VeriSign

INDUSTRY UPDATE

Internet Security Intelligence Briefing

June 2005 / Volume 3, Issue I

+ Executive Summary

The VeriSign Internet Security Intelligence Briefing reports current trends in Internet growth and usage as well as security events and online fraud. This briefing includes data and intelligence drawn from VeriSign intelligent infrastructure services, including Domain Name System (DNS) services, digital certificates (SSL), Managed Security Services (MSS), Payment Services, and Fraud Protection Services.* This briefing features data gathered from January to March 2005.

This briefing presents data and trends covering:

- Phishing and Pharming attacks
- Internet commerce
- Emerging threats and vulnerabilities
- Worldwide Internet usage

*. These services are described in detail on the last page of this briefing.

Table of Contents

+ Summary of Key Internet Statistics

During the period January through April, 2005, VeriSign has observed steady growth in overall Internet usage and e-commerce activity, as shown in the table below. Year over year, new .com domain registrations grew by 28 percent, and new .net domain registrations grew by 21 percent. Also, the average number of Secured Seals delivered daily experienced a significant rise in the first quarter of 2005, which demonstrates increasing consumer awareness of only transacting e-commerce with secured Web sites.

Key Internet statistics

	Q1 2004	Q2 2004	Q3 2004	Q4 2004	Q1 2005
Year-over-year growth by quarter in .com registered domain names	20%	23%	25%	26%	28%
Year-over-year growth by quarter in .net registered domain names	18%	20%	21%	21%	21%
Average number of DNS Queries answered per month in each quarter	337.0 B	379.9 B	380.3 B	389.2 B	395.8 B
Total number of active VeriSign® SSL Certificates worldwide	414,092	430,243	447,621	454,621	462,291
Average number of VeriSign® Secured™ Seals Served Daily	2.7 M	4.7 M	7.6 M	9.4 M	13.7 M
Total Dollar Amount of Settled Transactions Processed by VeriSign Payment Services	$8.68 B	$8.51 B	$8.77 B	$9.65 B	$10.69 B
Total number of Settled Transactions Processed by VeriSign Payment Services	58.66 M	57.45 M	61.62 M	67.79 M	71.29 M

+ Phishing & Pharming - The New Threats

On March 16, 2005, a hacker (or group of hackers) launched a widespread series of Domain Name Service (DNS) Cache Poisoning attacks. These attacks were possible because of vulnerabilities in several different products from a variety of vendors. When users tried to connect to popular Web sites like Google or eBay, they were directed to a malicious Web site from which spyware and adware were distributed.

At the time of this attack, VeriSign Managed Security Services (MSS) noted that many more attackers than usual were attempting to reach DNS servers on our customers' networks. Further analysis showed that these attackers were looking for DNS server versions in an attempt to locate vulnerable servers. (This activity was detected by intrusion detection system (IDS) devices managed and monitored by VeriSign MSS. No compromises were detected in our customers' networks during this attack. See Figure 1 below for details).

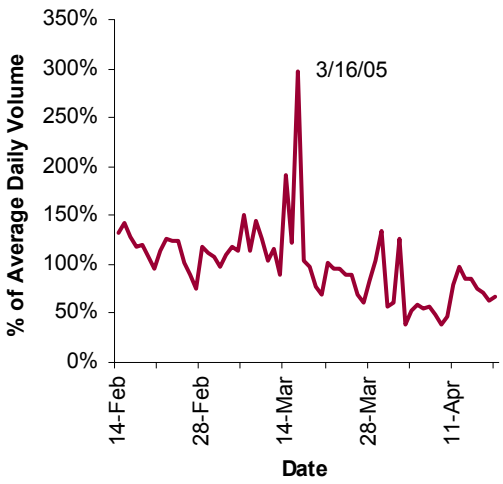

Figure 1 On March 16, 2005, Verisign MSS noted a large increase in the number of probes of DNS servers, corresponding with reports of DNS Cache Poisoning attacks.

Changing Attack Tactics

A phishing attack is a confidence trick that uses email spam to spread. In computer security terms, it is a "social engineering" attack, in that it does not exploit technical flaws, but fools people into revealing information. The consumer receives a message that appears to come from a bank, but which redirects the consumer to a malicious Web site. The attacker typically asks the consumer to verify his or her account information, often claiming that something bad will happen (for example, losing access to funds) if the consumer does not promptly comply. An unsuspecting consumer might go to a malicious Web site called a capture site, and give away private information to the attacker.

