VeriSign

INDUSTRY UPDATE

Internet Security Intelligence Briefing

March 2006 / Volume 4, Issue I

+ Executive Summary

VeriSign® Security Services presents this report with data and trend analysis on Internet security events and online identity fraud. This briefing includes data and intelligence drawn from a variety of VeriSign intelligent infrastructure services, including digital certificates (SSL and PKI), and Managed Security Services (MSS).

This briefing presents data and trends covering:

- Identity 2.0
- 2006 Threat Landscape
- Statistics on Worldwide Internet Security Events

Where it all comes together.™

Contents

+ Summary of Key Internet Statistics

Internet usage continued to increase in the fourth quarter of 2005. The number of active VeriSign SSL certificates approached half a million, and the average number of VeriSign Secured Seals™ exceeded 23 million.

	Q4 2004	Q1 2005	Q2 2005	Q3 2005	Q4 2005
Total number of active VeriSign® SSL Certificates worldwide	454,621	462,291	471,440	478,622	488,864
Average number of VeriSign® Secured™ Seals Served Daily	9.4 M	13.7 M	17.4 M	19.0 M	23.8 M

+ Can Identity 2.0 Help Stop Phishing?

The Problem of Phishing

Phishing is the use of social engineering to steal access credentials. A typical phishing attack consists of a spoof email message that purports to come from a legitimate source (such as a bank). It usually asks the recipient to verify sensitive information (such as account numbers or passwords) by entering the information into a form on a fake Web site run by the criminal.

The schemes used by phishers range from the simple to the highly sophisticated. As with most forms of Internet crime, there is no 'magic bullet' that works against every form of attack. Stopping phishing requires a combination of approaches. Security measures such as the VeriSign Anti-Phishing solution, a control measure designed to stop phishing attacks already in progress, must be combined with measures that close the basic security vulnerabilities exploited by the phishing schemes.

In the June 2005 issue of the Internet Security Intelligence Briefing, we described Secure Internet Letterhead, a method of defeating the social engineering component of a phishing attack. Secure Internet Letterhead allows customers to know with confidence that the messages they receive are a genuine communication from their bank. In this issue of the Internet Security Intelligence Briefing we will look at ways to defeat phishing by using access credentials that are difficult or impossible to steal.

Today's Solutions to the Phishing Problem

Today, it is difficult for an Internet user to understand what information they are disclosing, and to whom they are disclosing that information. Many anti-phishing solutions try to improve this situation by making stolen passwords less useful, or by helping users identify legitimate sites.

One method for addressing phishing is by adding multi-factor authentication. Most web sites require only single-factor authentication to log in: an end user types in their user name and password to authenticate. Multi-factor authentication requires an additional factor: a one-time password (OTP) value, a digital certificate (usually through a smart card or USB token), or a biometric identifier. The idea of two factor authentication is to require "something you know" with "something you have." If an attacker captures a username and password, that will not be sufficient to log in because the attacker doesn't have the right OTP value or digital certificate. If an attacker steals a user's OTP value or digital certificate, they will not be able to log in because they don't know the user's password.

Figure 1 shows a variety of devices that can be used as part of a multi-factor authentication system.

Figure 1 OTP and smart card tokens

Multi-factor authentication is a very powerful technique for reducing phishing related fraud. It is much more difficult for an attacker to capture useful information from a well designed multi-factor authentication system than from a simple password system.

One drawback of multi-factor authentication is that the extra factors may not be usable across web sites. A consumer with a need to regularly access their accounts at their bank, stock broker, retirement and health plans might need one token for each service—a total of at least four tokens. The more tokens the user must carry, the greater the inconvenience and confusion. Unless a way is found to make wearing a necklace of tokens the next fashion craze a way must be found that allows a single token to be used at multiple Web sites.

This is where the Identity 2.0 movement may hold the answer.

Tomorrow's Solution to the Phishing Problem: Identity 2.0?

