MessageLabs®

Be certain

MessageLabs Intelligence 2005 Annual Security Report

Cyber-criminals narrow their focus

Table of Contents

1 Executive Summary and Overview

This report sets out to summarize the major security trends and developments for 2005, outlining the key issues that have developed over the course of the year and how they have affected the security market. The report also aims to provide some insight into the key threats and security issues that are expected to emerge in 2006.

1.1 Key findings

It could be forgiven if 2005 is also remembered as the year in which the words Corporate Governance, Regulatory Compliance and Legislation all became part of the IT vernacular. As spam and viruses continue to threaten business continuity, unsecured communications can easily threaten non-compliance and the risks of non-compliance alone can be enough to irrevocably harm companies, leading to prosecution, damage to brand reputation and costly financial penalties. Increased spending in these areas is already having an impact on IT budgets as more resources are diverted to tackle these challenges.

2005 saw a significant increase in the number of targeted attacks on both business and organizations.

2005 saw a significant increase in the number of targeted attacks on both business and organizations. Targeted attacks come in a number of different guises, some more prevalent than others, such as malicious code hidden inside a trojan horse for the purpose of information theft; or the well documented examples of denial of service attacks (DoS), where email servers and web servers are flooded with connections from botnets disabling the site for the purpose of impacting business, blackmail or extortion. Such trojans can also focus on critical application vulnerabilities rather than just those of an operating system.

1.2 Top threats of 2005

- The overall spam trend for the first half of 2005 has seen a levelling of spam amounts in line with 2004 yearly figures, with an annual average percentage of 68.6% or 1 in every 1.46 emails being identified as spam; this compares with the annual 2004 average of 72.3%, or 1 in 1.38 emails.

- The equivalent annual average percentage of malware attacks is 2.8%, or 1 in every 36.15 emails contain a virus or trojan; in 2004 the annual average was 6.1%, or 1 in 16.39 emails.

- MessageLabs intercepted around 2-3 targeted attacks per week during 2005; in 2004 this figure was almost negligible.

- Phishing continued to be a major threat during 2005, accounting for an annual average of 0.3% or 1 in every 304 of all email traffic. In 2004 the annual average of phishing emails was 0.1% or 1 in 943. The peak phishing season in 2005 was January, although overall volumes were greater in May, the ratio in mail for January was 1 in every 126.5 emails, or 0.79%. Phishing also accounted for 27% of malicious email traffic intercepted in January 2005; the annual average was 13.1%. This compares with 2.4% of malware in 2004, highlighting a marked shift in cyber-criminal activity towards phishing in 2005.

- Botnets – security experts believe the sudden rise in phishing is due to the huge rise of zombie botnets being used to pump out massive volumes of scam emails. Although over the course of 2005 botnets have actually been shrinking in size, with the cyber-criminals seemingly preferring to have greater numbers of smaller and more discreet networks to be under their control.

- Increased data theft through IT security vulnerabilities – a rogue program exposed 40 million credit card accounts held by US payment processor CardSystems to possible fraud. An alleged industrial espionage ring was uncovered earlier in the year in Israel whereby malware hidden in email and files was developed with the express purpose to steal rivals' corporate secrets and monitor their activity.

