep-a-clean-machine (part of the US National Cybersecurity Awareness Campaign *STOP THINK CONNECT* which is focused on botnets and malware)
- Federal Bureau of Investigation (FBI): http://www.fbi.gov/scams-safety
- Royal Canadian Mounted Police (RCMP): http://www.rcmp-grc.gc.ca/is-si/index-eng.htm
- US National Initiative for Cybersecurity Education: http://csrc.nist.gov/nice/
- Federal Trade Commission (FTC): https://www.onguardonline.gov and http://www.consumer.ftc.gov/media/video-0103-hijacked-computer-what-do

C) Legal and Regulatory Best Practices

In the context of malware forensics, *Malware Forensics: Investigating and Analyzing Malicious Code*[11] suggests some best practices for malware investigations, which include:

- Frame and re-frame investigative objectives and goals early and often.
- From the outset, understand the importance of identifying inculpatory, exculpatory, and missing evidence.
- Design a methodology ensuring that investigative steps will not alter, delete, or create evidence, or tip off a suspect or otherwise compromise the investigation.
- Create and maintain meticulous step-by-step analytical and chain of custody documentation.
- Never lose control over the evidence.
- Define, re-define, and tailor these guiding principles throughout the course of an investigation in order to help clarify and make more attainable investigative goals and objectives.
- Think through the following important issues early on:
  - Does the jurisdiction of an investigation require any special certification or licensing to conduct digital forensic analysis?
  - What authority exists to investigate, and what are the limits to that authority?
  - What is the scope of the authorized investigation?
  - How will intruding on the privacy rights of relevant data custodians be avoided?

D) Best Practices for Industry and Government-Led Collaboration

Secure software development practices represent a best practice for limiting the spread of malware. The Software Assurance Forum for Excellence in Code[12] (SAFECode) is a global, industry-led initiative to identify and promote best practices for developing and delivering more secure and reliable software, hardware and services.

The US Federal Communications Commission's (FCC) Communications Security, Reliability and Interoperability Council (CSRIC) Working Group #7 released a voluntary Anti-Bot Code of Conduct for ISPs and network operators on March 22, 2012, as a cooperative industry-government initiative[13]. The Code focuses on residential Internet users and includes five areas of focus for ISPs: education, detection, notification, remediation, and collaboration. To participate in this Code, an ISP is required to engage in at least one activity (*i.e.*, take meaningful action) in each of the following general areas:

- Education – help increase end user education and awareness of botnet issues and how to help prevent bot infections;
- Detection – identify botnet activity in the ISP's network, obtain information on botnet activity in the ISP's network, or enable end users to self-determine potential bot infections on their end user devices;
- Notification – notify customers of suspected bot infections or enable customers to determine if they may be infected by a bot;
- Remediation – provide information to end users about how they can remediate bot infections, or to assist end users in remediating bot infections;
- Collaboration – share with other ISPs feedback and experience learned from the participating ISP's SAFECode activities.

Properly configured (hardened) operating systems and applications can also reduce the infection rate from malware. The United States National Security Agency (NSA) provides guidance on hardening computers against all threats including malware[14]. Additional information is available for routers, wireless, switches, VoIP, database servers and applications at the same location. Additionally, operating system and application resources for hardening against malicious software can be found in the National Institute of Standards and Technology's (NIST) check lists[15] (including Android devices).

The Korea Internet & Security Agency (KISA) provides a 'DDoS Shelter' service for free to small businesses which don't have proper tools to protect against a DDoS attack themselves. The DDoS Shelter filters malicious traffic of the DDoS attack and

passes normal traffic. Also, the KISA detects suspected zombie IPs in a spamtrap and has domestic ISPs take proper action against these IPs on their networks.

Further country-specific efforts can be found at the following websites:

- International: https://code.google.com/p/evidenceontology
- Botfrei: https://www.botfrei.de/
- Switzerland Melani: http://www.melani.admin.ch
- Finland Ficora: http://www.ficora.fi/en
- EU AC/DC Project: http://www.acdc-project.eu/
- Canada: http://fightspam.gc.ca
- Australia: http://www.acma.gov.au/Citizen/Stay-protected/My-mobile-world/Dealing-with-mobile-spam/dealing-with-spam-i-acma

E) Best Practices for ISPs

The malware threat can be minimized by reducing or eliminating infection vectors. E-mail is still a very effective method by which malware propagates itself. To mitigate this vector, most ISPs, hotels and free access points follow the industry best practices of blocking outgoing mail (port 25) from any computer on their network other than their own mail servers. This thwarts infected computers from propagating the malware via direct mailing.

In Europe, some ISPs have taken this a step further. Users on these networks by default only have Web access. Any traffic for all other ports is denied. To allow sophisticated users more flexibility, these ISPs provide tools to allow specific authorized users to use other ports/protocols and services.

In both instances, the monitoring of blocked traffic attempts can be used as early warning indicators of malware infected machines as well as hindering malware propagation and control and command communications.

F) Best Practices for Servers and Hosting Providers

Currently, one of the most prevalent reservoirs of malware is compromised Web servers. These servers become compromised either when current security patches are not applied for both the OS as well as support applications and Web frameworks, or due to insecure user passwords. These compromises are exacerbated in small and medium-sized business and at many hosting providers due to small abuse staff/teams. Automation is being used by some to ameliorate these issues and should become a world-wide best practice.

1. **Customer Terms of Service Requirements for Timely Security Updates**: All clients should agree to maintain current security patches or allow the hosting provider to update frameworks in their directories.

2. **Maintain Current Security Patches**: All security patches should be current. This process can be manual for very small systems or scripted for larger hosting providers.

3. **Use Audit Tools to Identify Hosts**: Tools to perform server-wide auditing for unsecure software versions should be run at least bi-weekly and identified software should be patched.

4. **Use IT Security Software**: Tools (such as Tripwire) should be used to monitor the integrity of each server.

5. **Run Antivirus**: Run antivirus software frequently (if possible two different packages) to monitor variable host files for contagion.

6. **Consider Using Cloud Servers**: Since cloud servers are professionally maintained and used by many clients, they tend to be better secured; on the other hand, they may be richer targets for attacks (e.g., DDoS). Nevertheless, cloud servers should be considered as a possible alternative for better security, bearing in mind the reputation of the cloud provider, the security measures put in place, and whether or not the servers have been attacked in the past. More information on Hosting and Cloud threats and best practices can be found later in this report.

Phishing and Social Engineering

Phishing refers to techniques that are used by malicious actors to trick a victim into taking an action they would not otherwise take online, often revealing sensitive information such as personal or financial data. Fraudsters pose as known entities (friends or businesses), leveraging existing trust relationships to compromise their victims.

Phishing has been steadily increasing in frequency, sophistication, and damage since it emerged as a major threat in the mid-1990s, and it shows no signs of abating. The type of data sought through phishing has also grown increasingly more valuable, evolving from simple access to e-mail and consumer bank accounts that incurred individual losses in the thousands, to current-day targets of corporate accounts with special privileges ("super-user") and corporate bank information.

These attacks can lead to massive data breaches where the personal information of customers is stolen en masse, the intellectual property of a company is exfiltrated, or the data and even physical systems are destroyed. Each single event can involve corporate intellectual property and impose financial losses up to tens or even hundreds of millions of dollars, with untold numbers of events occurring annually.

Phishers now counterfeit messages and Web pages that are indistinguishable from ones that are authentic, using armies of compromised legitimate machines (botnets) and infecting software (malware) to the same ends that previously required more overt end user interaction. Phishers also have developed mobile malware that can render some protective measures ineffective.

The Damage for Consumers and Industry

Measuring the impact of phishing to consumers and the economy is difficult work, with widely varying results. One point on which general agreement is reached is that phishing attacks are on the rise. The annual Verizon Data Breach Investigations Report shows that after a brief dip in 2010, phishing has risen for several years in a row. In 2014, phishing was recognized as the #3 cause for data breaches[16] and increased 23 percent from 253 to 312 in 2013. Also in 2014, attackers continued to breach networks with highly targeted spear-phishing attacks, which increased to 8 percent of attacks overall. These attacks were more sophisticated and targeted; with 14 percent less e-mail sent towards 20 percent fewer targets.[17]

The Anti-Phishing Working Group (APWG) produces quarterly reports on phishing trends; their 2014 report noted the largest number of phishing attacks seen since 2009. The same report documented the most targeting of brands than ever before, with 756 targeted institutions in the first half of 2014.[18,19] RSA's Monthly Fraud Report for December 2014 suggested single month losses to phishing of US$453 million globally or annualized losses of approximately US$5 Billion, with 75 percent of the attacks hitting the US and Canada.[20] While phishing is a small part of the estimated global losses to cybercrime, which are estimated at US$445 Billion[21], US$5 Billion is nonetheless a significant and preventable loss.

Why the "Ph"?

The term phishing is derived from "fishing", as internet scammers are use "lures" to "fish" for users' financial information and password data. Hackers have an endearing tendency to change the letter f to ph, and phishing is just one of these examples. The f-to-ph transformation is not new among hackers and this phenomenon first appeared in the late 1960s among telephone system hackers, who called themselves "phone phreaks."

Prevention has also become a considerable task, with the median time-to- click coming in at one minute and twenty-two seconds and data from the APWG suggesting that the infrastructure being used to wage these campaigns is quite extensive with over 9,000 domains and nearly 50,000 phishing URLs tracked each month across the Group's members.

The Phishing Landscape

Phishing is distinguished by the types of information sought, the types of targets attacked, and the channels through which attacks are conducted. Phishing is normally identified by an e-mail, SMS, or other message that contains a link that redirects the recipient to a fake web page that requests one's account information such as username and password, credit card number, or other personal information.

Goals of Phishing Attacks - What they're after

Information obtained by phishing is typically used for some type of financial theft, either directly against the victim, or on another target such as the victim's employer. As monetizing credit card information and Social Security numbers becomes increasingly difficult, "hackers will go after anyone with health care information," said John Pescatore, director of emerging security trends at the SANS Institute, adding that in recent years hackers have increasingly set their sights on EHRs (electronic health records) which can easily be turned into cash.[22] Further, phishing has been employed as a first stage in breaching corporate and government networks by obtaining credentials to allow for systems access.

Phishing, itself, is usually only a first step and does not necessarily immediately result in any direct financial theft. The rising trend in stealing health care records is usually started with phishing attacks to gain access to systems. Once access is obtained, thieves use other tools, like malware and spyware, to steal sensitive information - in the first quarter of 2015 over 120 million US patients have had their records stolen.[23] Further, spear phishing for credentials of corporate employees is often one of the first steps in a large-scale data breach and is therefore the first step in a significant portion of the staggering losses attributed to data breaches.

- Online and offline techniques that trick people into divulging information are often called "social engineering" and predate the Internet. When e-mail phishing emerged, the attackers were not very discriminating. They broadly sent general-purpose e-mails to as many people as possible hoping some percentage would be tricked. As defences against these attacks strengthened, and the attackers fine-tuned their strategies. There are four commonly known forms of phishing:

    *i) a **redirection** via a link contained in a message to a location on the Internet which may contain a fake banking, commerce, or e-mail site,*

    *ii) e-mails with **an html attachment** containing the phishing form,*

    *iii) a **link/listing** of a phone number that a victim is to click or call, or*

    *iv) a simple **reply-to** phish, where the message contains a request for the desired credentials and the user is asked to reply with the information.*

In the first two forms, the message recipient provides personal information most often by sending the criminal an e-mail containing the stolen credentials. Phone number based phishing can involve either an automated phone answering system that prompts the victim for their credentials or a live person attempting to socially engineer them. 419 scams, with promises of untold riches, and other Advanced Fee Fraud scams were early forms of social engineering via e-mail. Despite advances in phishing, these scams still persist.

419 Scams – ***Early, unsophisticated forms of phishing, so-named because of the Nigerian criminal code Chapter 38, section 419 which criminalizes this type of fraud. "Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years." These are the famous Nigerian prince e-mails or other advance fee schemes where the victim is tricked into spending money in return for untold riches at the end of the scheme.***

- **Spear Phishing / Targeted Phishing** – While traditional phishing attempts are often sent indiscriminately to nearly everyone, targeted phishing attacks are conducted against specific individuals or organizations. This type of phishing usually involves extensive research by the fraudsters, such as learning about their hobbies, charities, past employers, and social networks in an effort to make their attack much more plausible and credible. It can be customized to trick victims who are traditionally more valuable (and suspicious) than average users. These might be employees of a targeted company that an attacker is looking to penetrate. One variant on spear phishing that is particularly effective involves a fake message that appears to be from a supplier, creditor or organization known to the victim containing fraudulent payment instructions for commonly expected or normal transactions.

- **VoIP / Vishing** – As telephony and other voice activities migrate to Internet-based mechanisms, collectively known as "Voice over IP" or VoIP, so do the frauds. This integration of computers with phone systems makes it possible to trick victims into clicking fraudulent links that automatically place a telephone call, rather than go to a website. The call itself may directly generate revenue to the attacker, or it may direct the victim to a social engineer who convinces the victim to reveal information. Smartphones exacerbate the threat by simplifying this Internet/telephony integration for users. For more on this, see the Mobile and Voice section of this report.

- **Fax** – Fax was one of the earliest methods of electronic phishing and has been mostly replaced by the other attack methods outlined here. However, with the advent of Internet based faxing bringing costs down, it is experiencing resurgence. Since its use is uncommon, it is not always detected.

- **Social Networks** – These create a group experience conducive to a sense of trust, which is, in turn, beneficial for social engineering that exploits the victim's online relationships. This can work extremely well when the attacker mimics a message from a trusted online friend or has compromised their friend's account.

Timeline of a Typical Phishing Campaign

A common account credential phishing campaign has four elements to it:

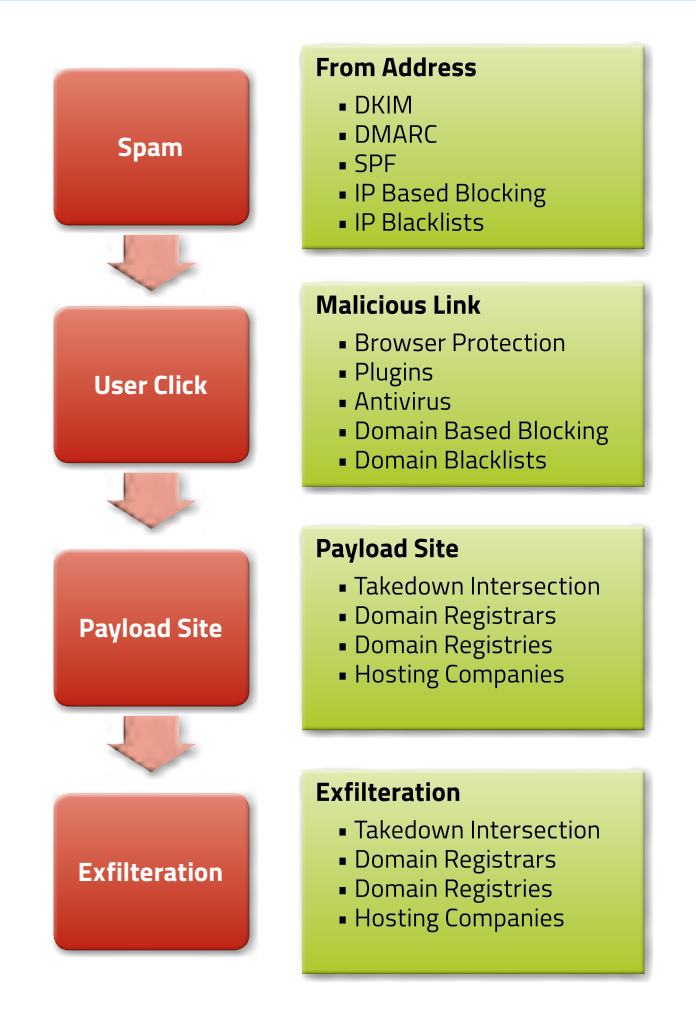
1. **Initial message (Spam)** – A message is delivered and seen by an end user. It appears genuine and therefore has a high degree of credibility, typically containing counterfeit elements of a legitimate message, and ostensibly emanating from a legitimate source, such as one's bank.

2. **Call to action (User Click)** – The victim is encouraged to click on a link or reply to the message with confidential information. The most effective calls to action prey on fear and greed, either personally, or with regard to the organization where the recipient works. A fear based message may indicate that the victim has already suffered a compromise or may lose access to a resource if they fail to act, or that their company is subject to a lawsuit or financial penalty. A greed based message may promise a discount or financial reward for taking a survey or providing information.

3. **Payload** – This content causes the victim to divulge the target information. It can be in the initial message or can be on a target website, called a "landing page". The website may be compromised, or can have a look-alike domain name to confound the end user. The payload usually has a form requiring the victim to enter confidential information. Some phishing sites also contain a "drive-by download" mechanism wherein the recipient's visit to the webpage begins an automated process of system inventory and exploitation resulting in malware being surreptitiously loaded onto the victim's computer, allowing the criminals to retrieve confidential data, after which the victim is redirected to a legitimate site.

4. **Exploitation/Exfiltration/Obtain Information** – The end-game of any phishing campaign is to convert the gathered credentials into value for the criminals. A broad array of schemes have been observed, with the simplest being to login to the account and use it to transfer funds or make purchases, while other much more sophisticated attacks begin by using phishing to gain access to an e-mail account and then using it as a base for additional social engineering and/or malware distribution with the potential to deeply infiltrate the recipient's organization. Extortion attempts have also been observed.

There are a number of points where the workflow of a phishing campaign can be prevented or disrupted, as noted in the diagram:



Evolving Methods of Exploitation

The most well-known and original form of phishing involved the criminals logging in directly to a financial institution and attempting to transfer funds from the victim's account to another account the criminals' control. When financial institutions began to more easily detect and block fraudulent international money transfers, the criminals adapted. By moving the money to a domestic account or same-institution account the fraud was often not as readily detected. Sometimes this was accomplished through online bill payment or simple account-to-account transfers. In these situations, the criminal, who was often overseas, needed to acquire the services of domestic criminals to act as money mules.

In other cases, the call to action contained in the phishing e-mail is meant to elicit the disclosure of credit card details. With the credit card number, expiration date, and CVV code, the card can either be sold on the black market or used for all manners of Card Not Present fraud. With credit card number, expiration and CVV, the phisher is free to visit nearly any online retailer and make purchases. To evade detection, secondary criminal markets for reshipping and remote terminal services are used. In order to defeat the retail fraud detection systems, phishers will purchase the use of a remote terminal services IP address in a geographic area matching the geography of the credit card victim. Likewise, if shipments must be sent, a place to receive the packages that corresponds with the victim's geography will be used as well.

Password reuse attacks are yet another online consumer threat that can result from a phishing attack. Because people often use the same password on many systems, the criminals are able to use these same user-ids and passwords in multiple places, including financial institutions, online retailers, and even corporate VPN systems (see the Malware and Botnets section for more information on creating and storing strong passwords).

The large-scale data breaches that have made headlines in recent years often start with some form of targeted phishing or spear phishing of executives or individuals with access to corporate network controls. Such attacks have led to direct financial crimes such as theft of user credentials and personal information, and the resale of these in the criminal underground. A large and growing number of spear phishing campaigns are also in furtherance of industrial espionage, criminal extortion schemes, state sponsored infiltration, and other non-financial crimes.

