



X-Force[®] Research & Development Newsletter

March 2006

 INTERNET|SECURITY|SYSTEMS[®]
Ahead of the threat.[™]

Happy Birthday Phishers

2006 marks the 10th anniversary of the first public acknowledgement of a Phishing attack. Way back in 1996, the objective of a phisher was to obtain AOL authentication credentials and higher download quotas, but it was not until March 1997 that the term “phishing” was publicly coined in a popular computing magazine. A lot of things have changed since then.

In the last 10 years we have seen phishers utilize e-mail spam engines, IRC or IM channels, Web banner advertising and even bulletin boards in an attempt to drive potential victims to fake or malicious Web sites. What began as an annoying “geek” theft of login credentials has now developed into a highly organized international business — complete with specialist tools, money laundering, international bank transfers, credit card manufacturing and identity theft.

In 2001, as organizations were being swamped with e-mail, the phishers focused upon slipping their fake messages past antispam filters and using obfuscated URLs embedded within HTML e-mails to fool recipients into visiting fake Web sites which would capture their banking credentials. For several years the e-mails became more and more sophisticated — using ever more devious technical tricks to fool recipients. Success figures as high as five percent were often quoted — meaning that one in 20 of all phishing e-mails sent, fooled the recipient into following an embedded link and submitting his or her authentication details.

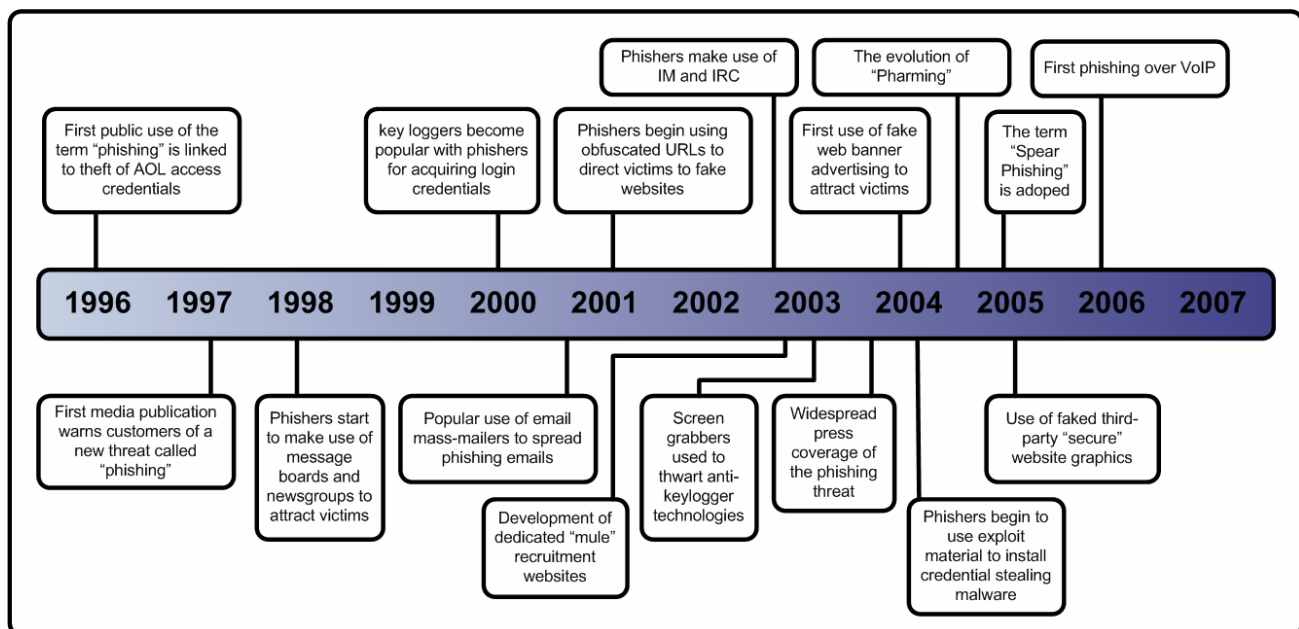
While it has been only a few years since phishing attacks first became front-page news, phishers’ use of sophisticated attack vectors has advanced

considerably. Manipulation of DNS records, such as changing IP address resolution information for popular Web sites to hosts that the phisher controls at an ISP level, have led to the new term “Pharming” and regional targeting of victims. Focused phishing attacks known as “Spear Phishing” — utilizing custom Trojans, keyloggers and restricted distribution lists (for example, e-mail recipients are all known to be customers of a particular organization or belong to a small regional ISP) — have made it almost impossible for legacy signature-based systems to provide preemptive protection.

Now, 10 years after the first acknowledgement of phishing, the expectation is that attacks will continue to evolve. Phishers will make use of each new popular electronic communication protocol to socially engineer message recipients into surrendering their identity and authentication details.

