SPY-PHISHING – A NEW BREED OF BLENDED THREATS

Jeffrey Aboud
(Formerly) Trend Micro, Inc.

Jaime Lyndon A. 'Jamz' Yaneza
Trend Micro, Inc., USA

Email Jamz_Yaneza@trendmicro.com

ABSTRACT

In this age of broadband, wireless, and network interconnectivity, we enjoy the unprecedented power of information exchange and commerce at our fingertips. Networks and systems are continuously evolving to become more robust, thereby maximizing our convenience and productivity – 24 hours a day, seven days a week.

But along with the overwhelming benefits of all this phenomenal connectivity come numerous threats to computer security – causing lost productivity, breaches in data integrity, and confidentiality leaks, to name just a few. Indeed, the more uses we find for networks, the more incentive there will be for malware authors to seek out new ways to infect those networks.

One of the most striking threat developments to emerge from this proliferation of online commerce is the dawning of a category of threats broadly defined as 'crimeware'. The category includes spyware, phishing, pharming, and a host of other profit-driven attacks, and the number of new cases found in the wild each month is beginning to outpace that of traditional viruses. Though it can take numerous forms, the common thread that joins this category of threats is the motivation of the writer. In crimeware, the attack is profit-driven, with the attacker seeking financial gain, rather than the fame and notoriety that motivates most virus writers.

An emerging crimeware technique, which *Trend Micro* calls 'spy-phishing', is unique in the sense that, though it is crimeware, it also capitalizes on the trend of 'blended threats', which has previously only been noted in the traditional virus world.

Spy-phishing borrows techniques from both phishing scams and pharming attacks – along with some new tricks – to target online banks, financial institutions, and other password-driven sites. *Trend Micro* believes that spy-phishing is the next progressive step for phishers and spyware authors to lure money and personal information from unsuspecting users.

This paper will investigate spy-phishing, and explain: the various market and environmental factors that enabled it to emerge; what it is and why it is of concern; and why *Trend Micro* expects it to become a more significant threat over the next year.

BACKGROUND – HOW SPY-PHISHING CAME TO BE

Just like any other computer security threat, spy-phishing did not just appear out of nowhere. Instead, it is just another point on the overall threat landscape. In fact, one can trace the progression that led to spy-phishing to a number of specific evolutionary factors in the threat world. This includes the shift in the overall intention of malicious writers, in addition to a number of technological evolutions, including spyware, phishing and pharming.

Continuous evolution of the threat landscape

Over the past few years, the threat environment has evolved at seemingly breakneck pace by introducing more techniques and classifications of threats than ever. When viruses and other computer threats began emerging in the 1980s, threats occurred one at a time (and one type/family at a time), and utilized relatively simplistic techniques. In today's highly complex technological ecosystem, however, we face multiple threats – on multiple levels – employing a seemingly endless array of techniques.

Providing much of the fodder for this dramatic evolution in threats is the rise in e-commerce – from online banking and stock trading, to online shopping, to the electronic funds that quickly and efficiently fuel those transactions. This extraordinary growth in e-commerce has provided a 'target-rich' environment for those seeking to prey on unsuspecting victims. These criminals have evolved their security attacks to coincide with the technological advancements of the commercial world.

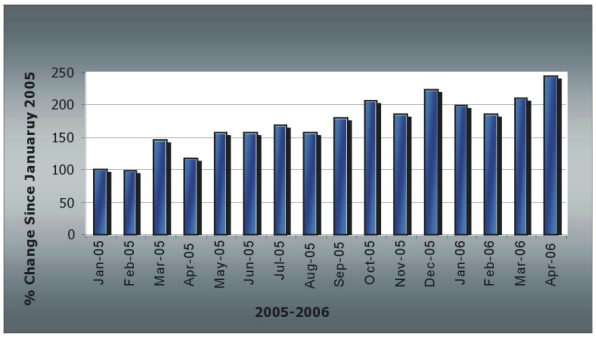
The security evolution of the 21st century – 'intent'

Perhaps the most significant evolution that has dramatically changed the threat environment is the *intent* behind malicious writers' crimes. Up until the past few years, malware writers developed their programs predominantly to show the world how smart they were. As such, most were bent on infecting as many users as possible, to claim some degree of notoriety – and therefore bragging rights. Many wanted to impress their friends and fellow writers. Others used their creations to 'battle' other writers, to prove their technical expertise – a kind of game, with computer users as the innocent victims. Today, however, fewer and fewer of these writers exist.