Increasing Leverage of Phishing Attacks

As more organizations have migrated to web-based mail systems, phishing attacks have become more prevalent for two main reasons. First, and unfortunately, many organizations use single sign-on environments, with the same password for both e-mail accounts and human resources tasks such as the bank account where money should be transferred on pay day. Second, once a corporate e-mail account is accessed, the criminal has a platform from which they can study the organization, learn who may have access to the most valuable digital assets of the company, including financial accounts and intellectual property,

and target those employees. Such attacks will be launched from an e-mail account of an employee that they know and trust, either through social engineering or the delivery of malware via e-mail attachments modeled on common business documents found in the compromised account.

Even for non-corporate e-mail, phishing attacks against e-mail providers such as Gmail, Yahoo, Outlook, and AOL are increasingly common for many of the same reasons. These accounts may seem to be "low value targets" and are not guarded as diligently as others, yet they control the ability to perform password resets or direct access to other accounts for a wide variety of attacks. These compromised e-mail accounts have led to significant volumes of financial crimes (e.g., account takeover, fraud wire transfers) that are well documented by financial institutions.

Other services such as social networks provide "single sign-on" for a wide variety of consumer services. This makes such accounts ripe targets for phishers, as they can directly monetize such services, redirect product shipments or generally take over many aspects of a person's online identity. The following diagram shows that if hackers can infiltrate a Google account, they often have access to a multitude of other information.

The same can be said for Apple and iTunes and within corporations, access corporate email accounts provides a 'delivery platform' for social engineering other corporate members.

The increased sophistication of criminals has led to targeting of infrastructure elements to provide them with even greater potential leverage. For example, phishers now gain access to third-party E-mail Services Providers (ESPs), who send bulk mail on behalf of the world's largest brands. Criminals access an ESP's infrastructure via compromised accounts, steal client lists, and send phishing spam or malware to unwitting recipients, who believe the message is from a legitimate company's mailing list.

Another recent trend is the increased targeting of Internet infrastructure elements such as hosting accounts or domain registration credentials. Once phishers obtain access to fundamental infrastructure controls like these, they can set-up websites, launch new attacks, and create new infrastructure elements like domain names to rotate their schemes through (see the Hosting and Cloud Services section). One particularly damaging tactic is to add malicious hostnames to a well-established domain name with a good reputation, leaving the original domain untouched. This allows criminals to exploit the good reputation of a domain in their campaigns to get around filters and avoid being blocked or shutdown (see Domain Names and IP Addresses section).

Best Practices to Counter Phishing and Social Engineering

There are a wide range of anti-phishing best practices available to organizations to protect their brand and their customers. That said, there is no "silver bullet" to the challenges phishing brings, and it needs to be addressed throughout the entire lifecycle of the process - any step that can be thwarted along the way can protect dozens to millions of victims depending on the scale of the attack involved and the reach of various solutions. Enterprises should treat this problem with a "defense in depth" approach - assume that some measures will be effective to prevent initial e-mails from arriving, but that some will get through and further defenses will be necessary. This section will highlight some of the major techniques and best practices, but far more detail and specific advice can be obtained from various industry organizations, government publications, and anti-phishing solutions vendors.

1. Preventing Phishing Attack Success

The first place to deal with phishing attacks is stopping them from reaching victims and/or keeping victims from visiting phishing sites in the first place. There are three primary touch points for accomplishing this: stopping the flow of lure e-mails, preventing lures from reaching users, and blocking access to phishing websites and other assets.

a. Outbound lure delivery prevention

Relatively recent e-mail-based authentication mechanisms facilitate some easily used protections against some forms of phishing and spoofing. These techniques rely on creating an authenticated e-mail infrastructure. The most common authentication mechanisms for e-mail are SPF (Sender Policy Framework)[24] and DKIM (DomainKeys Identified Mail)[25], which employ domain names[26] as validated identifiers. These allow the owner of a domain name to control the usage of that domain in e-mail and cut down on spoofing.

In order to address the problems of phishing and domain spoofing successfully, brand owners and ISPs need to share information with each other about their e-mail activity, such as policies for authentication and reports about problems. Historically, these arrangements were bilateral and private, between brand owners and individual ISPs. However, an ad hoc industry consortium developed a technical specification called DMARC (Domain-based Message Authentication, Reporting & Conformance)[27].

DMARC, introduced in early 2012, leverages SPF and DKIM to provide brand owners with a means for easily communicating to ISPs how they would prefer any improperly authenticated messages to be handled. DMARC also provides ISPs and other mail recipients with a mechanism for distributing back to brand owners aggregate feedback regarding the health of their e-mail authentication deployment as well as forensic level intelligence.

For mail-sending operations, the recommended approach is:

- *Audit* – by taking an inventory of all machines and systems that send e-mail on behalf of the organization, including external systems such as E-mail Service Providers (ESPs) or other authorized third parties
- *Publish* – authentication and policy records in the DNS
- *Modify* – mail-sending software to use authentication and conform to policy
- *Establish* – reporting relationships for activity using the domain name
- *Monitor* – all available reports for patterns requiring attention
- *Maintain* – operations for on-going conformance

For mail-receiving operations, supporting these new mechanisms primarily entails adding modules to existing mail-filtering systems.

b. Inbound spam filtering

One of the most important methods for stopping the harm from a phishing attack is effective spam filtering. Having spam filtering enabled is important, but effective filtering involves more than just having a commercial product installed at the e-mail gateway. Corporations and government agencies should also enhance their spam filter by adding threat intelligence feeds that help make the spam filter more effective.

This information can be obtained from blacklists created by specialized organizations such as Spamhaus, SURBL, and others (see references at the end of this section). Spam filtering is closely linked to Reporting, as the phishing e-mails that successfully penetrate a spam filter are the most urgent to be reported. Many e-mail services offer a "Report spam" or "Report phish" button which users should be encouraged to use.

Techniques for spam filtering include:

- *Authentication* – e-mail senders have the ability to enroll in authentication methods, including DomainKeys Identified E-mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting and Conformance (DMARC). When e-mail is received, it is checked for the presence of an authentication

token. Under DMARC, the sending domain is checked to see whether it requires authentication. If the token is invalid or missing, the e-mail may be fraudulent.

- *IP Reputation* – the IP address which sends the e-mail may already be known to be associated with the sending of spam. By rejecting e-mails from IP addresses with a poor reputation a great deal of spam can be blocked.
- *Content filtering* – rule-based filtering, checking the e-mail for the presence of forbidden words or phrases, or statistical analysis of the e-mail (Bayesian spam filtering) can identify e-mails that are likely to be spam. Informing content filters with data from reputation services for hostnames and/or URLs (e.g., DNSBL's like Spamhaus/SURBL) greatly improves this technique.
- *Spam traps* – by collecting e-mail sent to addresses which should receive no e-mail (non-existent users) patterns can be identified and applied to block e-mail sent to legitimate addresses.

c. Browser and other blocking

Protection against phishing attacks is built into many products and services that consumers, businesses and other organizations can take advantage of. With the widespread reporting of phishing attacks by brands and the general public, this data is fed into the products that are exposed to phishing such as web browsers, e-mail servers and clients, security appliances (firewalls, IDS/IPS systems, web traffic proxies, DNS firewalls), and online e-mail service providers. These tools/devices can provide even better protection if they are empowered with threat intelligence data. Examples of this include reputation data for IP addresses, hostname/domain names, URLs, e-mail addresses, and other "indicators" of dodgy behavior.

These can be delivered in various forms including DNS-based Blackhole Lists (DNSBL), Real-time Blackhole Lists (RBL), URL block lists, and a relatively new technology called DNS Response Policy Zones (RPZ). Such technologies and data can be implemented to cut off all communications to blocked Internet locations. Companies need to craft policy and operational norms to ensure that they enable such services in their environments. This is particularly important for e-mail gateway products and overall network security tools to create a "layered" defense. This security posture should be well-planned and updated on a regular basis.

Individual users can also protect themselves from many attacks simply by enabling such services in their browsers (e.g., Google Safe Browsing, Microsoft Phishing Filter), adding a "toolbar" to their browser, enabling anti-phishing or anti-spam settings on their web mail account, and activating anti-phishing protections in their A/V software.

2. Detection

Detection of phishing attacks both prevents the particular assault but also helps detect future attacks. Further, without detection, the sites can't be fetched for forensic analysis, blocked in browsers and spam filters, taken down, or investigated. Detection takes several forms, depending on the vantage from which the detection is occurring. When speaking of detection the ultimate goal is to detect the newly created phishing site or e-mail campaign, but often the means for the detection will be in the analysis of the messaging stream between criminals and potential victims.

- Consumer/Employee: because consumers are the most likely recipient of the message, it is important that potentially targeted brands communicate effectively with their customers on what to do if they see a suspicious e-mail. Spear phishing attacks will be directed at employees. Detection will often be in the form of an e-mail seen by a customer or employee of the targeted brand, so providing reporting facilities and user education are important steps for detecting attacks (see below).
- Rejected E-mail: for many years one of the most effective methods for convincing a potential victim that a phishing message is legitimate has been to use the sending domain of the imitated brand. E-mails from "@paypal.com" or "@bankofamerica.com" are likely to be taken at face value by potential victims who are unaware how easily From: addresses can be spoofed. Fortunately, when such messages fail to be delivered, often because the spammer is sending them to an account that is disabled, closed, or no longer receiving messages, the mail server on the receiving

end will "bounce" these messages. As described above, in the case of e-mail authentication, DMARC provides a protocol for directing where these rejected messages should be sent. Analysis of these rejected messages can often lead to the detection of new phishing sources and websites.

- Referring URLs: when a phishing kit uses a graphic, javascript file, stylesheet, or other property from the imitated brand, the log files of the imitated brand will show that the file has been referred to by a third party website. If "hackedsite.com/yourbank/verify.php" is a phishing page, and it uses a graphic from "yourbank.com/graphics/logo.gif" the log will show that "logo.gif" was referred to from "hackedsite.com." Analysis of these referring URLs is a great way to detect new phishing websites. This can be accomplished in-house with a well-trained staff or outsourced to one of many vendors.
- Outbound spam: from the perspective of an enterprise, a hosting provider or ISP, there are several ways to detect outbound phishing e-mails that are being generated from the network. Depending on Terms of Service for the service being provided, the network may be able to observe outbound e-mail from the presence of suspicious characteristics, such as unusual spikes in volume, mismatches in sender domain, attempts to use e-mail ports from non-allowed network space, or the inclusion of IP addresses owned by the network on various reputation lists.
- Credential reuse: a recent technique for the detection of phishing sites has been to require consumers to use a unique user ID and password pair to access a destination brand. A plug-in in the consumer's browser detects any attempt to use that user ID and password pair on any other location, and reports the URL to the destination brand as a suspicious URL to be investigated.
- Security products and open-source software tuned for phishing: e-mail servers, modern security appliances and cloud services employ feeds of known phishing sites, IP addresses, domain names, and patterns for phishing attacks. Based on both direct matches and heuristic analysis of URLs included in e-mail or transiting the corporate network, phishing lures and "clicks" can be detected for blocking, alerting, and action.

3. Reporting

Reporting of phishing attacks serves two purposes. It can help the brands that are being impersonated respond to the threat, and provide a trail, that may be helpful to law enforcement. Once a phishing attack is detected, there are several avenues for reporting it to help protect the broader community from receiving lures or visiting phishing sites. Brands and organizations being spoofed in the phishing lures and websites can alert their customers, employees, and constituents - the most likely victims. Individuals who come across phishing sites can also report them, and victimized brands can help by providing and promoting an easy methodology for their customers and others to report phish to them.

> ***To make reporting as easy as possible, many brands have created easy to remember email addresses such as "reportphishing@targetedbrand.tld". To encourage reporting, brands should make information about how to report a phish prominently available on their websites and are encouraged to make this information available in customer-facing interactions.***

Once an organization has learned that it is the target of a phishing campaign it is important to alert the anti-phishing ecosystem consisting of industry organizations, vendors, and incident responders. This can be done for the occasional phishing attack by reporting the attack through one of the sites listed at the end of this section.

Most major targets of phishing employ third party services that specialize in dealing with illegal/unwanted online content as a core competency, as they have established relationships and processes with major providers, language translation capabilities, and have threat intelligence investigators on staff. Regardless of the reporting method used, recognizing and reporting phishing attacks quickly can lead to the identification of the criminal.

Many compromised servers will contain log entries leaving a trail showing how they were hacked and how the criminal content was placed on the server. Also, each phishing website

must provide a means for the criminal to receive the stolen credentials. This is typically done via e-mail, but can also involve secret files on the webserver where the credentials are stolen. Analysis of identified phishing sites can help to identify, disable, or monitor these data exfiltration points and can lead to the identification of the criminals.

4. Corporate & Law Enforcement Investigations

Most phishing investigations are conducted by the corporation whose brand is being imitated, or by threat intelligence vendors or law enforcement agencies acting on their behalf.[28] Using many of the techniques described under "Analysis & Intelligence" above, investigators can identify and count victims and their losses, but also link together the many phishing sites created by or financially benefiting the same criminal.

Rather than attempting to resolve each case independently, corporations are encouraged to develop relationships with investigative agencies to understand the best methods for exchanging such information. In the United States, the FBI's InfraGard program and the US Secret Service's Electronic Crimes Task Forces are programs that help to develop such relationships. National centers such as the National Cyber Forensics & Training Alliance (NCFTA) also provide opportunities for Public-Private Partnership approaches to cybercrime investigations. Working with these organizations can help brands to be active advocates in the law enforcement process. Often having multiple victim brands represented in a single case leads to a more active law enforcement response, while also providing the "safety of numbers" to the victim brands, which may be uncomfortable being named as victims.

5. User/victim education

McAfee Labs reported in late 2014 that phishing continues to be an effective tactic for infiltrating enterprise networks. Their study found that 80 percent of business users are unable to detect scams, with Finance and HR department employees performing worse than average. Your employees can take their phishing quiz here: https://phishingquiz.mcafee.com.[29] Figures like these show how vital it is that corporations and government programs continue to provide mandated regular training for their employees. This was one of the recommendations of the Federal Financial Institutions Examination Council (FFIEC). SANS (www.sans.org) also has information about running a phishing program on their SecuringTheHuman website.[30]

While it is more difficult to provide training to consumers, companies that experience high rates of phishing are advised to provide education when they have an opportunity to interact with their customers, whether this be in the form of a bill insert, a special warning when the customer logs in to the online system, or through a recorded message while interacting with consumers by telephone. Corporations who are concerned with associating their brand with cybercrime can instead embrace a pro-active message, such as the "Stop. Think. Connect." campaign, or state that they are showing support for government-encouraged cyber awareness, such as the annual cybersecurity awareness weeks and months offered by most developed nations.[31, 32] Many resources are available as part of these public outreach campaigns that can be adopted by corporations.

The APWG encourages companies to assist with just-in-time training by adopting the APWG Phishing Education Landing Page as their home page.[33] Webmasters who take down a phishing website after being hacked are also encouraged to replace the page with the APWG Landing Page. Several organizations have developed their own excellent training pages to help educate users. These include Visa and Stay Safe Online:

http://www.visasecuritysense.com/en_US/phishing-attack.jsp
https://www.staysafeonline.org/

The US FTC uses a little light heartedness to alert consumers to the risks associated with phishing by depicting standard phishing ploys to alert consumers to this problem via online games and YouTube videos.

- Online games: http://www.onguardonline.gov/media/game-0011-phishing-scams, and
- YouTube videos: https://www.consumer.ftc.gov/media/video-0006-phishy-home.

6. Industry Involvement

Industry information sharing organizations such as the FS-ISAC (Financial Services Information Sharing Analysis Center) and the Canadian Financial Institutions' Computer Incident Response Team (CFI-CIRT) are also very important organizations for helping to address "cross-brand" phishing crimes.

Involvement in industry advocacy groups, such as the Anti-Phishing Working Group (APWG)[34], the Messaging, Malware, and Mobile Anti-Abuse Working Group (M³AAWG)[35], the Online Trust Association (OTA)[36], the Merchant Risk Council (MRC)[37], and the Forum of Incident Response and Security Teams (FIRST)[38] are some of the many membership-based organizations addressing online fraud and cybercrime. Their membership meetings, publications, and special interest groups offer many benefits to brands that are suffering from phishing. The APWG, for example, offers extensive information sharing capabilities and large-scale reporting of phishing sites to member organizations making, it a primary resource for entities being hit with phishing attacks.

References

Statistics

- Anti-Phishing Working Group Phishing Activity Trends Report / Domain Use Report
  http://www.antiphishing.org/resources/apwg-reports/

  [N.B.: The APWG can provide spreadsheets of source data for its reports back to 2006, upon written request. Contact: secretarygeneral@apwg.org]
- Anti-Phishing Working Group Global Phishing Survey:
  http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf
- The Anti-Phishing Working Group Web Vulnerabilities Survey
  http://www.apwg.org/reports/apwg_web_vulberabilities_survey_june_2011.pdf
- Phishing: How many take the bait? Government of Canada
  http://www.getcybersafe.gc.ca/cnt/rsrcs/nfgrphcs/nfgrphcs-2012-10-11-eng.aspx

User-Facing Programs

- The Anti-Bot Code of Conduct for Internet Service Providers: http://www.M3AAWG.org/abcs-for-ISP-code
- iCode.org - Internet Industry Association: https://icode.org
- Anti-Botnet Advisory Center - ECO (Germany): https://www.botfrei.de/en/
- STOP. THINK. CONNECT.: http://www.stopthinkconnect.org
- APWG Consumer Advice: http://www.antiphishing.org/resources/overview/
- APWG Educating Consumers: http://www.antiphishing.org/resources/Educate-Your-Customers/

Reporting Phishing:

Anti-Phishing Working Group:
http://www.antiphishing.org/report-phishing/
e-mail: reportphishing@apwg.org

Major browsers/webmail providers:
Google:
https://www.google.com/safebrowsing/report_phish/
Microsoft:
www.microsoft.com/security/online-privacy/phishing-scams.aspx#Report
Yahoo:
https://safety.yahoo.com/Security/IVE-BEEN-PHISHED.html

Security vendor online resources:
http://www.phishtank.org
https://submit.symantec.com/antifraud/phish.cgi
http://phishing.eset.com/report
http://toolbar.netcraft.com/report_url

United States:
The Internet Crime and Complaint Center provides centralized reporting of cybercrimes where losses have occurred:
www.ic3.gov/default.aspx
US-CERT also has a place where all phishing reports may be sent: https://www.us-cert.gov/report-phishing
e-mail: phishing-report@us-cert.gov
The Federal Trade Commission's spam reporting system feeds into the Consumer Sentinel Data Base, a law enforcement tool for investigative leads: UCE@ftc.gov

Canada:
Spam Reporting Center: fightspam.gc.ca
e-mail: spam@fightspam.gc.ca
Canadian Anti-Fraud Centre:
www.antifraudcentre.ca/english/reportit-howtoreportfraud.html
www.antifraudcentre.ca/francais/reportit-howtoreportfraud.html
Canadian Bankers Association lists the "Report Phishing" pages for most Canadian banks:
www.cba.ca/en/consumer-information/42-safeguarding-your-money/91-email-fraud-phishing

United Kingdom:
The National Fraud & Cyber Crime Reporting Centre allows the reporting of fraud, attempted fraud, and online scams or viruses. Consumers can use the link below to report fraud.
www.actionfraud.police.uk/report_fraud
The Action Fraud Business Reporting Tool is for knowledgeable security professionals who may need to report many fraud instances per day:
https://app03.actionfraud.police.uk/report/Account

Ireland:
https://www.botfrei.de/ie/ueber.html

Australia:
http://www.acma.gov.au/Citizen/Stay-protected/My-online-world/Spam/reporting-spam-i-acma
https://www.scamwatch.gov.au/content/index.phtml/tag/reportascam
https://report.acorn.gov.au/
e-mail: report@submit.spam.acma.gov.au

New Zealand:
http://complaints.antispam.govt.nz/

France:
https://www.signal-spam.fr
The French CERT-LEXSI, Europol, and the governments of Netherlands and Luxembourg also offer a site for reporting phishing:
https://phishing-initiative.eu

Best Common Practices

- What To Do If Your Website Has Been Hacked
  http://www.apwg.org/reports/APWG_WTD_HackedWebsite.pdf
- Subdomain Registries Advisory
  http://www.apwg.org/reports/APWG_Advisory_on_Subdomain_Registries.pdf
- Anti-Phishing Best Practices Recommendations for Registrars
  http://www.apwg.org/reports/APWG_RegistrarBestPractices.pdf
- Measures to Protect Domain Registration Services Against Exploitation or Misuse
  http://www.icann.org/committees/security/sac040.pdf
- M³AAWG Sender Best Communications Practices https://www.M3AAWG.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf
- Trust in Email Begins with Authentication (M³AAWG E-mail Authentication White Paper)
  https://www.M3AAWG.org/sites/maawg/files/news/M3AAWG_Email_Authentication_Update-2015.pdf
- M³AAWG /APWG Anti-Phishing Best Practices for ISPs and Mailbox Providers
  http://www.M3AAWG.org/sites/maawg/files/news/MAAWG_AWPG_Anti_Phishing_Best_Practices.pdf

Domain Names and IP Addresses

A variety of malicious and illegal activities take advantage of vulnerabilities in the Domain Name System (DNS) as a result of poor business and security practices among operators of Internet addressing infrastructure and domain name registries, registrars, resellers and providers of privacy and proxy services. Better management by network operators, and improved practices by organizations that manage IP addresses and domain names, or the organizations that provide domain name registration services, can mitigate these threats.