X-Force researchers continue to monitor the phishers and their techniques. Based upon past adoption tactics, phishers are likely to take full advantage of the increasing global use of VoIP in both commercial and domestic environments, along with the anonymity that VoIP can provide. It will be interesting to see what this vector gets called by the media — since all the previous vectors begin with a “ph”, are we looking at “Phiting” (Phishing over IP Telephony), “Phreaking” or something else entirely?

-- Gunter Ollmann, Director of X-Force



Threat Research

VoIP Protocols

Voice over IP (VoIP) is an important technology that X-Force has been researching for several years now as part of its operational strategy in keeping ahead of new threats. It is exciting to imagine a future in which our voicemail systems are integrated with our e-mail systems; where we have intelligent call filtering that can send nuisance calls to voicemail or direct emergency calls to us no matter where we are. It now costs the same to make a long distance phone call or hold a teleconference as it does to send an e-mail or instant message. Unfortunately, as with any complex new technology, VoIP also provides new attack vectors for malicious intruders.

There are two enterprise-class protocols for VoIP: SIP and H.323. Protocol H.323 was designed according to traditional telephony standards and mimics the structure of Integrated Services Digital Network (ISDN), an early digital telephony protocol. SIP was designed by the Internet Engineering Task Force (IETF) with the Internet in mind and incorporates specific features, such as the ability to employ e-mail-style addressing instead of traditional phone numbers.

Both standards suffer from being extremely complex. Call setup and voice content are transmitted using completely distinct protocols that operate on separate TCP or UDP ports, many of which are dynamically assigned for every call. There is an advantage to transmitting call setup separately from call content, as traffic traveling to the directory servers that perform call setup might follow a different route through the Internet from voice information intended for a phone. However, the complexity of these designs is a nightmare from a network security standpoint.

Firewalls need to parse SIP and H.323 packets to determine what ports to open dynamically for voice content. If a network administrator tries to encrypt the call setup packets, this will interfere with the firewall's ability to open these ports dynamically. There has been a mishmash of different security standards and protocols intended to work around these problems that do not work well together. Furthermore, H.323 packets are encoded with the infamous ASN.1 encoding scheme, which is very difficult to parse. This has led to remote code execution vulnerabilities in a wide array of H.323 systems as well as in firewalls that parse H.323.

Even more troubling is the typical company's local network environment in which these protocols run. Encryption and strong authentication are rarely used internally because the standards are still emerging and the performance impact can reduce quality of service. Individual telephones are usually

authenticated by an Ethernet MAC address. X-Force Research has given demonstrations illustrating the weakness of this environment. One local network inserted audio into an executive's telephone calls; another caused all of the telephones in an office to ring simultaneously. Just as in the movie "Lawnmower Man," a convenient message about Viagra could be displayed on the caller ID screen. Imagine being able to launch a denial of service attack against the CEO's telephone and then spoofing his MAC address so the intruder starts to receive all his phone calls. "Hello, Tom Noonan speaking" It can be done. X-Force researchers have seen this sort of attack successfully performed against real VoIP networks in penetration testing scenarios.

X-Force Research will continue to study these threats and develop more knowledge that can feed back into its protection technology. The goal is to enable ISS customers to embrace Voice over IP without fear that it will bring their businesses grinding to a halt.

-- Tom Cross, X-Force Advanced R&D

Malcode Corner

Double Trouble: Wireless Infection via Bluetooth and Multimedia Message Service (MMS)

Wireless malcode is becoming an increasingly popular threat vector. It has the potential to make today's mass-mailing worms seem relatively restrained. Mobile security threats are expected to continue to rise in 2006 as smart phones and other mobile devices become more prevalent. It is believed that the "I Love You" worm that infected tens of millions of PCs in just a few hours in 2000 would have spread wider and faster in smart phones, possibly infecting up to 200 million devices. The wireless propagation mechanism is relatively new and most handheld devices do not have antivirus filtering.

The first known cases of malware for mobile devices appeared in late 2000 targeting Palm devices. Then around the middle of 2004 came the release of proof-of-concept viruses for both Symbian smart phones and Pocket PC PDAs and phones. By the end of 2004 there were about 26 known viruses targeting mobile devices, including a Trojan embedded in a cracked version of a game called Mosquito that sent short message service (SMS) messages at premium rates while the game was being played, and a virus called Skulls which overwrote icons with a skull-and-crossbones image.

In March 2005 the first mobile phone virus capable of replicating via MMS messages was discovered: known as Commwarrior-A, it targeted Symbian

Series 60 phones. The ability of Commwarrior-A to spread over both Bluetooth and MMS really meant double trouble. Mobile phone viruses could not only infect devices within close proximity of the infected phone, but could also spread rapidly around the world like an e-mail worm.

As mobile malware continues to rise, additional variants of existing families are being discovered, as are new families that use new infection vectors. Examples of this over the last few weeks are a new Commwarrior-D variant, as well as two brand-new wireless infectors. One is a new proof-of-concept "crossover" virus designed to jump from PC to handheld. As reported by the Mobile Antivirus Researchers Association (MARA)*, this crossover virus is the first to be able to infect both a Win32 PC and a PDA running Windows Mobile for Pocket PC. When running on the PC, the virus detects the connection to the handheld, and uses ActiveSync to cross-infect the handheld. Once running on the handheld, it begins to erase files.