Each phishing attack only works for a short period of time. Most attackers indiscriminately send out thousands of email messages to potential victims. The bank quickly learns that it is being attacked; some of its customers might receive the email and contact the bank to confirm that the request is legitimate, and some people who are not customers might receive the email and contact the bank, asking why they received the email. To protect its brand, the targeted bank uses any means available to respond to the threat; the attack is a direct public challenge that the targeted brand cannot possibly ignore.

Some phishing gangs have begun to replace social engineering with software engineering, exploiting software flaws to redirect unsuspecting consumers to capture sites. These attacks require a far higher level of technical sophistication than social engineering attacks, but can be much harder to detect.

One technique for stealing private information through security flaws is through malicious software (malware) that monitors a user. Malware can be installed through viruses, worms, or Trojan horses, and is often included with downloaded software. This identity stealing software can monitor what a user types, forwarding this information to the hacker through the Internet. Luckily, users can mitigate such attacks through anti-virus, spyware detection, and firewall software.

Pharming

Pharming is an alternative technique that does not try to fool people through fake email messages, or spy on users through malware. Instead, this technique fools your computer into connecting you to a fake Web site

even when you enter the correct domain name information into your browser.

Like phishing attacks, an attacker sets up a capture site to collect identity information. But unlike a phishing attack, this technique does not require the user to follow a link in a fake email message. Instead, this technique exploits vulnerabilities in DNS servers to distribute fake address information.

The DNS infrastructure maps each domain name (such as bizybank.com) to an Internet Protocol address (such as 10.1.2.3). If the real bizybank.com Web site has the IP address 10.1.2.3, the attacker might set up a copy of the site at IP address 192.168.1.2. The attacker then manipulates the DNS infrastructure so that some bank customers are directed to the fake Web server (at 192.168.1.2) instead of the real Web site (10.1.2.3). Attacking the DNS in this way is known as DNS spoofing.

The simplest form of DNS spoofing attack is to send a request for a configuration change to the DNS registrar with which the targeted domain is registered.* It is important for banks (and other parties that might be a target for this form of attack) to ensure that their DNS registrar implements effective authentication and security measures to guard against these attacks.

Another form of DNS spoofing attack targets a part of the DNS infrastructure known as a caching server. The DNS is one of the most heavily used components of the Internet infrastructure: every time a user tries to connect to a new host using a domain name, their computer looks up the IP address through DNS. Every day, VeriSign responds to over 15 billion queries for the .com and .net top level domains (TLDs), but computers resolve many, many more addresses each day. To improve performance for end users and provide a more robust and resilient Internet infrastructure, most ISPs and many companies operate their own DNS caching servers. End users ask the local caching server to resolve domain names to IP addresses. These local servers store responses from other DNS servers (usually for a fixed period of time), responding to user requests locally, and thus more efficiently.

For example, suppose that BigISP.com has a million customers, several thousand of whom bank with bizybank.com. Each customer connects to the global DNS infrastructure through the local DNS caching server. The first time a customer visits the bizybank.com Web site, the DNS caching server contacts the global DNS system to obtain the IP address for bizybank.com. The result of the query is also stored in the DNS server cache. The next time a customer visits the bizybank.com Web site the DNS caching server returns the stored result.

Properly implemented, the use of DNS caching servers enables the exceptional robustness, reliability, and efficiency of the DNS. Answering queries from the local cache provides a faster response and reduces Internet congestion. Unfortunately, some DNS server software versions have flaws that allow an attacker to introduce false information into a DNS caching server. By exploiting these flaws, an attacker can cause the DNS caching server to return false information and direct a user to a malicious site (Figure 2).

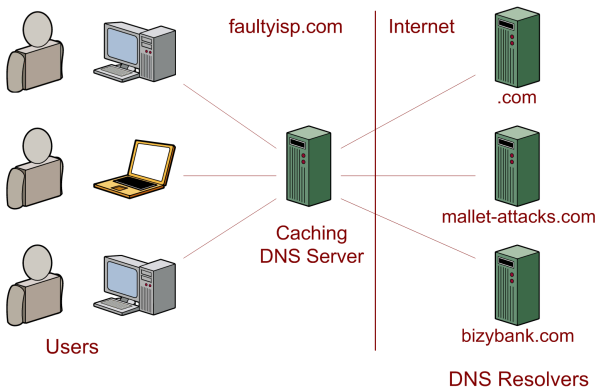

Figure 2 DNS caching server

*. For a report on a successful prosecution of this form of DNS spoofing see http://www.usdoj.gov/criminal/cybercrime/racinePlea.htm. The defendant was ultimately sentenced to 1000 hours of community service and a fine of $2,000.

