Internet and mobile technologies have been key drivers of the global economy over the past twenty years. As our laptops, smartphones and tablets have become integrated into our daily personal and business lives, our dependence on these devices has grown. The Operation Saftey-Net report provides readers with a plain language description of the threats facing businesses, network providers and consumers in the online and mobile environment.

With growing consumer and business dependency and rapid migration of commercial transactions to online and mobile platforms comes 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 primary focus of this report is not only to study the threats to the online, mobile and VoIP environment that burden 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, phishing and social engineering, internet protocol and domain name system exploits, mobile, VoIP and telephony threats, and hosting and cloud threats. This pamphlet provides a high-level overview of the report and selected examples of best practices for addressing these threats.

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.

To avoid detection criminals are continuously changing or "morphing" their malware. A growing proportion of malware can detect that it is being "monitored" 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.

Examples of best practices for addressing malware and botnets:

- Detect and Notify (ISP-to-User)
- Raise Awareness
- Implement Legal and Regulatory Frameworks
- Seek Industry and Government-Led Collaboration
- Follow the industry best practices of blocking outgoing mail (port 25) from any computer on your network other than your own mail servers

Examples of best practices for preventing hosting and cloud abuse:

- Prevent abuse at the network edge:
  - ↳ Consider hardware-based intrusion detection systems (IDS)
  - ↳ Use software-based security scans and firewalls
  - ↳ Maximize customer contact and protect identity
  - ↳ Strengthen customer passwords
- Detection and Identification:
  - ↳ Use confidential client identifiers
  - ↳ Establish role accounts for network domains
  - ↳ Maintain accurate SWIP and IP WHOIS records
  - ↳ Set up Feedback Loops (FBLs) and automated reports
- Remediation:
  - ↳ Respond swiftly and effectively

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.

The full report is available at:

LONDON ACTION PLAN
INTERNATIONAL CYBERSECURITY ENFORCEMENT NETWORK

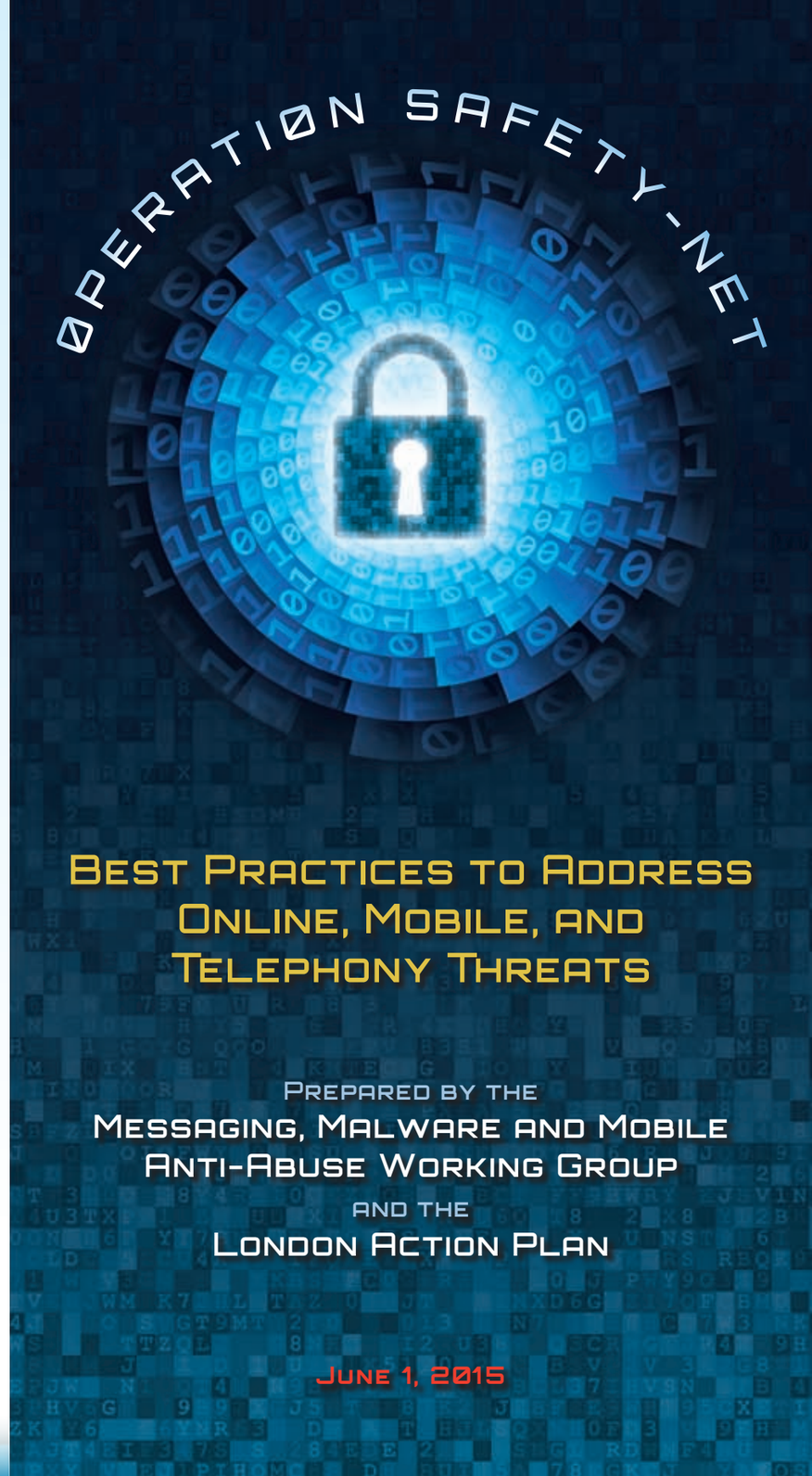
londonactionplan.org

M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

www.m3aawg.org

CAUCE

www.cauce.org



Phishing and Social Engineering

Phishing refers to techniques that are used to trick a victim into revealing sensitive personal, corporate, or financial information. Phishing has been steadily increasing in frequency, sophistication, and damage. In fact, phishing has been on the rise since 2011, and almost 1/4 of recipients open phishing e-mails and over 10% click on malicious attachments. 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 incur individual losses in the thousands of dollars, to current-day high-value targets.

Although phishing is not new, escalation in the number, targeting, and sophistication of the attacks in recent years represent an ever increasing threat to companies, governments, and consumers, and also erode 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.

Examples of best practices for fighting phishing and social engineering:

- Report
  - Alert customers, employees, constituents and anti-phishing organizations
  - Establish easy to remember reporting websites or e-mail addresses
- Conduct joint corporate and law enforcement investigations
- Conduct user/victim education
- Establish and use Industry and Government information sharing and advocacy groups

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. IP addresses are used to route traffic to and from computers. Like a phone number, each is unique. The Domain Name System (DNS) links a name that people can remember, like www.google.com, to its corresponding IP address 173.194.73.105 (for IPv4) or 2607:f8b0:4000:807::1012 (for IPv6). Since Internet users tend to look up the same sites repeatedly, networks and computers have caches that remember recent DNS queries and answers.

The most serious DNS exploits are resolver exploits, in which bad actors introduce forged data to redirect Internet traffic to fake versions of popular websites. In many cases consumers are completely unaware that they have been redirected to a fake site. Cybercriminals may also break into the web servers of legitimate sites and infect the domain and redirect users to a malicious destination site.

Examples of best practices for preventing resolver exploits and cache poisoning:

- Support the worldwide deployment of DNSSEC
- Use TSIG for all online DNS updates and for server-to-server "zone transfer" operations
- Keep your DNS software patched up to date
- Educate network and system managers

Examples of best practices for fighting web redirect abuse:

- Conduct URL reputation testing
- Support blocking compromised legitimate domains that serve malicious content, notify rapidly, retest and delist
- Encourage URL shortener services to check all redirects
- Develop educational resources for industry and users

DNS registration abuse occurs when cybercriminals use stolen credit cards to register domains, use high speed automated registration, or use resellers or proxies. Blocklist operators take time to recognize malicious domains and then to propagate reputation information, so by rapidly registering new domains, cybercriminals are able to evade detection.

Examples of best practices for preventing DNS registration abuse:

- Establish and monitor 'Know Your Customer' programs to prevent abuse of domain assignment
- Implement mandatory HTTPS and multi-factor authentication
- Improve reputation algorithms to include domain age
- Work closely with advocacy groups to address issues

Mobile, VoIP, and Telephony Threats

With the advent of the smartphone, e-commerce activities have moved to new platforms. Bad actors seeking to profit and defraud have been quick to follow. 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.

Examples of best practices for reducing the spread of mobile malware:

- Develop facilities for reporting and encourage use
- Collaborate, and exchange threat and abuse data with international, government, industry and specialized prevention groups
- Evaluate mobile security solutions
- Educate consumers

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 is only serving to make 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 the calls of legitimate individuals trying to reach, for example, the fire department or an ambulance, are unable to get through.

Examples of best practices for preventing VoIP and telephony threats:

- Set honeypot traps to detect system abuse
- Perform analytics to identify problem calling patterns
- Encourage use of Customer Premises Equipment (CPE)
- Implement Industry best practices and standards
- Enact and enforce anti-fraud and 'do not call' rules

Hosting and Cloud

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 to hosting 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.

Online and mobile threats exploiting hosting and cloud services 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.