We would like to create a better mechanism for users to understand what information they are disclosing, and to whom they are disclosing that information.

Identity 2.0 refers to a collection of technologies and initiatives that introduce new forms of identity-aware systems to the Internet. Recent initiatives include OpenID, LID, YADIS, Sxip and Microsoft InfoCard. Although there is considerable overlap in architecture, and in some cases technology, with established initiatives such as SAML, WS-Security and Liberty, the recent initiatives all target applications that did not exist when SAML was being designed. It is too early to predict which initiatives will succeed. However, it is clear is that the protocols that are adopted will support a three corner model.

Today the Internet lacks a common identity infrastructure. A user can be "alice" at one site, "alice1" at another, and "a22naa" at a third. Sometimes the ability to change identifier is desirable. For example, Alice may want to separate her work identity from her recreation identity. However, being forced to change identities (and passwords) from one site to another can be painful for many users. This pain is currently being felt in the blogosphere, the collection of several million personal Web logs that have grown up in the past few years.

Many blogs allow readers to post comments, but require the readers to provide information about their identity. Today, this usually means typing in a name and email address. This presents several problems. First, it is a hassle to type in this information each time you want to post a comment. Secondly, there is no way to authenticate a user across web sites. Some of the Identity 2.0 systems were first designed to simplify this process by providing end users with a common identity to use across blogs.

Although the goal of Identity 2.0 is to establish an identity infrastructure rather than an infrastructure for strong authentication, these are two sides of the same coin: authentication is what a person does to lay claim to his identity.

At first glance, the security needs of Web logs and banking may appear to be poles apart. In one sense this is true: very few Web logs involve any kind of payment at all and the few that do charge a modest fee. Online banks, on the other hand, are primarily concerned with handling large amounts of funds. However, both share a common architectural requirement: the need to identify their users. Instead of a user registering a separate set of credentials at each Web site they visit, Identity 2.0 allows them to register a single set of credentials with a trusted third-party called an identity broker.

When users want to claim their identities at a particular Web site, a three party communication takes place between the User, the Identity Broker, and the Web site (known here as the Relying Party). The details of the communication vary, depending on the proposal. In each case, however, the objective is to restrict the flow of information so that each party sees only the information they need to complete the transaction. The relying party does not need to see the user's authentication data, in fact, the Web site does not even need to know the type of authentication mechanism being used. The relying party only needs to know that the user was properly authenticated by the trusted identity broker. Figure 2 illustrates this three-party communication.

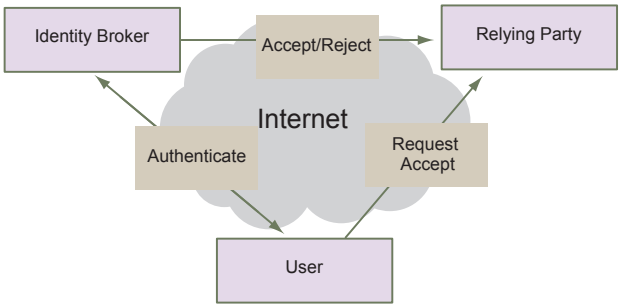

Figure 2 Three party identity protocol

Deployment of such an identity infrastructure has two important consequences for the phishing problem:

- First and foremost, the developers of the Identity 2.0 protocols must make certain that deployment of Identity 2.0 does not create new opportunities for credential theft. Theft of a credential valid at one site is bad; theft of a credential valid at multiple sites is a disaster.
- Secondly, a user should not need to wait for their relying party to offer technical support for strong authentication. The user should be able to make use of any authentication mechanism supported by their identity broker, whether that is an OTP device, a smart-token, or even a biometric technology such as iris or fingerprint scanner. This eases the burden of individual relying parties for absorbing the cost of implementing the Identity 2.0 infrastructure.

The only decision the relying party needs to make is whether the authentication method supported by the identity broker is acceptable. Such a decision would take into account business issues important to the relying party, rather than the technological issues. Identity brokers will need to make it their business to understand these issues.