Technology Overview

Internet Protocol (IP) Addresses

Every computer on the Internet has an IP address, which is used to route traffic to and from that computer. Traditional IP addresses, known as IPv4, are 32-bit binary numbers, invariably written as four decimal numbers, such as 64.57.183.103. The first part of the address, which in this example might be 64.57.183, identifies the network, and the rest of the address, 103 in this example, the particular computer ("host") on the network. The division between the network and host varies depending on the size of the network, so the above example is merely typical. A newer version called IPv6 uses much larger 128-bit numbers, written as blocks of digits separated by colons, such as 2001:500:2f::f. Nearly all IPv4 addresses have been assigned, so we are now in the midst of a gradual transition to IPv6.

For network traffic to flow from one computer to another, for example, from a user's PC to Google's web servers or vice-versa, traffic from the sending computer flows through intermediate computers, called routers, to the destination.

There are about 500,000 network routes visible to the Internet's largest routers, known as backbone routers. (The total number of networks is considerably greater, since a single backbone route typically covers dozens to thousands of customer networks). To maintain the tables of 500,000 routes, backbone routers use a system called the Border Gateway Protocol (BGP) to exchange information, so the routers can automatically adjust the tables when new networks come online or a link between networks fails or is being repaired.

Somewhat like telephone numbers, every world-visible IP address must be unique. Internet providers and large businesses get blocks of addresses directly from Regional Internet Registries such as ARIN, which allocates IP space for the United States, Canada, and parts of the Caribbean, while smaller businesses and individuals use parts of blocks assigned to their Internet providers. Some IP addresses are not world-visible, for example 192.168.1.1 or 10.0.0.51; they are analogous to Private Branch Exchange (PBX) extensions in a business telephone system, only reachable from within that organization's own network.

The Domain Name System

Since IP addresses are hard for humans to remember, and are tied to physical networks, the Domain Name System (DNS) is a distributed database of names that lets people use names like www.google.com rather than the corresponding IP address 173.194.73.105 (for IPv4) or 2607:f8b0:4000:807::1012 (for IPv6). Despite its enormous size, the DNS gets excellent performance by using delegation and caches. Since it would be impractical to store all of the names in the DNS in a single database, it is divided into zones that are stored on different servers but logically linked together.

In principle, to find the address of Google's www.google.com, the DNS lookup software on a user's computer, known as a resolver, first contacts one of the "root" DNS servers, which

responds that for all names in .com, ask a list of DNS servers that have authoritative information for .com (in this case, run by Verisign). It then contacts one of the .com servers, which in turn replies that for all names in google.com, ask a list of DNS servers that have information for names in google.com (run, of course, by Google). It then contacts one of those DNS servers, which provides the IP addresses for www.google.com.

Since Internet users tend to look up the same names repeatedly, every network and many individual computers have a cache that remembers recent DNS queries and answers, so if someone who uses the cache has recently asked for www.google.com, subsequent queries can be answered from the cache rather than going back to the master servers. Or if someone asks for mail.google.com or www.yahoo.com, the cache provides the servers for google.com (for mail.google.com) or the servers for .com (for www.yahoo.com), greatly reducing the number of queries to the master servers, and speeding responses to users.

Since there are a variety of ways that hostile parties can inject forged DNS data into caches and individual computers (some discussed below), DNS Security Extensions (DNSSEC) adds secure cryptographic signatures to data returned from DNS servers, so user computers can check the signatures for validity and ensure that the DNS data they use is valid, and actually came from the correct party. DNSSEC has been in development for 17 years, but has only achieved significant use in the past few years. The key management for DNSSEC is complex, and can present a challenge to managers of DNS servers.

DNS Exploits

The most serious DNS (Domain Name System) exploits are resolver exploits, in which cybercriminals introduce forged data to redirect web and other traffic to false versions of popular web sites.

Cache poisoning

One category of such exploits is cache poisoning, that is, using security holes to introduce forged data into DNS caches where it is then provided to victims' computers. Few users will have any capability to detect false DNS information in use by their computers. By blending multiple exploits together, a miscreant can present a perfect replica of any website, any trust seal, any logo, and show the correct domain name in the browser address bar. The result may be credential stealing, financial resource access, corporate or nation-state intelligence compromise, or just re-directed advertising revenue.

Resolver exploits occur completely within the NSP (Name Service Provider, such as an enterprise name server, or a public DNS service such as OpenDNS or Google DNS) and network operator's systems, needing no compromise of a user's computer.

DNSSEC when correctly deployed by all parties to a name lookup including the registrant, registry, and NSP, will prevent cache poisoning and other DNS misuse. At this time, DNSSEC is sparsely deployed, and is not yet considered a reliable defense against cache poisoning. The currently deployed defense against cache poisoning is called UDP Source Port Randomization, but this defense required, in 2008, that all DNS software be upgraded.

DNS software, like all Internet infrastructure software, must be updated periodically to correct known defects as they are discovered and repaired by the software vendor. Careful monitoring is recommended at all times to detect anomalous conditions in online infrastructure, but such monitoring is of paramount importance after each software update, since an update might fix some defects while introducing others.

Contextual security also warrants mention. If DNS software were completely bug-free, it would still be necessary to fully secure, update, and monitor the operating system including any virtualization systems as well as routers, switches, firewalls, and intrusion detection/prevention systems. RFC 2196, the Site Security Handbook, provides an overview of these issues.

Best practices:

1. Support the worldwide deployment of DNSSEC, to secure distribution of DNS data. This includes signing all authority zones with DNSSEC, and enabling DNSSEC validation in all recursive DNS servers.

2. Use TSIG for all online DNS updates and for server-to-server "zone transfer" operations, to ensure authenticity and authorization.

3. Keep DNS software patched up to the latest version recommended by the vendor, and monitor DNS infrastructure for anomalies at all times, but especially after installing a vendor patch.

4. Provide a Best Practice document for security policy for DNS resolvers, to educate network and system managers.

Malware that targets the DNS

The "DNS Changer" method is another way to falsify DNS answers. This malware modifies each victim's computer to change the DNS resolvers it uses, substituting the miscreant controlled DNS resolvers for the user's ISP's own resolvers. The miscreant then selectively provides falsified answers whenever doing so will bring in additional revenue.

The DNS Changer malware works not only on the users' computers but also on home or small business routers. The miscreant's advantage in altering the router settings is that the change is likely to be more long-lived and covers all computers, phones, iPads and other devices in the home or office - potentially including web-enabled home control devices, like thermostats, cameras, photo frames, wireless and wired networks, etc. The router may be inside the broadband service provided modem or may be an extra device purchased and installed by the user.

The FBI worked with private industry to deprive the DNS Changer cybercriminals of their resources (and their freedom).[39] The IP addresses used by the compromised resolvers were re-routed to accurate resolvers which ran for a few months while volunteer groups notified ISPs and users who were affected. Note: the basic strategy used by the DNS Changer criminals would work equally well if tried again - all of the necessary underlying vulnerabilities are still present in wildly popular equipment that can't be upgraded by the vendor.

Detection of misdirected DNS traffic can be conducted at the ISP level by monitoring outgoing customer DNS traffic that goes to a resolver other than one that they provide. Note that it is very common for technically advanced users - or those intentionally subscribing to a different DNS service - to send their DNS traffic elsewhere. Careful design of the detection systems is necessary to avoid false positives.

In the future, users may be tricked into switching to a miscreant's DNS resolver by social engineering or some enticement. For example, if ISP resolvers are required to deny access to some DNS names (such as pirated or otherwise illegal content), users may respond to offers that promise uncensored DNS access. There are many legitimate reasons to allow users to choose their DNS resolver service without censorship or interference.

Best practices:

1. Educate the public about the dangers of DNS resolver changes, to limit social engineering attacks.

2. Encourage network operators to share anonymized feeds of the top non-local DNS caches being queried from their networks, to identify possible rogue DNS resolvers.

3. Provide the feed to all vetted anti-abuse researchers to aid detection of services that have tricked users or are falsifying DNS responses and to distinguish them from legitimate DNS resolver services.

4. Develop metrics based on that aggregated data to help identify cybercriminals for legal action, update a blacklist of fraudulent resolvers, and create coordinated mitigation operations such as occurred with DNS Changer.

5. Establish best practices for anonymization sufficient to prevent connecting original users, their ISPs, and the DNS activity, to prevent retaliation against users who circumvent censorship as this would otherwise simply drive users to use harder to detect, but still possibly compromised DNS resolvers.

Attacks through abuse of domain name registration services

The ease with which cybercriminals can register and use new domains helps them conduct their frauds. Providing false identity information and often using stolen financial credentials makes tracing the true owners of domains that are used to commit frauds difficult. The burden of detecting malicious use of domain names rests on the shoulders of anti-abuse researchers, often long after the malicious activity has begun, or sometimes ended. The burden of mitigating malicious domains is on every company that provides Internet access to users - either via requests to shut down malicious activities, or the often slow propagation of domain blocklists. Blocklists are necessary because requests to redirect, suspend or delete domain names are often ignored.

Cybercriminals exploit domain registration services by using stolen credit cards to register domains, by registering many domains at high speed using automation, by registering domains through resellers or privacy/proxy providers that are not responsive or that appear to permit malicious activity, and by cycling through domains, which they can use within minutes or even seconds after registration. Abuse researchers typically can only monitor newly registered DNS registration data by snapshots every 24 hours. Blocklist operators take time to recognize malicious domains and then to propagate reputation information after the miscreant has carried out the malicious act.

Cybercriminals can create any subdomain based on domains they own, such as bankname.ssl-cgi.Cybercriminalsexample.com. There is no limit on how many such names they can create - and at no cost. Fooling users doesn't require a brand name—just anything that seems plausible. Names such as secure-order.verified.example.com are accepted by most users since they look like other things they have often seen.

Some entities actually help commit IP abuse by creating domain names that are likely to mislead consumers. These services create domain names that purposefully mimic brand names by using typos such as SEARZ with the letter 'Z' instead of the letter 'S', or PAYPA1 with a digit '1' instead of a letter 'L'. While these domains may never be used in a phishing campaign, there are millions of such domains which make it difficult for abuse researchers to distinguish relatively harmless typosquatters from the next malicious activity before it happens.

In addition, attackers hijack domain names through other techniques, including:

- Compromising the registrant's access credentials to the registrar's control panel (stealing the password the customers use to log into their domain management site),
- Compromising the registrar's own systems in order to steal all or some of the passwords (known as EPP codes or auth-codes) required to transfer domain names from one registrar to another, and
- Compromising the registrant's own name servers or DNS related database in order to alter the data in the victim's domain in-situ, without any upstream redirection.

Best practices:

1. Domain name registries in both the generic Top Level Domain (gTLD) and country code Top Level Domain (ccTLD) spaces, as well as the registrars they do business with, should implement and closely oversee 'Know Your Customer' programs to prevent abuse of domain assignment. That will allow them to determine if and when they should avoid conducting business with a registry, a registrar, a reseller or a privacy/proxy service provider.
2. All domain name registries, registrars, resellers and privacy/proxy providers should implement mandatory HTTPS and multi-factor authentication, to reduce the risk of theft of customer account credentials and to better protect their customer's transactional sessions.
3. Domain name registries and registrars should consider cooperative agreements or memoranda of understanding with organizations that help protect the consumers, such as LegitScript and the Anti-Phishing Working Group (APWG). By establishing pre-defined levels of trust, reports of abuse received from these organizations can be addressed by registries or registrars in a much faster and more effective way, such as the APWG's Malicious Domain Suspension Program.

4. Domain name registries and registrars should check rigorously for stolen credit cards used for registrations, to prevent malicious domains from being registered.

5. Enforce legal (in their own national jurisdictions) and contractual obligations that providers of domain registration services, including all registries, registrars, resellers and privacy/proxy service providers must comply with, with regards to acting on reports of abuse.

6. For privacy/proxy services, there is an urgent need for accreditation programs to be implemented and enforced. This will clarify the rules and processes for handling requests to relay, pass communications to the underlying customer, and reveal, disclosing the customer's identity. This applies to all privacy and proxy services, regardless of whether they operate in the gTLD space or the ccTLD space and regardless of whether they are owned, managed or operated by a registry or a registrar.

7. Registries and registrars for both gTLDs and ccTLDs spaces should avoid doing business with privacy/proxy service providers not covered by an accreditation program.

8. Prior to processing requests to register new domain names or accept incoming transfers of domains, registrars and ccTLD operators who offer registration services directly to the public should validate the reputation of certain registration data elements, such as:

   a. e-mail addresses used by the registrant, account holder or any of the other Whois contacts,

   b. the IP address from which the transactions are being requested,

   c. the nameservers that the customers want to set for their domain names,

   d. the registrant's postal addresses, and

   e. a statistically valid sample of domain names already registered by the same customer.

   As an example, a reputation validation service is provided at no cost by The Secure Domain Foundation that allows registrars and applicable registries to decide to decline to create new domain names, or accept incoming transfers, if any of the data elements has a poor reputation, which indicates significant recent malicious activity.

9. Improve reputation algorithms to include domain age: domains more than a year old are less likely to be "throw away" domains, some mail accreditors prevent clients from using domains less than a month old, and examining domains less than a day old is currently an effective way to find malicious activity.

10. Since domain hijackers use IP addresses that are usually different from those used by the registrants, registrars and resellers should enable account activity tracking of IP addresses. If a customer's account is accessed from a new IP address, the registrar or reseller should notify both the registrant and the administrative contact for the given domain name.

11. Continue browser improvements and user education to recognize browser signals of extended validation ("green bar") certificates, and to prevent confusion by sites that use terms such as "secure" or "ssl".

12. Educate corporations to send user notifications that are hard to imitate to deter phishing and social engineering.

13. For sites and software that use domain blocklists, encourage a multi-layer approach with a variety of types of blocklists, including pre-emptive blocking methods as well as longer-lived but reactive blocklists, to improve blocking effectiveness.

14. Support passive DNS projects such as Farsight Security Inc's (FSI) Security Information Exchange (SIE) which provide early warnings to both academic and commercial researchers about malicious subdomains actively in use.

15. Consider DNS firewall technologies such as Response Policy Zones (RPZ), an open multi-provider multi-consumer marketplace supplying DNS resolution policy recommendations to recursive DNS operators. (See http://dnsrpz.info/).

Web and other server DNS attacks

Cybercriminals exploit the reputation of legitimate domains by breaking into their web servers and depositing malicious files that then infect the legitimate domain in the URL. (This technique is immune to domain blocklists unless those blocklists are willing to list legitimate domains that are serving malicious content, thereby blocking some legitimate content along with the malicious.)

Cybercriminals use web redirections to first present a domain with a good reputation—then redirect the user to the malicious destination site. These individuals then use multiple levels of redirection and recently even redirect to URLs with numeric IP addresses rather than domain names.

The success of such techniques depends on inadequate detection methods that are only able to recognize such attacks if users fail to "act like a victim would" by following the redirects. Unfortunately some marketers further complicate the threat by using multiple redirect levels to track customer response to marketing e-mail. URL shortener services are often abused and used to redirect from a well-known domain such as bit.ly to the cybercriminal's malicious website. It is difficult for a user to differentiate among millions of legitimate bit.ly URLs used to shorten a long web address for Twitter posts, from ones that will lead to malware or, for example, an ad for illegal pharmaceuticals sales.

Recently, ICANN itself was victimized by a group of hackers accessing ICANN's domain registration account at Register.com. In this case, the attackers altered the DNS configurations of several domains (icann.net iana-servers.com, icann.com, and iana.com) and rerouted visitor traffic to a defacement web site.

Best practices:

1. Establish and maintain a system that blocks compromised legitimate domains that serve malicious content, along with rapid notification, retest and delist, and assistance to improve the security hygiene on all web servers at the exploited site.
2. Encourage URL shortener services to check and recheck all redirects in the chain for each redirection they supply, and to work with multiple abuse protection providers to identify new abusers.
3. Develop education and resources for industry and end users on how to identify and avoid URL shorteners that lack adequate anti-abuse measures.
4. Improve the effectiveness of URL reputation testing, by, among other things, including testing redirects, using tests that appear to be a real user during testing, and developing policies regarding maximum redirect depth, all to limit abuse of URL shortening services and other vulnerable URL redirection services.

IP address attacks

IP address attacks fall into two general categories, e-mails lying about their IP addresses (spoofing), and networks using ranges of IP addresses they are not authorized to use (rogue announcement).

IP address spoofing

Each packet of data sent over the Internet includes the "source" IP addresses of the computer from which it was sent, and the address of the computer for which it is destined. It is possible for a hostile computer to put a false (spoofed) source address on outgoing traffic. For transactions in which the destination sends return packets back to the source address, notably the DNS, this can create unwanted traffic to the true address that was spoofed. It is easy to send small DNS requests that result in large DNS results, causing denial-of-service to the spoofed address.

Best practices:

1. ISPs and transit networks should filter incoming mail, keeping track of the range of addresses assigned to each customer network, and discarding traffic with source addresses outside the assigned range, to prevent their customers from sending traffic with spoofed addresses. This is generally known as BCP 38[40], after an IETF best current practices document. BCP 84, another IETF best current practice, recommends that upstream providers of IP connectivity filter packets entering their networks from downstream customers, and discard any packets which have a source address which is not allocated to that customer.[41]
2. Encourage a universal practice of ingress filtering for all connected customer or peer networks.

Rogue Announcements

Each network can announce via BGP their own ranges of IP addresses. Hostile networks can announce network ranges they are not authorized to use. This can result in rerouting and diversion of traffic intended for the real network, or it can allow "stealth" traffic by announcing a range of addresses, performing an attack, and then withdrawing the announcement. Unless the victims are aware of the rogue announcement, they will blame the legitimate owner of the addresses.

Best practices:

1. Network operators should implement BCP 84 ingress route filtering[42] (discussed above), in which incoming BCP announcements from customers and peers are limited to an explicit list of networks known to be assigned to that customer or peer.
2. ISPs should endeavor to, insofar as possible, implement BGPSEC (BGP security) to cryptographically protect route announcements and prevent publication of rogue data.

