



**IBM Internet Security Systems X-Force®
Research and Development Newsletter**

January 2007

Phishing at High Tide

Happy Birthday Phishers

January marks the 11th birthday for the threat commonly referred to as 'phishing.' In that 11-year period, we've observed a threat whose growth has left Moore's Law in its wake; following a parallel trajectory that matches the exponential rise of spam. While the term 'phishing' has evolved from e-mail solicitation to encompass an entire category of related threats (e.g. pharming, vishing, 'spear phishing,' etc.), the most popular and successful vector is still delivered personally via the inbox.

"It used to be that you could make a fake account on AOL so long as you had a credit card generator. However, AOL caught on and now verifies every card with a bank after it is typed in. Does anyone know of a way to get an account other than phishing?"

—The first public acknowledgement of 'phishing' – mk590, "AOL for free?" alt.2600, January 28, 1996

At its heart, phishing is about socially engineering a message recipient into providing personal or confidential information that can later be used by the phisher to conduct fraudulent activities. The methods used by the phisher to coax the information from their victims are as many as they are varied, but the most commonly encountered vector is through an e-mail that appears to be from the victim's bank. The e-mail purports a problem with the victim's account, which requires them to follow an embedded URL that takes the victim to a fake instance of the bank's Web site. There the victim is prompted to 'login' with their confidential authentication details – thereby enabling the phisher to steal a copy of the victim's login details.

As with all contemporary Internet threats, phishers are well organized and are constantly evolving and improving their techniques – trying to stay one step ahead of both their intended victim and the security products deployed to thwart them. Phishers have adopted cutting-edge malware

technologies, exploit public and private vulnerabilities, manipulate DNS servers around the globe, purchase expired domains to influence page-ranking of search engines, make use of new communication channels (e.g. Instant Messenger,

Internet Telephony, Virtual Chat, etc.), and tune their delivery for specific organizations and people. Don't underestimate the criminals behind the threat; phishing is a very successful business.

With all that in mind, what advances does the future hold for phishing attacks, and how will that influence protection strategies?

A High Tide

With more than a decade of technical innovation already under their belts, phishers will inevitably continue to advance their trade into the future. In the short-term (i.e. the next two years) we can expect phishing to evolve in the following ways:

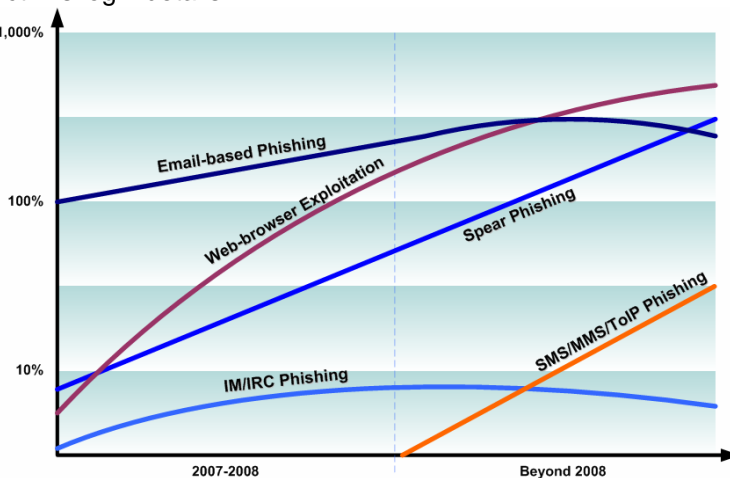
- There will be a greater shift towards the use of exploit material within message payloads in order to compromise the host and ensure successful installation of malware agents.
- Phishing e-mails will likely continue to mimic the exponential growth of spam; employing many of the same antispam bypass techniques and maintaining the same phishing-to-spam ratio.
- Payload and exploit obfuscation will advance and mature. By 2008, the majority of client-focused exploitation will utilize advanced obfuscation techniques designed to bypass static signature-based protection systems.
- More advanced social engineering will be used in phishing e-mails – with an emphasis on linking to timely events (e.g. sporting events and disasters).
- Non-English speaking countries will increasingly be targeted by phishers using the local language.
- Fake Web sites used by phishers will more frequently be hosted in environments where the phishers can control dynamic DNS entries as well as host multiple, fake virtual Web sites upon compromised hosts.

• The percentage of phishing attacks that utilize custom malware for a specific targeted audience will continue to rise and will likely constitute upwards of 10-20 percent of all phishing attacks.

• Phishers will increasingly target Web-browser vulnerabilities as they provide a reliable infection vector. The increase in "managed

exploit providers," developing off-the-shelf exploits will further drive this phishing vector.