Combining multi factor user authentication with the Identity 2.0 mechanisms may help achieve true mutual authentication, and help users manage their online identities better than ever before. If Identity 2.0 can address the technical obstacles to deploying strong authentication for users while meeting the business needs of the relying party, a solution to the phishing problem may be close at hand.

+ 2006 Threat Landscape

At the end of 2005, we decided to look for patterns and trends from the past few years to help us predict the biggest security threats of 2006. This report summarizes what we found during 2005, and what we expect to see in 2006.

Recently, the motivations of attackers have changed from creating malicious code for the sake of notoriety to creating malicious code for financial gain. Methods have also progressed from simple to more sophisticated code, and from single attacks to multi-variant wave attacks. The following outline identifies significant historical notes for 2003 through 2005:

- 2003: "Year of the Worm"
  - + Notoriety as main motive
  - + Dawn of "code for cash"
  - + Bounty program established
- 2004: "Worm Wars" and Criminal Code
  - + Bounty program curbs notoriety attacks
  - + Bounty program hardens criminal gain attacks
  - + Hundreds of variants, source code release
- 2005: "Year of the Bot" and Adware/Spyware
  - + Criminalization and commoditization well developed
  - + Targeted Attacks: Espionage and hacker for hire quickly escalate
- 2006: Threat of the Unknown: "Year of the Rootkit?"
  - + Windows rootkits will become increasingly prevalent
  - + Guerilla warfare for personal and financial gain

2005 Malicious Code Activity

In 2005, 16,627 unique malicious codes were documented and/or analyzed by a 24x7x365 Malicious Code Operations team in VeriSign iDefense Security Intelligence Services. The following table shows the total number of malicious code reports published in 2005.

Table 2 Malicious code reports in 2005

Severity	Number
Low	16,251
Medium	337
High	38
Extreme	1

In general, a large number of low-severity, minor variant codes emerged in 2005. This was due, in part, to the predicted boom in bots, Trojans, and sophisticated multi-stage attacks launched throughout the year. Only one report, issued for the rapid exploitation of the Universal Plug-and-Play (UPnP) bot (MS05-039) vulnerability, was rated as an EXTREME-severity threat.

The majority of reports were not for completely new attacks. Instead, they were reports of minor variations on existing malicious code. This can be attributed to several key factors:

- The source code for many malicious codes is now publicly available, making it trivial for attackers to quickly create new minor variants that are highly functional.
- Bots are becoming increasingly automated and prevalent, which resulted in thousands of new variants in 2005.
- Multi-variant wave attacks have proven an effective and popular attack method with authors of common worms like Bagle and Sober.
- Trojan authors have continued to create many new minor variants to avoid detection for various attacks. The advent of adware and spyware has also resulted in the use of many downloader Trojans and minor variants to launch such attacks without being detected by anti-virus protection systems.

Multi-variant and multi-stage attacks will be a major factor in 2006. Today, it only takes a single non-compliant, compromised computer to impact the integrity of an entire network.

2005 Vulnerability and Exploitation Activity

VeriSign iDefense scours more than 1,500 sources on a 24x7x365 basis to monitor over 10,000 products. In 2005, VeriSign iDefense Security Intelligence Services published 2,646 new vulnerability reports and 12,734 updates to previous reports. These numbers illustrate the increased sophistication and analysis required for new vulnerabilities. Improvements in secure coding and vulnerability management have resulted in the disclosure of more difficult vulnerabilities, resulting in increased ongoing expert analysis of such threats to an enterprise network.

VeriSign iDefense released 180 exclusive vulnerability discoveries in 2005 and 149 exclusive vulnerability discoveries in 2004. On average, clients are warned of Microsoft vulnerabilities 119 days in advance, and 48 days in advance for other vendors' vulnerabilities. There are approximately 73 exclusive vulnerabilities for which clients have workarounds that are currently pending public release. Twenty-one percent of Microsoft Security Bulletins in 2005 included an iDefense exclusive.