Stealing address ranges

In the early days of the Internet, address allocation was often done quite informally, with incomplete records. As a result, there is considerable *legacy* address space assigned that may be obsolete, either because the organizations have forgotten about the address they used, or the entities no longer exist. Cybercriminals have taken advantage of these abandoned addresses by forging documents or re-registering abandoned domains used in e-mail, to gain control of legacy address space.

Best practice:

1. Regional Internet Registries should implement and follow procedures to verify the identities of purported owners of legacy space, to keep cybercriminals from gaining control of address space. ARIN, the RIR for North America, has detailed procedures for this.[43]

References

- Wikipedia, Discussion of DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions
- RFC 2196, *Site Security Handbook*, B. Fraser, Ed., September 1997, http://www.rfc-editor.org/info/rfc2196
- RFC 4034 *Resource Records for the DNS Security Extensions*. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4034
- RFC 4035 Protocol Modifications for the DNS Security Extensions. R. Arends, R. Austein, M. Larson, D. Massey, S. Rose. March 2005, http://www.rfc-editor.org/info/rfc4035
- US CERT Vulnerability Note VU#800113, "Multiple DNS implementations vulnerable to cache poisoning", http://www.kb.cert.org/vuls/id/800113/
- DNS Changer Working Group, http://www.dcwg.org/
- Brian Krebs, "A Case of Network Identity Theft", http://voices.washingtonpost.com/securityfix/2008/04/a_case_of_network_identity_the_1.html
- Open Resolver Project, http://openresolverproject.org/
- M³AAWG Senders Best Practices, https://M3AAWG.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf FCC
- FCC CSRIC III Working Group 4 reports on BGP Security Best Practices: http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Mobile and Voice Threats

The Mobile Environment

With the advent of the smartphone and the applications markets for Android, Apple, Windows, and Blackberry devices, consumers are increasingly using their mobile devices to access online accounts, make purchases and conduct other financial transactions. Smartphones represent 70 percent of the nearly 1.85 billion mobile phones sold worldwide in 2014[44], with Android and iPhone being the dominant devices currently in use. Tablets, which blur the delineation between phone and traditional computer, have also become a significant player in this arena. Retail sales from mobile devices, including tablets increased from 11 percent of the overall e-commerce market in 2011[45] to 13 percent in 2014[46]

Globally, there are approximately 3.7 billion active mobile phones users[47], exceeding 50 percent of the world's 7.3 billion population,[48] and mobile phones are the primary Internet access for much of the world. In the fourth quarter of 2014 vendors shipped over 500 million mobile units across the world.[49]

App Markets

Unlike the PC software marketplace, where major applications are developed by a number of well-known and trusted vendors and users are less likely to install applications from less trusted sources, the mobile application ecosystem encourages end users to load large numbers of low-cost applications from smaller and often less trustworthy vendors, including single-person enterprises. In many countries, most applications are obtained from app markets with inadequate security, which feature malware laden apps. In other countries, users may be initially limited to loading applications only from phone OS vendors or carrier-approved app markets; however, users may override settings, allowing access to any app market. Major phone OS vendors, including, Google, Apple, Microsoft and RIM operate high-volume application markets with tighter security. Apple, for example, has 1.4 million apps in its App Store, generating a cumulative US$25 billion in sales for app and game developers to date. However, the scale of even the most secure app markets makes it extremely difficult to prevent malware from occasionally being offered. As e-commerce has migrated to the mobile environment, bad actors and fraudsters have been quick to follow.

Particular Threats and Best Practices

App Store Security

Smart phones can be compromised by the installation of new software, often obtained from a store controlled by the phone operating system (OS) manufacturer. In 2014, Symantec found that 17 percent (over 160 thousand) of all Android apps were actually malware in disguise[50]. In a review of the 100 health apps in the App Store, 20 percent transmitted user credentials without encrypting them, more than half (52 percent) did not have any visible privacy policies and, on average, each app contacted five Internet domains (typically a mix of advertising and analytics services)[51].

Some operating system vendors and app stores have the ability to remove malicious apps from the user's phone if that app was originally obtained from their app store. Other malicious apps will be rejected prior to getting into the store if they violate the security policies set by that store.

Apple has placed more restrictions on apps and developers before allowing them into their app store. The Google Play store has a more open acceptance policy and is more reliant on removing accepted apps which are found to be malicious and/or in violation of app store policies.

When a consumer purchases a smart phone, access to unofficial app stores is typically disabled; the phone is locked into a small set of "official" app stores (e.g., the OS manufacturer's and the mobile carrier's). Mobile devices that use the Android operating system have a setting called "Unknown Sources" with a checkbox to authorize installation of non-Market apps. The user can reconfigure Android phones to allow connection to unofficial or alternative app stores. Apple devices require a more technically difficult "jailbreaking" process; however, for less-savvy users, jailbreaking is offered as a low-cost service at many kiosks and points of sale. Even to access legitimate alternative app stores such as the Amazon Appstore, this checkbox may need to be on. Unfortunately, the phone is subsequently wide open to installing any unknown sources. Users can then be more easily tricked into installing malware. The malware writer gets a free pass without supervision by any official mobile app store once access to unofficial app stores is enabled.

There are also new ways for fraudsters to evade app store restrictions even if the phone is configured to only use the official app store. Mobile device web browsers can be used to install HTML5 mobile apps, which place an icon on the home screen of the device that resembles an app installed from an app store. Attackers can then exploit vulnerabilities in the stock browser that comes with the mobile device, or alternative browsers that the user may choose to install. Linkages from the browser to native functions of the device such as camera, microphone, phone diallers and geo location can be used by a criminal to obtain personal data and current activities of the mobile device user.

The username/password login that each mobile device uses to access the app store and authorize purchases is a significant point of vulnerability. Once in possession of these credentials, criminals can run up financial losses and install spyware. Both Apple and Google mobile operating systems presently require the same username and password as the keys to the app store and all other services including laptops, cloud file storage, contacts, calendar and e-mail. Whereas a username and password would formerly have only allowed an attacker to access a subscriber's e-mail account, the same credentials now provide access to the app store. In multiple cases, users have had laptops and phones wiped of data after criminals obtained this key information. Various third parties offer anti-virus protection for some phones and make attempts to test all new applications in app stores for malicious activity or malicious intent.

Best Practices for Industry and Government for app stores:

1. "Application Neutrality": Allow users, network operators or other trusted parties to explicitly specify additional "trusted" app stores, and perhaps the level of trust associated with each. This allows consumers to choose other reputable app stores without exposing them to risky app downloads from unknown sources.
2. Identify apps with malicious potential with rigorous security scans before allowing them into app stores instead of relying on complaints afterward.
3. Provide warnings, controls and education to users to reduce the incidents of users being tricked into following malicious instructions to get past security measures.
4. Improve security policies for app store password reset mechanisms to prevent criminals from obtaining app store credentials that do not belong to them.
5. Handsets may be locked to access only the official app stores as an anti-competitive measure. While consumers may be well protected by this model, it invites consumers to employ workarounds that introduce security holes (e.g., jailbreaking, rooting or unlocking devices). Policies that permit or assist in app-store locking should be weighed against the impact of the security holes created by the unlocking.
6. Encourage app stores to become members of botnet/online threats analysis centers, so that they can benefit from analyses, alerts, and reports coming from these centers. Malicious apps can then be detected, flagged and deleted in the swiftest way possible.
7. Provide mechanisms that allow users to report potentially malicious apps.

Mobile Malware

Malicious apps, known as mobile malware exist for Android, iOS, Windows Phone, Symbian (Nokia) and Blackberry devices. Currently the majority of mobile malware targets the Android platform in areas with abundant use of unofficial app markets.

Most malware is or appears to be a useful application, and is distributed on websites or via unofficial app stores. Often, the promoters of malware will corrupt legitimate apps by inserting "Trojan horse" code. Thus, users may install these modified apps, unaware they contain malicious code. Criminals are increasingly using digital advertising as a vehicle to spread malware; this is known as Malvertising. Also, 2014 saw the emergence of the "SMS Worm"[52] which propagates via SMS through infected handsets' contact lists. Recipients are tricked into clicking on the malicious link contained within the SMS which leads to the exploit. If they install the exploit then their contacts will receive the same malicious SMS making this attack vector highly viral.

Typically malware performs actions that generate revenue for the attackers. Direct monetization schemes cause direct financial loss to the victim and include malicious applications that can perform a wide variety of functions, including: sending premium SMS messages to a short-code registered by the attackers; downloading pay-per-download content; click pay-per-click links; make outbound phone calls to toll phone numbers; intercept online banking credentials; and demand a ransom payment to unlock victims' devices. Attackers can also generate revenue indirectly by collecting phone numbers for SMS spam, collecting device and user data for marketing, displaying advertisements, selling commercial spyware applications and using the infected device to mine crypto currencies. In addition, commercial spyware applications allow a party to monitor a person of interest and collect device and user data such as SMS messages, e-mails, location, and call logs.

Below are noteworthy examples of malware for Android, Blackberry, and iOS.

Oleg Pliss Attack (2014): The Oleg Pliss attack uses a compromised iCloud attack to lock users out of their iPhones.

Slocker.A (2014): Slocker.a is apparently the first instance of file encrypting mobile ransomware. It encrypts user data files on Android devices, and then demands a payment for the decryption key.

SMScapers (2013 – to present): This malware comes in the guise of an adult natured app and is disseminated through mobile display advertising. It covertly charges users by sending an SMS to a premium rate short code and suppresses notification of relevant incoming SMS. The campaign predominantly targeted the UK however regulatory enforcement has contributed to a sharp decline in such activity. The campaign was split over twenty different legal entities therefore adding complexity to the enforcement process. The campaign continues to be live in 15 other countries[53,54].

Worm.Koler (2014 to present): 2014 saw the rise of Android Ransomware where numerous samples such as ScareMeNot, ScarePackage and ColdBrother emerged. The US saw Worm.Koler spread itself via SMS to contacts stored on infected handsets. The exploit also locks victims out of their device with a fake FBI warning stating that illegal content was found on their handset. They are then encouraged to pay a fine to avoid criminal charges and liberate their handsets.

DeathRing (2014 to present): DeathRing predominantly targets Asia and is malware that attempts to phish sensitive data from victims by displaying fake SMS. The attack vector is unique as the malware appears to be factory installed suggesting that the criminals infiltrated the supply chain at some point.

Best Practices for Industry and Government to protect against Mobile Malware:

1) Educate consumers, using public service announcements, web pages, pamphlets and other media to do the following:

a) Obtain applications only from reputable vendor application marketplaces that perform verification on applications or developers or directly from well-known application vendors themselves.

b) Review and understand permission screens, end user license agreements, privacy policies, and terms of agreement when installing new applications.

c) Maintain the default security restrictions on the device, and do not jailbreak the device (jailbreaking is discussed in more detail below).

d) Install remote locate and lock software to aid in recovery and protection of data in lost and stolen phones. For example, IMEI (International Mobile Equipment Identity) is a 15- or 17-digit code that uniquely identifies a mobile phone. The IMEI code can enable a GSM or UMTS (Universal Mobile Telecommunications Service) network to block a misplaced or stolen phone from making calls.

e) Install and run mobile security software on all devices.

2) Develop facilities for and encourage consumers to practice reporting of suspicious applications.

3) Encourage, automate and facilitate back up of phone data to a cloud and/or personal storage medium (e.g., a PC).

4) Evaluate the use of mobile security solutions such as secure browsers, mobile device management (MDM) solutions, enterprise mobile sandboxes, and data loss prevention applications to minimize the risk of infection and resulting impact.

An excellent example of consumer education on Mobile best practices was created by Ofcom and can be found here: http://consumers.ofcom.org.uk/files/2014/1394750/using-apps-safely-and-securely.pdf

Blended Threats

Mobile devices are now being used in the multi-factor authentication process for high value account logins. An example of the two factor authentication blended threat is a user visiting a financial website on their desktop computer and logging in with a username and password as was done in the past. But now, the bank requires another step for the user to gain access to their account: receiving a call or text message on their cell phone with a code which the user then types into the desktop computer web browser. This extra step was added because so many users' desktop computers are infected with malware which has given away their banking password to criminals. Criminals have proven to be persistent in attacking each new method of protection. Now they need to compromise both the users' financial passwords and then their cell phone, and be able to relate the two together.

This makes phones an even more valuable target for criminals to compromise and gain control of. This control may be physical in the case of stealing the phone from the owner, or accomplished remotely with mobile device spying software. Either way, blended threats require more effort from criminals and are likely to target higher value accounts or systems.

Mobile device apps are also used as token generators, such as the six digit codes we used to see only on individually issued physical key fob two-factor authentication devices, such as Google Authenticator and Amazon AWS Virtual MFA.

Depending on the criminals' vantage point, they may be able to observe the content of traffic going to and from some mobile devices and pick up on authentication codes. This is the case with codes sent by e-mail or SMS, which some banks offer as an option. SMS (mobile text message) traffic is not encrypted.

The lack of a framework to share information regarding blended threats may itself be viewed as a threat; it allows a large number of exploits that could otherwise be suppressed. What is needed is to devise and implement defence strategies and frameworks that involve technical, policy, law enforcement, and legal entities in multiple countries.

Modifying Mobile Devices

Many Original Equipment Manufacturers (OEMs) and Mobile Network Operators (MNOs) establish secure mobile computing environments to maintain device stability, security, and uphold a positive user experience. In many cases, modifying these environments creates security vulnerabilities that may expose user information, enable theft of service in the form of unauthorized phone calls or text messages, enable remote control of device resources such as microphones or cameras to listen in or view without user knowledge, or enable an adversary to perform a long list of other unauthorized activities.

There are numerous techniques to modify the hardware and software of a device, but three of the more well-known modifications include "jailbreaking", "rooting", and "unlocking".

Jailbreaking a Device

"Jailbreaking" is when someone supersedes the embedded controls on a device. The manufacturer may use OEM controls to enforce application permissions, protect critical areas of the file system on a device, force applications to authenticate to the device, enforce password complexity, among many other management and administration functions.

Why do people jailbreak devices? One reason is that, even with hundreds of thousands of available mobile apps, some people want custom or modified versions of mobile apps. In some cases, a modified app may cost less than the official app (but may infringe on copyright); however, the less expensive app may also contain malicious content.

Rooting a Device

Jailbreaking enables a user to supersede controls, and elevates user access to gain root privilege to a device, which ultimately grants the user all privileges of the operating system. "Rooting" a device allows a user the highest privileges of an operating system.

Example: Zeus Mitmo (Man in the middle/mobile)

Zeus is a Trojan horse application that targets Windows machines and attempts to steal banking information though browser keystroke logging coupled with form grabbing. The typical mechanisms for Zeus proliferation was through drive-by download activities and phishing attempts duping the user into navigating to a malicious site. It was first identified roughly in 2007 and has received many updates which have increased its sophistication, most recently being leveraged to attack within the mobile space. This update serves to benefit the Zeus malware since many companies including financial institutions are now using SMS as a second authentication vector, so having both the online username and password is not enough in the identity theft process. The evolution of this threat vector establishes an alternative planned by a Zeus gang: infect the mobile device and sniff all the SMS messages that are being delivered. The scenario is outlined below.

- The attacker steals both the online username and password using a malware (ZeuS 2.x).
- The attacker infects the user's mobile device by forcing him to install a malicious application either via SMS or via malware impersonating a legitimate banking or productivity application.
- The attacker logs in with the stolen credentials using the user's computer as a socks/proxy and performs a specific operation that needs SMS authentication.
- An SMS is sent to the user's mobile device with the authentication code. The malicious software running in the device forwards the SMS to another terminal controlled by the attacker.
- The attacker fills in the authentication code and completes the operation.

The hackers then use this information to take over the victims' bank accounts and make unauthorized transfers to other accounts, typically routing them to accounts controlled by money mule networks.

Why do people root a device? In addition to loading custom or unauthorized apps and bypassing controls, root access enables a user to alter components and functionality of, or entirely replace the operating system on a device. Some mobile device operating systems are based on a form of UNIX with reduced command sets, by altering the OS, users can free storage by eliminating functions not needed for most users of mobile devices. Rooting a device may also enable a user to load additional commands as desired.

Unlocking a Device

Mobile Network Operators (MNOs) may subsidize cell phone sales under a contract that requires the use of the MNO's network for a period of time. To help prevent fraud and theft, MNOs often use a technical means known as "locking" to restrict the use of the phone to their own network. A device can typically be unlocked by entering a unique "unlock code" provided by an MNO on request or satisfaction of a contractual commitment. Consumers may also find or purchase an unlock code online. If obtaining the code from third party sources, users run the risk of losing personal information or having malware installed by an untrustworthy vendor.

Best practices for Individuals regarding modification of mobile devices:

1. Jailbreaking, rooting and unlocking devices in not recommended to anyone who seeks a standard, stable device with long-term OEM support as it may introduce vulnerabilities unknown to the user.
2. Do not utilize unofficial 'third party' unlocking services.

Best practices for Industry and Government regarding modification of mobile devices:

1. Develop and promote consumer education on and awareness of the risks of modifying mobile devices.
2. Create stronger protections against overriding OEM.
3. Conduct appropriate law enforcement against promoters of abuses of mobile platform.

Baseband Threats

There are several classes of baseband threats. Some may involve the creation of an illicit GSM (Global System for Mobile communications) network that lures devices to connect to it. Others may involve attacks in which specially crafted messages attempt to exploit security holes in mobile devices. With the growth of low-cost research and criminal GSM installations, these threats have proliferated.

Traditionally, operating a GSM network required a significant investment, which made research impractical outside of large institutions, limiting the discovery and exploitation of network-based attacks. For example, to spoof a GSM network, an attacker would need to operate a Base Transceiver Station (BTS). When GSM technology was implemented, network-based attacks against end devices were not much of a concern, so phones were not required to authenticate the networks to which they attached. Recently, however, free open-source software such as OpenBTS has allowed anyone to create their own GSM network at a fraction of the cost of carrier-grade equipment, bringing GSM security studies within reach of both security researchers and criminals.

Baseband Attacks

The attacker will operate a rogue Base Transceiver Station (BTS) in the vicinity of the targeted Mobile Station (MS). The rogue BTS transmits system information messages announcing the availability of a network that the targeted mobile station is willing to connect to. As the primary criterion for network reception is signal strength, the attacker can force the MS to connect to the rogue base station by simply transmitting with a stronger signal than the legitimate base station. This will not happen instantaneously, but the process can be sped up by using a GSM jammer to selectively jam the frequency of the legitimate BTS. This scenario is very similar to the one used by International Mobile Subscriber Identity (IMSI) catchers. Since GSM will not always provide mutual authentication, there is no protection against fake BTSs.

Best Practices for Industry and Government to protect against baseband threats:

As carriers adopt new technologies (e.g., 3G and 4G/LTE), handsets should be required to authenticate the carrier infrastructure to which they attach.

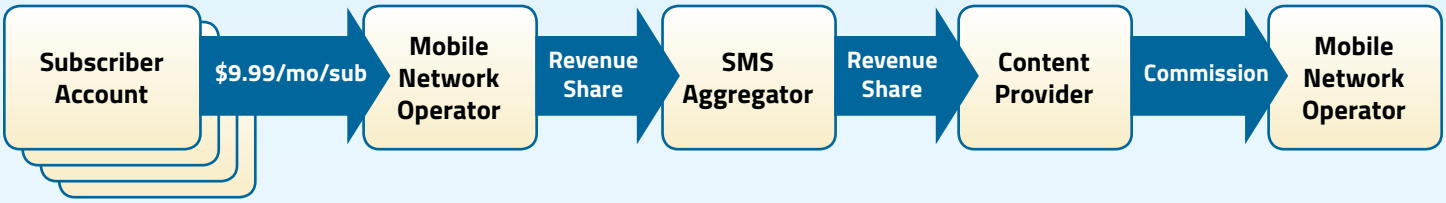
1. Service providers can work with handset manufacturers to notify users when the handset opens a session that does not use mutual authentication This would alert the user of this possible threat vector.