Instead, most writers have learned that there is a great deal of financial gain to be had in malware writing. Some develop their own spyware programs to steal credit card numbers, account log-ins, or a variety of other types of personal information; others develop and/or enhance bot networks, which are then sold or leased to other individuals or groups, to launch their malicious programs; still others 'phish' for personal information; the list goes on and on. Moreover, some of these writers are 'self-employed', attempting to use the data for their own purposes, while others are paid by crime groups to write and disseminate their malicious programs. Regardless of the category in which they fall, however, this 'new breed' of writer tends to behave in the opposite manner as do his predecessors. Instead of seeking fame and glory, these writers prefer to go unnoticed, favouring a series of relatively small infections, rather than one large-scale attack that attracts a flurry of attention. Many of these writers will even choose to employ small 'targeted' attacks as a technique, over that of spamming to the masses of users.

The growing spyware problem

Spyware is software that installs itself secretly on a user's computer and runs in the background, transparently logging



Source: Trend Micro

Chart 1: Trend Micro grayware index.

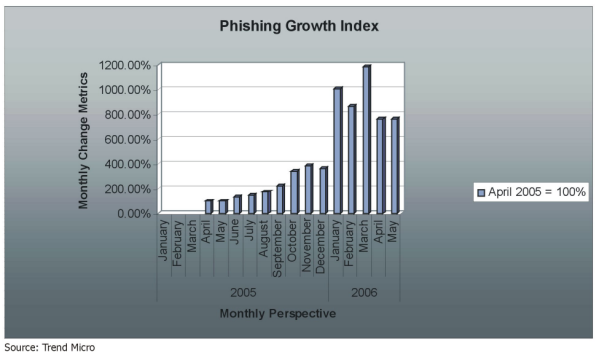
personal information such as user activity, web browsing histories, and online purchases. Though approximately 95 per cent of all spyware is considered to be 'nuisance spyware', utilized by advertisers to trigger pop-up ads, the remaining five per cent is still prevalent enough to be of concern. This is primarily due to two intersecting factors: first, though a relatively small percentage of the problem, five per cent still accounts for thousands of new spyware programs every year; and second, the fact that the sole intent of malicious spyware is to steal passwords, bank account information, credit card numbers, social security numbers, and any other form of sensitive information – then use that information for profitable purposes.

As Chart 1 illustrates, in addition to the growth rate of spyware, in general, *Trend Micro* has noted a marked increase in the number of password stealers downloaded – with the highest monthly increase in history recorded as recently as March 2005. This, coupled with the noticeable increase in downloaders and other 'delivery vehicles' for downloading new spyware, is a concerning trend.

The evolution of phishing attacks

Phishing is actually two online identity thefts used together. In phishing scams, the identity of the target company is stolen first in order to steal even more identities – those of unsuspecting customers of the target company. Modern-day phishing scams employ professional-looking, HTML-based emails that include company logos, font styles, colours, graphics, and other elements to successfully spoof the supposed sender – and a call to action that prompts recipients of the email to react immediately to correct the alleged problem.

As Chart 2 illustrates, phishing has increased more than 500 per cent over the past 12 months, with the average user being subjected to as many as 2,200 phishing scams per month.



Source: Trend Micro

Chart 2: Trend Micro phishing growth index.

More telling, however, is the way in which phishing has evolved over the past two years – into a professional-appearing, complex scam. The plain ASCII emails have largely been replaced by professional-looking, HTML-based emails that include font styles, colours, graphics and other elements to successfully spoof the supposed sender. Most also contain a link to a website, which is nearly always an exact replica of the spoofed site, thereby luring users into parting with their personal information. In many present-day phishing scams, the grammatical and spelling errors have ceased, now replaced with a polished, professional look and feel one would expect from a bank or other target of phishing attacks.

The harvesting of the information on the back-end has also become far more complex. Gone are the script kiddies who obtained a credit card number for their personal use. Current phishing scams utilize an organized and systematic means of gathering, collating and exploiting stolen information so as to maximize profit – lending credence to the belief of some industry experts that present-day phishing scams may be run by organized crime groups.