Nearly 3,000 malicious codes exploiting vulnerabilities disclosed in 2005 were discovered in that year. The following table identifies the number of malicious codes known to exploit specific vulnerabilities, originally reported by iDefense in 2005.

Table 3 Vulnerability-specific codes in 2005

# of Codes	Vulnerability Exploited
1,357	LSASS Vulnerability
526	WebDAV Vulnerability
469	Cumulative Update for Microsoft RPC/DCOM Vulnerability
404	Microsoft ASN.1 BERDecBitString() Buffer Overflow Vulnerability
368	Workstation Vulnerability

Table 3 Vulnerability-specific codes in 2005 (Continued)

# of Codes	Vulnerability Exploited
357	Microsoft Plug-and-Play Buffer Overflow Vulnerability
220	Microsoft Windows DCERPC DCOM Heap Overflow Vulnerability
216	UPnP Vulnerability
172	SQL Server Vulnerability
113	IIS5 SSL Denial of Service (DoS) vulnerability

In 2005, 598 exploit codes emerged that ranged from proof-of-concept codes to Metasploit Project modules and fully functional, freestanding exploits. Exploits are becoming increasingly automated and available to hackers.This is similar to the trend seen several years ago in worm generation kits, until these kits became more private and used for criminal gain. It is likely that exploitation frameworks and kits will evolve in a similar manner, and be leveraged for criminal gain in 2006.

VeriSign iDefense found that of the first 43 Microsoft vulnerabilities disclosed in 2005, an exploit code was released an average of 46 days after disclosure. Half of those vulnerabilities had related public exploit codes, with 39 percent of all the vulnerabilities ranking as HIGH-severity. Normally, exploit code emerges within the first six days following disclosure, or more than one month later.

Increasingly Sophisticated Attacks Targeting Servers

In 2005, attackers increasingly targeted Web and DNS servers, using more sophisticated methods. For example, in January and February 2005, hackers managed to gain remote access to, and control of, multiple servers in various global locations. Servers were compromised through opportunistic attack vectors, including an AWStats.pl vulnerability. Once hackers compromised the computers, they leveraged the systems for a highly sophisticated adware, spyware and malicious code attack. More than 2,000 DNS servers were poisoned, and millions of consumers were likely silently redirected to hostile Web sites.

The hostile Web sites were managed by the attackers, who rotated IP addresses every few hours and days to avoid being discovered and shut down. The hostile Web sites attempted to exploit vulnerable versions of Internet Explorer to silently install up to 20 MB or more of code, including 45 or more individual malicious files and up to 17 different malicious code families in just a single silent attack.

The primary motive for these attacks was financial gain. Unfortunately, this was a highly sophisticated attack that persisted in the wild for at least three consecutive months before being mitigated. Attacks of similar and larger scope are highly likely in 2006.

Hackers Broadening Their Business Case

Hackers are making money any way they can. To that end, they attempt to leverage any stolen data or resources for cash. Hackers are even stealing shipping account numbers for popular shipping companies in an attempt to sell them for cash. This was the case with Diabl0, author of several MyTob worms and ZoTob.

Diabl0 is the brains behind the bot associated with the MyTob and ZoTob creations. He is a member of the 0x90 Team and has been very active in the bot scene for months. He is currently under investigation for his alleged involvement in a fraud ring and peddling code to another suspected hacker. Russian hackers also got in on the PnP exploitation by offering a PnP bot for $500 USD.

In Spring 2005, another incident revealed that dozens of individuals participated in a large-scale industrial espionage operation involving a private investigation firm. The firm paid a programmer to develop custom Trojans that would be undetected by anti-virus companies, and then sent them to specific targets. More than 80 companies were targeted in an 18-month period, and more than 20 people have been arrested in connection with this incident. One programmer was arrested for creating roughly 15 or more codes for thousands of dollars each. Espionage will likely prove one of the largest threats to networks, especially from insiders and direct competitors, in 2006. Concurrently, targeted attacks are becoming more common and are increasingly likely in 2006.