- Advances in IM/IRC/P2P phishing techniques and compromises are expected in 2007, but will probably dwindle by 2008.



- Phishers will increasingly utilize “secure” communication protocols to send their messages and host Web sites (SMIME, SSL, HTTPS) – thereby lending a false sense of security to their targets and future victims.

Beyond 2008

While protection technologies will have advanced, in a future beyond 2008 we can still expect to see phishing as a major threat to organizations. The technologies and techniques used by phishers will continue to build upon the knowledge and successes of each passing year. As such, we anticipate the phishing threat evolve in the following ways:

- Phishing e-mails will continue to be more sophisticated from a social engineering perspective, and piggyback upon the advances made in spam technologies.
- Generic e-mail-based phishing will continue to be replaced by targeted ‘spear phishing’ messages as a preferred route to reach the victim – most likely including custom content-level payloads (e.g. office documents) that were originally sourced from within the targeted organization.
- DNS entries will be tuned on a one-for-one basis to the potential victim – thereby making it much more difficult to investigate a phishing attack or Web site once the victim has visited it once. This will be consistent with the polymorphic approach to attack personalization observed in browser-based exploitation.
- Web-based phishing delivery will take precedence over e-mail-based delivery as antispam and anti-phishing technologies finally make it a less successful attack vector.
- Phishers will begin to actively exploit “softer” message delivery vehicles such as SMS, MMS and Telephony over IP (ToIP) while the protection against classical e-mail and Web delivery vehicles are still maturing.
- The addition of Internet proxies within malware will accelerate and become a standard component of phishing attacks – thereby helping the phisher to overcome any client authentication processes.
- Command and control, along with information ‘extrusion’, will switch to encrypted communication channels in order to bypass perimeter detection systems.

Protection Priorities

Obviously, as the phishing threat evolves, so too will the protection systems deployed to either prevent or marginalize the threat. Organizations that invest in robust defense-in-depth strategies will (continue) to feel the least amount of pain from phishing attacks.

What are the most important protection technologies in combating phishing? As we commence 2007, the top five most successful protection technologies are:

1. Antispam e-mail filtering
2. Behavior-based malware detection systems
3. Signature-based antivirus systems
4. URL content filtering
5. Attachment blocking

Over the next few years, we can expect more advanced, dedicated, anti-phishing technologies to appear and combat the advances of phishers – eventually making it an unprofitable business model for criminals to pursue. However, the social engineering aspect of this class of threat means that the phishers will likely always find a victim somewhere.

– Günter Ollmann, Director of Security Strategy

The Wilted WildList

Malware yardstick showing its age

For several years The WildList, compiled by The WildList Organization International (<http://www.wildlist.org/>), has been used as one of the industry benchmark test sets for validating antivirus (AV) products. Although never intended as the sole test set for AV products, regardless, a significant amount of emphasis has been placed on The WildList by the industry. As an example, the Checkmark certification program by West Coast Labs (<http://www.westcoastlabs.org/>), one of the most widely recognized standards in measuring AV performance, is solely based on WildList coverage. Unfortunately, The WildList, while important, can no longer serve as an accurate, sole indicator of AV protection capabilities.



The WildList began as a list created by Joe Wells, from a collection of reports of viruses found spreading in the real world that he had gathered over several years. The first official list was published in November 1993 and, after going through several years of refinement and standardization, The

WildList Organization International was formed to protect the integrity of The WildList and develop it further. The WildList went on to become the world’s foremost authority on viruses that are cause for concern based on their status of being ‘in the wild.’ The list is updated once per month by a team of volunteers (of which IBM Internet Security Systems

is a contributor), and administered by The WildList Organization International. For a virus to be considered 'in the wild,' it must be reported by at least two reporters, which acts as evidence that it is most likely spreading as opposed to merely existing. Viruses that exist in multiple locations but are not spreading (e.g. proof-of-concept malware, samples that were traded amongst AV vendors, etc.), are not considered 'in the wild.'

As the malware threat landscape continues to be driven with financial gain in mind, malware that no longer self propagates or replicates has become increasingly popular. Designed to "stay under the radar," malware is once again trending back towards the classically defined Trojans, adware, spyware, backdoors, etc. – much of which is custom designed for use against a particular organization or group of potential victims.



While protection is critical for these threats, they are not included as part of The WildList. It was for this reason that AV-Test (<http://www.av-test.org/>), a leading independent antivirus testing organization, recently conducted a

large test of 32 AV products using data more representative of today's threats. This continuously updated and live data extends far beyond the 1,000 or so viruses and worms that form the basis of The WildList, and comprises of close to 300,000 samples of backdoors (20%), bots (25%) and Trojans (50%).