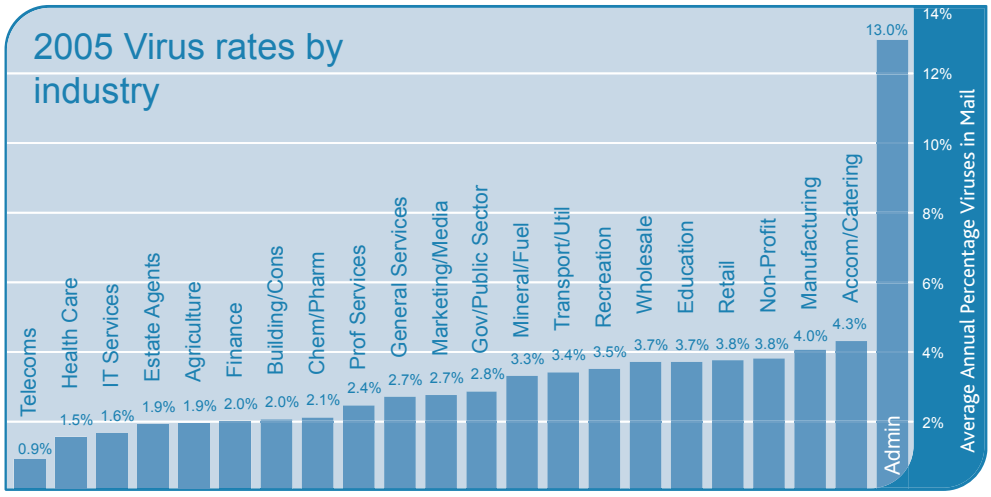
1.3 Top sectors under attack in 2005

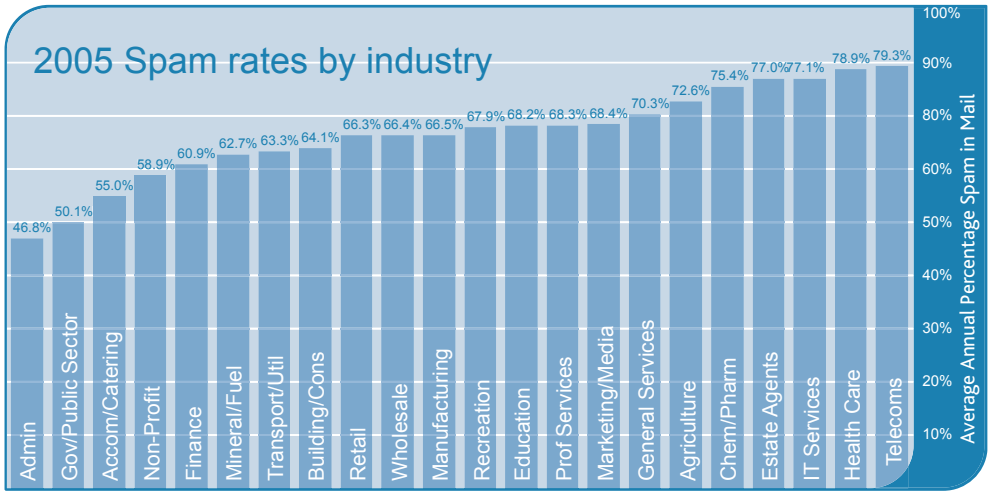
- Government and infrastructure – the UK's National Infrastructure Security Coordination Centre reported on approximately 300 UK government departments and businesses critical to the country's infrastructure were the subject of Trojan horse attacks, many reportedly originating in the Far East

- Banks and financial institutions – this sector still ranks amongst the most threatened, both from direct and indirect assault (through phishing emails and targeted Trojans)

- Retail – online retailers are also suffering due to the increase of phishing emails that result in the loss of consumer confidence in internet commerce

- Home user – with the increase in the amount of phishing emails and Trojan viruses, home and personal computer users are on the front line, as their PCs have limited protection and can provide criminals with not only the personal data on the PC, but can subvert the PC to form part of a network of zombie computers (botnets) that can massively increase the potency of a new threat



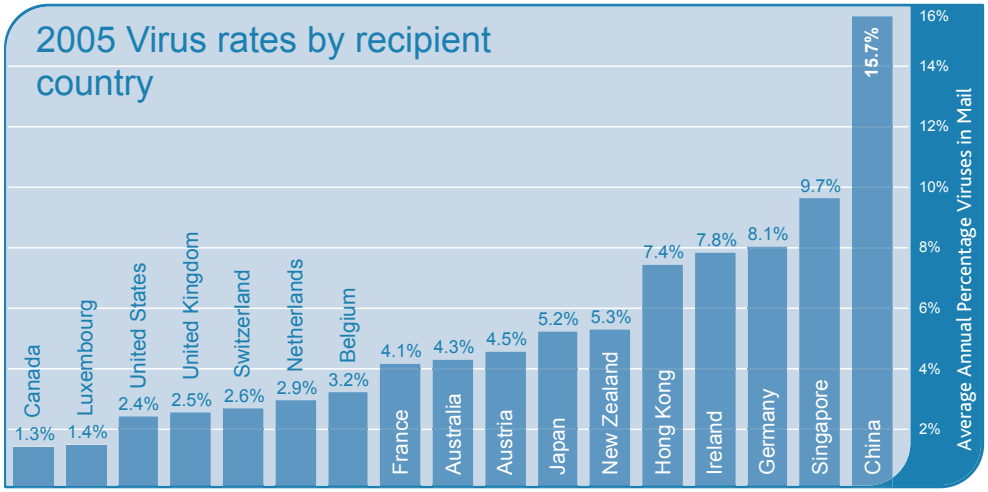


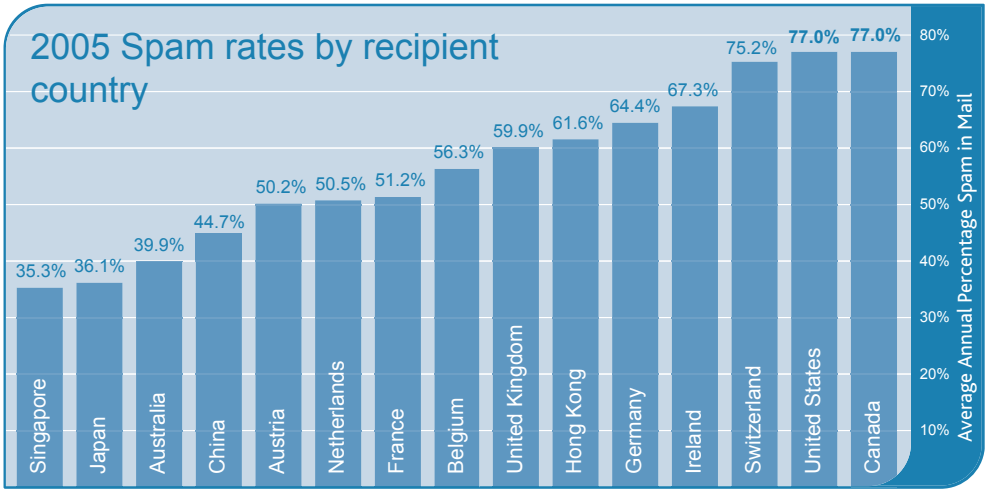
1.4 Geographical trends in 2005

Attacks from new countries – Most organized cyber-criminal groups now operate internationally with a casual disregard for any legal jurisdiction; the threat to and from emerging and developing countries is therefore increasing. For example, the numbers of reported incidents originating from China have risen in 2005 for a number of reasons, such as the rapid growth in the economy and the less regulated IT environment along with communication challenges with the western security community.

Cyber criminals take advantage of poor international cooperation against cyber-crime and launch cross border attacks with little personal risk. It then becomes far more difficult to trace the attacks back to source, especially when trends show attacks are increasingly originating from regions such as Eastern Europe and Asia where sanctions are more lenient and enforcement is limited.

Increasing technology and skill levels, coupled with very low risk of legal consequences and the potential for very large ill-gotten gains means that international cyber-criminals are continuing to devise new and more sophisticated attacks directed at businesses and organizations. While recent arrests of high profile spammers and hackers continue in the West, this does not resolve the threats posed by developing countries such as China, now a major target given the phenomenal growth seen in the country's economy over recent years. However, this threat poses a new challenge and it is predicted that the number of incidents emerging from developing countries will geometrically increase over the coming year.





