



X-Force[®] Threat Insight Quarterly

Phishing and other significant threats of 2004

February 2005

 INTERNET | SECURITY | SYSTEMS[®]

Ahead of the threat.

Contents

Introduction	1
Focus Topic - Phishing	2
Prolific and Impacting Events of 2004	4
Conclusion	6
Future Topics for 2005	6
References	7
About Internet Security Systems	8

Introduction

Most security professionals would agree that the weakest link in any corporate security strategy is the end user. Awareness and education efforts have come a long way since the 1999 Melissa virus that used social engineering to trick users into opening e-mail attachments. Today, however, the stakes have increased — even the most security-savvy users are fooled by hackers, who have adjusted their social engineering techniques to incorporate fraudulent e-mails or pop-up ads that appear legitimate, but pack a much more dangerous punch. This report will focus on "phishing," a specific method of social engineering that continues to grow in popularity. Phishing can be defined as a malicious attempt to lure an unsuspected user to either provide sensitive information (passwords, credit card information, etc.) or compromise the user's system.

Additionally, this report will review some of the common challenges faced by security professionals throughout 2004.

About This Report

The X-Force Threat Insight Quarterly (Threat IQ) is designed to highlight some of the most significant threats and challenges facing security professionals today. ISS' X-Force security intelligence team produces the quarterly report. Each issue will focus on a specific challenge and provide a recap of the most significant recent online threats.

ISS' X-Force is a primary security research organization that discovers vulnerabilities and security flaws in computer networks and tracks emerging Internet threats. The X-Force serves as trusted security advisor to the U.S. Department of Homeland Security as well as many other federal, state and local government organizations, helping create governmental security standards and initiatives.

X-Force research forms the basis for ISS' Proventia® Enterprise Security Platform (ESP). By researching vulnerabilities, ISS is able to update its products and services to prevent attacks before they negatively impact an organization. All ISS products and services rely on X-Force research to preempt threats.

Questions or comments regarding the content of this report should be addressed to X-ForceThreatIQ@iss.net.

Spammers, Phishers and Fraudsters

“Phishing” uses spoofed e-mails, malicious Web sites and various vulnerabilities to trick users into divulging financial and personal information. As one of the fastest growing threats of 2004, phishing drew a lot of media attention, especially with regard to how it can be used for identity theft.

With every successful phishing attack, there is a ripple effect that ensnares multiple victims. Individuals who provide their personal information join the millions of Americans who have fallen victim to identity theft. A Federal Trade Commission survey released in September of 2003 indicated that an alarming 27.3 million Americans had become victims of identity theft within a five-year period. The severity of the individual incidents is directly related to the amount and substance of the information provided.

Spam is the most common method for spreading dangerous phishing scams across the Internet. Spam, a relentless everyday nuisance, affects everyone with an e-mail account and every provider that offers e-mail services. The key distinction between spam and phishing is the intent of the sender. While spam e-mail is annoying but benign, phishing scams can cause disastrous consequences for unsuspecting victims. Phishing has become an extremely lucrative crime. Reports from all over the world suggest that crime syndicates are the probable source of most of most phishing scams.

The Evolution of Phishing

Originally, the majority of phishing scams adopted a threatening tone and relied on the victim's concern and cooperation to produce the desired outcome. For example: An e-mail tells a user there's an accounting problem that must be corrected immediately to avoid serious financial repercussions. Concerned, the user inspects the URLs, Web sites, logos, text and login information — it all seems perfectly normal. But hackers are attempting to fool the user into submitting personal information using source code from the institution's official Web site. While the request appears to be legit, if the user falls for the trick, he or she will submit their information to an entirely different location — right into the hacker's hands.

The current phishing scam is generally flawless in appearance, including the proper logos, graphics and even the font used by the official Web site of the mimicked organization. The users targeted are increasingly savvy. Internet Security Systems' X-Force Threat Analysis Service often features information regarding the introduction of new and significant changes in phishing within its Assessment Summary.

Phishing Outbreaks in 2004

In early November 2004, the X-Force Threat Analysis Service reported information regarding a new vulnerability in IFRAME affecting Microsoft Internet Explorer. Within a few weeks, phishers had utilized the IFRAME vulnerability to compromise a banner ad service and publish an e-mail worm. The worm, known as Bofra, enticed its victims to click on a link in a banner ad that resulted in system compromise using the IFRAME vulnerability. Popular European Web sites acted as jumping points, linking the victims to the servers that contained malicious code. This was the first example of a banner ad service being used to launch a phishing scam. At the time, no vendor security patch was available, but ISS' security solutions did block the malicious code from compromising customer systems.