Example of a DNS Spoofing Attack

Mallet wants to direct traffic to his fake Web site for www.bizybank.com, and the IP address of this site is 193.168.42.69.

1. Mallet registers the domain name mallet-attacks.com and sets up a DNS server for it.
2. Mallet sends out spam emails that advertise www.mallet-attacks.com.
3. Alice, a customer of faultyisp.com, receives the spam and clicks on the link to visit www.mallet-attacks.com.
   a. Mallet's DNS server returns information for both www.mallet-attacks.com and false information that gives the IP address of www.bizybank.com as 193.168.42.69.
   b. The DNS caching server at faultyisp.com accepts the IP address information for www.bizybank.com and stores it in its cache.
4. Anyone who uses the faultyisp.com DNS caching server and attempts to visit www.bizybank.com will be directed to the fake site.

Stopping Pharming

Much has been written about the need for user education to prevent phishing attacks. Unfortunately, diligent end users can still be victims of pharming attacks. Pharming attacks target the network infrastructure, so network managers, not end users, have the primary responsibility for preventing this type of attack.

The Secure Socket Layer (SSL) protocol is designed to protect against this form of attack. The attacker cannot cause the SSL padlock security icon to appear unless they know the private key corresponding to the digital certificate for the BizyBank site. Unfortunately a consumer can only check that they are on the real BizyBank site if the bank protects their entire site with SSL security. Some banks only enable SSL security after the customer has entered their username and password; by the time the SSL padlock icon appears, it is, sadly, often too late.

For Immediate Action

Like the traditional email phishing attack the pharming attack exploits vulnerabilities in the Internet infrastructure. Unlike the vulnerability exploited in the email phishing attack, the vulnerabilities being exploited in the pharming attack were anticipated in the design of the DNS system and are largely addressed by existing technology. Furthermore, deployment of this existing technology is considerably easier than attempting to change the email infrastructure. The Internet has a billion users and educating each user to be on their guard against phishing attacks or persuading them to upgrade their email software to versions that resist phishing attacks can be a long and difficult process. The number of DNS administrators is considerably smaller and, unlike the users, they have accepted a duty of care for the infrastructure they maintain.

Steps for Preventing Phishing and Pharming Attacks

Banks and other parties that are likely to be the subject of a pharming attack should:

- Ensure that all pages that contain a form for entry of username and password data are SSL secured.
- Ensure that their DNS domain names are 'locked' by their registrar to prevent unauthorized modification or transfer.

All network administrators should:

- Ensure that all DNS Server software is up-to-date and configured securely.

IT Auditors should:

- Verify that their clients have implemented these safeguards.

Software Providers should:

- Perform a code audit to determine whether products contain DNS code, and if so, audit the code for cache poisoning vulnerabilities.

The following DNS Server Software is considered secure:

- Windows® 2003 DNS Server
- Windows® NT 4.0 with SP4* provided the SecureResponses Registry key is set to the value 1
- BIND release 9

The following DNS Server Software has known vulnerabilities and should be upgraded:

- BIND 8.4.3 and earlier
- Windows NT 4.0 prior to SP2

*. SP4 for NT 4.0 includes a patch to enable checking of DNS responses but this checking is not enabled by default. To enable checking the registry key SecureResponses must be set to 1. For more information see http://support.microsoft.com/default.aspx?scid=kb;en-us;241352

DNSSEC Deployment Planning

Deployment of existing security measures provides a high degree of resistance to pharming attacks but cryptographic authentication techniques provide a higher level of assurance. The DNS Security (DNSSEC) specification is an IETF proposed standard for using cryptography to secure the DNS.

The fact that organized criminals are exploiting DNS security vulnerabilities for criminal profit creates new urgency for deployment of a comprehensive cryptographic security infrastructure for the DNS. It is vital therefore that DNS infrastructure providers and software providers ensure that this infrastructure can be deployed as expeditiously as possible.

Takedown Response

Both phishing and pharming attacks require a capture site for collecting use information. An effective method for stopping phishing attacks is to ask the ISP hosting the capture site to remove the site. The same approach (taking down capture sites) can be used to stop pharming attacks.