With little prospect for relief from legislation and law enforcement, businesses must take concerted measures to protect themselves. The consequences of a security breach for any business can mean severe disruption to business operations, downtime, employee frustration and potential heavy financial loss.

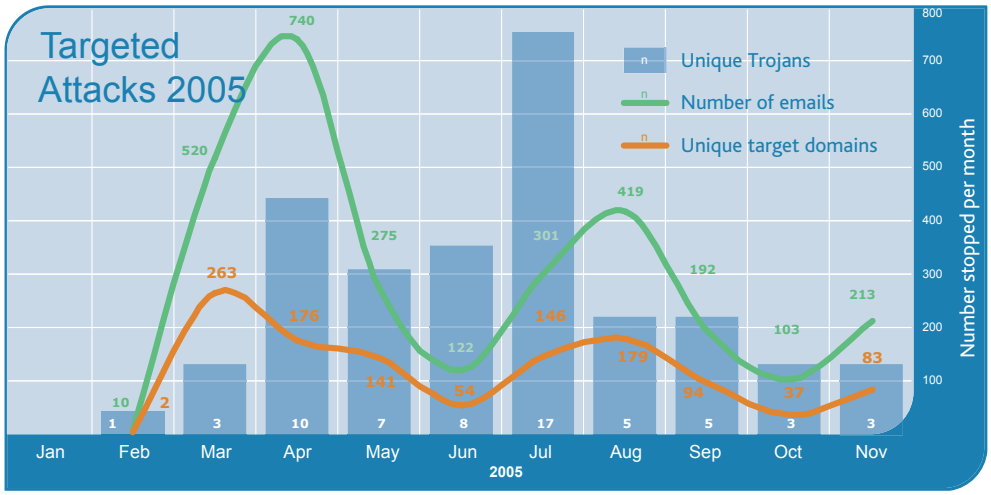
2 Email Security Trends and Developments 2005

2.1 Targeted attacks on businesses takes center stage

Criminal activity in the virtual world has continued to accelerate; MessageLabs is seeing a new wave of security threats for businesses with much more sophisticated and malevolent techniques at their disposal. Old style virus proliferation, characterized by the indiscriminate shot gunning of the Internet world at large, has been superseded by new targeted email attacks from criminals aimed at defrauding business, stealing intellectual property or extorting money.

According to MessageLabs Intelligence data, these targeted email attacks against business, which are often financially, competitively, politically or socially motivated, although still small in number, have grown in consistency and cunning this year.

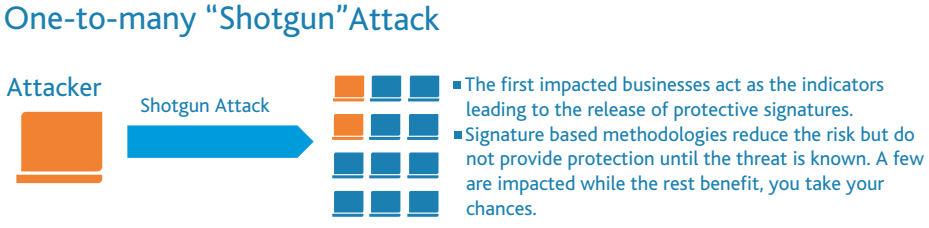
Criminal activity in the virtual world has continued to accelerate; MessageLabs is seeing a new wave of security threats for businesses with much more sophisticated and malevolent techniques at their disposal.

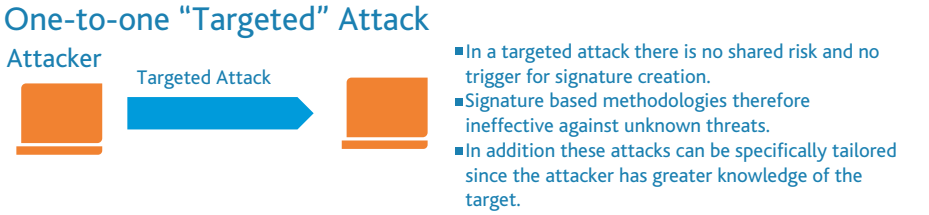


Since the beginning of 2005, the number and sophistication of targeted email-borne attacks on businesses has increased. These attacks are often directed at government departments, military organizations and other large organizations, particularly in the aerospace, petroleum, legal, and human rights fields. Several high profile cases hit the headlines in 2005 but it is believed many more attacks go undetected by businesses.

2.1.1 Examples

During June, police arrested two computer consultants in the UK alleged to be part of a massive industrial espionage scandal uncovered in Israel in which Trojan software was used by leading companies to allegedly steal confidential information from competitors and monitor their activity. Well known businesses were accused of using the malware to send to competitors' computers via an email attachment, purporting to be a normal business proposal to trick users into downloading spyware.