The MyDoom.M e-mail worm first hit the Internet in July of 2004. The worm, one member of the inexhaustible MyDoom family, masquerades as a warning from internal IT staff asking the end user to click and install a file attached to the e-mail. Unseen by the end user, MyDoom.M also installs a backdoor on port 1034, leaving an infected system open to future attacks.

In April, Microsoft publicly announced a vulnerability in Windows' Local Security Authority Service, which works with both local and Active Directory authentication and performs other Active Directory functions. Microsoft and ISS released coverage for the issue on April 13th, nearly a month before the Korgo worm first appeared. The Korgo worm does not require user interaction to compromise a system — once Korgo infects a system, it installs a keylogging Trojan designed to steal online banking information and secretly transmits the information collected back to the scammer.

The Consequences

X-Force research analysts monitor phishing scams from a multitude of sources. Some of the more inventive phishing scams utilized social engineering techniques using bait such as applying software patches, donating to hurricane disaster relief and providing information to the FDIC. Scams associated with such relevant topics can make the average person suspicious of even legitimate messages — and in some cases this actually helps the hacker element.

As people become wary of security announcements about a software patch, requiring further verification before applying the fix, it may actually increase the period of time in which a system remains vulnerable to attack. This extension would allow more hackers to manually exploit a system, or enable a worm or virus to automatically compromise more machines.

Phishing Statistics

The Anti-Phishing Working Group recorded 1,974 attacks in July 2004, up significantly from the 176 recorded in January 2004. While the increase is significant, so is the growing sophistication of the scams, which now combine subject matter with household names to trick unsuspecting victims.

It's also growing, explosively; an April 2004 Gartner Research survey found an estimated 57 million Americans think they have received phish-mail. Some 1.8 million people gave up confidential information to the phishers and more than half suffered identity-theft fraud, amounting to more than \$1.2 billion in losses*.

The Radicati Group, Inc., a technology market research firm, predicts that the number of unique phishing attacks worldwide will grow an astonishing 115 percent — from an average of 51 unique attacks per month in 2004 to 110 unique attacks per month by 2008. “If corporations and consumers do not implement some form of protection against e-mail phishing and Internet fraud attacks, e-mail phishers will continue to tarnish the reputation of organizations both online and offline while simultaneously ruining consumer trust in the Internet and e-commerce,” says Dr. Sara Radicati, president and CEO of the Radicati Group.

** (source: CNN)*

Protection and Prevention

Due to unprecedented publicity this year, even non-savvy Internet users have probably heard of phishing, even though they may not fully understand how it works. The “known” but misunderstood threat is why phishing works and will continue to work. By design, phishing creates uncertainty, which in turn prompts even the more knowledgeable user to make poor choices. However, phishing is certainly not infallible.

There are several actions individuals and corporations can implement to reduce the effectiveness of phishing scams, including user education and software patching. Corporations should proactively patch software vulnerabilities closer to their publication, host educational seminars and put antispam and antivirus solutions to work. Reducing the amount of spam and potentially infectious e-mails reaching the end user reduces the number of successful infections from the phishing menace. Furthermore, the ability to identify malicious e-mails presents an opportunity to escalate or report the phisher to a federal or anti-phishing agency.

Educational seminars or notifications can help an end user identify a phishing scam prior to revealing personal information. If the scam is not identified prior to this, the incident should be reported internally, and to appropriate authorities as well. A reference section for phishing information has been provided at the end of this report.

Federal and local law can provide information to corporations or individuals wanting to pursue legal action against phishers. Following legal guidelines will help preserve any collected data, which may be necessary for prosecution.

Prolific and Impacting Events of 2004

Phishing was not the only major cyber-security issue affecting e-commerce this past year. In many ways, phishing merely added another level of severity and publicity to already significant issues. Internet Security Systems (ISS) X-Force analysts evaluated 3,344 vulnerabilities within 2004.

