



INDUSTRY
UPDATE

Internet Security Intelligence Briefing

November 2004 / Vol. 2, Issue II

+ Executive Summary

The VeriSign Internet Security Intelligence Briefing reports current trends for Internet growth, usage, security, and online fraud. This briefing includes data and intelligence drawn from VeriSign's Internet infrastructure services, including Domain Name System (DNS) services, digital certificates (SSL and PKI), Managed Security Services (MSS), Payments, and Fraud Protection Service¹. This briefing reports on data gathered from July through October 2004.

This briefing presents:

- Threat and vulnerability trends across the Internet from July through September 2004
- A spotlight on spam
- Best practices with which to thwart spam and phishing
- Detailed trends on Internet usage

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



Where it all comes together.™

TABLE OF CONTENTS

+ Threats and Trends	3
+ Managed Security Services Event Statistics	3
Top Attacks seen during Q2 and Q3 2004	4
+ Spotlight on Spam	
Email Traffic Characteristics	5
Addressing spam	6
Tactical and Strategic Approaches to Phishing	8
+ Data Trends for Internet Usage	9
Internet Commerce and Fraud	9
Top Countries by Volume of Fraudulent Transactions	9
Top Countries by Percentage of Fraudulent Transactions	10
+ Internet Usage and Security	10
Domain Name Registration	10
DNS Queries	10
Growth in SSL Certificates	11
Growth in Secured Seals Served	11
+ About the Internet Security Intelligence Briefing	12

+ Threats and Trends

This past quarter, security professionals have observed one clear phenomenon: Attackers are honing their craft. They are getting not only faster but more creative; they are widening their net and becoming increasingly persistent.

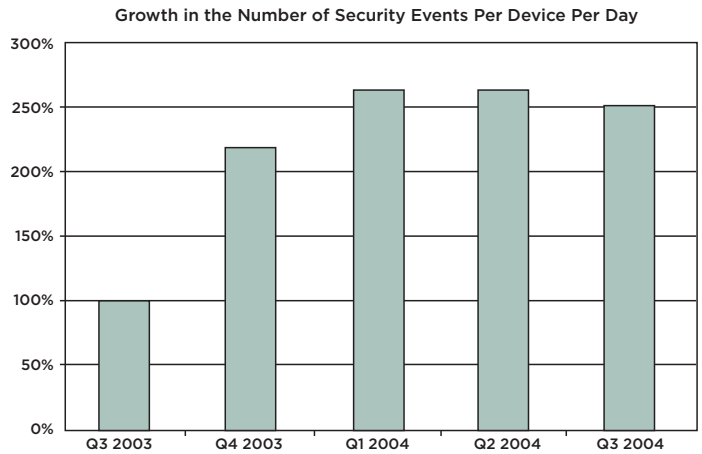
The past few months have brought on a growing number of hybrid attacks. “Hybrid,” in that they no longer simply create Denial-of-Service conditions and terminate, as did Code Red, SQL Slammer, and many other attacks. In this recent series of hybrid attacks, hackers leverage system exploits as the first stage in a larger information/identity theft attack. Several complex attacks have been launched recently that not only exploit vulnerabilities in the Windows OS and Microsoft Internet Explorer, but also launch social-engineering attacks via AOL Instant Messenger, all as part of a larger effort to install keystroke loggers in a victim’s computer for the purpose of phishing.

Attackers have apparently been brushing up on their programming skills as well. Exploit code has become increasingly sophisticated lately. Sample exploits, those that can be quickly found online, used to be of very poor quality, requiring a skilled programmer to painstakingly edit the code in order to produce a working exploit. In contrast, sample exploit code this past quarter has been surprisingly simple to make work. This refined skill on the part of the experts is in turn enabling junior hackers, A.K.A. “script kiddies,” to wreak havoc much more quickly.

Persistence is apparent on the virus/worm front, where an almost constant stream of MyDoom, Bagle, and Netsky mutations continue to appear. The complexity and sophistication of each variant has also been steadily increasing, as spammers align themselves with virus authors in an attempt to increase revenue.

Leaving no platform untouched, viruses and worms also pose a threat to PDAs, cell phones, and other mobile devices. This quarter, multiple pieces of malware began to mount a slow but steady attack on these mobile operating systems. Rapidly becoming the “low hanging fruit” of network targets, mobile computing devices are just starting to become recognized by security managers.