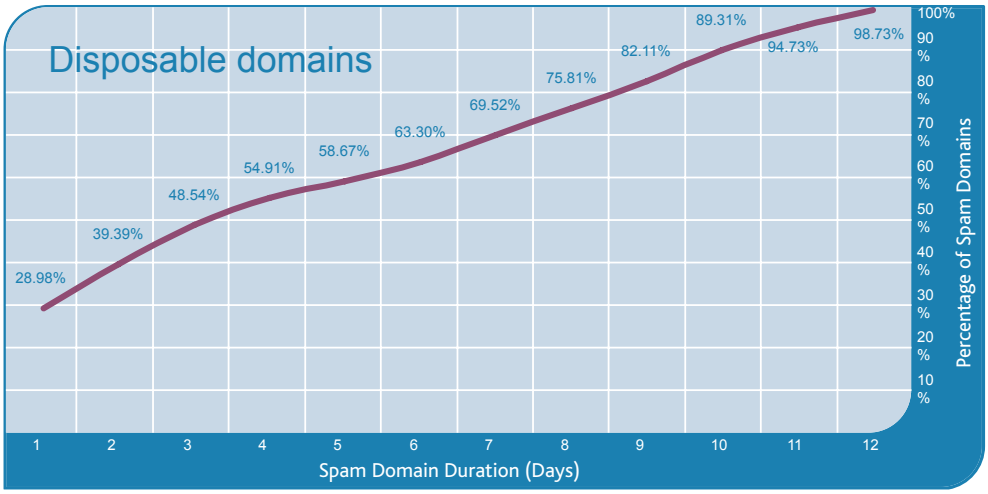


Typically, and naturally, many organizations tend to distance themselves from such attacks, and think "it won't happen to me," but it should be noted that attacks such as these have already happened to many leading organizations - large and small - worldwide. Every business organization needs to take steps to protect their intellectual property and resources and consider the increasingly pervasive nature of electronic communications and the new vulnerabilities that come with it.

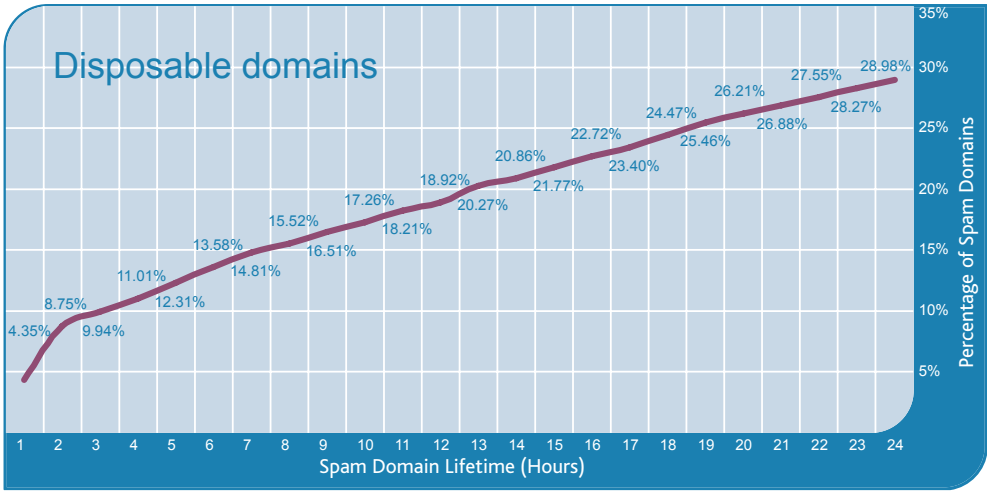
Traditional anti-virus solutions that are signature-based provide a reactive approach and require signature updates to be effective, providing little or no defense from these kinds of often unique targeted attacks. As can be seen from the graphic above, traditional anti-virus software can offer protection after a major outbreak has occurred, but these carefully targeted Trojans, that sometimes will only be sent to one or two targets, never attract that kind of attention. Studies by MessageLabs have shown that the typical time for signatures to appear for targeted Trojans is between one and three months. Companies need to realize that they cannot rely solely on traditional reactive methods.

2.2 Spam Sweatshops and Disposable Domains

MessageLabs has spent the latter part of 2005 tracking spammers who register disposable domain names, and then carry out short-lived, but fairly aggressive spam runs (domain hopping). The charts below show that these spam domains can last for anything from a few hours to a few days, with the maximum useful life being about 12-days.



It can be seen from the graphs that the tapering off is a very 'straight-line.' For example, 28.9% of domains last under 24-hours, and 9.9% are used for fewer than 3 hours.

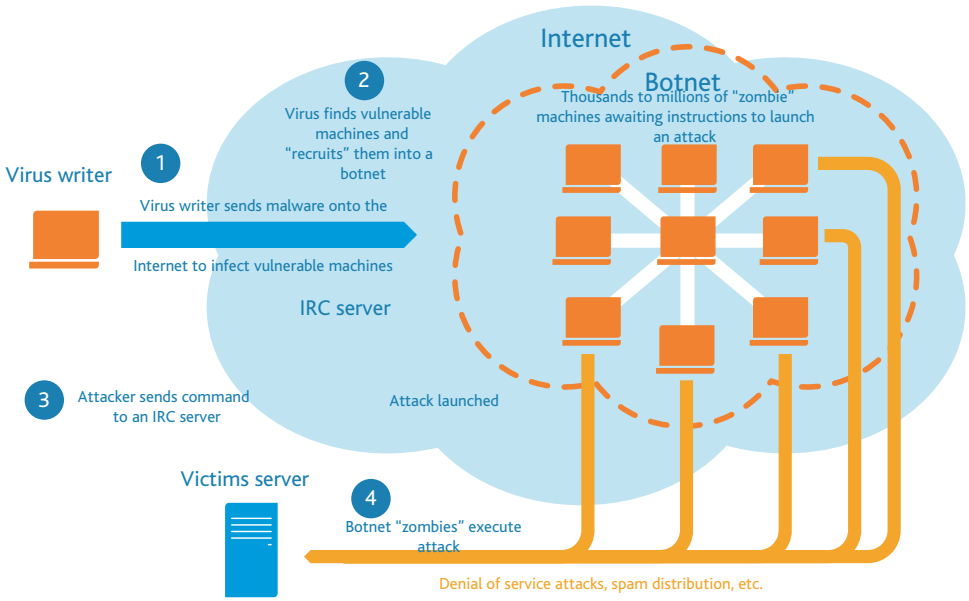


Although many of the domains used are still live, MessageLabs no longer sees email spam luring people to these sites after this time.