2004 Vulnerabilities/Quarter Total for Year - 3344

1st Quarter Total - 778: Low 140, Med 386 & High 252

2nd Quarter Total - 719: Low 161, Med 341 & High 217

3rd Quarter Total - 861: Low 187, Med 410 & High 264

4th Quarter Total - 986: Low 205, Med 422 & High 359

A significant percentage of the vulnerabilities within the X-Force research database, as shown in the above illustration, swiftly became the focal point of malicious code writers who produced viruses, worms and/or targeted exploits. The next section of the report features some of the more significant and precedent-setting threats of 2004. The year has been divided into financial quarters to emphasize the impact each event represents.

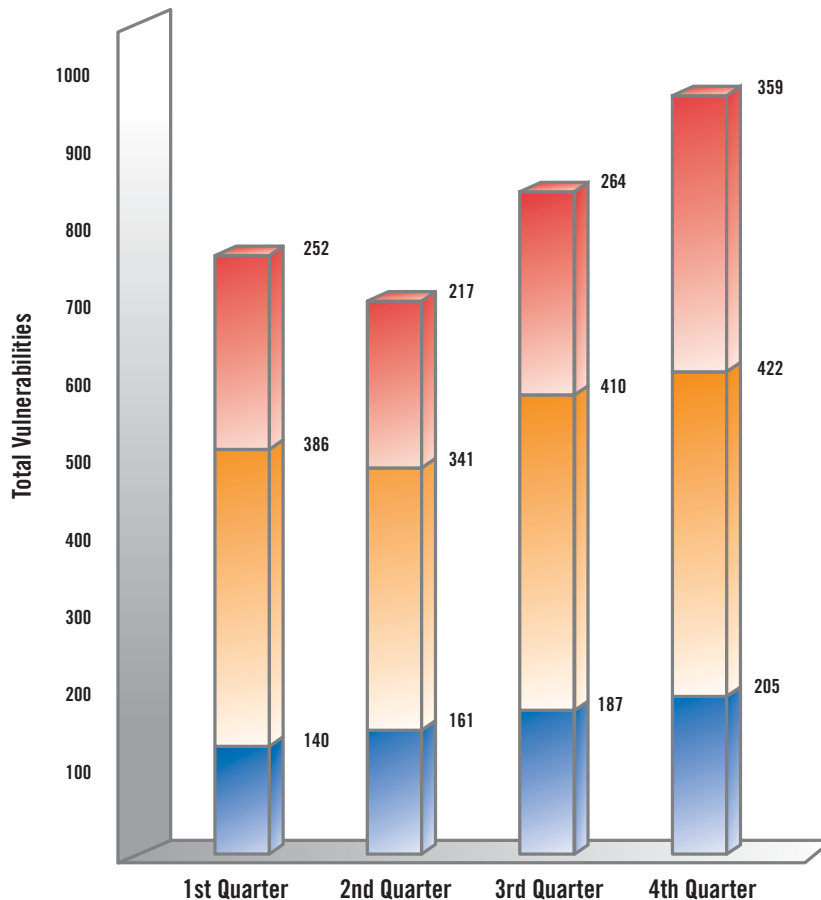
First Quarter 2004

Multiple Vendor H.323 Implementation Vulnerabilities

In mid-January, ISS released an alert on multiple reported vulnerabilities in a slew of H.323 based Voice over Internet Protocol (VoIP) products. The University of Oulu in Finland developed a suite of test tools which target products using the H.323 call-signaling protocol H.225. The H.323 protocol most commonly supports VoIP and video conferencing applications. As this technology becomes more prevalent as an alternative to traditional telephone services, vulnerabilities such as those discovered by the University of Oulu may prove to be more detrimental to the average corporation.

MyDoom Mass E-mail Worm

MyDoom, a mass-mailing e-mail worm, began its aggressive propagation across the Internet in late January. The worm was designed to overload servers and consume network bandwidth. MyDoom quickly morphed into a new variant. It added a secondary propagation vector, Kazaa (P2P), and a component to launch a targeted denial of service (DoS) attack against predefined commercial Web sites. Throughout the year, over 30 variants of this worm were released, with each new release introducing a slew of different methods of exploitation from disabling security software to leveraging other vulnerabilities to phishing threats.



The partnership between phishing and mass-mailing mechanisms as a distribution vehicle set a new precedent — one that will continue to be a popular and dangerous means of delivering near zero-day exploits across the Internet. Layered security protection, adherence to a sound patch-management strategy and increased end-user education is the key to minimizing these types of threats.