The second new threat discovered was a Java Trojan called RedBrowser.A, which is the first malware to infect not only smart phones but any mobile phone running Java applications using J2ME.

PCs have become increasingly protected these days, so malware writers are fast turning to wireless devices. Most users currently consider wireless inherently immune, just as PCs were thought to be 20 years ago. By the end of 2005, the number of known viruses targeting handheld devices had increased more than fivefold, to approximately 142. The extent of further increases over the next 12 months will depend largely on the speed at which smart phones gain popularity, the growth in the use of these devices to transfer data, the convergence of mobile platforms and the relative speed at which both device- and network-based filtering is put in place by mobile carriers.

-- Vernon Jackson, X-Force VPS Manager

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 February 2006.

Vulnerabilities:

Last month saw 555 new vulnerabilities being disclosed, processed and analyzed by X-Force. This represents a 47 percent increase compared with February last year.

Overall, thus far in 2006, X-Force has covered 30 percent more vulnerabilities than for the same period in 2005.

	Reported					YTD
	Crit.	High	Med.	Low	Total	
Feb	0	85	324	146	555	1034

Of these vulnerabilities, 491 were remotely exploitable, 75 could only be exploited locally and 11 could potentially be exploited both remotely and locally.

Vulnerability Breakdown	
Bypass Security	36
An attacker can bypass security restrictions such as a firewall or proxy, and an IDS system or a virus scanner.	
Data Manipulation	88
An attacker is able to manipulate data stored or used by the host associated with the service or application.	
Denial of Service	77
An attacker can crash or hang a service or system, or take down a network.	
File Manipulation	11
An attacker can create, delete, read, modify or overwrite files.	
Gain Access	224
An attacker can obtain local and remote access. This also includes vulnerabilities where an attacker can execute code or execute commands, because this usually allows the attacker to gain access to the system.	
Gain Privilege	31
An attacker can gain privileges on the local system only.	
Obtain Information	61
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

Top 5 Vulnerable Vendors	
Microsoft	29
Linux Kernel	14
Mozilla	12
IBM	11
myBB	9

* Right-hand column represents unique vulnerability count

Malcode:

In February, the X-Force alpha-testing platform for the Virus Prevention System (VPS) (codename Catfish) identified four unique zero-day (0-day) malware attacks — before any other antivirus vendor.

Two of these unique 0-days were brand-new Bagle mass-mailer variants, one was a new IRC Bot related to family of variants reported in last month's newsletter, and the final 0-day malcode capture was a new family of backdoors with rootkit capabilities.

X-Force Security Content:

	Level-0	PAM Sig.	PAM Blocks	IS	ES
Jan	0	15	10	0	0

Level-0 XPU:

In February the X-Force team did not need to respond to any level-0 vulnerabilities or their public exploits. The team remained *Ahead of the threat*.

Extended Protocol Support:

During February, X-Force engineers extended 13 existing Protocol Analysis Module (PAM) protocol parsers. This included the following protocols:

- RPC
- NDMP
- MSRPC
- SMTP
- HTTP
- UDP
- FTP
- SIP
- TCP
- ISAPI
- TLS
- IRC
- Veritas

New and Extended Content Support:

X-Force engineers created or extended seven PAM content parsers, including the following content formats:

- HTML
- TIFF
- BMP
- JPEG

- MDB
- GIF
- WMF

New Vulnerability Discovery Algorithms:

X-Force added the following security coverage to its products:

- Oracle_Default_Username
- Winny_P2P_Detected
- Veritas_NetBackup_VolumeMgr_Overflow
- MOV_STSD_Atom_Overflow
- Image_JPEG_Quicktime_Bo
- Image_TIFF_Quicktime_Overflow
- Image_GIF_Netscape_SubBlock_Corrupt
- HTML_WebConf_Code_Injection
- Image_WMF_HeaderFileSize_Underflow
- Image_BMP_MediaPlayer_Bo
- Win_IGMP_Option_DoS
- MSRPC_WebClient_Message_Bo
- HTML_Embed_Overflow
- SMTP_Timeout_Bo
- DNS_RRDataLength_Underflow

New Default Blocking Decodes:

- CVS_Directory_Double_Free
- CVS_Argumentx_Double_Free
- CVS_Request_Argument_Overflow
- CVS_Request_Tag_Overflow
- CVS_Request_Option_Overflow
- Image_EMF_Points_Write_Overflow
- Image_WMF_HeaderFileSize_Overflow
- Image_WMF_HeaderFileSize_Underflow
- Image_BMP_MediaPlayer_Bo
- HTML_Embed_Overflow

* www.mobileav.org.

Copyright© 2006 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, Proventia, the Proventia logo, SiteProtector and Ahead of the Threat are trademarks or registered trademarks of 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.

Distribution: **CONFIDENTIAL**