2.3 Botnets continue to fuel the cyber-criminals progress

Attacks have become increasingly multi-purpose. For example, earlier this year, in May, MessageLabs intercepted 800,000 incidences of the Glieder trojan horse, linked to a new variant of the Bagle virus family. Unlike previous trojans, Glieder had the capability to launch a multi-staged assault on it targets, demonstrating a greater level of "cooperation" between its progenitors and other attacks. Glieder would be in the vanguard, and it had three objectives: firstly to infect its victim, secondly to disarm any protection including firewall and anti-virus software, and then finally to turn the machine into a zombie, controlled from a number of 'botnets' – global robot-networks of compromised computers which can be remotely controlled by cyber-criminals.

The number of Trojan borne emails has increased significantly over the past year. It is evident that the bad guys have adapted from sending mass-mailing viruses to sending more targeted trojans using botnets.



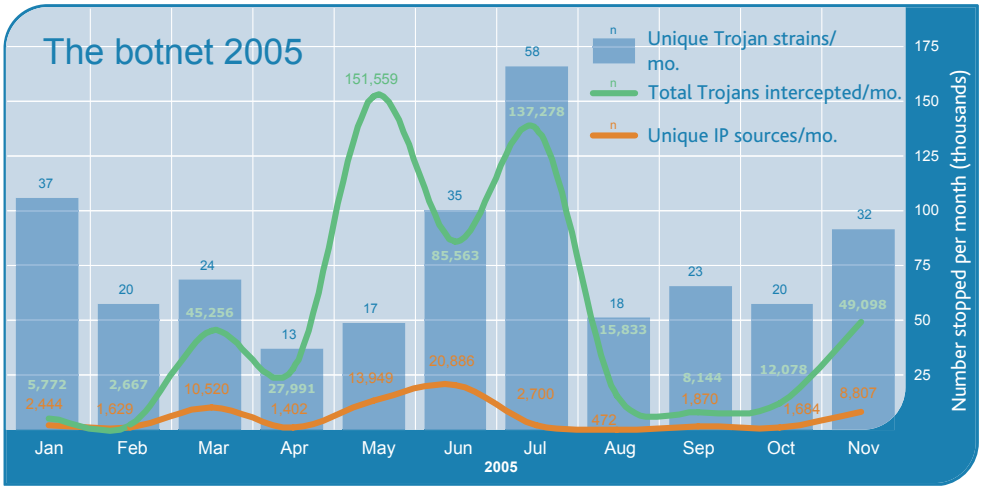
Botnets such as these are hired by spammers, phishers, adware and spyware merchants and other criminal gangs for fraudulent or criminal purposes. According to research from a group of security researchers known as the Honeynet project, more than one million computers globally have been hijacked in this way in order to attack websites, pump out spam and send out insidious payloads to extend their reach.

As increasing competition between domestic Cable and DSL providers pushes down the cost of bandwidth, and the amount of bandwidth per connection increases, more people will find themselves becoming a very attractive target for the cyber-criminals.

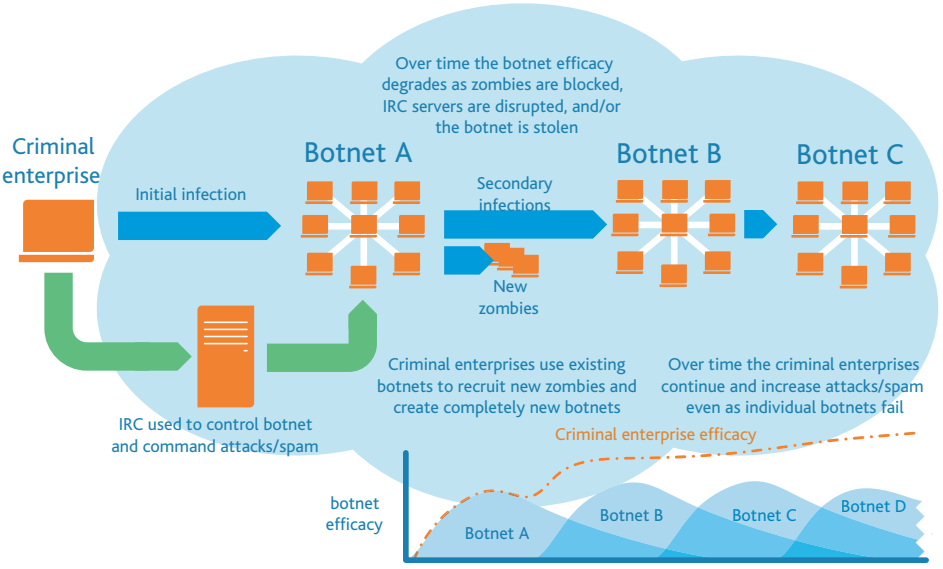
During 2004, botnets were sometimes used by cyber-criminals to drown victims' websites and email systems with tens of thousands of simultaneous connections under their control, threatening the livelihood of an online business.

The overall spam trend for the first half of 2005 has seen a leveling of spam levels in line with 2004 yearly figures, with an annual average percentage of 68.6%, or 1 in 1.46 emails identified as spam. The equivalent average percentage of malware attacks is 2.8%, or 1 in 36.15 emails contain a virus or trojan. Phishing emails reached an annual average of 0.3%, or 1 in 304 of email traffic.

The number of Trojan borne emails has increased significantly over the past year. It is evident that the bad guys have adapted from sending mass-mailing viruses to sending more targeted trojans using botnets.



From the chart above it would seem that the number of unique trojans is roughly inversely-proportional to the number of IPs used to send them, suggesting that the remnants of each botnet (after heavy use and just before they are about to fully decay – i.e. become spent) are used to send trojans out to increase the size of the botnet. So the trojan activity goes up when the botnets are close to full decay.