+ Managed Security Services Event Statistics²



In Q3 2004, we observed a 150% growth in the number of security events per device per day over Q3 2003. Q1 and Q2 2004 showed more than 150% growth as compared to Q3 2003. The decrease in Q3 2004 growth amount from Q1 and Q2 2004 reflects the reduced threats and exploits exposed during the quarter. No new major threats were unleashed in the third quarter of 2004.

TOP 10 REGIONS OF SECURITY EVENTS GENERATED IN JULY-SEPTEMBER 2004

Source Country	Percentage of total security events generated
United States	90.75%
Canada	2.51%
China	1.15%
United Kingdom	1.03%
Germany	0.87%
Korea	0.86%
Japan	0.86%
France	0.76%
Italy	0.68%
Russia	0.53%

United States and Canada continue to remain at the top as sources of security events generated. New regions that made the top ten list for Q3 2004 are France, Italy, and Russia. Australia, Netherlands, and Uruguay were in the top 10 for the first half of 2004, and have since dropped off the list.

² Note: In February 2004, VeriSign acquired Guardent, a recognized leader in Managed Security Services. Guardent’s security consulting and managed services are integrated into VeriSign’s solution portfolio. MSS historical reporting has changed to reflect the integration.

Top Attacks seen during Q2 and Q3 2004

RANK	Q2 2004	JULY 2004	AUGUST 2004	SEPTEMBER 2004
1	Telnet Server 2000 rexec password overflow attempt	Windows RPC race condition exploitation	RExec password overflow attempt	Netscape NSS SSLv2 library Client Hello with pad challenge length overflow attempt
2	DDOS shaft synflood	ICMP Ping Flood	Netscape NSS SSLv2 library Client Hello with pad challenge length overflow attempt	NNTP article post without path attempt
3	ASN.1 BER Length Overflow Heap Corruption	MS-SQL version overflow attempt	MS-SQL Slammer Worm attempt	MS-SQL version overflow attempt
4	ICMP Ping Flood	SYN Flood	ICMP Ping Flood	Microsoft SSLv3 library invalid Client Hello attempt
5	SYN Flood	PCT Client_Hello overflow attempt	MS-SQL version overflow attempt	MS-SQL stack based overflow attempt
6	RPC DCOM overflow attempt	TCP port scan detected	Microsoft SSLv3 library invalid Client Hello attempt	RPC portmap request NFS UDP
7	RPC portmap request NFS UDP	FTP Client format string attack attempt	Microsoft Windows ASN.1 library buffer overflow attempt	Netscape NSS SSLv2 library Client Hello challenge length overflow attempt
8	PCT Client_Hello overflow attempt	DCE RPC Locator Service overflow attempt	RPC portmap request NFS UDP	ICMP Ping Flood
9	MS-SQL version overflow attempt	LSASS buffer overflow attempt	Netscape NSS SSLv2 library Client Hello challenge length overflow attempt	SMTP - suspicious attachments (PIF extension)
10	RPC mountd UDP export request	RPC DCOM overflow attempt	Cisco catalyst command execution attempt	SMB remote activation request attempt

Examination of quarterly top attacks and the timeline they follow is a near mirror of the monthly Microsoft patch cycle. Mixed among a barrage of scanning and port-enumeration activity that serves as perpetual attack white-noise, we observed the clear presence of 60-day-or-newer system vulnerabilities under attack. While the most prevalent attacks employ the most readily available tools, “script-kiddie” exploit tools, one must take a broad view of the IT-security landscape; patching can no longer be viewed as a luxury, but a requirement that must be addressed within weeks if not days of release.

Systems not connected to the Internet edge are still at grave risk if they leave the office and become attached to home LANs. Machines infected while connected to cable or DSL networks, and then returned to the office, are a prime target in the hybrid attack model discussed above. These systems now place internal networks at risk for data to be siphoned outside the company.

+ Spotlight on Spam

Over the past 12 months, Internet crime has become increasingly more organized and motivated by financial gain. While “script-kiddie” vandalism remains a serious problem, a significant number of teenage hackers have grown up and are now looking to make a living from crime.