The results of these first tests were surprising to the industry at large, most of which were previously accustomed to seeing AV vendors scoring 100 percent of The WildList.

Such a result is easy to accomplish given the relatively small size of The WildList data set and the fact that it is generally available in advance of the tests. Most surprising to the industry were the relatively poor scores of AV vendors who have been active in the field for more than a decade.

This serves as a firm indication that it is becoming increasingly difficult for signature-based AV solutions to keep pace with new malware outbreaks, further elevating the importance of behavioral-based AV technologies.

The top three 'products' out of the 32 evaluated were WebWasher (by Secure Computing), followed by AntiVir (by Avira) and finally AVK (by G-Data). Both



WebWasher and AVK are products that employ multiple AV engines (i.e. utilizing the AV solutions from multiple vendors and combining their output into a single protection offering), with WebWasher using both AntiVir and Secure Computing's own engine, and AVK using engines from BitDefender and Kaspersky.

This particular test therefore highlighted AntiVir as the superior individual engine. Further, it also highlights the misconception created by the AV industry about the validity of coverage against The WildList and it also exposes the trend towards multi-engine AV products.

Such a trend is consistent with the combination of signature-based AV with our behaviorally-based Virus Prevention System (VPS) within IBM ISS Proventia® Desktop Endpoint Security, which unfortunately wasn't available for these first tests. Indications are that had this product been included in the test, it would have received a very high ranking. This will inevitably be confirmed in future tests which in turn will highlight IBM ISS leadership in the protection of the broader malware threat space that typifies the threats of today – threats that extend far beyond The WildList.

– Vernon Jackson, Manager X-Force VPS Team

A Month in Review

In this section of the newsletter, X-Force briefly covers some of the security content developed or processed in the month of December 2006.

Vulnerabilities:

The 12 months of 2006 saw vulnerabilities increase by 39.5 percent over the previous year, reaching a staggering 7,247 new security vulnerabilities – the highest year on record. But it wasn't all bad news.

Looking closer at the security risk these vulnerabilities would typically introduce, it was quite noticeable that independent bug hunters had advanced the technology of 'fuzzing' and uncovered many content-level flaws – vulnerabilities typically classed as medium risk. Consequently the proportion of high impact vulnerabilities actually decreased in 2006 when compared to any previous year.

	Reported					YTD
	Crit.	High	Med.	Low	Total	
Dec	1	113	334	118	566	7247

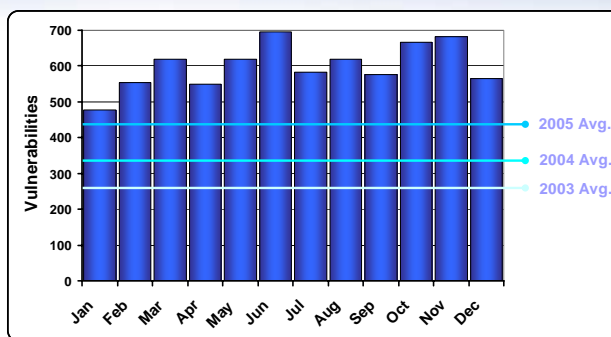
Of these vulnerabilities, 525 were remotely exploitable, 50 could only be exploited locally and

nine could potentially be exploited both remotely and locally.

Vulnerability Breakdown	
Bypass Security	32
An attacker can bypass security restrictions such as a firewall or proxy, an IDS system or a virus scanner.	
Data Manipulation	73
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
Denial of Service	67
An attacker can crash or hang a service or system, or take down a network.	
File Manipulation	9
An attacker can create, delete, read, modify or overwrite files.	
Gain Access	288
An attacker can obtain local and remote access. This also includes vulnerabilities in which an attacker can execute code or execute commands, because this usually allows the attacker to gain access to the system.	
Gain Privilege	14
An attacker can gain privileges on the local system only.	
Obtain Information	63
An attacker can obtain information such as file and path names, source code, passwords or server configuration details.	

* Right-hand column represents unique vulnerability count

Vulnerabilities per Month vs. Annual Average



Top 5 Vulnerable Vendors	
Microsoft	21
Mozilla	13
IBM	11
Apple	11
Novell	10

* Right-hand column represents unique vulnerability count

Sample Harvesting:

It is worth noting that as part of X-Force's continued strengthening of IBM Internet Security Systems antivirus, anti-spyware and anti-malware protection, we investigated and added another 62,022 new samples to our malware zoo this month.

Copyright© 2007 IBM Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, Proventia, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of IBM Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owner and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.