The first step in taking down a capture site is to locate the server hosting the site. In phishing attacks, it is simple to find the capture site: it is listed in the phishing email. But it can be more difficult to find the capture site in a pharming attack. ISPs will need to develop new reporting infrastructure to aid in identifying pharming capture sites. DNS spoofing attacks propagate information by sending false information to DNS servers. One method for identifying capture sites when they appear is to look for this irrelevant, unsolicited information on DNS servers.

Secure Internet Letterhead

The solution to the pharming problem is to eliminate certain vulnerabilities in the Internet DNS infrastructure that are the result of software errors. The solution to the traditional phishing attack is to eliminate vulnerabilities in email clients and Web browsers that are the result of design oversights; these are much harder to solve but the sooner we start the sooner the work will be completed.

The first design oversight is the lack of an authentication infrastructure for email. An attacker can impersonate anyone they choose. In particular they can impersonate a business that a consumer already trusts (such as a bank) and use the trusted reputation as their own.

The second design oversight, and one that is shared by all Internet applications, is that the mechanisms used to communicate authentication information to the user are inadequate. Only a small proportion of Internet

users know that they should look for the padlock icon before entering sensitive information into a Web form. Of this proportion an even smaller number know that it is necessary to click on the padlock icon to find out the real identity of the certificate holder. The proportion who do so on a regular basis is even smaller still.

Considerable attention was paid to the problem of how the business should authenticate customers, but the equally important question of how the customers should authenticate the business has received far less attention than it deserves.

Digital Certificates provide a secure means of authenticating the bank to the consumer, but considerable advances are needed in the presentation of security information to users to make this authentication effective against phishing fraud. The padlock icon that many browsers display only tells the users when encryption is being used. In order to confirm the identity of the site being visited the user must click on the padlock icon and verify that the X.509v3 Subject identity is correct and the certificate issuer is trustworthy.

In the real world few consumers know what an X.509v3 Subject identity is, let alone how to use one to authenticate a business Web site. Instead, consumers recognize businesses by their brands: a mechanism that is familiar and immediate. The idea behind Secure Internet Letterhead is to provide a secure and reliable means of using the same cue to verify the authenticity of brands in cyberspace.

In place of displaying the padlock icon, a browser enabled with Secure Internet Letterhead displays the company brand. This allows the user to immediately see where they are. If they are used to seeing the brand on the bank Web site they are much more likely to know to be cautious when it is absent.

In order for Secure Internet Letterhead to be secure it must not be possible for an attacker to impersonate it. This means that the browser must implement appropriate security measures and a trusted third party must verify ownership of the brand logo used.

Eventually businesses will likely use Secure Internet Letterhead in every form of official communication over the Internet. Just as every official company letter is written on official company letterhead, every official company email will carry Secure Internet Letterhead, as will every Instant Message, telephone call, and Web site (Figure 3).

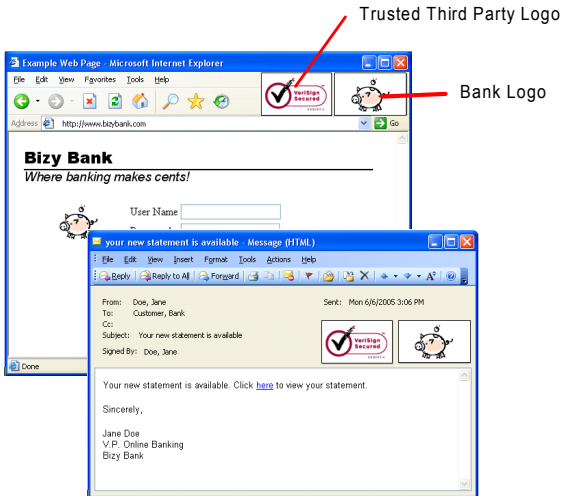

Figure 3 Secure Internet Letterhead

+ Internet Commerce and Fraud

In tracking the growth of over 135,000 merchants over the past 12 months, VeriSign has observed rapid growth in Internet commerce. Using the second quarter of 2004 as a base line, the number of transactions increased by 30 percent over the past year. The average transaction value increased four percent from $144 in the fourth quarter of 2004 to $150 in the first quarter of 2005 (Figure 4).