Second Quarter 2004

The timeframe between the publication of a vulnerability and the release of malicious exploit code is often referred to as the "patching window." This "window" reflects the amount of time security teams have to identify vulnerable systems and either apply a vendor patch or employ some remediation measure (such as firewall or intrusion prevention systems.) During the second quarter of 2004, the hacker community provided two clear-cut examples of how this patching window has been drastically reduced. Both are described below and reflective of the dangerous and growing trend facing security professionals.

Microsoft SSL Library Remote Compromise Vulnerability

In April, ISS' X-Force published a remotely exploitable buffer overflow condition in the Microsoft Secure Sockets Layer (SSL) library. SSL is an encryption technology commonly used to secure Web and e-mail communications. Exploitation of this vulnerability could lead to complete system compromise. Within one day of the publication of this vulnerability, basic exploit code was released on the Internet. Within a week of publication, more robust exploit code had surfaced.

Microsoft LSASS Sasser Worm

In mid April, Microsoft announced a serious vulnerability in the Local Security Authority Subsystem (LSASS) process in many of their core operating systems. Within two weeks of publication, the vulnerability described in Microsoft Security Bulletin MS 04-011 was incorporated in an aggressive self-propagating worm coined the Sasser worm. This exploitation spread with the speed and ferocity of the SQL Slammer and MS Blaster/Nachi worms of 2003. The sheer scope of potential targets for this vulnerability has made it a popular "payload" for other mass exploits such as the MyDoom variants listed earlier. Today, ISS' Managed Security Services detects a steady flow of activity as Sasser and its variants' propagation continues.

Third Quarter 2004

Microsoft GDI+ JPEG Processing Vulnerability and Exploitation

In September, Microsoft Security Bulletin MS04-028 outlined a critical vulnerability in the GDI+ image-viewing library "gdiplus.dll." This library is supplied by default with Windows XP and Windows Server 2003, and is used by many applications to display the common and usually "trusted" JPEG image files. The X-Force observed active exploitation due to the multiple functional exploits circulating the Internet. The nature of this issue displayed great potential for automatic exploitation in the form of a network-propagating worm. As we move into 2005, this is one of the multiple vulnerabilities ISS' X-Force will continue to closely monitor. A number of backdoors and Trojans have been published which utilize the vulnerability. As mentioned above, this has already been incorporated into phishing scams.

Fourth Quarter 2004

Microsoft WINS Server Vulnerability

As 2004 came to close, a newly-discovered vulnerability in the Microsoft Windows Internet Naming Service (WINS) was announced. Proof-of-concept exploitation code targeting this vulnerability was quickly released, though the likelihood of widespread exploitation via a worm is minimal. Internet Security Systems products provided preemptive protection against the vulnerability almost a month prior to the vendor's security/patch release in December.

The security issues acknowledged within the body of this report as well as the extensive list of X-Force alerts and advisories published in 2004 alone should demonstrate the seriousness of cyber-related issues facing all industries. These issues are not limited to a single vendor's product as reflected by the comprehensive listing of the X-Force alerts and advisories available via the X-Force research Web site at: <http://xforce.iss.net/xforce/alerts>. These attacks are also listed in the X-Force Catastrophic Risk Index (CRI) — an up-to-date list of the most serious, high-risk vulnerabilities and attacks, available online at <http://xforce.iss.net/xforce/riskindex/>.

An Alarming Trend

Though most computer users are incapable of writing or deciphering code, the increasing importance of computers means more people possess the in-depth knowledge of writing and deciphering code that labels them as "elite" users. Being "elite" does not qualify the user as malicious or non-malicious; it merely infers that they possess the knowledge and technical sophistication required to be a hacker. As more people possess this technical proficiency, it stands to reason that there will be a rise in the number of people willing to use their skills for hacking.

In mid-October during an interview with CNETAsia, Internet Security Systems Chief Scientist Robert Graham called 2004 a major turning point in “the rise of the professional hacker.”

Graham states that many hackers are graduating into the professional ranks, a development that carries worrying implications for corporate security. “Before this year, we really

saw just kids playing and pretending to be masterminds,” said Graham, who did important early work in the development of intrusion prevention systems. “But this year, we saw the rise of the professional hacker.”