Spam solicitations have become increasingly aggressive. This may reflect the growing use and effectiveness of spam filtering solutions, forcing the spammers to maximize the profits wrung out of their victims. The change may also be in part a response to a new Federal law, the CANSPAM Act, which since January 1, 2004 has effectively criminalized the most profitable forms of commercial spam. Among other provisions, the new law provides stiff criminal penalties, prohibiting false or misleading headers and deceptive subject lines, and requiring commercial emailers to identify their content as an advertisement and provide a valid physical mailing address. For a more detailed description of the CANSPAM Act, see <http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm> .

Spam is the primary vehicle for each of the principal Net crimes, such as advance fee fraud, phishing fraud, and work-at-home carding schemes. The use of networks of captured machines (botnets) to send spam is now routine. Botnets are also used to aggressively seed virus distributions and to perform Distributed Denial-of-Service (DDoS) attacks. A trend towards the monetization of Internet crime is also reflected in these attacks. Captured machines are traded between hacker gangs on both rental and freehold terms. Denial-of-Service attacks are increasingly accompanied by extortion.

The problem of **spyware** is also gaining increased attention. Consumers are now alert to the threat posed by adware, programs that monitor the users surfing in order to deliver targeted advertising. While spam remains the primary tactic employed by phishing gangs, the use of phishing spyware known as theftware is increasing both in the number of attacks and their sophistication. Theftware allows the attacker to perform detailed surveillance of their target in order to enable a complex identity theft such as applying for a fraudulent mortgage in their name.

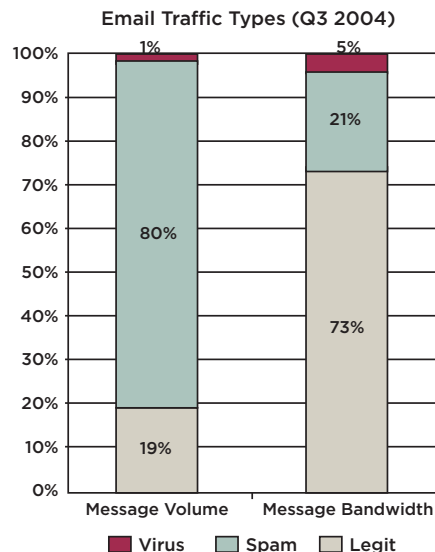
The transition from mindless vandalism to the money motive creates new opportunities for traditional law enforcement approaches. The strategy ‘follow the money’ can now be applied. Even though Internet criminals use captured machines to conceal their connection to their crimes in the same way that traditional bank robbers used stolen cars as get-away vehicles, the flow of stolen funds to the perpetrators is considerably harder to conceal.

In order to profit from phishing schemes, Internet criminals must convert the stolen credentials into fence-able (easily resold) goods or cash. The rise of phishing crime has been matched by a rise in ‘carding’, converting the credentials into laundered funds or fence-able goods. A common tactic of carding gangs is the promotion ‘work at home’ schemes where gullible individuals are recruited to perform the parts of the process most likely to result in arrest. A “**Package Reshipper**” recruit receives goods bought with a stolen credit card and forwards them to the carding ring via an international shipper. A “**Money Mover**” recruit performs a similar function with stolen money.

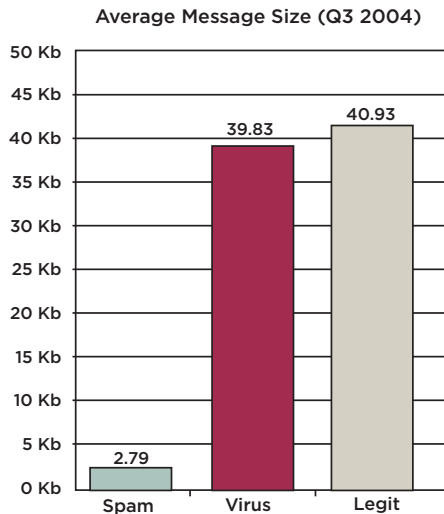
Email Traffic Characteristics

Examining the breakdown of email messages received³ during the period from July 1 to September 30, 2004, we can debunk a commonly held myth about spam traffic: that storage and bandwidth costs are the main problems spam poses to business.

While spam messages represented 80% of email traffic by volume for this period, these messages only constituted 21% of email bandwidth. By contrast, 19% of email messages were “legitimate,” but these messages consumed 73% of the total email bandwidth.



³ VeriSign has partnered with FrontBridge to provide the VeriSign Email Security Service.