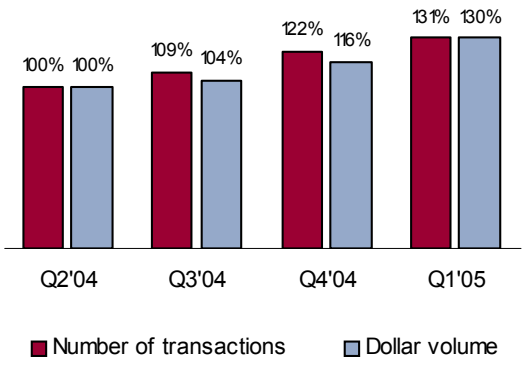

Figure 4 Data Trends for Internet Usage

During the first quarter of 2005, most fraudulent transactions were actually from the United States, Canada, and the United Kingdom, as shown in the following table. A criminal might find it easier to defraud a US merchant from overseas, but committing fraud from the United States, the United Kingdom, or Canada also has some advantages. First, the number of computers with broadband connections is very large in these countries, so many potential criminals have easy access to the internet. Secondly, many of these computers have been compromised with bots, Trojan horses, or worms, enabling a criminal to use them as an anonymous proxy to commit fraud.

Top countries by volume of fraudulent transactions

Rank	Country	% Fraudulent Transactions*
1	United States	84.9%
2	Canada	5.2%
3	Great Britain	1.1%
4	Australia	0.9%
5	Germany	0.9%
6	Japan	0.7%
7	Romania	0.4%
8	Israel	0.4%
9	Mexico	0.4%
10	Ghana	0.3%
	Other Countries	4.8%

*. The country of origin is determined by IP Address used in the payment transaction. It is possible that hackers use proxies or break into ISP infrastructure in other countries to hide their true origin.

During the first quarter of 2005, most attacks focused on a few vulnerabilities: buffer overflows in unpatched Microsoft SQL Server installations, buffer overflows in the Windows LSASS module, and unprotected Windows file shares, as shown in the table on the next page.

The attacks focused on NETBIOS SMB file sharing are especially interesting because the many bots use these vulnerabilities to propagate. See the next section for more information on bot networks.

A network administrator can easily protect against these attacks by keeping their security patches up to date, using a firewall to control access to their networks, and by not exposing unnecessary services to the Internet.

Attacks seen from January to March 2005

Rank	January 2005	February 2005	March 2005
1	MS-SQL version overflow attempt	MS-SQL version overflow attempt	MS-SQL version overflow attempt
2	WEB-MISC PCT Client_Hello overflow attempt	WEB-MISC PCT Client_Hello overflow attempt	WEB-MISC PCT Client_Hello overflow attempt
3	WEB-MISC admin.php file upload attempt	WEB-MISC admin.php file upload attempt	NETBIOS SMB-DS IPC$ share unicode access
4	NETBIOS SMB-DS IPC$ share unicode access	WEB-CGI htsearch arbitrary configuration file attempt	Client_Hello with pad Challenge Length overflow attempt
5	NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt	MS-SQL:REG-STACK	EXPLOIT SSLv2 Client_Hello Challenge Length overflow attempt
6	WEB-MISC SSLv3 invalid Client_Hello attempt	NETBIOS SMB-DS IPC$ share unicode access	WEB-MISC SSLv3 invalid Client_Hello attempt
7	NETBIOS SMB-DS C$ share unicode access	MS:LSASS-ACCESS	NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt
8	MS:LSASS-ACCESS	MS-SQL probe response overflow attempt	NETBIOS SMB-DS C$ share unicode access
9	WEB-MISC SSLv3 invalid data version attempt	WEB-MISC SSLv3 invalid Client_Hello attempt	MSRPC_Popup_Message
10	NETBIOS SMB NTLMSSP invalid mechtype attempt	MSRPC_Popup_Message	NETBIOS SMB Data Service Session Setup AndX request unicode username overflow attempt

Threats and Trends

For all of us who work in computer security, it was business as usual during the first five months of 2005. More security holes were found and subsequently patched in operating systems like Windows, Linux, Solaris, Mac OS, and Cisco IOS, in applications like Firefox, Internet Explorer, and in server software like MySQL, PHP, and Oracle. Additionally, more viruses and worms like Sober, MyDoom and Mytob spread among desktop machines. None of these events have been particularly memorable or newsworthy, partly because they happen so frequently, and partly because vendors' efforts at fixing security problems have been fairly effective.

However, a few security trends are worth noting.