Threats and Trends for 2006

2006 will likely be known as the Year of the Rootkit. In 2006, malicious activity will likely focus on concealment and criminalized code for illicit financial gain. In addition, malicious actors are expected to employ many of the techniques outlined above to make money, thereby increasing the number of malicious code variants. Exploit creation and testing kits, such as the Metasploit Project, will only exacerbate this growing problem.

Web gangs and organized criminal groups are expected to cash in on any and all opportunities presented throughout the year, but with more sophistication and organization than ever seen before. Microsoft Windows will remain the single most exploited operating system in 2006. Unfortunately, there is no magic bullet for defending against the many different actors, motives and attacks expected to emerge this year. As always, due diligence, along with accurate and actionable intelligence, will provide the best possible defense for key infrastructures in the coming year.

+ Statistics on Worldwide Internet Security Events

This section includes statistics describing Internet security events between October and December of 2005. These statistics were compiled exclusively from VeriSign internal sources, including Managed Security Services and the VeriSign Secured Seal Program.

Table 4 Top attacks between October and December 2005

Rank	October 2005	November 2005	December 2005
1	WEB-IIS %2E-asp access	MS-SQL version overflow attempt	MS-SQL version overflow attempt
2	MS-SQL SA brute force login attempt TDS v7/8	MS-SQL Worm propagation attempt	MS-SQL version overflow attempt
3	WEB-MISC SSLv3 invalid Client_Hello attempt	WEB-IIS %2E-asp access	WEB-IIS %2E-asp access
4	MS-SQL Worm propagation attempt	WEB-MISC SSLv3 invalid Client_Hello attempt	WEB-MISC SSLv3 invalid Client_Hello attempt
5	MS-SQL version overflow attempt	NETBIOS SMB-DS Session Setup unicode andx username overflow attempt	MS-SQL SA brute force login attempt TDS v7/8
6	NETBIOS SMB-DS Session Setup unicode andx username overflow attempt	TCP SYN Host Sweep	NETBIOS SMB spoolss AddPrinterEx unicode little endian overflow attempt
7	TCP SYN Host Sweep	NETBIOS SMB Session Setup unicode username overflow attempt	NETBIOS SMB-DS Session Setup unicode andx username overflow attempt
8	WEB-IIS view source via translate header	WEB-IIS view source via translate header	NETBIOS SMB Session Setup unicode username overflow attempt
9	NETBIOS SMB Session Setup unicode username overflow attempt	MS-SQL SA brute force login attempt TDS v7/8	WEB-IIS view source via translate header
10	TCP_Probe_SQL	WEB-MISC cross site scripting attempt --- 1497	TCP SYN Host Sweep

Top Attacks

Table 4 lists the top attacks detected against our Managed Security Services customers between October and December of 2005. Most of these attacks were from worm traffic or network reconnaissance.

Top Sources of Attacks

Table 5 lists the top sources of attacks between October and December 2005. To determine the top sources of attacks, we looked at data from our Managed Security Services customers during this timeframe. We excluded all packets from private and unallocated internet addresses (such as RFC1918 addresses) from our analysis. We focused only on packets dropped by firewalls, and excluded packets accepted by firewalls (most of which were legitimate) to produce our statistics. We found that 68.8% were from the United States, ten times the traffic from the next country on the list (China, at 6.6%).