Conclusion

Security statistics and research indicate that the financial impact to any industry due to an online attack continues to increase. Computers and the Internet are indissoluble portions of world commerce today, and phishing is a great example of how one incident can affect industry on multiple levels — from the end user to corporate IT — as it capitalizes on an endless number of software flaws.

After conducting vulnerability assessments to determine what is at risk, organizations can set obtainable goals regarding user education and determine the correct security solution that fits their needs. User education should include basic and ethical security-related subject matter to ensure that corporate users are aware of the clear-cut risks and how to identify those that are at times in the grey area.

An ideal security solution offers preemptive protection that shields software vulnerabilities and blocks attacks before they can disrupt business operations. By conducting research on threats and vulnerabilities, Internet Security Systems is the only security vendor able to provide products and services that keep organizations ahead of the threat.

Ultimately, the appearance of phishing is just the next in the progression of hybrid threats. These threats will become more complex and dangerous as industry becomes more dependent on computers.

Future Topics

For many years, hackers were content with the thrill of breaking into other systems, or with whatever elevated peer status they achieved through their exploits. But not anymore, according to Graham, who says that both the patterns of hacker attacks and the motives behind the attacks are changing. Hackers are now far more coordinated, and they no longer merely rely on copycat tools and random attacks. What's more, Graham detects a dangerous intent to profit financially from hacking.

The threats described in this report are but a sample of the challenges facing corporate security teams. ISS is committed to producing this report on a quarterly basis to provide ongoing education into the threat and vulnerability landscape.

Future topics for the X-Force Threat IQ may include:

- *VoIP Security*
- *Spyware/Adware/Trojans*
- *Wireless/Cellular*
- *IPv6*

References

For additional information on topics included in this report, please consult the following sources:

Phishing, Fraud and Identity Theft

Agencies:

- *Federal Trade Commission: Home:*
<http://www.ftc.gov/index.html>
- *Federal Trade Commission: Identity Theft:*
<http://www.consumer.gov/idtheft/>
- *NFIC/IFW:* <http://www.fraud.org/welcome.htm>
- *Internet Fraud Complaint Center (IFCC):*
<http://www.ifccfbi.gov/index.asp>
- *For Consumers, For Business, For Law Enforcement: Curbing Identity Theft*
http://www.consumer.gov/idtheft/business_curbidt.html
- *Anti-Phishing Working Group:* <http://anti-phishing.org/>

Guidelines and Laws:

- *Federal and State Laws:*
<http://www.consumer.gov/idtheft/federallaws.html>
- *Instructions for Completing the ID Theft Affidavit:*
<http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf>
- *Computer Crime and Intellectual Property Section (CCIPS):*
<http://www.cybercrime.gov/compcrime.html>
- *Information Compromise and the Risk of Identity Theft: Guidance for Your Business:*
<http://www.ftc.gov/bcp/online/pubs/buspubs/idthrespond.htm>

Educational Material:

- *How Not to Get Hooked by a 'Phishing' Scam:*
<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>
- *Identity Thief Goes "Phishing" for Consumers' Credit Information:* <http://www.ftc.gov/opa/2003/07/phishing.htm>
- *Interview with ISS CSO Robert Graham:*
<http://insight.zdnet.co.uk/internet/security/0,39020457,39171753,00.htm>

General

Vulnerability Alerts and information:

- *US CERT Vulnerability Note VU#842160 - Microsoft Internet Explorer vulnerable to buffer overflow via FRAME and IFRAME elements* <http://www.kb.cert.org/vuls/id/842160>.
- *22.11.2004 - Falk AdSolution Support Notice (provides details concerning the inadvertent redirecting of ad requests to the Bofra/IFrame-Exploit through Falk's network.* <http://www.falkag.com/news.php?id=26>
- *Internet Security Systems X-Force Alerts and Advisories* <http://xforce.iss.net/xforce/alerts>
- *X-Force Catastrophic Risk Index (CRI) - an up-to-date list of the most serious, high-risk vulnerabilities and attacks. Developed by the X-Force, the CRI enables cost effective and proactive protection around threats and vulnerabilities that pose the greatest risk to confidentiality, integrity and availability of critical business systems and applications.* <http://xforce.iss.net/xforce/riskindex/>

NOTE: Internet Security Systems is not responsible for any content on the above Web sites.

About Internet Security Systems

Internet Security Systems is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call **800-776-2362**.