Clearly, there is a large disparity between the average message size for spam email and that of viruses and legitimate mail (almost 3Kbytes vs. 40Kbytes). This is because spammers need to send as many messages as possible in as short a time as possible, so they need to keep their message-sizes down. However to bypass filtering while continuing to deliver additional content to unsuspecting recipients, spam messages increasingly contain only links to external images hosted on a spammer's Web server, resulting in messages of only a few hundred bytes.

In operating an email infrastructure, there are both fixed and variable costs in processing each email message. Besides being a nuisance and drain on productivity, spam is a problem primarily because of its impact on the fixed costs (consuming network sockets, creating and deleting spool files, parsing messages, etc.), and secondary on the variable costs (such as the impact on aggregate network bandwidth or disk space). By focusing on reducing the fixed costs, we can lessen spam's impact on the email infrastructure.

Addressing spam

Spam is likely to remain the primary means of Internet crime for some time. Spam is the swamp in which Internet crime breeds! Draining the swamp has thus become an urgent public safety issue.

VeriSign believes that spam control requires both tactical and strategic approaches. Spam and anti-virus filtering services such as VeriSign's Email Security Service employ a tactical approach that provides users with immediate relief. In order to drive spammers from the Internet, a tactical approach must also be combined with strategic measures.

The Aspen Institute roundtable on Internet security identified the lack of accountability in the Internet as a chief cause of the security vulnerabilities of the Internet. When the Internet began, Users were held accountable to the academic institution that provided them with access. These mechanisms were very effective within a small academic community but have failed to scale as the Internet has grown.

To establish accountability it is necessary to decide who to hold accountable. Holding individual users accountable will prove to be unpractical. The generally preferred unit of accountability is a domain name owner—either the domain name given in the email sender's address or the domain name of the mail server which sent it.

The technical architecture for establishing accountability has three parts:

1. Authentication

First, it is necessary to know whether the email is genuinely from the party that is purported to have sent it. Email that is unambiguously identified as a forgery should be refused or discarded.

2. Accreditation/Reputation

Next, it is necessary to know whether the sender is likely to be sending spam. Ownership of a domain name only proves that the sender paid the registration fee. Some form of reliable accreditation is required; this could be provided by third-party verification of bona fides used to authenticate SSL certificate requests or some form of reputation-based system.

3. Consequences

Finally, spammers must face consequences for their actions. Effective sanctions include civil lawsuits, criminal prosecution, or sites refusing to accept further email from the sender.

The authentication technology used for this purpose does not need cryptographic strength; it is more important for the technology to gain broad adoption and deployment. The Sender Policy Framework (SPF) and Sender-ID Framework developed by the Internet Engineering Task Force (IETF) MARID working group are entirely appropriate for this purpose, and VeriSign strongly recommends that all domain name owners publish SPF records (<http://spf.pobox.com> and http://www.microsoft.com/mscorp/twc/privacy/spam_senderid.msp).

TECHNIQUES TO REDUCE EMAIL ADDRESS ABUSE

Email addresses are often **harvested** using robots or spiders that crawl the Web and gather these addresses. All parties that publish email addresses are strongly encouraged to help prevent harvesting. Spammers are interested in harvesting large numbers of addresses with the least effort possible. Even simple measures show a marked reduction in the number of times an address is harvested.

Prevention - if you must expose email addresses, then

- a) Spell out the special characters e.g. securitybriefing AT verisign DOT com
- b) Display it as a graphic
- c) Use explicit html equivalents

Newsgroups, standards groups, discussion boards:

Anyone who has posted a message to a public newsgroup is exposed to spam. Some groups archive the discussions. Some groups are closed and place appropriate safeguards to limit exposure.

Prevention - use an email address specifically established for participation in public group discussions. This will enable better monitoring and disposal of spam.

Brute-force attacks on mail servers:

Here, an attempt is made to send every conceivable combination of letters that form names. Short email addresses suffer the most e.g. bob@foo.com. The email addresses that generated responses are marked as active.

Prevention - Spammers sometimes harvest addresses through 'dictionary' attacks on mail servers, trying a list of common usernames against the domain name of the email server. Most mail servers now provide mechanisms to defeat this type of attack by limiting the number of responses to queries from a given IP address.

Directory harvesting attacks on mail servers:

Prevention - Many mail server software packages have features for preventing dictionary attacks, usually by slowing down or dropping connections after a sender makes multiple attempts to send email to a non-existent address. For example, Sendmail includes the BadRcptThrottle configuration option. For other mail server software, see your server's documentation or contact your software vendor.