The stealth techniques of pharming

Pharming can be performed in a variety of ways, including DNS poisoning, domain hijacking, or URL hijacking (also known as URL redirection). Though nobody knows for sure how prevalent a problem pharming has become, most empirical evidence leads to the conclusion that the problem is relatively rare. However, regardless of their lack of prevalence, pharming techniques remain dangerous threats, due to their power and complexity, as well as the stealth nature of their activities.

There are two major ways in which pharming can be accomplished – DNS poisoning and URL hijacking. In 2005, when pharming was gaining some popularity amongst the press and media, as well as with some security vendors, DNS poisoning was really the topic of discussion – most likely because of its extraordinary level of technical difficulty, coupled with the fact that the attack was waged in an area previously assumed to be insurmountable. In DNS poisoning, the address is actually changed on the DNS server – so when the user types a 'legitimate' URL, he is sent elsewhere, once that URL is translated by the compromised DNS server.

Despite DNS poisoning's appeal in the prose, however, URL hijacking was becoming the more common attack. URL hijacking is typically performed via a trojan, which either adds a malicious bookmark to the user's system, or modifies an existing bookmark, so the user is redirected to a malicious website when he selects the bookmark he previously registered in his browser. But it can also be performed by malicious code running in the background of the user's system, which redirects URL requests to a disparate site. All of these techniques occur without the user's knowledge and, as with phishing attacks, redirect to a site that has been designed to look and feel exactly like the one the user intended to visit.

Other enabling technologies

In addition to the aforementioned technologies, two other significant factors have led to the occurrence of spy-phishing: the rapid increase in application and operating system

vulnerabilities – particularly in the *Microsoft Windows* environments – that have been discovered over the past 12 months; and the closing gap between the discovery of those vulnerabilities and the time corresponding exploits appear – including the notable swell in zero-day vulnerabilities discovered since the latter half of 2005.

The growing number of attacks on application vulnerabilities – particularly against published vulnerabilities in *Internet Explorer* – is a concerning trend. According to the *SANS Institute*, *Internet Explorer* vulnerabilities are responsible for many thousands of computers being infected with spyware and adware. In fact, the Institute has determined, there have been so many vulnerabilities that *Microsoft* has found it necessary to issue 'cumulative security updates' for *Internet Explorer* alone, three separate times in the past six months – in December 2005, February 2006, and April 2006.

In addition to this plethora of *IE* vulnerabilities, however, the past six months has also witnessed the rapid exploit of other critical vulnerabilities. The Windows Meta File (WMF) vulnerability discovered in the closing weeks of 2005 and the more recent *Windows* DOC vulnerability – both of which were exploited successfully to launch malicious attacks against scores of users – are two examples that underscore the need for more proactive measures to be taken.

As noted above, the vulnerability-to-exploit window is a major contributor to the problem – and of significant concern. In October 2000, MS00-0078 was announced, and 11 months later, the Nimda worm successfully exploited this vulnerability. Over the next five years, this gap has closed exponentially, to the point where in August 2005, MS05-039 was successfully exploited by the Zotob worm in just five days. Figure 1 highlights some of the major system exploits throughout this timeframe, and illustrates the shrinking vulnerability-to-exploit gap with each successful attack.

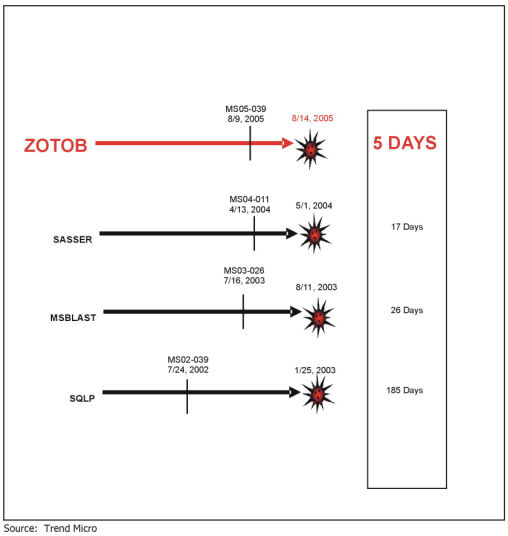


Figure 1: Historical timeline – vulnerability to exploit.