Therefore, it is very important to ensure security defenses are strengthened to safeguard against such carefully crafted and specialized Trojan attacks, which may enter an organization via a number of different protocols and techniques, including the Web and IM.

2.3.1 Examples of Botnets

In October 2005, police in the Netherlands arrested three men who were allegedly in control of a botnet comprising over 100,000 zombie PCs. The botnet was seemingly used to conduct an extortion attempt against a US company and distribute phishing attacks and various forms of adware and spyware.

Similarly, in November, the FBI in California arrested a 20-year-old man that was accused of illegally controlling a botnet of 400,000 compromised computers, and it was reported that he made money by renting them out to spammers and other criminals.

Also in November, MessageLabs thwarted a number of large email-borne outbreaks, this time of the Sober and Bagle worms (Bagle on a lesser scale to the Sober worm, which was the largest outbreak of the year).

This recent activity also indicates that botnet controllers have been bolstering their botnets in the run-up to the Christmas holiday period, for them to rent them out to the 'spam sweatshops' and adware merchants to spread their wares.

The trend now is rather than have control over fewer, but larger botnets, the bad guys seem to be moving towards having greater numbers of smaller botnets, to evade detection and maintain the control over a greater number of zombies by using multiple command and control channels. The Sober outbreak was started when the botnet controller issued an update command and all of the zombies under his control were updated with the latest version of the software, which subsequently tried to spread via email as well.

Although many anti-virus vendors had 'generic' detection for Sober by 16th November, it highlights the fact that if your computer is already part of a botnet, then your anti-virus defenses are effectively down; millions of computers already infected had their defenses effectively disarmed by the trojan already installed on their computers.

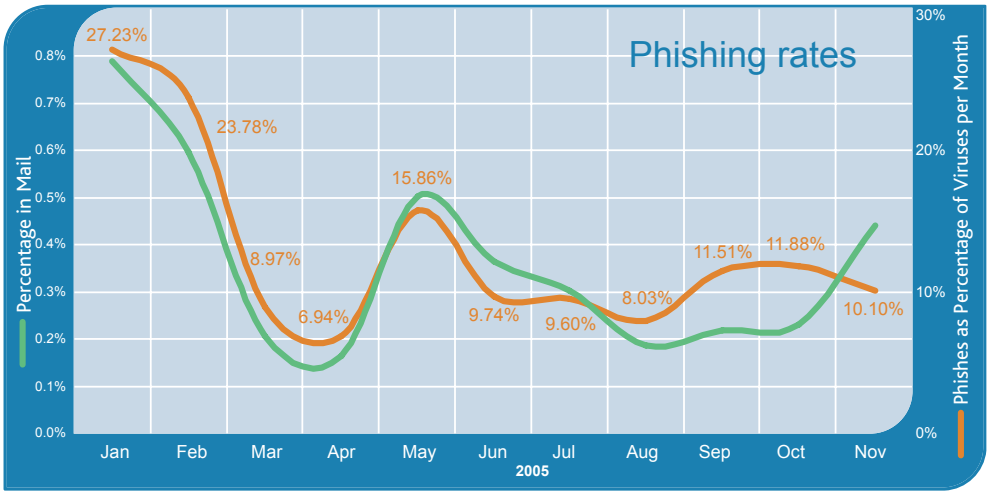
2.4 Phishing: Spear Phishing hooks new victims

Another rising trend in more targeted attacks is from 'spear' phishing, where criminals bombard businesses with highly targeted spam that appears as though it has originated from inside the organization, typically from the IT or HR departments. Often, the perpetrator will offer a small reward in return for information and individuals who are duped into thinking the emails are legitimate often comply. They unwittingly reveal information that will enable the criminal to access secure areas of the corporate network which can result in the theft of intellectual property and other sensitive corporate data.

Spear phishing as a social engineering technique in itself has also been used to bait people into opening malware, for example, some strains of the MyTob virus can infect a computer from clicking on a link in an email purporting to come from security personnel at the same organization as the recipient. For all intents and purposes, this appears to be a phishing attack, but the objective is to trick the recipient into visiting a website that will attempt to install some malicious code via a vulnerable web browser. The first Mytob (a mixture of MyDoom and 'bot' functionality) was released in February 2005, and by July there were over 30 known variants of this malware. At one point, the authors appeared to be releasing new variants each time anti-virus vendors published signatures.

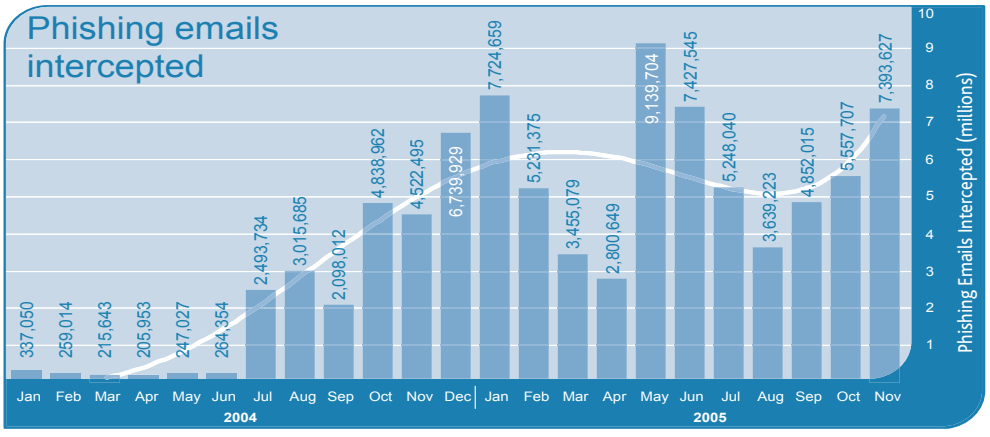
This further highlights the more blended and converged nature of the more contemporary threats that organizations were confronted with during 2005, and this is only set to increase in the coming year.