Google searches, a simple search of "@.com" results in over a 100 million hits:*

Of course, one can simply buy CDs full of email addresses rather than do the work, but it is trivial to write a parser to extract email addresses from the results of these searches.

Prevention - Nothing can be done regarding this, other than limiting the exposure of your email address using the above preventative suggestions.

In order to help the accountability net to gain critical mass, VeriSign is providing a free accreditation service based on information that has already been collected by the VeriSign Digital Certificate business. The VeriSign Verified Domains List (VDL) is currently available to anti-spam product vendors on application. VeriSign is proposing to make the VDL available to the general public using a DNS based protocol, the details of which have been submitted to the Internet Research Task Force (IRTF) for discussion.

Protection Message 1: Stop, Think and Ask

Consumers can protect themselves against phishing fraud if they remember to stop, think and ask when they see a suspicious message coming from their bank.

Stop:

The old Quaker advice of counting to ten works well in most situations. Even in the Internet age there are few situations that genuinely require immediate action and none that require an immediate response to someone you have never heard from before.

Think:

Are the claims made plausible? A bank that has a security problem will contact you by paper mail. The chances of winning a lottery are slim, the chances of winning a lottery you never entered are zero. Before buying anything from an Internet merchant ask if they can be trusted.

Ask:

Fraudsters will often try to persuade their target not to talk to anyone else. They know that a target who talks to a second person is more than twice as likely to become suspicious. Simply trying to explain a scheme to a second person is usually enough to raise suspicions.

This is based on advice from the Federal Trade Commission.

Tactical and Strategic Approaches to Phishing

Phishing crime should also be approached through a combination of tactical and strategic measures. In the short term we must do all that we can to limit the success of the criminal gangs through tactical measures, but we must also plan a strategy for eliminating this form of crime.

The VeriSign Anti-phishing solution provides financial services companies and other brand owners a set of services to help them minimize the successes of the phishing gangs that target them. These services include early detection of phishing attacks and the assistance with the shutdown of phishing capture sites when an attack is in progress.

Like the strategic solution for the problem of spam, a strategic solution to phishing will require changes to the Internet infrastructure and ultimately, changes to the financial services infrastructure. This is likely to take several years. The phishing problem is the result of the fact that the existing email infrastructure allows any party to impersonate any other party at will. The customer authentication problem has traditionally been viewed in one direction only—authentication of the customer to the bank. It is now time to pay serious attention to authentication in the reverse direction—authentication of the bank to the customer.

The SPF / Sender-ID Framework scheme developed to control spam provides a useful tool, and VeriSign strongly recommends that all financial services providers implement this framework as a matter of extreme urgency.

The authentication provided within the SPF / Sender-ID Framework is acceptably strong for spam prevention and is the best currently available. It is available in a form that is suitable for ubiquitous deployment such that every email message is authenticated. In order to meet all the requirements that are desirable in a strategic anti-phishing solution, however, a stronger authentication mechanism is required—one that provides greater resistance to attack and also allows for email users to be provided with conspicuous proof of the authenticity of legitimate email messages.

These requirements dictate the use of a cryptographic authentication scheme such as the Identified Internet Mail proposal developed by Cisco or the Domain Keys proposal by Yahoo!. An industry wide working group is currently being formed to address this need.

A longer term strategic approach to the problem of phishing crime is to move away from the use of static passwords and credit card numbers as the authentication mechanism to a form of credential that changes every time it is used. A number of European banks have already taken the first step in this process and now issue their customers sheets of passwords with a scratch-off coating. To log into the online banking site, the customer scratches off the next box on the card to reveal the password they should use. The bank keeps track of the passwords as they are used and sends out a new card when the old one is used.

Protection Message 2: Recruits are Expendable

Recruits into Package Reshipping and Money Moving schemes should be made clearly aware that they are involved in a criminal enterprise and that the gang expects them to be caught.

A recruit in a carding scheme faces at least three types of risk:

1. **Monetary loss.** Recruits into carding schemes are usually held liable for the lost funds when they are caught. The fraudulent transfer of funds into their bank account will be reversed. Their transfer of funds to the criminals usually cannot be reversed.
2. **Prosecution and Jail.** Package reshipping is a form of accepting stolen goods. Money movers are participating in money laundering. Recruits need to be made aware that there are no legitimate businesses of this type and that they are almost certain to be arrested and very likely to be prosecuted.
3. **Identity Theft.** Carding gangs frequently perform identity theft on their recruits after they have no further use for them using the details provided when they were recruited.