THE NEXT LOGICAL STEP IN THE THREAT LANDSCAPE

What is spy-phishing?

At its most basic level, the term 'spy-phishing' refers to a phishing attack that employs other threats, usually spyware and backdoor trojans. The term is by no means meant to replace existing threat categorizations. Rather, it is meant to add focus and clarity to a specific element of the larger threat category referred to as 'crimeware', which has gained popularity in the security industry over the past year. Crimeware is a rather generic industry term, frequently employed as a large umbrella definition to describe any threat that results in fraudulent financial gain, and is therefore by no means bounded to a particular type of threat. And since each security vendor – and even members of the press and media – employs the term divergently, it has become a term that begs some degree of sub-categorization, for the sake of clarity. Spy-phishing is one such sub-category.

Spy-phishing is a complicated phishing attack that also involves the use of various malicious applications, typically Trojan horses and spyware, to perpetrate online information theft. The most common targets are banking credentials, but this could easily escalate into proprietary and corporate information, as well. The downloaded applications sit silently on the user's system until the targeted URL is visited wherein it activates, sending the information to the malicious third party.

As its name would imply, spy-phishing is a blended threat, employing components of both spyware and phishing. It utilizes phishing techniques to initially present itself to users and typically engages a host of other techniques and exploits to surreptitiously download and install spyware applications in the background. These applications oftentimes download additional spyware applications to further extend their functionality.

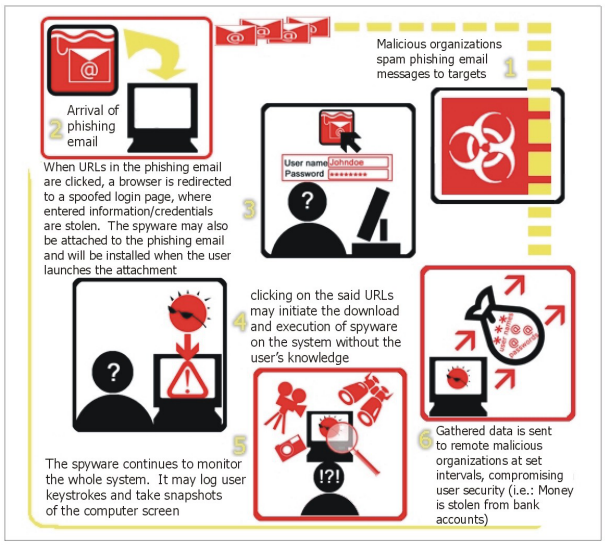
Why the extra steps?

Spy-phishing is obviously a more complex attack for the writer to launch than is traditional phishing, which begs the question 'why bother?' The answer lies primarily in the probability of success for each attack type. Though phishing scams have proven to be a successful form of crimeware, these attacks have a limited life span. Even if the recipient is successfully fooled with the initial email, phishing sites are relatively unreliable vehicles from which to launch attacks, since they become known quantities to law enforcement and the security industry, from the moment the initial email is discovered. As a result, they are frequently only intermittently available – and have an average life span of between two and five days, prior to being shut down permanently. Therefore, the payoff must be immediate, by tricking users into entering their credentials into the phishing site immediately.

But through the use of spyware and other trojans, spy-phishing attempts to prolong the initial phishing attacks beyond the point at which the phishing website is available – and avoids many of the complications with the forced instability of the sites during the course of their life span. Instead, the stealth installation of these trojans theoretically enables the attack to last indefinitely, since the trojan will continue to remain active for as long as it remains installed on the system. And since they were installed without the user's knowledge, they can theoretically remain installed for the life of the computer.

How does spy-phishing work?

As discussed earlier in this paper, spy-phishing borrows techniques from both phishing scams and pharming attacks



Source: Trend Micro

Figure 2: Behaviour of a typical spy-phishing attack.

– along with some new tricks – to target online banks, financial institutions, and other password-driven sites. In spy-phishing, the author seeds email messages with either a trojan or a link to download the trojan. When downloaded and executed, either manually or via an exploited vulnerability, this malware monitors web traffic until it detects web access to the target page. When this happens, it sends any login or confidential data back to the attacker. Figure 2 illustrates the behaviour of a typical spy-phishing attack.