The peak phishing season for 2005 was actually in January, although overall volumes were greater in May. The ratio in mail for January was 1:126.5 or 0.79%, and phishing accounted for 27% of malicious email traffic intercepted by MessageLabs, the average for 2005 was 13.1%.



South American banks were a prime target for online fraud criminals during 2005; however, the overall amount of phishing emails generally declined during the first half of the year, but increased again towards the end of the year. It is also believed that the rise in phishing activity has also been due to the increased use of botnets being used to pump out massive volumes of scam emails, as cyber-criminals look to increase their profits through more aggressive targeting. As computer users are becoming more aware of the risks associated with the Internet and email threats, the perpetrators of phishing attacks also develop new techniques to increase their chances of success.

The attack vector is also beginning to change: in order to succeed, phishing will become less reliant upon social engineering to dupe the recipient into believing they are dealing with a bank; and edging further towards defeating the multi-factor authentication schemes that many banks are now deploying. For example, W32/Grams – the silent-but-deadly Trojan spyware, waits for the authentication process to complete before cleaning out the victim's account.



2.5 The fight back begins – but with limited effect

Governments have started to cooperate on a global scale to address the mounting problem. The London Action Plan set up in October 2004 is an international action plan organized by the UK Office of Fair Trading and the US Federal Trade Commission and backed by 35 government agencies from around the world to launch an awareness campaign aimed at pressuring Internet Service Providers (ISPs) and other Internet bodies to take a responsible role in helping to clamp down on email attacks. However, this is just a small step in what is turning into one of the most serious challenges facing the global online community today – and such initiatives take time to have any impact.

3 Outlook and Predictions for 2006 – a year of evolution

During the transition from 2005 to 2006, mail processing volumes will come down fractionally over the holiday period; however, this will go largely unnoticed as the vast majority of email is unwanted content and not in fact legitimate mail, and the proportion of spam will increase over this time.

While we see evidence of the aggressive malware trajectory now starting to level off, we will continue to see more low-level targeted Trojan attacks during the coming months.

Initiatives such as GetSafeOnline in the UK, StaySafeOnline in the US and NetAlert in Australia will have assist in improving security habits of users and businesses connected to the Internet. However, as user awareness grows, this will be matched by the increasing sophistication of the virus writers who will create more virulent and aggressive threats.

With increased convergence of technology and communications media, we can expect to see more viruses specifically designed to attack mobile communications devices, if 3G applications become more widespread that could also become a more vulnerable target - especially for spam.

Spammer operations will further shift towards overseas markets where the legislation is difficult to enforce, or very weak, for example, Russia, China and Eastern European countries.

We expect to see more new cyber-criminals entering the field - with much more automation and 'off the shelf' technology available, it is already possible for virus, spammer or phisher novices to buy a ready-made 'phishing kits' that can be downloaded from the Internet, including mailing systems and lists of the IP addresses of the 'proxies' (or bots) to mail through.

The use of disposable or "throwaway" domains is predicted to rise, as it continues to pose little challenge to any self-respecting spammer to register a vast array of spam domains without needing to verify his or her own true identity, as would be required when purchasing a secure web certificate for example.

However, with the shift towards more illegal activities such as targeted attacks and cyber-crimes like phishing, we can expect to see more active involvement by the FBI and other international law enforcement agencies as priorities and resources begin to shift in favour of investigating such illegal activities. In April 2006, the UKs NHTCU (National Hi-Tech Crime Unit) will become absorbed into the new Serious and Organised Crime Agency, or SOCA. This will represent a major change in how this crime is tackled in the UK.

As the criminals intent on industrial espionage, with their thirst for intellectual property unslaked, we can expect to continue to see around 2-3 targeted email attacks per week. Similarly, such targeted attacks will continue with increasing sophistication in order to remain below the radar, therefore we expect the interception rate to remain fairly constant.

Web (HTTP) and instant messaging protocols will continue to present growing areas of concern relating to threats. Spyware distributors will continue to use 'typo-squatting' of domains (e.g. googkle.com) to host a mass of malicious software, posing a concern for organizations faced with confronting such threats. In May, Russian media also reported a scenario in which webmasters were being lured into setting up web sites hosting spyware via the iframedollars.biz website. Not only do they then install spyware on the machine of every visitor to the site, but also the criminals apparently reward each infection with 6 cents. A staggering $11,890 was said to have been paid in one week alone.

With increased convergence of technology and communications media, we can expect to see more viruses specifically designed to attack mobile communications devices, if 3G applications become more widespread that could also become a more vulnerable target - especially for spam. Sharp increases in web/http attacks are expected, including spyware and adware.

3.1 Instant Messaging – a backdoor to your network

Currently the IM space broadly comprises of three main vendors, namely MSN, AIM and Yahoo! Crucially, these three main IM ecosystems do not yet talk to each other. So, from the bad guys' perspective, they are vastly unattractive when compared to email because the latest SPIM (Spam for Instant Messaging) attacks will stay locked inside whichever ecosystem they were initially seeded. However, in the not too distant future we will see these ecosystems begin to merge and common standards will appear between them. At that point, such a network will have immediate appeal to criminals and we can start to imagine how an aggressive threat roadmap will start to evolve.

3.2 VoIP – the next target?

Of course, after IM the next logical target from a messaging stand point will be VoIP. Although largely blue-sky at present, the dramatic cost savings achievable via VoIP solutions would certainly indicate this is a communications technology that is proving to have a very fast adoption rate. As soon as this happens, we will have yet another attractive critical mass installed base available via the Internet which will in turn become a target.