Premium Rate Service Abuse

Normally offered as services for voice and text applications billed to a subscriber's prepaid or postpaid cellular account, premium rate services include one-time and recurring pay-per-call horoscopes, disaster-relief charitable donations, gaming credits, advice and chat services, monthly SMS love advice, and a wide range of other schemes.

Premium Rate Business Model:

The desire to create a widespread, developer-friendly application ecosystem has led to complex and lengthy billing environments with various revenue sharing models such as the typical US$9.99/month SMS premium service subscription payment path, that are criminally-exploitable (depicted below).



In this example, a mobile network operator allows independent "SMS Aggregators" to obtain routing of a block of "short codes" (typically 4-7 digit phone numbers routable within some part of the global phone network). The SMS Aggregator then sells two-way SMS mobile connectivity to a horoscope application owner known as a content provider. The content provider pays a per-subscription commission to an advertising affiliate. Adjacent parties may be only loosely related.

The parties and relationships become progressively more problematic towards the right side of this diagram. In a number of cases, content providers permit poorly-authenticated Internet-only relationships with advertising affiliates to facilitate plausible deniability of their own or affiliates' spamming and/or fraud. Nearly anonymous payment mechanisms such as transfers to foreign banks, unregulated Internet virtual cash or online payment mechanisms lower barriers and enable spam to facilitate fraud.

Premium Rate Malware

Phonepay Plus, the UK premium rate services regulator, issued fines of £330,000 in December 2014 to three different companies after discovering they were using mobile malware to generate charges to Android phone owners. The malware was contained in apps that downloaded automatically without users' consent when they visited specific adult websites. Once installed consumers could inadvertently initiate a subscription by clicking anywhere on the screen. The app would then send hidden premium rate text messages so that the owner would not see a record of these messages in their phone log.

Premium Rate Service scams have been occurring for many years, but the increased penetration of mobile services, the evolution of mobile data, and the establishment of a global cybercrime ecosystem have led to increases in the number and variety of

attacks. Fraud can occur at nearly any step of the service or payment processes, from tricking the user into inadvertently using or subscribing to a service, an affiliate falsely claiming subscriptions, to mobile malware that surreptitiously sends messages to Premium Rate Services without the knowledge of the subscriber.

A common exploit involves a fraudster establishing a Premium Rate Service number, and placing a "1-ring" voice call or sending a text message to a victim, hoping to lure them to respond. This leads the caller to pay-per-call service without their knowledge or consent. Unauthorized subscription, "cramming" to Premium Rate "love advice" or other text message services by affiliates and/or content providers have also been commonplace.

This has caused many SMS Aggregators to implement secondary verification, typically involving a confirmation message or PIN exchange between the SMS subscriber and SMS Aggregator. But even these have been exploited; for example, the GGTracker Android malware sends an SMS subscription and confirmation messages without the subscribers' knowledge.[55]

Spoofing the subscriber's identity, via unauthorized access to signaling networks or cryptographic exploits, is yet another method for committing Premium Rate fraud.

Best Practices for Industry and Government to protect against Premium Rate Scams:

Premium Rate fraud is similar to many other kinds of cybercrime, and is therefore appropriately addressed by a number of common techniques including self-protection, consumer education, and consumer protection and anti-malware measures.

Many mobile carriers have established a reporting service to allow subscribers to report SMS spam by forwarding messages to a short code (e.g., 7726 which spells "spam"). Many governments and enforcement agencies responsible for SMS spam in some countries have established their own numbers for reporting such as 1909 in India, 33700 in France and 0429 999 888 in Australia.

Specific measures to protect against Premium Rate Scams include early defense, partner actions, and additional confirmation.

1. **Complaints to TSPs or Regulators**: Encourage the filing of consumer complaints. These complaints allow TSPs to identify the source of threats and implement defense mechanisms that enable early detection, before any money has been transferred. By including and enforcing anti-abuse clauses in their terms and conditions, TSPs and premium rate service platforms can stop payments to criminals before they occur. The TSP is warned at an early stage through complaints and enforces its terms and conditions, undermining the criminal's business case. Similarly, complaints to regulators and enforcement authorities provide rich intelligence that can lead to law enforcement against scammers.

2. **Partner Actions Regarding Relationships and Payments**: Fraud depends on extracting monies to a hidden and/or unrecoverable location. Parties may protect themselves by requiring full identification, qualification and authentication of other parties, by using reputable payment mechanisms or by delaying payment for a sufficient period.

3. **Additional Confirmations**: As many of the exploits involve cramming or falsified communication between adjacent parties in the payment chain, notifications and confirmations between more reputable parties can prevent or quickly identify fraud. Examples of this include an SMS Aggregator or Mobile Network operator confirming subscription with the subscriber rather than relying solely on assertions from the downstream side of the payment flow.

Mobile Spam

The following scenario describes recent international spamming activity and demonstrates the critical role for international collaboration, particularly inter-carrier collaboration, as vital to anti-abuse defense of networks and subscribers.

Carrier A and Carrier B are in different countries; both countries have many speakers of the same language. Spam originating in Carrier A's network accounts for the majority of spam entering

Carrier B's network. Carrier A tracks spam in its network through shortcode-based spam reporting and analysis of messaging server logs. Carrier B also has shortcode-based spam reporting, but does not collect the originating numbers of messages that are reported as spam. Carrier B does, however, perform automated anti-spam scanning on messaging traffic. As a result, Carrier B's network gathers information about sources and content of spam.

Carrier A and Carrier B learned separately of the spam originating in Carrier A's network and being received by Carrier B. Carrier A shuts down spammers that it identifies on its network, but only if it has received a certain volume of spam reports against a given originating number. Thus, as long as a spammer in Carrier A's network sends only to numbers outside of Carrier A's network, he can send limitless spam to Carrier B's subscribers, because:

a) Carrier A will never receive spam reports from his own subscribers, his requirement for triggering a shutdown; and

b) There are no information sharing practices to thwart international spammers.

In the absence of data sharing among operators, spammers may operate quite freely within a given country if they take care to send their spam only to subscribers of operators other than the network on which they have their accounts.

Data from the case described above show that Carrier A received zero spam complaints for more than 85 percent of the numbers sending spam from his network to Carrier B. Carrier A's own subscribers only sent spam complaints against approximately 5 percent of the numbers sending spam from Carrier A to Carrier B.

Best Practices for Industry and Government to protect against mobile spam:

Dialogue and data-sharing: Spammers exploit vulnerabilities among service providers in anti-abuse policies, defences and knowledge. One of the central lessons learned from the proliferation of Internet e-mail spam from its infancy in 1993 to the present, when spam now accounts for approximately 90 percent of all Internet e-mail traffic, is that when ecosystem participants share information, it changes the game for spammers. Inter-carrier dialogue and data-sharing involving third-party enablers such as technology developers and industry bodies is vital to protecting the mobile ecosystem from spam and spammers migrating tools and techniques honed on the Internet over a decade or more to the open, increasingly IP-based and already globally interconnected mobile world.

While the following data points are not critical for collaboration among service providers, they are helpful to thwart spammers, and can be captured through spam reporting:

Data Elements	Notes
Mobile number of Spam originator	MSISDN (the unique number associated with a subscriber's handset) or IMSI (the unique number of a SIM card)
Number of Spam reports received	Requires collection and correlation of reports
Number of unique Spam reporters	Useful but not critical
Network of Spam originator	Derived by lookup

Note that none of the data elements identified above give personally identifiable information on the spam reporter. Information is only collected on the number being reported as originating spam.

As in the example of Carrier A and Carrier B above, data sharing of the elements above helps combat spam within a given country just as much as it does across country borders.

There are benefits and risks to the international inter-carrier sharing of select data from spam reporting. Benefits include enabling remediation of voluntary subscriber complaints. Data-sharing and anti-spam dialogue among operators also facilitates their efforts to monitor, refine, and enforce their own Acceptable Use Policies. Finally, data-sharing can provide corroborating evidence for operator shutdown decisions, as well as for law enforcement, and regulatory actors. International, inter-carrier collaboration toward these goals will make it more difficult for mobile spammers to hide.

On the other hand, legal, privacy, and security concerns need to be studied when implementing any international collaboration in this space. Currently, these concerns act as an impediment to collaboration across borders. Some have noted, however, that these privacy concerns are unwarranted because 1) spam reports are voluntarily submitted by subscribers, 2) it is not necessary to include any personally identifiable information (PII) when sharing complaint data, and 3) it is not critical to include message content in the sharing of complaint data. (Sharing message content may increase the risk of accidental sharing of PII of reporters or persons other than the spammer. However, the content of messages reported as spam can also be helpful in identifying and blocking spam.)

In summary, inter-carrier, international sharing of certain data elements changes the game for spammers as it leaves them fewer places to hide. Data sharing will require dialogue and consensus on the data to be shared as well as formats for data exchange among ecosystem participants.

Industry should also endeavor to inform law enforcement personnel when they become aware of unlawful conduct on their networks and systems. Coordinating with law enforcement, on both the criminal and regulatory side, can often get to the source of the threat, and further discourages others from engaging in such conduct.

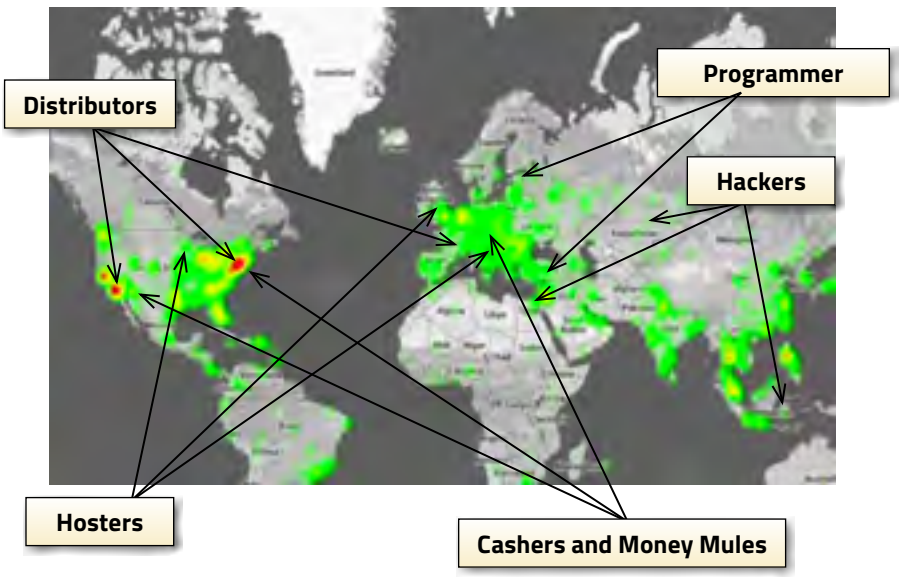
Growth of Cross-border Exploits

As nations address internal attacks and threats, attackers turn their attention elsewhere to identify and exploit international vulnerabilities. For example, the North American "free iPad/iPhone" spam campaign originally targeted the United States. Canadian and US carriers implemented technical defences to block spam sent to their subscribers. The attackers quickly identified this and began sending SMS spam to Canadian subscribers from US-based phones, thereby evading defences. Similar cases exist in fraud, phishing, malware and spyware. In most cases (e.g., spam and malware defence), it has been found that stopping abuse at the source is necessary, as receiving nations may not be able to identify abuse hidden inside high-volume communications streams. Like the Internet, mobile communications networks are global, and require an international defence approach and international collaboration.

International Considerations

Cybercriminals have a strong preference for operating in a transnational environment. For example, an illegal online pill seller living in the US might send spam advertising those drugs from a compromised computer in Brazil, pointing potential purchasers at a website with a Russian domain name (while physically hosting that website in France). Credit card payments for orders might be processed through a bank in Azerbaijan, with orders being drop shipped from a site in India, and proceeds funneled to a bank in Cyprus. Criminals know that by operating in this manner, many factors complicate any official investigation into their online crimes, and reduce their likelihood of being caught. These factors include a lack of cooperation, regulatory differences from one jurisdiction to another, and the cost of international investigations.

Victims
(colored by concentration)



Jurisdiction and International Cooperation

Law enforcement officers do not have unlimited powers. In particular, a law enforcement officer from one city or country will normally not have jurisdiction to subpoena documents or arrest a criminal beyond their own jurisdiction. Cross-border investigations require international cooperation between the domestic and international police agencies, a process that may involve dauntingly complex formal processes, not to mention the time and resources required. The complications associated with these processes may delay investigations, or render some investigations impossible.

Statutory Coverage and Common Law Precedent

An activity that's illegal in one jurisdiction may not be illegal elsewhere. For example, some countries have no laws regarding e-mail spam, nor have they criminalized the dissemination of malware. In other jurisdictions, the legal system may not be able to keep up with a steady stream of new, chemically different but equivalent, drugs. In other cases, a law may be on the books, but the country may have no history of successfully prosecuting those who've violated that statute. Each of these conditions are challenges to law enforcement and collaboration.

Example: Indian Call Center Swindle

Up to 60,000 people in the UK recently became the victims of a £ multi-million Indian call centre and internet loan scam. Investigators believe the sheer number of people victimized by the loans scam makes it one of the biggest frauds ever carried out in the UK. At its height, more than 1,000 people a day who had legitimately sought unsecured loans with banks and finance companies were being 'cold called' from call centres in New Delhi – with approximately 100 per day being duped into signing-up and paying a 'processing fee' to secure non-existent cash. According to Indian police at least £10million was stolen.

Cost of International Investigations

Everything about operating internationally costs law enforcement more than working strictly local cases. If an investigator needs to travel to a foreign country, airfare and other travel costs may be substantial. Cash-strapped agencies may thus simply not be able to afford to work cases with international aspects.

Ironically, at the same time that it is expensive for a law enforcement officer to work a crime that has international aspects, cyber criminals are often able to purchase illegal goods or services abroad via the Internet at bargain prices. For example, a talented malware author from an economically depressed nation might be willing to write malware that will cause millions of dollars in damages for just a few hundred dollars. These conditions give cyber criminals a substantial incentive to work cross-border, and many in fact do.

Best Practices for Industry and Government regarding Cross-Particular Issues:

1. **Collaboration**: The heart of effective international defence is collaboration. First, government and non-government parties in the affected nations must become aware of the issue. Next, collaboration is needed to devise and implement defence strategies and frameworks that involve technical, policy, law enforcement and legal entities in multiple countries. Major challenges in achieving the needed collaboration include identifying the right set of forums and obtaining appropriate attendance.

2. **Threat/Abuse Data Exchange**: The exchange of threat and abuse information is essential to combat cross-border challenges. While human-to-human communications are needed, the breadth and scale of abuse (e.g., the billions of daily spam and phishing messages) dictate the need for mechanized approaches. Here again, for a mechanized international framework to be successfully implemented, it must consider the obstacles to widespread implementation and adoption, including fragmentation among many disparate systems; differing functional needs of different nations (including legal impediments and technical/ technological issues); and differing needs of different carriers.

A general framework for abuse information exchange should also support peer-to-peer and centralized server models and identify both format and transfer protocols.

3. **Training**: In order to recognize and respond to mobile threats, professionals and law enforcement need to stay current with emerging trends and threats.

Voice Telephony Threats

The Voice Telephony Environment

Consumers have many choices with regard to voice telephone calls: wireline, wireless, alternative sources (e.g., computer). These calls can traverse the Public Switched Telephone Network (PSTN) via Time Division Multiplexing (TDM), Voice over Internet Protocol (VoIP), or a combination of both TDM and VoIP. Internet telephony refers to the integration of telephone services into computer networks. In essence, the process converts analog voice signals that were traditionally sent via landline into digital signals. These signals are transmitted via the Internet and then converted back into analog voice signals.

The number of worldwide fixed-telephone subscriptions peaked in 2006 and has declined annually since. For example, fixed-telephone subscriptions were just under 1.11 billion subscriptions in 2014, down from over 1.14 billion in 2013. Simultaneously, the number of mobile-cellular subscriptions is increasing worldwide, and is quickly approaching the number of people on earth. Mobile cellular subscriptions reached almost 7 billion by the end of 2014, corresponding to a penetration rate of 96 percent, but growth rates were at their lowest-ever level (of 2.6 percent globally), indicating that the market is quickly approaching saturation levels.

Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions and is most commonly found in VoIP or internet telephony applications.

Time Division Multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line.

By the end 2014, the number of mobile-broadband subscriptions reached 2.3 billion globally, almost 5 times as many as just six years earlier (in 2008). Mobile-broadband subscriptions were 2.1 billion in 2013.

Fixed-broadband penetration continues to grow, albeit slowly (at 4.4 percent globally in 2014). As services are becoming more affordable, fixed-broadband uptake has shown strong growth and by 2013, there were almost 700 million fixed-broadband subscriptions, corresponding to a global penetration rate of 9.8 percent. The number of Internet users globally has reached almost 3 billion by year end 2014, up from 2.7 billion people in 2013.[56]

With the widespread growth of Internet telephony, it is vital that the infrastructure supporting this technology remain secure and available. A small amount of "downtime" has the potential to cost businesses millions of dollars in lost revenues and customer support issues.

VoIP Threats

This section provides a simple Voice Telephony threat taxonomy, covering the issues that affect voice and Unified Communications (UC) systems and best practices for preventing and remedying these threats. This section is focused on voice, but the threats may affect other forms of communication, including video and messaging. These threats are mostly applicable to enterprises, but can also affect service providers, small businesses, and consumers.

One-ring scams:

Wireless consumers receive robocalls from phone numbers with area codes that spoof domestic numbers, but are actually associated with international pay-per-call phone numbers. These robocalls usually disconnect after one ring, not giving the consumer time to answer the call and tempting them to return the call. Customers who return these calls drive extra traffic to these foreign carriers, and the scammer may receive a portion of the terminating charges (or possibly premium charges) that the foreign service provider collects from the wireless customer's carrier.