The process of launching a spy-phishing attack can be broken into three distinct phases: the initial phishing email to lure the user; downloading of the trojan; and the ongoing monitoring and reporting functions of the trojan.

Figures 3 and 4 are real examples of a phishing email and its corresponding phishing website, taken from the *Trend Micro Phishing Encyclopedia*, which chronicles each phase in a bit more detail.

In this example, the phisher spoofs a bank and spams the message to thousands of users, in the hopes that some percentage of recipients will be customers of the targeted institution, and be lured into clicking the link, thereby visiting the phishing site. The trojan(s) reside on the phishing site and utilize HTML, browser, or other vulnerabilities to install on the user's system. In other cases, the trojan may be attached to the initial email itself, masked as account details, screen shots, or other content that may be of interest to the unsuspecting recipient. The advantage of this technique is that it bypasses the requirement for a phishing website, and therefore avoids the many pitfalls associated with these sites.

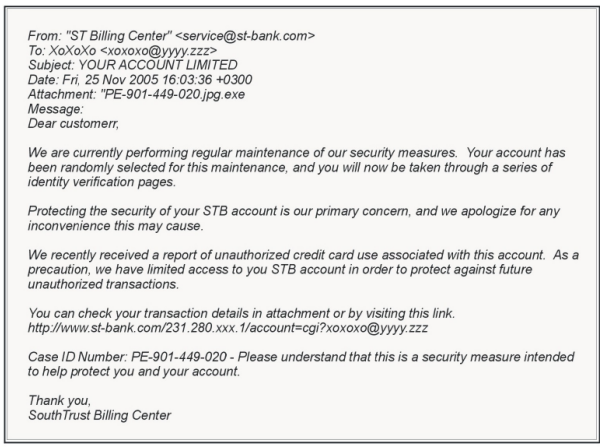
Traditionally, banks and other e-commerce institutions have been the initial victims of such scams. However, over the past year, more targeted attacks have gained in popularity amongst malware writers. As a result, the text in the spammed email need not be related to financial institutions. It can be related to the target individual, a group with known interests or hobbies, or a company. As such, the message may employ a variety of forms of social engineering, similar to those utilized for traditional viruses and modern-day phishing attacks.