Table 5 Top sources of attacks between October and December 2005

Rank	Country	Percent
1	UNITED STATES	68.8%
2	CHINA	6.6%
3	RUSSIAN FEDERATION	4.0%
4	UNITED KINGDOM	3.0%
5	CANADA	2.4%
6	SWITZERLAND	2.1%
7	JAPAN	1.3%
8	FRANCE	1.3%
9	GERMANY	1.1%
10	KOREA, REPUBLIC OF	0.9%
	Other Countries	8.6%

New Alerts

Using iDefense research, we examined the number and type of new security alerts issued over the past twelve months. (Alerts are often revised over time to reflect more information. This data only shows the first alert for each piece of malicious software, vulnerability, or threat.) As shown in Figure 3, the vast majority of alerts were for malicious code, accounting for 93.4% of alerts in 2005. Moreover, the number of alerts for malicious code more than tripled, from 487 in December 2004 to 1567 in December 2005

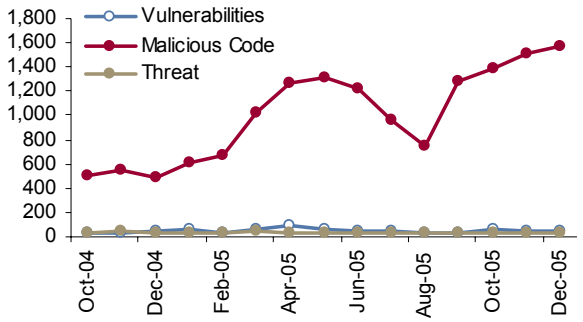

Figure 3 iDefense security alerts by month

VeriSign Secured Seals Served

The number of Verisign Secured Seals delivered continues to increase rapidly, reaching an average of 25.3 million per day in December 2005. More Web sites are featuring the VeriSign Secured Seal, and more users are seeing this seal than ever, as Web sites use the seal to assure their users that their connection is secured through a VeriSign SSL Certificate. To learn more about the VeriSign Secured Seal Program, please visit **http://seal.verisign.com**.

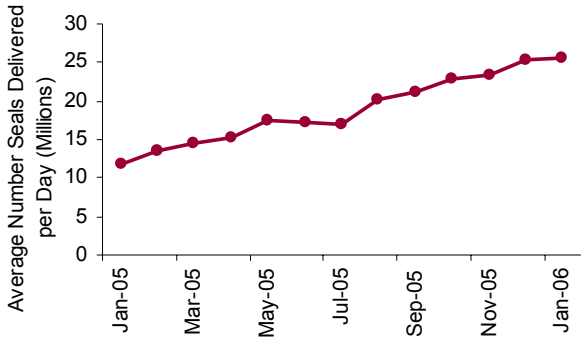

Figure 4 Average number of VeriSign Secured Seals delivered per day, by month

+ About the Internet Security Intelligence Briefing

The Internet Security Intelligence Briefing is primarily based on data and intelligence correlated from critical intelligent infrastructure services that VeriSign operates. These services include:

- **Domain Name System (DNS) Services** – VeriSign Naming Services manages over 50 million domain names in over 300 languages. VeriSign is the authoritative directory provider for all .com, .net, .cc, and .tv domain names. Using our proprietary global infrastructure, VeriSign processes over 14 billion interactions each day, more than three times the number of phone calls made in the United States daily. VeriSign helps registrars expand markets and increase renewals with critical technology and unmatched experience.
- **SSL Digital Certificates** – VeriSign is the leading secure sockets layer (SSL) Certificate Authority enabling secure e-commerce and communications. 93 percent of Fortune 500 companies, the world's 40 largest banks, and 47 of the top 50 e-commerce sites use VeriSign SSL technology. Over 37,000 web sites display the VeriSign Secured Seal.
- **Managed Security Services** – To keep pace with increasingly complex network security threats and safeguard critical information takes more than integrating the latest security hardware and software. A comprehensive security program includes 24/7 management and monitoring by security experts, real-time security intelligence, and a global infrastructure. Our unique combination of people, process, intelligence, and technology makes our customers more secure by proactively managing risk, monitoring compliance and identifying and mitigating evolving security threats.

For more information, send an email to securitybriefing@verisign.com.

Previous briefings are available online at:

http://www.verisign.com/Resources/Intelligence_and_Control_Services_White_Papers/internet-security-briefing.html