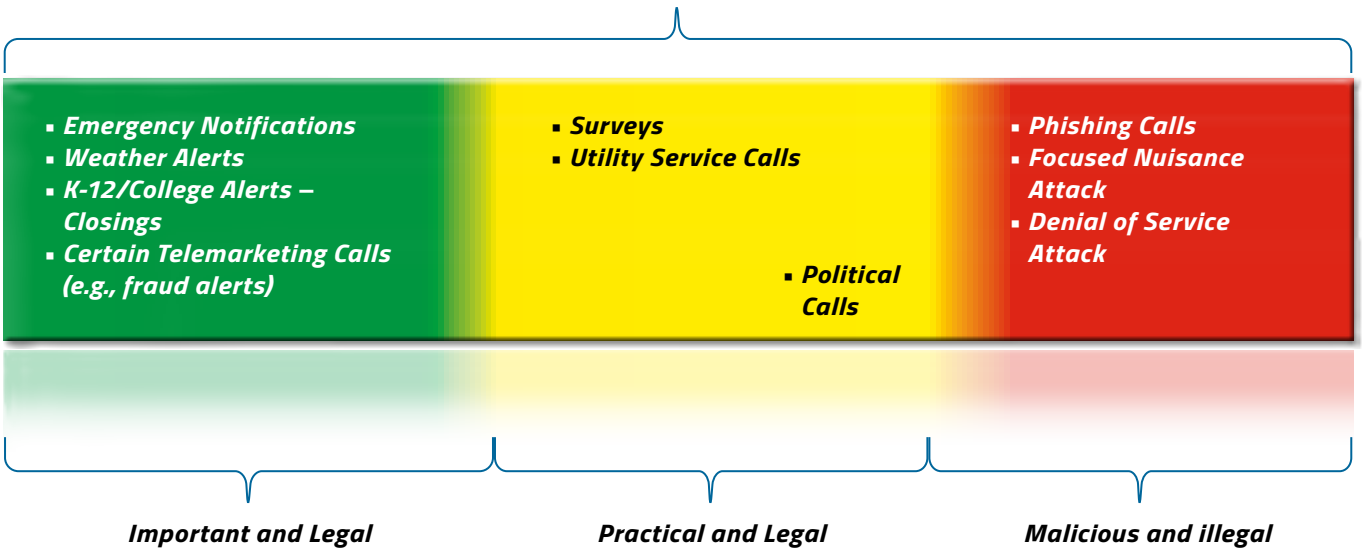
Robocalls

Robocalling, using automatic dialing systems to place voice calls, is an increasingly problematic form of voice service abuse. It is typically used for calls related to sales, marketing, or polls. For example, when an opinion or some other type of poll is being conducted the pre-recorded message may ask the answering person to press a digit corresponding to the pre-set response of their choice. Another common use is for emergency notifications, announcements, or reminders. This is frequently used by Public Safety officials via a system called an Emergency Notification System (ENS). Robocalling, however, is also commonly used to scam consumers or for other illegal purposes.

In the US, for example, Robocalls particularly affect landline customers, who are often targeted by unscrupulous telemarketers and fraudsters[57]. Robocalls were the FTC's top consumer fraud complaint in 2014. Recently, carriers have begun to field a growing number of complaints from wireless customers as well. For example, the "one-ring" scam was recently aimed at inducing wireless customers to inadvertently dial international pay-per-call numbers[58]. Phishing calls specifically aimed at gaining access to private personal and financial information, often referred to as vishing, are also common.

Robocalls are also frequently used to overwhelm both wireline and wireless customers in Telephony Denial of Service (TDoS) attacks by creating mass calling events that prevent legitimate calls from being completed.

The Full Spectrum of Mass-Calling Events



Best Practices to Combat Robocalls:

Carriers or third party vendors may offer tools and solutions to combat Robocalls. No one solution exists, however, to eliminate all unwanted or illegal Robocalls.

Honeypots: A honeypot is a trap set to detect, deflect, or counteract attempts at the unauthorized use of a network or system. Generally, honeypots mimic a computer, data, or a network site, but they are actually isolated, protected, and monitored. They are built specifically to bait attackers. Once baited, bad-actors can be tracked and monitored.

Data Collection and Analytics: Information is a powerful tool in preventing robocalls. By collecting information about normal traffic flows in a particular network and combining this data with analytics to identify suspicious calling patterns based on call volumes, call routing, call destinations, and call durations and completion rates, providers can identify and investigate suspect call patterns to identify illegal robocalls. They can use this information to establish Blacklists to block calls from certain numbers, or Whitelists, which define the calls that can be received. Once a robocall pattern is identified, network operators and enforcement agencies can use traceback techniques to identify and pursue the responsible parties.

Customer Premises Equipment (CPE): Tools are available from both carriers and third-party vendors to manage the calls that ring on phones. Common types of equipment include:

- ***Caller ID:*** Caller ID displays the number that is calling. Customers can use this well-known technology to filter calls from unknown sources. Call blocking services and devices rely on the Caller ID information transmitted with incoming calls to block calls from numbers on a blacklist.
- ***CAPTCHA***[59] ***devices:*** pass certain calls through menus designed to weed out non-human callers.[60]
- ***Apps:*** wireless customers can download a variety of apps that use the Caller ID functionality to reject or screen calls from telephone numbers that the apps identify as suspicious based on various techniques such as crowd-sourcing algorithms or blacklists.[61] Users can also take advantage of their smartphones' built-in features which permit them to manage which calls will ring on their phones and which will not.
- ***Public/Private Key Identification:*** this system is being developed to authenticate the caller or network address associated with the call originator.

Regulatory regimes: Many marketers have used telephony to advance marketing campaigns. Most Do Not Call regimes prohibit robocalls unless the consumer has consented to receiving such calls from the calling entity. Moreover, consumer annoyance with unwanted solicitations led many nations to regulate all commercial calls, with some jurisdictions operating opt-in 'do not call' regimes (for example Germany, Austria and Israel) and many operating some form of opt-out 'do not call' regime (some voluntary; some compulsory). In countries such as Australia, the USA, and Canada, national do not call registries are complemented by additional laws for telemarketers commonly including rules about calling times, caller identification (CLI) and obligatory disclosures.

Penalties can be significant and, along with the high risk of reputational damage, have been instrumental in ensuring that good corporate citizens have policies and procedures to ensure their compliance.

The International Do Not Call Network, part of the London Action Plan, established an annual forum and periodic conference calls for the discussion of common and emerging issues in managing unsolicited telemarketing calls globally and opportunities for collaborative law enforcement.

Industry Standards: Service providers, industry standards bodies, and enforcement agencies have been working cooperatively and independently to mitigate these types of illegal calls. Service providers and private entities are developing or currently have services and features available to consumers to address illegal Robocalls[62] and should continue to develop and implement these standards.

Service providers should also consider improving the front line business office or other inbound call centers, online access for customers, as well as repair and technical support inbound centers, and should educate their personnel on the features of Caller ID, the legitimate uses of Call Spoofing, and current known malicious spoofs.

Some providers may consider establishing specific Annoyance Call Bureaus or security teams to address issues such as these. Customers who continue to have concerns after their contact with front line personnel or online resources can be referred to that group for additional assistance depending on the providers' specific processes. Customers may be asked to share relevant information such as the dates and times they have received spoofed calls, and other appropriate specifics for the investigation of the calls. Annoyance Call Bureaus or security teams can provide valuable efforts to address these concerns, such as:

- Provisioning and monitoring call tracing equipment on customers' telephone services,
- Tracking, translating, and identifying call sources through central office switching locations and network monitoring and analysis systems,
- Utilizing billing, address and facilities systems to identify call sources where possible,
- Working directly with long distance, local exchange carriers, wireless and various other communication providers and annoyance call bureau departments,
- Working with Law Enforcement on releasing identified party information, and
- Contacting identified parties on behalf of customers where appropriate to resolve problems ranging from life threatening or harassing calls to computer generated and auto-dialed calls, spoofing, blast faxes and any other annoyance call types identified by customers.

Law Enforcement: While regulatory compliance regimes can address unwanted calls from legitimate businesses, they are not an adequate deterrence to those who seek to deceive the public. For those actors, strong law enforcement is often the only means to address these abuses. Some nations have taken an aggressive stance against the use of telephony, either through VoIP or other means, to mislead consumers. Prosecution of cases under consumer protection laws in both civil and criminal proceedings has resulted in substantive penalties as well as prison terms. To fully address the problem of telemarketing fraud, it is essential that law enforcement, industry, and regulators continue to track down and prosecute scammers whose use of caller ID spoofing and automated calls have resulted in hundreds of millions of dollars in fraud worldwide.

Telephony Denial of Service (TDoS) Attacks

TDoS is an attack aimed at disabling the telephone system of a corporation or public service. By saturating a phone number from the outside, or even the totality of the entity's communication channels, attackers can quickly disable all incoming and outgoing calls. TDoS attacks are very similar to dedicated denial of service attacks (DDoS) on websites. The attackers benefit by holding the phone system hostage and disrupting the system until the victim pays a specified sum.

To initiate a TDoS attack, the attacker must have access to several communication channels or several Session Initiation Protocol (SIP) accounts (usually hacked). They then use automated calling machines to simultaneously and repeatedly call one or several of the victim's phone numbers. "Tools" or "kits" for TDoS attacks are readily available on the Internet. It is also very easy to commission such an attack from unscrupulous persons. This is type of attack is normally done for disruption, extortion, or to cover up fraud.

TDoS Best Practices:

Application Layer Gateways: It is important that companies of all sizes secure their VoIP and telephony systems. VoIP systems are like any other computer network system, and thus require protection from the same classes of cyber-attacks as any other network server. While legacy firewalls may have trouble properly handling the unique requirements of VoIP systems, many modern security appliances have application layer gateways (ALG) designed specifically to handle VoIP-specific protocols. Some of these ALGs can even provide VoIP-specific security functionality, such as preventing SIP directory harvesting, or network level DoS attacks.

Protecting Essential Services

The Canadian Interconnection Steering Committee (CISC) explored the issue of Telephony Denial of Service attacks within the Emergency Services and Network working groups and has suggested best practices for protecting essential systems.

http://www.crtc.gc.ca/public/cisc/nt/NTCO0570.docx

Reporting to Law Enforcement: TDoS attacks have the potential to disable key critical infrastructure including emergency services, hospitals and first responders. This can raise issues of national security, and should therefore be referred to the appropriate law enforcement agency as soon as an attack is detected.

Call Spoofing

Calling-number spoofing is a method of falsifying the originating caller information. While this is not an attack *per se*, it is commonly used to mask the identity of an attacker or to make attacks more effective. Through such spoofing, fraudsters target consumers with calls that appear to originate from the consumer's area, calling code, or a trusted source. Some callers have used numbers associated with government agencies and have impersonated government officials in tax and immigration scams. Often the source of these calls is from a continent away, adding more complexity to tracking and stopping the frauds.

Selective Call Blocking/ Reporting (*09)

Vertical service codes, such as *09, should be defined by industry to allow consumers to easily initiate the automatic capture and analysis of network information related to unwanted calls. This system works by enabling a consumer who receives a telemarketing, fraudulent or other type of unwanted call, to hang up the phone and press *09 to report the complete information of the call to their carrier, law enforcement and regulators, and also automatically block future calls from that number.[63]

Call Spoofing Prevention Best Practices:

Fraud legislation: It should generally be universally illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value.[64]

In the US, for example, the Truth in Caller ID Act of 2010 prohibits spoofing, or deliberately falsifying the telephone number or name relayed as the Caller ID information to disguise the identity of the caller *for harmful or fraudulent purposes*.[65] This type of definition allows the use of spoofing for non-deceptive purposes, such as use of a physician's office number when she calls from her private line.

Consumer Education: Consumer trust in the telephone system is at risk, with the increase of Caller ID Spoofing and automated calls. To protect consumers from frauds and other harms that rely on misuse of the telephone platform, government agencies have launched education campaigns. For example, the US Federal Trade Commission (FTC) has posted warnings on its websites, published blog posts and promoted their law enforcement efforts to raise consumer awareness about robocalls and caller ID spoofing.[66] Encouraging greater consumer awareness of the use of spoofing may help reduce the resulting harm that can result from the frauds that are promoted through this technique. Consumer education efforts should also raise awareness of the various tools that consumers can use to protect themselves from unwanted calls.

Hosting and Cloud Services

Cloud services and hosting represent one of the most significant recent shifts in information technology. Corporations are excited by the opportunity to better control capital costs, increase agility and divest themselves of complex information technology infrastructure. Concerns over security and loss of direct control are, however, stifling adoption and growth of this new technology.

Online and mobile threats are on the rise for hosting and cloud services. According to a recent article in The Economist, the global market for cloud-computing services is expected to reach US$176 billion in 2015. This amount still represents a small portion of total IT spending, but spending on hosting and cloud services is growing fast. Currently, most other parts of the industry are stagnant or even declining but by 2017 cloud spending is expected to reach a total of US$240 billion annually.[67]

This section categorizes types of hosting, and outlines areas of concern. It provides a look at the current threat landscape in the online hosted and cloud environment, and a brief look at the remediation methods being used to address those critical issues.

Types of Hosting

Hosting providers facilitate the operation of the global Internet and operate the nuts and bolts that make the Internet work. Hosting providers range in size from sole proprietorships to global Internet businesses known worldwide. What differentiates Internet infrastructure providers from other aspects of the Internet is their relative anonymity. These businesses generally operate behind the scenes facilitating use of the Internet for business as diverse as a local dry cleaner or a global bank.

Internet Infrastructure Forms

The Internet infrastructure services market is best understood in terms of the underlying forms used by the service provider to deliver services to the end user. There are three components to this these underlying forms:

- **Facility:** The facility, commonly referred to as a data center, is the basic physical building block of an Internet infrastructure provider. It may be owned by the infrastructure provider or operated by a third party. This facility houses the routers and switches that connect to the Internet along with the servers - physical and virtual - that host content, data and applications.
- **Physical server:** The physical server lives in a cabinet or rack housed in a data center. It is where content and applications are stored and secured.
- **Virtual server:** The virtual server is a virtualized partition of a physical server. The virtual server acts and performs just like a physical server with a marginal difference in performance. A single server can literally house up to dozens of virtual servers.

Hosting providers can generally be placed in one of five main categories:

i. Shared Hosting
ii. Standard Managed Hosting
iii. Complex Managed Hosting
iv. Cloud Infrastructure
v. Colocation

Internet Infrastructure Categories

Shared Hosting: Shared hosting is shared space on a physical server with no isolation between users and the absence of defined resource allocation. The finite resources of a physical

server are shared - often unevenly - among all the customers that reside on it. Providers can literally host hundreds of customers on a single server.

Shared hosting is commonly used to publish static or dynamic website content. Blogging platforms like WordPress and simple e-commerce applications often run in shared hosting environments and are enabled with automated installation.

Organizations with very limited resources use shared hosting to communicate and build a presence on the Internet. Shared hosting typically exists at the lower end of the infrastructure market. Typical users are: consumers, small businesses, home offices, and bloggers.

Standard Managed Hosting: An infrastructure provider who provides standard managed hosting typically leases dedicated physical servers (sometimes referred to as bare metal servers) or virtual servers housed in the infrastructure provider's data center facilities. Customers typically lease the server resources on a fixed contractual basis.

In standard managed hosting, customers have root access to the server and typically self-manage. The infrastructure provider provides a basic level of support and handles certain but limited management tasks such as hardware maintenance, backups and installation of operating system and web server software.

The actual server is owned by the provider and leased to the customer. As a result, the customer does not face an IT refresh cycle. They can simply move to another server that fits their requirements. They do not usually pay for hardware refreshes or have any obligation to stay on the server they have leased.

Standard managed hosting is designed to accommodate relatively straightforward configurations and workloads. Small businesses generally use standard managed hosting as an alternative to buying and installing IT assets.

Complex Managed Hosting: Complex managed hosting also applies to both physical dedicated servers and virtual servers. There are many similarities between standard and complex managed hosting, but the key difference is the level of administrative and engineering support that the customer pays for. These differences are due to both the increased size and complexity of the infrastructure deployment. The infrastructure provider steps in to take over most of the management.

Complex managed hosting involves a wide range of expertise and capabilities in the areas of systems administration, database management, security, monitoring, log management, disaster recovery, and backup. The management services can even extend to the application layer, though this tends to be rare outside the most standard enterprise applications. A typical managed hosting deployment will have a number of additional devices, including databases, application and web servers, firewalls, and load balancers. Instead of local storage, customers often use network-attached or storage area networks. They will also purchase backup and replication services or set up disaster recovery scenarios. Some infrastructure providers augment their standard offerings by providing consulting services that go above and beyond the standard managed services layer.

When it comes to complex managed hosting, the hosting relationship tends to be limited to a small number of applications versus the total that actually exist within the enterprise. Complex managed hosting is in many ways used as an extension to the on-premises data center.

Complex managed hosting is used for large and complex configurations and workloads. It is also an option when organizations need very specific and specialized capabilities such as security and compliance. Managed hosting is an alternative to buying and installing IT assets and has a cost savings component. It is a way to relieve the burden on internal IT staff and free up resources.

Cloud Infrastructure: Cloud infrastructure is basically a more flexible and scalable form of virtual server hosting. The key feature of cloud infrastructure is resource availability. The size of a server can be scaled up and down either on the fly or within a very short time frame. So instead of a set amount of resources, the end user can adjust infrastructure capacity according to demand (or lack thereof). Typically, cloud is consumed by the hour, but is now even beginning to be billed in minute-by-minute increments, thereby enabling utility-based consumption.

Cloud is also highly resilient with no single point of failure. Cloud resources are mobile and can automatically fail over to another physical host. They can be restarted anywhere at any time with the right toolset and capabilities. This flexibility enables cloud to be integrated in hybrid environments in any data center, whether outsourced or on-premises.

Colocation: Colocation is the supply of data center capacity for organizations that need a place offsite to house or "colocate" servers, storage, and networking gear they own and manage. The basic building blocks of colocation are space, power, cooling and Internet connectivity. In the colocation model, the customer has access to a designated area within a facility where they install gear they own or have rented. Many colocation providers offer remote management and monitoring services. Some providers lease equipment to customers.

The reality of the Internet infrastructure industry can become more complex, as infrastructure service segments continue to blur. For example, the line between standard managed hosting and complex managed hosting is increasingly unclear as providers move up-market and expand into value-added services. The same can be said for the line between managed hosting - of the virtual server variety - and cloud infrastructure. A number of virtual server hosting offerings look like cloud infrastructure. They might not have all the characteristics of cloud, but display enough to blur the line and create some grey areas.

The Threat Landscape

Below is a list of the types of abuse most commonly seen at hosting and cloud service providers. The list does not purport to be complete and will invariably change over time.

- **Spam (outbound)**: Spam is any unwanted or unsolicited commercial electronic e-mail. Providers should ensure that end users are following the M³AAWG Sender Best Current Practices.[68] Hosting providers will also want to subscribe to as many relevant Feedback Loop reports as it is possible to process.
- **Spamvertising (hosted redirect and payloads)**: Spamvertising occurs when a hosting provider's end user engages a third party to advertise its Web presence. Most spam complaints are caused by end users sending e-mails to potential customers that tout some overhyped product or service. Providers who receive one of these complaints are most likely in the loop either as the sender of the e-mail or the host of the site being advertised.
- **Phishing outbound (hosting and inbound for client credentials)**: Phishing happens primarily when an end user's account has been compromised, almost always as a result of outdated scripts run by end users. A phishing site is a fraudulent site purporting to be a legitimate company, like a bank, credit card company, or PayPal which directs the individual to enter confidential information. The phishers then have everything they need to defraud the individual. (See Phishing and Social Engineering section for further information.)
- **Hacked or defaced pages (hosted client-side)**: While phishing complaints will often fall into this category, not all hacked accounts will be used for phishing. Some may simply be defaced and the end users' data corrupted or destroyed. Frequently hackers will also inject malicious code or upload bots that are set to cause additional problems like exploit sites, drive-by downloads or redirectors to other malicious content. Third parties and law enforcement agencies analyze these events and provide information about how to repair hacked sites. Most accounts are compromised due to end users' out-of-date CMS (Content Management System) installations such as Joomla or WordPress.
- **Child sexual abuse material (hosted client-side)**: For appropriate handling of these issues, see the M³AAWG Disposition of Child Sexual Abuse Materials Best Common Practices (https://www.M3AAWG.org/sites/maawg/files/news/M3AAWG_Disposition_CAM-2015-02.pdf).
- **Copyright and trademark/intellectual property issues (hosted client-side)**: For online US copyright law, see http://www.copyright.gov/reports/studies/dmca/dmca_executive.html. Other copyright regimes apply in other jurisdictions.