Since in this example, phase 1 attempted to lure the recipient to a phishing website, the trojan resides there. Note that the information bar toward the top of the page, just below the address bar, prompts the user to install *Flash Player 8*. However, this application is not *Flash Player*. Instead, it is a spyware trojan, disguised as this legitimate ActiveX Control. If the user accepts the installation, the following code compilation will occur in the background, without the user's knowledge:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows NT\CurrentVersion\Winlogon\Notify\directut
DllName = "directut dll"
Startup = "directut"
```

It is important to note that in this case, there are actually two methods for potential theft – immediate and long-term. The user may enter his credentials directly as requested, in which case the theft occurs immediately. If not, however, the trojan that has now been installed will continue to monitor the user's system, looking for a future opportunity. This longer-term attempt is the subject of 'phase 3', which is detailed below.

Before detailing phase 3, however, two additional points should be made regarding the phishing website. First, notice



From: "ST Billing Center" <service@st-bank.com>
To: XoXoXo <xoxoxo@yyyy.zzz>
Subject: YOUR ACCOUNT LIMITED
Date: Fri, 25 Nov 2005 16:03:36 +0300
Attachment: "PE-901-449-020.jpg.exe
Message:
Dear customerr,

We are currently performing regular maintenance of our security measures. Your account has been randomly selected for this maintenance, and you will now be taken through a series of identity verification pages.

Protecting the security of your STB account is our primary concern, and we apologize for any inconvenience this may cause.

We recently received a report of unauthorized credit card use associated with this account. As a precaution, we have limited access to you STB account in order to protect against future unauthorized transactions.

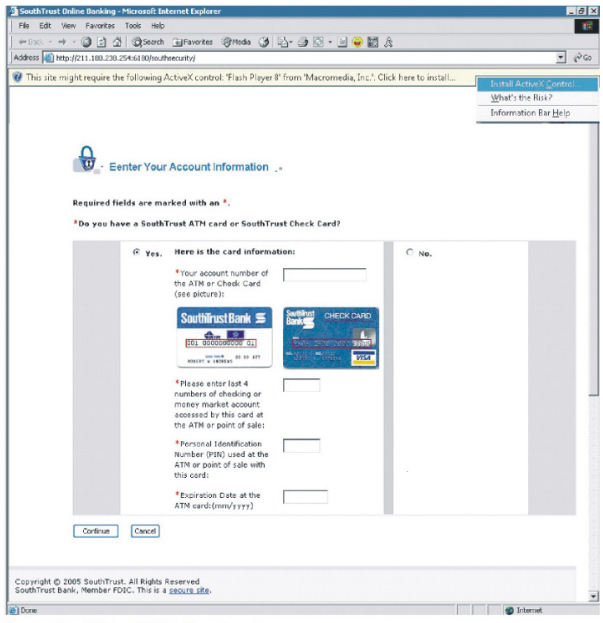
You can check your transaction details in attachment or by visiting this link.
http://www.st-bank.com/231.280.xxx.1/account=cgi?xoxoxo@yyyy.zzz

Case ID Number: PE-901-449-020 - Please understand that this is a security measure intended to help protect you and your account.

Thank you,
SouthTrust Billing Center

Source: Trend Micro Phishing Encyclopedia

Figure 3: Phase 1 – the phishing email.



Source: Trend Micro Phishing Encyclopedia

Figure 4: Phase 2 – dowloading of the trojan.

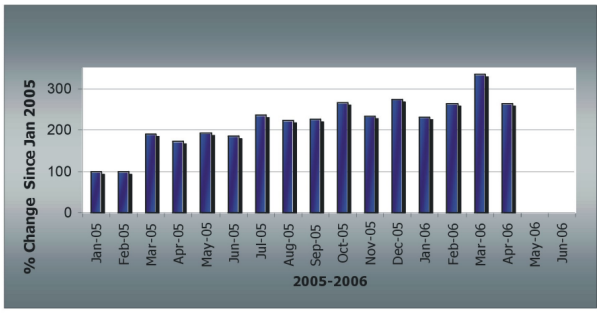
the authentic-looking site above, including the use of the financial institution's type faces, logo, and even legal attribution language, to make the site appear genuine. As noted earlier in this paper, the professionalism with which the modern-day phisher approaches his work can fool even the most savvy of users. Second, the information bar that prompted the user to install the bogus ActiveX Control can easily be circumvented in many cases, by employing a well known vulnerability in many versions of *Internet Explorer*. When this vulnerability is exploited, the browser's warnings are bypassed altogether, and the trojan may be installed automatically, with neither the permission from, nor the knowledge of, the user.

Once the trojan is installed, the third and final stage can occur. In phase 3 of the above example, the dropped file ('directut.dll') monitors every instance in which the user visits the *legitimate* banking site. At some point in time it even downloads other components from the Internet to take randomly timed snapshots of the victim's screen and sends this data to a predefined email drop.

This final step is crucial to the success of the attack, since it is responsible for the continuation of the attack, up to *years* after the point at which a traditional phishing attack would have permanently been neutralized. It is also this step which preys on the user's everyday online activities – at legitimate commerce sites.

HOW PREVALENT IS THE PROBLEM?

As with traditional phishing attacks, the specific incidence of this threat will vary widely by user. However, according to data collected by *Trend Micro*, as well as a number of supporting industry collections, the amount of trojan spyware such as that employed in spy-phishing attacks has been increasing steadily over the past year. According to the *Trend Micro Trojan Spyware Index*, illustrated in Chart 3, the incidence of trojan spyware has increased by over 250 per cent over the past 16 months.

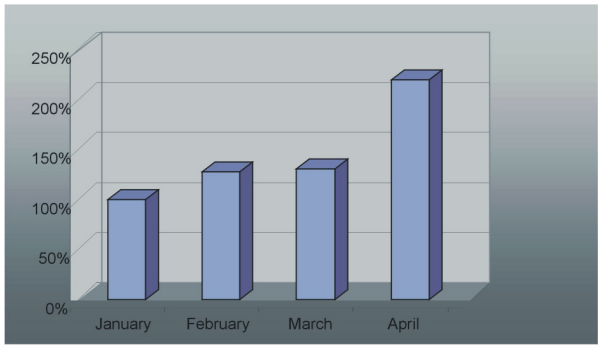


Source: Trend Micro

Chart 3: Trend Micro trojan spyware threat index.

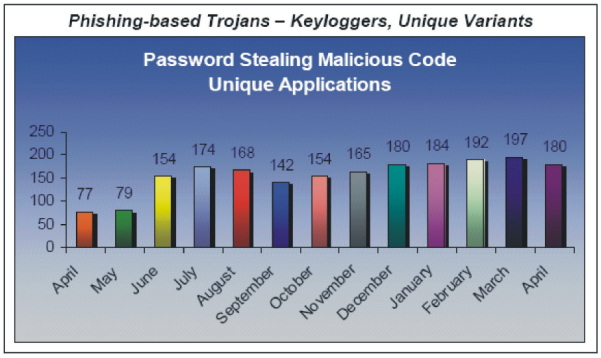
Trend Micro's data can be supported by looking at similar statistics from *CERT Australia*, on recently reported phishing attacks over the first two quarters of 2006. Utilizing that data, *Trend Micro* calculated the aggregated growth of spy-phishing components that include various threat types such as viruses and worms, trojan backdoors and droppers, spyware and keyloggers. The result of this analysis is illustrated in Chart 4.