VoIP threats to businesses are not expected to become commonplace until around 2007, but in the same way that attackers are now targeting application vulnerabilities, a maliciously crafted VoIP packet may perhaps be able to crash the VoIP application and render control to the attacker. It is however more likely that this ecosystem will become a playground for a new breed of spammers in the realm of SPIT (Spam for Internet Telephony), as they reap the same benefits as those adopting the new technology at home, namely the extremely low cost.

3.3 Mobile threat to become significant

More and more organizations will promote and support remote working - whether at home or on the road - and this effectively extends the corporate network to an environment beyond the control of the IT manager. According to IDC, 69 million workers will be mobile by 2009 across Europe. As we begin to see more trains and planes being furnished with Wi-Fi, the risks for businesses also increases. Hence controlling the flow of traffic to and from the internet is more important in order to secure the workstation and therefore the business network - a VPN does not secure the computer from the internet, so once the laptop is exposed, the VPN is also exposed.

Securing mobile devices will certainly become a higher priority as they become a ubiquitous part of the workplace. Theft or misplacement of such devices will inevitably increase, thus we may see increased adoption of biometric or fingerprint-type security to protect them. With more and more businesses rolling out Blackberry solutions or something similar, it is more important than ever to filter the increasing amount of spam from the corporate inbox, as any spam that reaches the inbox will also reach the mobile users - rendering the devices almost useless if the spam is not controlled. The other issue that mobile devices present is securing devices being brought into the organization, bypassing the firewall. The challenges of authenticating and securely managing these devices will prove difficult.

3.4 Banks get smart

Banks will start to deploy two-factor authentication devices on a grander scale, perhaps starting with key-fobs but moving on to personal card-reader devices that can be attached physically to a computer to authenticate an online transaction.

3.5 Phishing gets smarter

Phishing attempts will increase in sophistication both in their targeting and the design of the emails and spoof websites they often create to dupe victims. Trojans will begin to target desktop applications much more, more than traditional operating system vulnerabilities perhaps, and subsequent spear phishing sorties will only strengthen the bad guys resolve as they endeavor to learn more about an organization and which applications to target.

4 Conclusion

The risks associated with messaging attacks are not only technically led (data loss, infrastructure downtime), but potentially libelous, impacting brand reputation, as well as employee, client and partner relations. Consequences are potentially damaging and costly, with major effects on revenues, share price and bottom line – and above all loss of intellectual property and trade secrets. Analysis of MessageLabs Intelligence data suggests that the sophisticated targeted email attacks are a relatively new phenomenon and have only been directed against businesses and organizations on a regular basis for the past year and a half. MessageLabs is now intercepting several incidences a week and expects this trend to continue and grow.

Businesses today are increasingly targeted by more malicious and insidious messaging attacks than ever before, and can no longer afford to be complacent. This does not however, mean that the cyber-criminals have won. Companies can take control of their security and through education, vigilance and the adoption of a managed services approach that goes far beyond traditional desktop or gateway protection; they can gain peace of mind and the reassurance that the problem is being addressed.

MessageLabs Intelligence

MessageLabs Intelligence is a respected source of data and analysis for email security issues, trends and statistics. MessageLabs provides a range of information on global email security threats based on live data feeds from our control towers around the world. The information relating to MessageLabs services contained in this report is based on data generated internally by MessageLabs unless otherwise indicated.
For more information on MessageLabs Intelligence and the analysis provided, please visit: www.messagelabs.com/intelligence

About MessageLabs

MessageLabs is the leading provider of messaging security and management services with more than 12,000 clients around the world. Delivered across an Internet-level, globally distributed platform, its fully managed services ensure the integrity of your electronic communications, helping organizations to manage and reduce risk while securing critical business infrastructure and information integrity. For more information on MessageLabs, please visit www.messagelabs.com.

www.messagelabs.com
info@messagelabs.com

Freephone UK
0800 917 7733

Toll free US
1-866-460-0000

Europe
HEADQUARTERS
1270 Lansdowne Court
Gloucester Business Park
Gloucester, GL3 4AB
United Kingdom

T +44 (0) 1452 627 627
F +44 (0) 1452 627 628

LONDON
3rd Floor
40 Whitfield Street
London, W1T 2RH
United Kingdom

T +44 (0) 207 291 1960
F +44 (0) 207 291 1937

NETHERLANDS
Teleport Towers
Kingsfordweg 151
1043 GR
Amsterdam
Netherlands

T +31 (0) 20 491 9600
F +31 (0) 20 491 7354

BELGIUM / LUXEMBOURG
Cullinganlaan 1B
B-1831 Diegem
Belgium

T +32 (0) 2 403 12 61
F +32 (0) 2 403 12 12

DACH
Feringastraße 9
85774 Unterföhring
Munich
Germany

T +49 (0) 89 189 43 990
F +49 (0) 89 189 43 999

Americas
AMERICAS HEADQUARTERS
512 Seventh Avenue
6th Floor
New York, NY 10018
USA

T +1 646 519 8100
F +1 646 452 6570

CENTRAL REGION
7760 France Avenue South
Suite 1100
Bloomington, MN 55435
USA

T +1 952 886 7541
F +1 952 886 7498

Asia Pacific
HONG KONG
1601
Tower II
89 Queensway
Admiralty
Hong Kong

T +852 2111 3650
F +852 2111 9061

AUSTRALIA
Level 6
107 Mount Street,
North Sydney
NSW 2060
Australia

T +61 2 8208 7100
F +61 2 9954 9500

SINGAPORE
Level 14
Prudential Tower
30 Cecil Street
Singapore 049712

T +65 62 32 2855
F +65 6232 2300