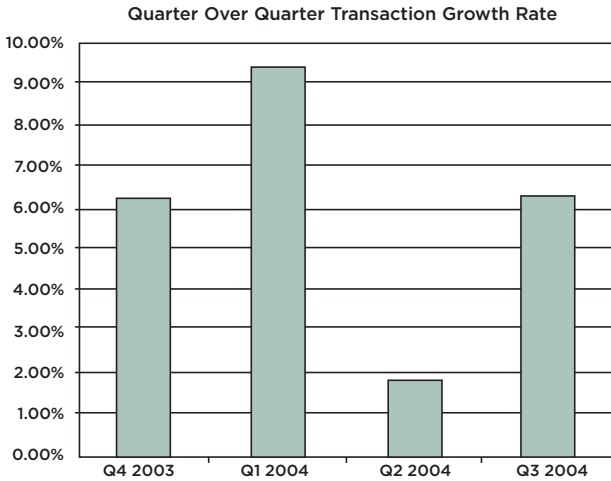
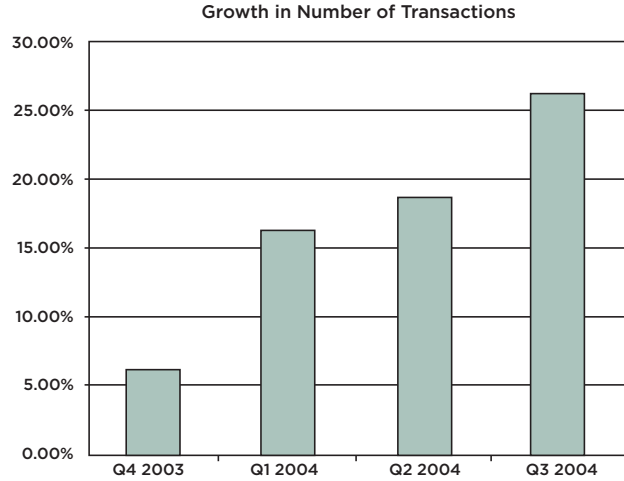
Danger signs.

1. The 'employer' only contacts you by Internet. The carding gangs prefer to use only the Internet because they believe know how to hide on the Internet.
2. The 'employer' asks you to transfer funds through your personal bank account. If you do this you are effectively guaranteeing their transactions.
3. The 'employer' tells you that they have to do business this way because well known companies will not do business with them.

+ Data Trends for Internet Usage

Internet Commerce and Fraud

In tracking the growth of over 700 of the top 1,000 VeriSign Payment Services transacting merchants over the past 12 months, data correlated by VeriSign in the chart below indicates strong growth in Internet commerce with the normal expectations for typical seasonal fluctuations. The chart shows significant growth during Q1 2004 (over Q4 2003) possibly due to post-holiday e-commerce sales as well as improvement in overall U.S. GDP growth rate. The relatively lower growth rate in Q2 2004 over Q1 2004 could be due to traditionally slack retail sales during this period while the more robust growth rate in Q3 2004 over Q2 2004 shows the increase in spending to be expected during the summer months (e.g. online back to school shopping).



Overall, as seen in the chart below, Q3 2004 growth was over 25% higher when compared to the same quarter of the previous year which is further evidence of recovery and even resurgence in Internet commerce. This is likely due to both continued e-commerce expansion into new markets as well as growth in existing markets. In addition, more consumers and businesses are continuing to realize the significant savings by conducting business over the Internet.

Top Countries by Volume of Fraudulent Transactions

There was a change in the ranking of countries for volume of fraudulent transactions during the third quarter of 2004 as compared to our prior H1 2004 report. The United States continues to dominate the list, and Vietnam, Taiwan, Switzerland, and France joined the list as newcomers. Dropping off the list were Ghana, Nigeria, India and Turkey. The emergence of new countries could be due to the continued rollout of high-speed Internet access across the world, which allows more users to access the Internet. Countries were selected based upon the number of transactions that originated from identified IP addresses from that nation.