Similarly, according to the 2006 report published by the *Anti-Phishing Working Group* (*APWG* http://www.apwg.org/), and illustrated in Chart 5, an average of more than 188 new samples of trojan spyware have been utilized in spy-phishing



Trend Micro Analysis, Using CERT Australia Source Data

Chart 4: Aggregated spy-phishing component growth, using CERT Australia data.



Source: Anti-Phishing Working Group (APWG)

Chart 5: APWG statistics on unique trojan spyware samples.

attacks each month in the first four months of 2006 – a 234 per cent increase over the same period in 2005.

POSSIBLE APPLICATIONS – WHO IS AT RISK?

Perhaps the most concerning aspect of spy-phishing is its wide variety of potential uses by malicious authors. As with traditional phishing attacks, consumers and other individual end-users are an obvious target – but the potential uses for spy-phishing technologies and techniques transcend this group. In addition to them, businesses of all sizes are also potentially at risk, as spy-phishing can also just as easily be utilized for corporate espionage. In fact, due to the trojan components – and the long-term, stealth capabilities they typically employ – the threat to sensitive corporate information is perhaps greater than is the risk to the individual, if only due to the magnitude of the potential for loss.

As discussed throughout this paper, the key differentiator with spy-phishing versus traditional phishing and other types of security threats is the long-term repercussions of a successful infection. Virus payloads tend to be swift and immediate, but are eradicated within hours; spam is a nuisance, with no permanent repercussions; 95% of spyware, though intrusive, is non-malicious in nature; traditional phishing attacks are unstable and have a limited life span, relying largely on websites that can be traced and disabled within days; pharming attacks are too technically complex for most malware writers to execute successfully – and DNS servers are reset every 24 hours, thereby dramatically limiting the window of opportunity for thievery.

But spy-phishing combines phishing techniques with *malicious* spyware, with the intent of stealing sensitive personal or corporate information; it can be spammed to tens of thousands of users, or targeted to a small, identifiable group; it can utilize a website to install the trojan(s), or the trojan(s) can be attached to the email, itself; the trojan can target one specific site, or be written to cast a wider net, to activate when any number of targeted sites are visited by the user.

Most importantly, for purposes of determining who is most at risk of this type of attack, the flexibility afforded to the writer enables the spyware to target a wide array of potential victims. Most malware today is written in modular format, with an extraordinary amount of malicious code freely available on the Internet for fast and easy replication. Thus, a malicious writer need only take the base code – or even 'mix and match' modules from a variety of sources – to develop a new threat.

Spyware modules and payloads are no different. A keylogger can be easily programmed to capture a wide range of information, and the trojan can be programmed to sit silently on the user's system, activating only when a predetermined target site is visited. This, coupled with the fact that with a little social engineering the attack can target a multitude of individual or corporate end-users, makes the potential target pool theoretically limitless. Therefore, though online banking and other e-commerce providers are typically perceived to be the primary targets today – and thus far these institutions have indeed been the primary victims – corporate financials, business strategies, and other proprietary information are every bit as much at risk from a spy-phishing attack.

SECURITY GUIDANCE

It is important to reiterate that spy-phishing, though a relatively new threat with its own set of techniques, is yet another point on the overall threat landscape. And, as with any security threat, there are a number of precautions all users – from enterprises to consumers – can take to help protect themselves from this threat.

Corporate users and IT staff

- **Keep your security definitions updated.** Set pattern updates to daily. This is your first line of defence against viruses that can also be hosted on web pages. Many vendors even provide beta definitions with the same quality as the daily download. These should be applied when the threat is particularly severe.