Convergence of internet crime techniques:

As we discussed above, phishing gangs are becoming more sophisticated. There have been several incidents where domain name service vulnerabilities have been exploited to redirect users to different Web sites. Although we have not yet seen a full blown pharming attack designed to harvest user information, a skilled attacker could certainly exploit domain name service vulnerabilities for this purpose. We have also begun to see connections between bot networks, phishing, and pharming. A bot is a piece of malicious software that allows an infected computer to be controlled remotely, usually through an Internet Relay Chat (IRC) server. A bot receives commands through this server to do different things: propagate itself, open an anonymous Web or email proxy, launch denial of service attacks, or do just about anything else a computer can be told to do. Bots spread through different security

vulnerabilities, often by mechanisms for which patches are available through vendors. Most bots are Windows-based, but a few Linux bots have been found in the wild. Most bots are found on computers connected to broadband (cable or DSL) connections. Few computer users with infected hosts are aware that their computers are infected.

For years, we have seen criminal hackers amass networks of bots (sometimes thousands of hosts), and sell these to other criminal hackers who use these networks to launch denial of service attacks and blackmail Web site owners. But more recently, we have seen bot networks used for spamming and launching phishing attacks. Bots can be an ideal source for spam, or an excellent hosting site for a fake Web site. Access to bots is indirect and often anonymous, making it much more difficult to trace the perpetrator of an attack. Furthermore, because bots are plentiful and cheap, it can be very difficult for network operators to block access to malicious sites.

Cell phone and Instant Messaging viruses:

We have seen several instances where malicious software has propagated through non-traditional means, or infected non-traditional devices. The Cabir virus has begun to infect some mobile devices running the Symbian OS. Worms affecting Instant Messaging networks (specifically the Gabby.A worm) have disrupted service for Reuters and AOL, and the Bropia.A worm propagated over MSN Messenger.

Data privacy leaks:

During the first five months of 2005, we learned that several different large companies lost (or sold) detailed personal information about millions of people. Most notoriously, Choicepoint revealed that it had sold personal information on 400,000 Americans to a criminal ring engaged in identity theft, and Reed Elsevier (a subsidiary of Lexis Nexis) allowed information on 310,000 people to be accessed fraudulently. Bank of America lost a backup tape containing names and credit card numbers for 1.2 million government employees. Just last week, newspapers reported that personal data on 4 million consumers may have been exposed when UPS lost a shipment that Citigroup was sending to the Experian credit bureau. Credit card data on tens of thousands of customers was stolen from several major retailers, including BJ's Wholesale Club and Polo Ralph Lauren, prompting these retailers to sue their technology providers. Additionally, several banks contracted with a fake "deadbeat locator service" and collection agency called DRL Associates, disclosing private information on 676,000 people. (Interestingly, this gang did not care about the quality of the identity information. People with collection accounts have trouble obtaining more credit, so it's unlikely that this gang intended to use this information themselves. More likely, they were simply seeking identity information for sale on the black market.)

While the underlying causes of these incidents were quite different (improper customer screening, inadequate authentication and access control, insufficient physical security, and unnecessary data storage), the impact of each of these incidents was quite similar: personal information was improperly revealed at no fault of the customers.

+ Internet Usage

Growth in Domain Registration

In the first three months of 2005, the number of new .com domain name registrations grew by 29 percent over 2004, and the number of new .net domain name registrations grew by almost 23 percent, indicating that the demand for new domain names is accelerating (Figure 5).

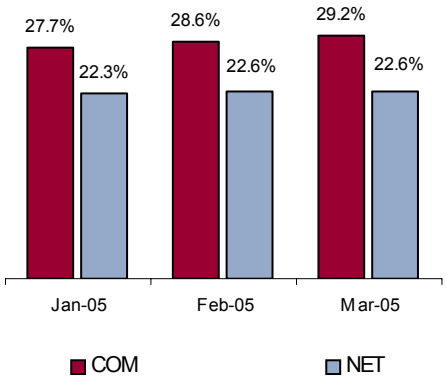

Figure 5 Growth in domain name registration

In operating the generic Top-Level Domain Registries (gTLD) for .com and .net, VeriSign processed an average of 15 billion transaction per day during the first quarter of this year

Growth in SSL Certificates

The number of active VeriSign SSL Certificates has continued to grow over the past year; at the end of the first quarter, the number of active certificates was 12 percent greater than one year ago, as shown in the following table.