TOP COUNTRIES⁴ BY TOTAL VOLUME OF FRAUDULENT TRANSACTIONS	
<i>Country</i>	<i>Rank</i>
United States	1
Vietnam	2
Indonesia	3
Great Britain	4
Taiwan	5
Canada	6
Israel	7
Switzerland	8
France	9
Germany	10

⁴ Note: The country of origin is determined by IP Address used for the transaction. It is possible that hackers use proxies or break into ISP infrastructure in other countries to hide their true origin.

Top Countries by Percentage of Fraudulent Transactions

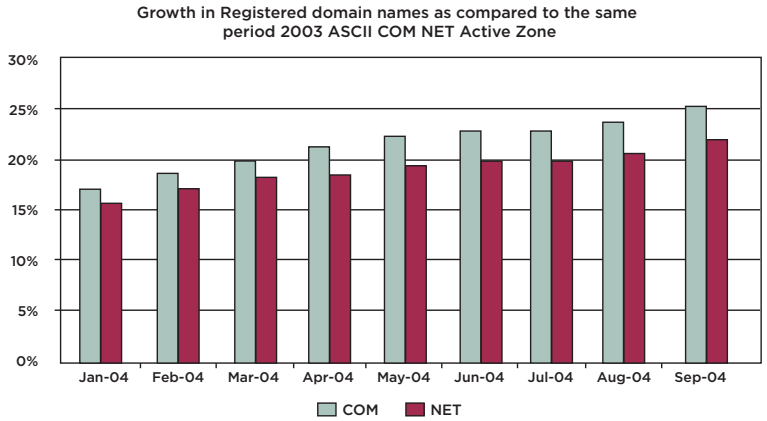
Compared to our H1 2004 report, only three countries with the highest rates of originating fraudulent transactions stayed on the list for the third quarter of 2004. Dropping off the list were Cameroon, Slovenia, Brunei Darussalam, Kenya, Lebanon, and Romania. In addition, the percentage of risky transactions has dropped compared to the numbers presented in the previous briefing. In H1 2004 all of the top ten originating countries were over 80%; that is, 80% of the originating transactions were considered to be risky. Currently, 50% of the top ten originating countries are below 80%. This could be due to wider availability of Internet access resulting in more legitimate transactions entering the system, as well as more stringent fraud screening methods and proactive efforts between security vendors, merchants, financial institutions, and Governments to shut down suspected fraudulent organizations.

TOP COUNTRIES BY PERCENTAGE OF TOTAL RISKY PAYMENT TRANSACTIONS⁵	
<i>Country</i>	<i>Q3 2004</i>
Macedonia, The FYR	100.00%
Nigeria	86.67%
Ghana	85.71%
Vietnam	85.15%
Egypt	81.82%
Indonesia	69.57%
Taiwan	67.21%
Jordan	63.64%
Israel	57.14%
Switzerland	54.00%

+ Internet Usage and Security

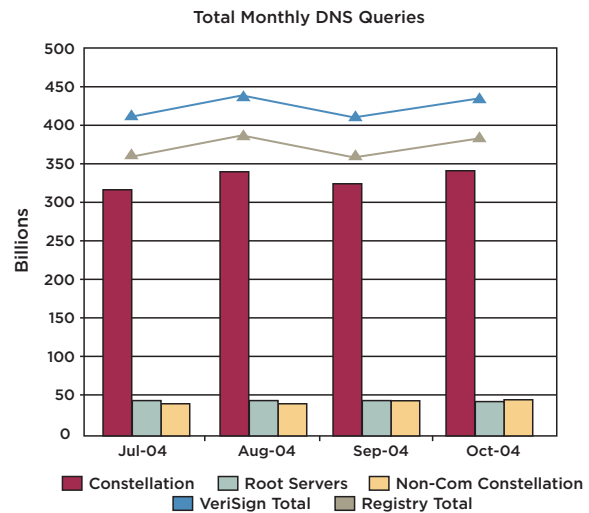
Domain Name Registration

Both .com and .net top-level domains continued to exhibit strong growth as compared to the previous year.