- **Make sure your security product is complete.** Regardless of the security provider you use, they should offer a comprehensive, *integrated* suite, which includes multiple layers of protection – from the gateway, to the server-level, to individual clients. If laptops and other removable devices that can be taken home are part of your network configuration, it is absolutely essential that your security solution also includes a built-in client-side firewall and an anti-spyware engine, to prevent spyware, backdoors and bots from entering your network when the removable devices are reintroduced to your network. In the age of VoIP, VPN, mobile and cellular devices with network and WiFi capability, border security has been reduced to a myth.
- **Ensure that your anti-spyware solution is robust.** A solid anti-spyware product will check your *Windows* startup and Registry to ensure your entries are qualified and will block attempted spyware installations. As with your larger security solution, make sure you set definition updates to daily.
- **URL filtering.** Make sure either your anti-virus or anti-spyware product has a URL filtering feature to prevent accidental clicks on known malicious sites. A substantial reduction in this risk can be attained by utilizing IP Reputation Services, which reside at the gateway.
- **Be cognizant of ActiveX exploits.** As with HTML, ActiveX controls are wonderfully user-friendly – but they are also rife with vulnerabilities. Consider either turning off ActiveX in your browser, or installing a browser plug-in that will display the true address of the page being viewed. Another helpful add-on would be one which prevents HTML scripts from running without the user's consent. When *Windows Vista* is released, it promises to resolve this vulnerability by separating ActiveX dependency from the browser.
- **Educate your users.** As technical users and IT staff, the education you provide your users is the first – and *best* – line of defence you can provide your network and clients. Be sure your users are familiar with security best practices, as well as your company security policies. It is also prudent to ensure that they understand some of the warnings their security product will provide them, and what these warnings mean (including what actions, if any, they should take when they are presented with such a warning). A non-exhaustive list of end-user security precautions is provided in the section below.
- **Take central control.** Employ group policies to limit access to critical services, thereby limiting the potential for damage. Additionally, physically and logically segregate access points and install Network Access Control (NAC) services to ensure all users follow a base model of security.

Consumers and other end-users

- **Scrutinize every email.** The vast majority of all email is innocuous, and much of it is necessary for effective, efficient communication in the information age. However, it is also important to remain vigilant and to pay special attention to emails containing attachments, or those from unexpected or unknown sources. And, due to spoofing capabilities, it is essential to scrutinize even mail that apparently has come from a *known* source, if the contents of that mail seem out of character or untimely for that source.
- **Know your bank's communication policies.** It is crucial to remember that embedded attachments and links are a tried and true social engineering technique – and that banks and other legitimate e-commerce institutions almost *never* communicate this way! Therefore, avoid the urge to use these 'conveniences'. If you have any reason to believe that an email communication may be authentic, take the extra time to enter the institution's URL (the one you know – *not* the one embedded in the email!) directly into your browser. And they *absolutely*

would *never* include sensitive information via an attachment. This information can only be gained by signing-on or calling the institution.

- **Ensure that your system and your applications have the latest patches installed.** If available, use the automatic update settings and choose a daily off-peak schedule. This prevents most common exploits from being used against you.
- **Ensure that your security solutions are fully updated.** To remove the manual burden of doing this, most antivirus companies offer an automated update option within their security product.
- **Configure your email client to display plain-text only.** Avoid HTML formatted mail – though it makes for more attractive mail, HTML also carries a wide range of inherent vulnerabilities that are easily exploited by malicious authors. Switching to plain-text or rich text-formatted mail may lack some of the ease of use, but it is one of easiest ways to avoid malicious scripted mail.
- **Avoid providing unnecessarily personal information online.** Much of this information is necessary to conduct legitimate e-commerce transactions. However, these legitimate sites will also employ security measures such as secure socket layer (SSL) protection. The URL for these sites will typically be denoted with 'https://', as well as some graphical representation that the site is secure (such as a padlock).