Total active VeriSign SSL Certificates worldwide

2004				2005
Q1	Q2	Q3	Q4	Q1
414,092	430,243	447,133	454,621	462,291

Secured Seals Served

The number of VeriSign Secured seals delivered has continued to increase dramatically, growing by almost 225 percent over the past year (Figure 6). To learn more about the VeriSign Secured Seal Program, please visit http://seal.verisign.com.

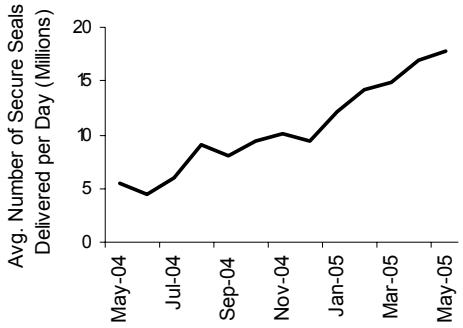

Figure 6 Growth in Secured Seals

DNS Queries

The gTLD constellation servers answered approximately 400 billion Domain Name Service queries for .com and .net domain names during each of the first four months of 2005 (Figure 7). VeriSign servers responded to 1.043 trillion queries during the first quarter of 2005, 14 percent greater than the 918 billion queries in the first quarter of 2004.

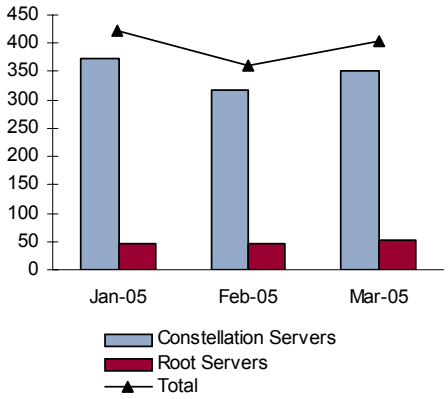

Figure 7 Total monthly DNS Queries

DNS Queries by Type (Email vs. all Others)

Over the past six months, the average number of queries per day has grown to 15 billion, and the percentage of MX (email) queries has remained steady at approximately 15 percent (Figure 8).

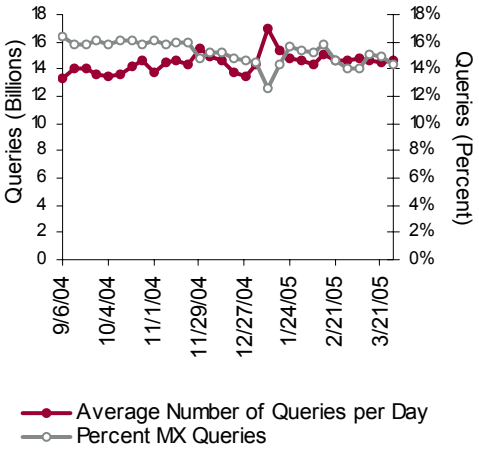

Figure 8 DNS Queries by Type (Email vs. All Others)

+ About the Internet Security Intelligence Briefing

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

- **Domain Name System (DNS) Services** — The DNS allows people to use names (e.g., www.abc.com) to identify Web servers, rather than IP addresses (e.g., 204.14.78.100). There are 13 root servers that contain the authoritative name server information for every top-level domain (e.g., .com, .net, .us, .uk). VeriSign currently operates two of these thirteen root servers. In addition, the .com and .net domains are supported by 13 name servers run by VeriSign, located around the world, that manage over 14 billion resolutions every day.
- **SSL Digital Certificates** – SSL certificates are the de facto standard for secure Web sites and Web servers (All Web sites that begin with *https* are secured using SSL certificates). VeriSign is the leading provider of SSL certificates, securing hundreds of thousands Web sites and servers through its certificates.
- **Managed Security Services** – VeriSign provides 24/7 monitoring and management of firewalls, intrusion detection systems, and other network security devices on a global basis. Each managed device in our customers' premise logs security related information. These logs are then aggregated in our data centers, normalized, correlated, and then analyzed by the VeriSign® TeraGuard™ Platform. Further, detailed analysis is then carried out by a team of VeriSign Security Research Analysts.
- Payments and Fraud Protection Services - VeriSign provides online Payment and Fraud Protection services to over 135,000 customers. Over 37 percent of North American e-commerce payments are processed through VeriSign.

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/page_005574.html.