- **Distributed denial of service and other outbound hostile traffic**: While cloud service or hosting providers may have better protections than smaller individual businesses, these services providers also suffer from a higher risk of DDoS attacks than other online businesses because they, in effect, aggregate the risk of all their customers. An attack on one customer can affect others and potentially the entire hosting operation because of the heavy reliance on shared infrastructure.
- **Malicious signups**: hackers build a botnet using only free trials and "freemium" accounts on online application-hosting services. The hackers then use an automated process to generate unique e-mail addresses and sign up for those free accounts en masse, assembling a cloud-based botnet of thousands of computers.

Major Areas of Concern

Vulnerable/Out-of-Date CRM Installations:

Considering that there are more than 67 million WordPress sites, which represents 23 percent of all websites[69], around the world—and that publishers are using the platform to create blogs, news sites, company sites, magazines, social networks, sports sites, and more—it's not surprising that many online criminals have their sights set on gaining access through this Content Management System (CMS). For example, Drupal, a rapidly growing CMS platform, was targeted in 2014 via third-party software installed on the Drupal.org server infrastructure.

It isn't just the popularity of these systems that makes them desirable targets. Many of the sites on these servers, though active, have been abandoned by their owners. There are likely millions of abandoned blogs and purchased domains sitting idle, and it is probable that many of these sites have been corrupted by cybercriminals. Cisco security experts predict the problem will only worsen as more and more people in emerging Internet markets around the globe establish a blog or a website, only to let it languish later.

The widespread use of plugins, which are designed to extend the functionality of a CMS and to power videos, animations, and games, is also proving to be a boon for cybercriminals looking to gain unauthorized access to the platforms. To exacerbate this problem many plugins are left un-updated by their writers and force those who use and depend on the plugins to not upgrade their current installation at the cost of losing business or functionality on their site. Many CMS compromises observed by Cisco researchers in 2013 can be traced back to plugins written in the PHP web scripting language that were designed poorly and without security in mind.

Statistics gathered by the security company Sucuri show a total of 3143 vulnerabilities in WordPress in 15 different categories.[70] With this mass of vulnerabilities, consumers of WordPress have started keeping their software up to date but over 30 percent of WordPress sites are still using version 3 or lower[71] leaving those sites open to exploitation by malicious parties.

DDoS Attacks:

Because DDoS attacks had long been considered "old news" in terms of cybercrime techniques, many enterprises were confident the security measures they had in place could provide adequate protection. That confidence has recently been shaken by large-scale DDoS attacks in 2012 and 2013, including Operation Ababil, which was directed at several financial institutions and was most likely politically motivated.

Industry leaders warn that DDoS attacks should be a top security concern for organizations in the public and private sector because future campaigns are expected to be even more extensive. Organizations, particularly those that operate or have interests in industries that are already prime targets such as financial services and energy, need to be exceptionally wary. From 2010 to 2013 unplanned outages due to DDoS attacks increased from 2 percent overall to 13 percent.[72] In fact, a comparison of fourth quarters in 2013 and 2014 showed DDoS attacks increase by 90 percent, underscoring that attacks are only increasing.[73] The total average cost of these outages has also increased from US$613,000 to US$822,000 in the same time frame.[74]

Some DDoS attacks have taken a troubling turn. They have been used to divert attention from other nefarious activity, such as wire fraud. These attacks can overwhelm bank personnel, prevent transfer notifications to customers, and prevent customers from reporting fraud. Financial institutions are rarely able to recoup their financial losses. One such attack that took place on December 24, 2012 targeted the website of a regional California financial institution and helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than US$900,000.

Rapidly deepening expertise in compromising hosting servers will only make it easier for cybercriminals to launch DDoS attacks and steal from targeted organizations. By commandeering a portion of the Internet's infrastructure, malicious actors can take advantage of large amounts of bandwidth, positioning themselves to launch any number of powerful campaigns. It's already happening: in August 2013, the Chinese government reported that the largest DDoS attack it had ever faced shut down the Chinese Internet for about four hours.

Even spammers are using DDoS attacks to strike back at organizations they believe are standing in the way of their revenue generation. In March 2013, the non-profit Spamhaus (which tracks spammers and created the Spamhaus Block List, a directory of suspect IP addresses) was the target of a DDoS attack that temporarily shut down its website and slowed Internet traffic worldwide. The attackers were allegedly affiliated with the Netherlands- based CyberBunker, a hosting provider with permissive terms of use, and STOPhaus, which has publicly expressed its dislike for Spamhaus' activities. The DDoS attack came after the widely used Spamhaus service included CyberBunker on its blacklist.

Misconfigured Servers in Unmanaged Environments:

With the advent of the Cloud, users now have the ability to create and setup an entire server environment in a fraction of the time that was required for physical hardware. This has allowed users to be able to easily create their own infrastructure with little or no knowledge of how the systems they are setting up work. While this change has allowed users the ability to do much more than they have before it has opened up a new challenge in preventing and stopping abuse of these systems.

Many of the virtualized and unmanaged servers are not being maintained with the vigilance that has already been established in the managed physical hardware world. Operating Systems and programs are not being updated correctly (or not at all) to address security fixes and vulnerabilities. Permissions are rarely changed or are set to where anyone with access to the server can make changes, leaving a server that has an open door to the outside world susceptible to malicious activity.

Some programs use methods of communication both incoming and outgoing that if not correctly configured leave a server as a weapon to be used in DDoS reflection, SSH login, SQL injection, and other attacks with the ability to bring the targeted systems down for significant amounts of time. Further, these misconfigurations allow malicious parties to access sites or information hosted on the server that result in theft of data, phishing sites, and hosting malware.

Monitoring of these misconfigured and updated systems is a monumental task for the companies hosting these servers therefore little is done to these systems until they have already been compromised.

Best Practices

Prevention:

1) **Vet customers before they cause problems**: Hosting providers are at the mercy of their clients' worst practices. Providers must a vetting process to proactively identify malicious clients before they undertake abusive activities. Making efforts to target clients who will be a good fit for the hosting company is another way to preserve the safety of the hosting environment.

2) **Require customers to keep software updated**: Failure to maintain up-to-date software and hardware or firmware in the environment is one of the primary causes of abuse in the hosting space. Customer agreements should specify that customers will make a best effort to keep their systems updated.

3) **Train customer-facing staff in security awareness**: Customer-facing teams such as support, sales and marketing do not face the majority of daily challenges that are the norm for the abuse or security teams. Training should provide these teams with knowledge of when to tell a customer or prospect that their practices do not abide by the terms and Acceptable Use Policy of the system they are on, or where they are trying to provision an environment.

4) **Prevent abuse at the network edge**:

   a) Consider hardware-based intrusion detection systems (IDS).

   b) Use software-based security scans and firewalls.

   c) Promote the use of Web application firewalls.

   d) Use tiered-rights allocation for valued customers.

   e) Contract with customers to protect security.

   f) Maximize customer contact and protect customer identity.

   g) Encourage the use of strong customer passwords.

   h) Use best practices on IPv6 networks: IPv6 provides so many addresses that there is no need—and no reason—to share a single IP address among multiple customers. The best practice is to assign each customer a separate /64 of IPV6 address space. Even on the smallest physically shared systems, each customer and each website should have a unique address. This makes it easier to track the source of abuse, makes it possible for recipients of abuse to block the offending customer without blocking everyone else on the same host, and may make it easier to suspend and renew service when required.

   i) Hosting providers must maintain strong internal security practices and systems. All the recommended measures above are pointless if bad actors can guess the passwords the provider's staff uses. Hosting providers should follow PCI Compliance Standards.

Detection and Identification:

1) **Use confidential client identifiers**: Hosting companies should create a unique identifier for each specific customer. This identifier must be apparent only to the hosting company and be unintelligible to outside parties. This maintains the privacy of the customer's identity yet gives the hosting company a simple, effective way to identify customers.

2) **Establish role accounts for network domains**: RFC-specified role and common practice e-mail accounts must be set up for every domain and client domain provisioned on a network.

3) **Maintain accurate SWIP and IP WHOIS records**: Hosting companies should maintain clear and accurate entries with their Regional Internet Registry (RIR) for IP space allocation, including sub-allocations greater than a /27 to clients. These WHOIS listings should include functional role accounts for abuse reporting.

4) **Set up internal telemetry that reports on the state of the network**: Examples include,

   a) Network self-scans,

   b) Traffic analysis, and

   c) Outbound spam filter monitoring

5) **Make community abuse reporting straightforward**: Hosting providers must provide facilities for members of the public to submit reports about abuse they perceive emanating from the network in question. Providers must then acknowledge the submission of these reports and take action as appropriate. Hosting providers should maintain redundant communication channels to account for failure of any given channel.

   a) E-mail

   b) Telephone

   c) Instant message (chat)

   d) Ticketing systems (See Appendix 4)

   e) Website status reports, and

   f) Social media presence.

6) **Respond promptly to complaints**: Individual submissions should have an auto-acknowledgement (AUTO-ACK) message with enough specificity to be discrete from other submissions the complainant has made. They should include the original complaint, an original ticket number, and any other information that will assure the user that the complaint has been received and is being acted upon.

7) **Consider designating trusted reporters**: Complaint submitters may be determined to be of high quality or high priority. These sources may be both internal and external. Provision should be made for a priority lane-style service while maintaining specified priority levels. For example, a contact at a widely-used DNSBL (Domain Name System Blacklist) may be designated an appropriate priority reporter, although a spam complaint from that source would obviously remain less significant than a DDoS issue happening simultaneously.

8) **Set up Feedback Loops (FBLs) and automated reports**: Consuming FBL Data Signing up for FBLs helps providers avoid DNSBL listings, limits reputation damage, and allows staff to proactively deal with abusive and abused (compromised) clients.

9) **Implement Comparison Metrics**: Establishing systematic metrics for use by hosting providers enables hosting providers and law enforcement to identify abuse and effectively compare data across the industry.[75]

Remediation:

Remediation priorities provide hosting companies and customers with guidelines to resolve issues. Recommendations regarding the priority of complaints must also take into account the severity and seriousness of the abuse and the scope of a given issue. Additionally, the source of the report and the severity of the damage to the reputation of the hosting company and of the customer must be taken into account. A massive spam campaign may be of higher priority than for the presence of a dormant botnet. There must be a case-by-case assessment of issues that may alter the priority level for a given provider or a given customer.

Respond swiftly to high-profile/high-priority issues:

The majority of complaints received by any hosting company only require an acknowledgement of receipt. Some cases, however, such as high profile complaints, takedown requests and blacklist removal, require an additional response. The customer or reporting agency should be contacted initially to communicate that the issue is being addressed. They should be contacted again when the issue is resolved. Only if there are lingering or exceptional issues should multiple communications be necessary.

Communicate proactively when industry or company-wide events occur.

In the event of a serious compromise or vulnerability that could put multiple clients or a specific group of clients at risk, a communication plan should be developed to make them aware of the issue and provide general instructions on how to resolve the issue. If the breach involved access to personally identifiable information, you should know what your obligations are under regional or national requirements, including the scope of your notice to effected persons, and notice to appropriate law enforcement authorities. These communications must be sent in a timely manner. Additionally, the support staff should be made aware of the issue and have proper instructions on resolving the matter with customers who need assistance.

Deal effectively with problem customers:

1) Confirm the validity of the complaint.

2) Notify the customer of a compromise. Include any vetted instructions to the customer that will assist in the resolution of the issue.

3) Provide the customer with the pertinent Terms and Conditions and/or any applicable government regulations that may have been breached and caused the notification of violation or suspension of service. By doing this, the agreement with the customer is intact. Notification of the customer protects the hosting company from potential customer or outside complainant issues that could result in litigation.

4) Grant time to the customer to remediate the issue or, if an agreement is in place, allow time for the provider to remediate the issue themselves.

5) Confirm that the complaint has been resolved.

6) Close the incident. If necessary, notify the reporting party that the issue has been resolved. Suspend service to non-responsive customers.

Online Harassment

Not a day goes by that online and traditional media don't report on some form of online harassment. While it varies between the annoying and actions that are deadly serious, it is clear that as Internet services become increasingly available world-wide, so too will the problem of online harassment rise in frequency. Online harassment can range from embarrassing or cruel online posts or digital pictures, to online threats, bullying, and negative comments, to stalking through e-mails, websites, social networks and text messages.

Every age group is vulnerable to online harassment, which is a growing problem in schools on college campuses and even in the workplace. Online harassment has become an issue because the Internet provides some anonymity which is appealing to aggressors because their intimidation is difficult to trace. Unfortunately, rumors, threats and photos can be disseminated on the Internet very quickly.

There have been attempts of varying viability to regulate[76] and even write law[77,78] to deal with some aspects of the issue, but overall this is an area that is, as yet, both omnipresent, and in need of further examination and best practice development.

The following provides a list of the varying forms of online harassment and is followed by some simple guidance on avoiding harassment.

Catfishing – A fake profile is set up on dating sites and social media to lure a potential victim into an online relationship, then scam them out of their money.

Classifieds (Craigslist) Harassment – Ads are created claiming a person is looking for rough sex or other atypical personal behaviour with responses set up to go to the victim's home telephone number or e-mail address.

Cyberbullying – Basically cyberstalking, but related more to kids and teens being harassed online by other students via web sites, social media sites, message boards, e-mail or smartphone apps and texting.

Cyberstalking – When the online stalker has been asked to stop and continues to repeatedly contact the victim online. This can take many forms – e-mail, web site posts or comments, message boards, cell phone texts, comments and posts via smartphone apps, etc.

Doxing – Finding out personally identifiable information about an individual, then posting the information online, including home address, home phone number, cell number, work address and phone number, relatives' information, etc.[79]

Impersonation – When an online user creates profiles or accounts using another's name, photos and identifying information, then posting as that person. This can be used to discredit the victim, or in some cases as a first step towards fraudulent activities for financial gain. For example, by stealing photos and information from a social media profile, and creating a new one, a miscreant can befriend the victim's friends and relations and contact them with a 'stranded traveller'[80] scheme, wherein the person claims to have travelled somewhere but has lost their wallet. Close friends are more likely to fall for this con, and sending money because they believe the faked profile to be real.

Mobbing – When a group of online users targets one or more individuals and as a "gang" harasses and stalks the victim(s), hoping to drive them off the Internet, be expelled from school, or lose their employment. [81]

Outing – Disclosing the fact (or allegation) that someone is gay, lesbian, trans-gender, or sharing information about fetishes, medical conditions, etc. online without permission.

Online Identity Theft – Stealing personal information and either taking over the identity or selling the information so it can be used to fraudulently obtain credit cards or other financial instruments, like loans or mortgages.

Revenge Reviews – Posting fake or extremely critical reviews to sites such as ripofferport.com. These can also take the form of posting judgemental, personal information about a person on sites like thedirty.com.

Revenge Porn – Posting semi-nude/nude photos or videos on web sites and other forums without the party's consent. As with other online harassment methods, most perpetrators attempt to remain anonymous while engaging in revenge porn by creating free e-mail accounts or fake profiles to post about their victims.

Sexting – Semi-nude/nude photos or videos are shared online via apps such as Snapchat, Instagram, Vine or web sites such as Facebook. While Sexting in and of itself is not online harassment, it can become harassment if photos are sent to unwilling recipients or if the recipient in turn distribute them further afield.

SWATting – Making a fake call to police to invoke an armed response, usually by the SWAT Team[82]. This sometimes takes the form of a faked bomb threat or a false report of an armed hostage-taking.

Trolling – Online users who attempt to incite reaction by posting intentionally tangential or aggressively rude comments. This also sometimes includes hired trolls, for example individuals associated with political campaigns may be paid to incite arguments or post ludicrously extreme viewpoints of their opponents to discredit them.

Best Practices to Limit Online Harassment[83]:

Limit where you post personal information: Be mindful of who can access contact information or details about your interests, habits or employment to reduce exposure to aggressors. This may limit the risk of becoming a victim and may make it easier to identify the aggressor if you are victimized.

Avoid escalating the situation: Responding with hostility is likely to provoke an aggressor. Depending on the circumstances, consider ignoring the issue. Often, cyberbullies and aggressors thrive on the reaction of their victims. If you or your child receives unwanted electronic messages, be they SMS text messages or e-mail, consider changing the electronic address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

Document cyberbullying: Keep a record of any online activity (e-mails, web pages, social media posts, etc.), including relevant dates and times. Keep both an electronic version and a printed copy.

Report cyber bullying to the appropriate authorities: If you or your child are being harassed or threatened, report the activity to the local authorities. Your local police or national police are often good starting points. There is a distinction between free speech and punishable offences. Law enforcement officials and prosecutors can help sort out legal implications. It may also be appropriate to report it to school officials who may have separate policies for dealing with activity that involves students.

Own your online presence: When available, set the privacy and security settings on websites to your comfort level for information sharing. For example, change the settings on your social media sites to limit the visibility of posts to 'friends only'. It's ok to limit how you share information.

Use strong passwords and challenge questions: Do not re-use passwords between sites. If you have trouble remembering passwords, use a password manager such as iPassword (Agilebits) and use two-factor authentication whenever possible on social media and e-mail accounts. If you post personal information like your elementary school and mother's maiden name to social media, use different answers to challenge questions you may be asked at your financial institution, so answers can't be determined easily. Also, rather than using real personal information, consider choosing a nonsensical phrase which you can remember and use that for all such questions (e.g., mother's maiden name: Batman).

Safer for me, more secure for all: What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

Educate your community: There are many resources available that can help discourage cyberbullying. Provided through government authorities.[84]

Conclusion

In recent years, the online and mobile threat environment has changed dramatically, targeting a broader range of individuals, businesses, and networks. The emergence of new technologies allows for more sophisticated attacks to be developed by leveraging vulnerabilities across a broader range of services, channels, and platforms.

Traditional methods to address online threats, with anti-virus software, firewalls, and education campaigns continue to be an important part of the defence. The malware and botnets that emerged in the past few years havetransformed themselves to avoid detection and remediation. To address these new and emerging threats, the international community needs to step further into the Internet ecosystem and collaboratively develop multi-faceted and multi-lateral approaches to combat them.

This report provides best practice recommendations for consumers, industry and governments to address online and mobile threats. These include recommendations for consumers to be more proactive in securing their own devices; for service providers to implement recommended security technologies and practices without delay; for governments to ensure modern regulatory and legislative environments are in place and enforced, and to work with international organizations to champion collaborative efforts.

These recommendations are a set of tools to manage online, mobile and voice threats. However, the threats described in this report are just a snapshot of the threat environment today. As online activities change, the use of mobile computing grows, and Internet users and businesses change their responses and defences to existing threats, these threats will shift and adapt to exploit new vulnerabilities and pursue new targets.

Putting these recommendations into practice will take a concerted multi-lateral approach. To that end, the authors of this report strongly encourage the OECD and other international organizations to join M³AAWG and the LAP and engage with the organizations that govern and administer Internet infrastructures. In addition, in order to stay in front of the changing threat environment, all organizations concerned should begin to more proactively collaborate in monitoring threats and implementing new measures as needed to address them.