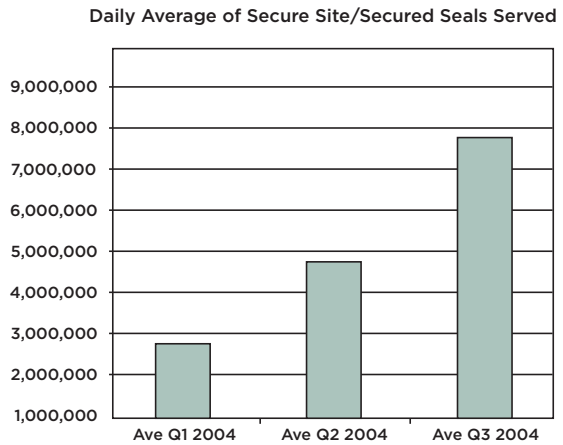
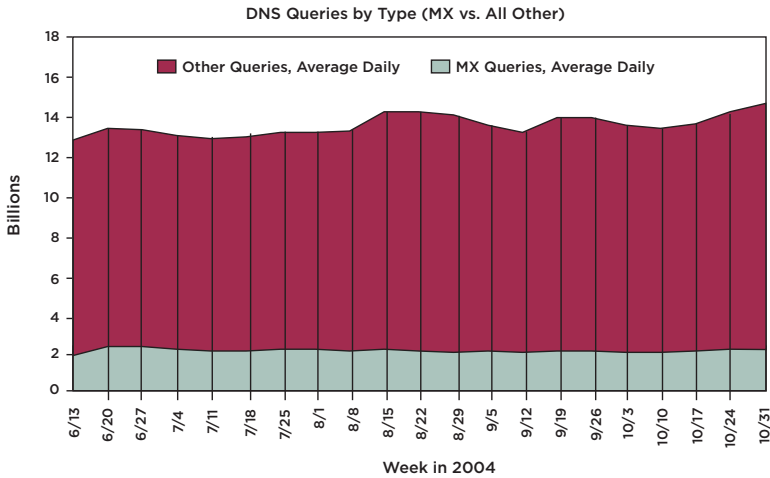
DNS Queries

The total number of Domain Name System queries on a monthly basis hovered between 400 and 450 billion during the third quarter of 2004.



This graph depicts the total number of DNS queries answered by the entire gTLD constellation (13 geographically diverse DNS servers that direct most of the internet's traffic). In addition, this graph includes the total number of queries that were answered by the two Internet Root Servers managed by VeriSign and the non-com constellation.

⁵ Note: Countries were selected based upon the number of risky transactions that originated from the identified IP addresses from that nation. Transactions are deemed risky based upon review of multiple fraud screen filters, including identification of stolen credit card numbers, comparison of shipping and mailing addresses for discrepancies, as well as other techniques.



During the third quarter 2004, the Email based DNS queries (MX query type) remained fairly even—around 2.25 billion queries on a daily average basis. This results in a percentage of email based queries vs. other DNS queries fluctuating between 19% and 24%. In Q4 2003, the average percentage of MX queries vs. other DNS queries was 14%. Obviously, some of the increase in number of queries seen is due to natural growth. However, the increase in DNS queries is also attributable to the growth in malicious activity discussed in this briefing.

Growth in Secured Seals Served

This chart represents the average number of requests for secured site verification on a daily basis. This corresponds to the total number of page views that carry a VeriSign® Secured™ Seal. This chart indicates increased demand among Web site operators for the endorsement implied by the VeriSign Secured Seal, and that increased demand stems from broad awareness among those who shop online to transact only with secured Web sites.

	2003 Q3	2003 Q4	2004 Q1	2004 Q2	2004 Q3
Total Active VeriSign SSL Certificates Worldwide	374,829	384,006	414,092	430,243	447,133

Growth in SSL Certificates

The number of active VeriSign SSL certificates worldwide continues to increase as can be seen by the number in the table above. A healthy 19% increase in Q3 2004 as compared to Q3 2003 which reflects the increasing awareness and demand for security of Internet communications and transactions.

+ About the Internet Security Intelligence Briefing

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

- **Domain Name System (DNS)** – 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/Web servers (e.g., Web sites whose address starts with “https” are secured using SSL certificates). VeriSign is the leading provider of SSL certificates, securing hundreds of thousands Web sites/servers through its certificates.
- **Managed Security Services** – VeriSign provides 24x7 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 analyzed by VeriSign's TeraGuard™ Platform. Further, detailed analysis is then carried out by our Security Research Analysts.
- **Payments and Fraud Protection Services** – VeriSign provides online Payment and Fraud Protection services to over one hundred thousand customers. Over 30% of North American e-commerce payments are processed through VeriSign.

For more information, email securitybriefing@verisign.com.