Glossary

- **419 Scam:** so-named because of the Nigerian criminal code Chapter 38, section 419 which addresses fraud. "Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years." These are the famous Nigerian prince e-mails or other schemes where it is required to spend money in return for untold riches at the end of the scheme.
- **Advanced Fee Fraud:** e-mails offering prepayment, including an overpayment, for services offered. In the most common form, the overpayment is requested to be sent to a third party. After the third party liquidates this payment, the original payment is found to be counterfeit and retracted from the victim's bank balance.
- **Border Gateway Protocol (BGP):** the protocol which makes core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems.[a]
- **Caches:** store recently-used information in a place where it can be accessed extremely fast. For example, a Web browser uses a cache to store information regarding recently visited websites on your hard drive. Because accessing your computer's hard disk is much faster than accessing the Internet, caching websites can speed up Web browsing significantly.[b]
- **Distributed Denial of Service (DDoS):** a type of cyber-attack aimed at overwhelming or otherwise disrupting the ability of the target system to receive information and interact with any other system. For example, sending either one or a large number of unwanted messages to keep a server or network from working properly.
- **Drive by Downloads:** the unintended download of computer software from the Internet. A user may authorize a download without understanding the consequences, like a counterfeit executable program, or the download can occur entirely without a user's knowledge.[c]
- **E-mail Service Providers (ESPs):** a company that provides e-mail services to other businesses. These services can include collecting and keeping lists of e-mail addresses, sending bulk e-mail to the addresses on the lists, removing addresses that bounce, and dealing with complaints and abuse reports caused by mass e-mailings.
- **Firewall:** a hardware and/or software device on a computer that controls the access between a private network and a public network like the Internet. A firewall is designed to provide protection by stopping unauthorized access to the computer or network.
- **Global System for Mobile Communication (GSM):** a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones.[d]
- **Ingress filtering:** a technique used to make sure that incoming packets are actually from the networks that they claim to be from by blocking packets from fake IP addresses.[e]

- **International Association for Assigned Names and Numbers (ICANN):** coordinates unique identifies including the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions.[f]

- **Money Mule:** a person who transfers stolen money or merchandise from one country to another, either in person, through a courier service, or electronically. Online money mules typically exist as a result of phishing or malware scams[g]

- **Node:** in data communication, a physical network node may either be a data circuit-terminating equipment (DCE) such as a modem, hub, bridge or switch; or a data terminal equipment (DTE) such as a digital telephone handset, a printer or a host computer, for example a router, a workstation or a server.

- **JavaScript:** a scripting language which allows authors to design interactive web pages.

- **Phishing:** an attempt to obtain personal information for identity theft or other sensitive information such as credit card numbers or bank account details for fraud. For example, an e-mail message may appear to be from the receiver's bank asking them to visit a website to confirm account details, but instead directs them to a false website where the personal information is collected.

- **SMShing - phishing via SMS or text message:** a link which leads to a fraudulent website is sent via SMS, or the message directs the recipient to call a telephone number where the social engineering attack will continue.

- **Spoofing:** pretending to be another person or organization to make it appear that an e-mail message or telephone call originated from somewhere other than its actual source.

- **Top Level Domains (TLDs):** TDLs are at the highest level in the hierarchical Domain Name System of the Internet and is the last part of the domain name. For example, in the domain name www.example.com, the top-level domain is .com. Responsibility for management of most top-level domains is delegated to specific organizations by the Internet Corporation for Assigned Names and Numbers (ICANN), which operates the Internet Assigned Numbers Authority (IANA), and is in charge of maintaining the DNS root zone.

- **Typosquatters:** rely on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to an alternative website owned by a cybersquatter. Once in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site through the use of copied or similar logos, website layouts or content.[h]

- **VoIP:** routing of voice conversations over the Internet. This is distinct from a telephone call, which is made from your home or office phone which goes through the Public Switched Telephone Network.

- **Vishing - phishing via Voice over IP:** a call is placed to the recipient, often using a common VoIP ability to set a false caller-id, requesting the caller to visit a website or call a telephone number where the social engineering attack will continue. Several common schemes include "Microsoft Technical Support", overdue tax problems, or "you will be arrested if you fail to pay a fine."

- **Web injections:** a type of security exploit in which the attacker adds code to a Web form input box to gain access to resources or make changes to data. Input boxes are typically for user authentication, however most Web forms have no mechanisms in place to block input other than names and passwords. Unless such precautions are taken, an attacker can use the input boxes to send their own request to the database, which could allow them to download the entire database or interact with it in other illicit ways.[i]

References

- a. http://en.wikipedia.org/wiki/Border_Gateway_Protocol
- b. http://www.techterms.com/definition/cache
- c. http://en.wikipedia.org/wiki/Drive-by_download
- d. http://en.wikipedia.org/wiki/GSM
- e. http://www.expertglossary.com/security/definition/ingress-filtering
- f. http://www.icann.org/en/about/welcome
- g. http://en.wikipedia.org/wiki/Money_mule
- h. http://en.wikipedia.org/wiki/Typosquatters
- i. http://searchsoftwarequality.techtarget.com/definition/SQL-injection

Endnotes

1 DCWG, http://www.dcwg.org/

2 Conficker Working Group, http://www.confickerworkinggroup.org/

3 WinFixer, Wikipedia, http://en.wikipedia.org/wiki/WinFixer

4 Symantec, 2015 Internet Security Threat Report, Volume 20, http://www.symantec.com/security_response/publications/threatreport.jsp

5 McAfee, McAfee Labs 2014 Threats Predictions, http://www.mcafee.com/ca/resources/reports/rp-threats-predictions-2014.pdf

6 Microsoft, Download Center, http://www.microsoft.com/en-us/download/details.aspx?id=44937

7 Secunia, http://secunia.com/vulnerability_scanning/personal/

8 PCMag, "The Best Password Managers for 2015", http://www.pcmag.com/article2/0,2817,2407168,00.asp; PCMag, "You Can't Remember Good Passwords, So You Need a Password Manager", http://securitywatch.pcmag.com/security-software/332153-you-can-t-remember-good-passwords-so-you-need-a-password-manager

9 PCMag, "The Best Free Antivirus for 2015", http://www.pcmag.com/article2/0,2817,2388652,00.asp

10 Internet Engineering Task Force (IETF), "Recommendations for the Remediation of Bots in ISP Networks", http://tools.ietf.org/html/rfc6561

11 Aquilina, James, Eoghan Casey, and Cameron Malin, Malware Forensics: Investigating and Analyzing Malicious Code, Elsevier, Inc., 2008.

12 Safe Code, http://www.safecode.org

13 M³AAWG, "ABCs for ISPs", https://www.m3aawg.org/abcs-for-ISP-code

14 National Security Agency, Security Configuration Guides, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

15 National Vulnerability Database, "National Checklist Program Repository", http://web.nvd.nist.gov/view/ncp/repository

16 Verizon, 2014 Data Breach Investigations Report, http://www.verizonenterprise.com/DBIR/2014/

17 *Ibid.*

18 APWG, "APWG Phishing Attack Trends Reports", https://apwg.org/resources/apwg-reports/

19 APWG, "APWG Global Phishing Survey 1H2014: Trends and Domain Name Use", http://docs.apwg.org/reports/APWG_Global_Phishing_Report_1H_2014.pdf

20 RSA, "2014 Cybercrime Roundup", www.emc.com/collateral/fraud-report/h13929-rsa-fraud-report-jan-2015.pdf

21 Center for Strategic and International Studies, "2014 McAfee Report on the Global Cost of Cybercrime", http://csis.org/event/2014-mcafee-report-global-cost-cybercrime

22 O'Connor, Fred, PCWorld, "Monetising Medical Data is Becoming the Next Revenue Stream for Hackers", March 21, 2015

23 IT Governance, "123 Million Health Care Records Breached so far this Year", March 26, 2015, http://www.itgovernanceusa.com/blog/123-million-health-care-records-breached-so-far-this-year/

24 Sender Policy Framework, "Project Overview", http://www.openspf.org/

25 DKIM.org, http://dkim.org/

26 ICANN, http://www.icann.org/

27 DMARC, http://dmarc.org

28 In most western countries, financial institutions will reimburse consumers for fraud losses that were made through the financial institution.

29 McAfee, "McAfee Labs Report Highlights Success of Phishing Attacks with 80% of Business Users Unable to Detect Scams", September 4, 2014, http://www.mcafee.com/us/about/news/2014/q3/20140904-01.aspx

30 SANS, "Building an Effective Phishing Program", http://www.securingthehuman.org/media/resources/presentations/STH-Presentation-PhishingYourEmployees.pdf

31 Stop. Think. Connect., "Resources", www.stopthinkconnect.org/resources/

32 StaySafeOnline.org, "National Cyber Security Awareness Month", https://www.staysafeonline.org/ncsam/

33 APWG, "How to Redirect a Phishing Site Web Page to the APWG.ORG Phishing Education Page", http://phish-education.apwg.org/r/how_to.html

34 Anti-Phishing Working Group (APWG), apwg.org

35 Messaging Malware Mobile Working Group, m3aawg.org

36 Online Trust Alliance, otalliance.org

37 Merchant Risk Council, merchantriskcouncil.org

38 Forum of Incident Response and Security Teams, first.org

39 FBI, "DNS Changer Malware" November 9, 2011, http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

40 RFC Editor, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", May 2000, http://www.rfc-editor.org/info/bcp38

41 RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84 https://www.arin.net/policy/nrpm.html

42 RFC Editor, "Ingress Filtering for Multihomed Networks", March 2004, http://www.rfc-editor.org/info/bcp84

43 https://www.arin.net/policy/nrpm.html

44 Counterpoint, "Market Monitor: Handset and Spartphone Markets Q4 2014", January 29, 2015, http://www.counterpointresearch.com/marketmonitor2014q4

45 The Realtime Report, "Mobile Comemerce: Online Retail Sales from Mobile Devices Double in Last Year", May 3, 2012, http://therealtimereport.com/2012/05/03/mobile-commerce-online-retail-sales-from-mobile-devices-double-in-last-year/

46 Corra, "Mobile Shopping Trends by Device", February 3, 2015, http://corra.com/mobile-ecommerce-trends-2015

47 GSMA Intelligence, "Global Data", https://gsmaintelligence.com/

48 Worldometers, "Current World Population", http://www.worldometers.info/world-population/

49 IDC, Llamas, Ramon, Anthony Scarsella, William Stofega, "Worldwide Mobile Phone 2015-2019 Forecast and Analysis", April 2015, http://www.idc.com/getdoc.jsp?containerId=prUS23455612 (subscription required)

50 Symantec, "Internet Security Threat Report", April 2015, Volume 20, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA- internet-security-threat-report-volume-20-2015-social_v2.pdf

51 *Ibid.*

52 Adaptive Mobile, "Selfmite: Attack Using SMS Worm to Increase Pay-Per-Install Income", June 25, 2014, http://www.adaptivemobile.com/blog/selfmite-worm

53 Australia, Bulgaria, Belgium, France, Germany, Ghana, Greece, Ireland, Kenya, Netherlands, USA, South Africa, Spain, Sweden, Switzerland

54 Lookout, "2014 Mobile Threat Report," https://www.lookout.com/static/ee_images/Consumer_Threat_Report_Final_ENGLISH_1.14.pdf

55 Bibat, Aerol, "GGTracker Malware Hides as Android Market", Android Authority, June 21, 2011 http://www.androidauthority.com/ggtracker-malware-hides-as-android-market-17281/

56 ICT, "Statistics", http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
ICT, "ICT Facts and Figures, The World in 2014", http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf; http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf

57 *Compare for example:* 47 U.S.C. § 227(b)(1)(A)(iii) *with* 47 U.S.C. § 227(b)(1)(B) and 47 U.S.C. § 227(b)(2)(B).

58 FCC, "'One Ring' Phone Scam," *available at* http://www.fcc.gov/guides/one-ring-wireless-phone-scam.

59 CAPTCHA stands for "Completely Automated Public Turing test to tell Computers and Humans Apart"

60 See for e.g., T-Lock Call Blocker – Version N2, http://hqtelecom.com/callblocker?gclid=CMmt_raT6cECFc1_MgodhnEAWg; CPR Call Blocker Product Page, http://www.cprcallblocker.com/purchase.html; Digitone Call Blocker Plus, http://www.digitone.com; and Sentry Dual Mode Call Blocker, http://www.plugnblock.com/?gclid=CJmKkbaT6cECFSFgMgodJRIAGA; Privacy Corp Caller ID Manager, http://www.privacycorps.com/products/.

61 Weisbaum, Herb, "Want to get rid of those $#%@ robocalls? There's an app for that," http://www.cnbc.com/id/101758815#.

62 Alliance for Telecommunications Industry Solutions, "Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document," https://www.atis.org/docstore/product.aspx?id=26137

63 NANPA, Vertical Service Codes, Code Definitions, http://www.nanpa.com/number_resource_info/vsc_definitions.html

64 Prepared Statement of The Federal Trade Commission Before the United States Senate Committee on Commerce, Science and Transportation, Subcommittee on Consumer Protection, Product Safety, and Insurance on 'Stopping Fraudulent Robocall Scams: Can More Be Done?', Washington, DC, July 10, 2013 ("Senate Hearing"), , http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=c1eec086-3512-4182-ae63-d60e68f4a532&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=7&YearDisplay=2013

65 *Truth in Caller ID Act*, 47 U.S.C. § 227(e); cf. 16 C.F.R. Part 310.4(a)(8).

66 Federal Trade Commission, "Robocalls Gone Wrong", https://www.consumer.ftc.gov/media/video-0027-robocalls-gone-wrong

67 The Economist, "The Cheap, Convenient Cloud," April 18, 2015, http://www.economist.com/news/business/21648685-cloud-computing-prices-keep-falling-whole-it-business-will-change-cheap-convenient?fsrc=scn/tw/te/pe/ed/thecheapconvenientcloud

68 M³AAWG, "M³AAWG Sender Best Common Practices, Version 3, Updated February 2015," https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

69 http://w3techs.com/technologies/history_overview/content_management/all/y

70 https://wpvulndb.com/statistics

71 http://w3techs.com/technologies/details/cm-wordpress/all/all

72 http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 13

73 http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html

74 http://www.emersonnetworkpower.com/documentation/en-us/brands/liebert/documents/white%20papers/2013_emerson_data_center_cost_downtime_sl-24680.pdf Page 14

75 Noroozian, A. et al., "Developing Security Reputation Metrics for Hosting Providers, http://www.tudelft.nl/fileadmin/Faculteit/TBM/Onderzoek/Publicaties/hosting-metrics.pdf

76 Twitter boss vows to crack down on trolls and abuse: http://www.theguardian.com/technology/2015/feb/26/twitter-costs-dealing-abuse-harassing-dick-costolo

77 Suicide of Rehtaeh Parsons: https://en.wikipedia.org/wiki/Suicide_of_Rehtaeh_Parsons

78 Granby, Quebec, Canada moves to fine people insulting police on social media: http://www.cbc.ca/news/canada/montreal/granby-moves-to-fine-people-insulting-police-on-social-media-1.3045816

79 4chan Bullies Fitness Guru Scooby Off YouTube With Doxxing and Threats: http://newmediarockstars.com/2013/07/4chan-bullies-fitness-guru-scooby-off-youtube-with-doxxing-and-threats-video/

80 How I got caught up in a 'stranded traveller' phishing scam: http://www.theguardian.com/money/2013/nov/13/stranded-traveller-phishing-scam

81 How One Stupid Tweet Blew Up Justine Sacco's Life: http://www.nytimes.com/2015/02/15/magazine/how-one-stupid-tweet-ruined-justine-saccos-life.html?_r=0

82 The World Has No Room For Cowards: http://krebsonsecurity.com/2013/03/the-world-has-no-room-for-cowards/

83 Stay Safe Online, https://www.staysafeonline.org/stay-safe-online/for-parents/cyberbullying-and-harassment

84 From the US FTC, https://www.consumer.ftc.gov/articles/0028-cyberbullying ; Nigeria, http://www.mamalette.com/parenting-3/cyber-bullying-nigerian-parents-need-know/; ACMA, http://www.cybersmart.gov.au/Schools/Cyber%20issues/Cyberbullying.aspx; RCMP, http://www.rcmp-grc.gc.ca/cycp-cpcj/bull-inti/index-eng.htm; South African Police Service, http://www.saps.gov.za/child_safety/teens/cyber_bullying.php;

Steering Committee

Andre Leduc, Manager, National Anti-Spam Coordinating Body, Industry Canada

Alyson Hawkins, Policy Analyst, Industry Canada

Christina Adam, Policy Analyst, Industry Canada

Jerry Upton, Executive Director, Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG)

Lisa Foley, Policy Analyst, Industry Canada

Neil Schwartzman, Executive Director, CAUCE.org

Contributors

Alex Bobotek, Lead, Mobile Messaging Anti-Abuse Strategy and Architecture, AT&T

Amy Hindman, Principal Engineer, Verizon

Betsy Broder, Counsel for International Consumer Protection, Federal Trade Commission

Bruce Matthews, Manager, Anti-spam Team, Australian Communications & Media Authority

Carlo Catajan, iCloud Mail & iMessage Anti-Abuse, Apple Inc.

Carlos Alvarez, Sr. Manager, Security Engagement, SSR Team, ICANN

Chris Boyer, Assistant Vice President, Global Public Policy, AT&T

Christian Dawson, President, ServInt and Chairman, i2Coalition

David Jevans, Chairman, Anti-Phishing Working Group (APWG)

Eric Freyssinet, Ministère de l'intérieur, France

Foy Shiver, Deputy Secretary-General, APWG

Francis Louis Tucci, Manager, Network Repair Bureau, Verizon Wireless

Frank Ackermann, M³AAWG Public Policy Committee Co-chair

Gary Warner, Director of Research in Computer Forensics, University of Alabama at Birmingham

Jay Opperman, General Manager, CSP, Damballa

Jayne Hitchcock, President, WOAH

Jeff Williams, Dell SecureWorks

Jessica Malekos Smith, Student, UC Davis School of Law

John Levine, President, CAUCE.org

Johnathan Curtis, Norsecorp

Justin Lane, Anti-Abuse Manager, Endurance International

Karen Mulberry, ISOC

Lee Armet, Senior Investigator, TD Bank Group

Mary Retka, Director, Network Policy, CenturyLink

Matthew Bryant, Ofcom

Matthew C Stith, Manager, Anti-abuse, Rackspace Hosting

Michael Hammer, American Greetings

Michael O'Reirdan, Comcast Fellow

Patrick Tarpey, Ofcom

Paul Vixie, CEO, Farsight Security

Peter Merrigan, Government of New Zealand

Phil Shih, Structure Research

Richard Feller, Hedgehog Hosting

Rod Rasmussen, President and CTO, Internet Identity (IID)

Sanjay Mishra, Distinguished Member of Technical Staff, Verizon

Sara Roper, Manager Information Security, CenturyLink

Sid Harshavat, Symantec

Steven Champeon, Enemieslist

Terry Zink, Program Manager, Microsoft

TR Shaw, SURBL

Venkata Atluri, Associate Professor, Alabama A&M University

Participants

Adam Panagia, Adria Richards, Alexander Falatovich, April Lorenzen, Autumn Tyr-Salvia, Bill Wilson, Bulent Egilmez, Chris Lewis, Dave Crocker, David Dewey, David Levitt, Donald McCarthy, Donald Smith, Dylan Sachs, Eric Chien, Franck Martin, Hein Dries-Ziekenheiner, Jacek Materna, Jack Johnson, Jared Mauch, Jean Marie Norman, John Cunningham, Julia Cornwell McKean, Kaio Rafael, Karmyn Lyons, Ken Simpson, Lucas Moura, Mark Collier, Matteo Lucchetti, Michael Shoukrey, Mustaque Ahamad, Nabeel Koya, Nitin Lachhani, Olivier Caleff, Patricia B. Hsue, Paul Ebersman, Peter Cassidy, Raymond Choo, Richard Clayton, Richard Gane, Rudy Brioche, Sid Harshavat, Steve Jones, Steven M. Wernikoff, Suresh Ramasubramanian, Toni Demetriou, Trent Adams, Will Clurman

EVALUATE
RESPOND
DEVELOP
DETECT
COLLABORATE
PREVENT
TRACK
UPDATE
REPORT
EDUCATE
SHARE

PREVENT
TRACK
UPDATE
REPORT
EDUCATE
SHARE