VeriSign®

INDUSTRY UPDATE

Internet Security Intelligence Briefing

February 2005 / Vol. 2, Issue III

+ 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 and PKI), Managed Security Services (MSS), Payment Services, and Fraud Protection Services.[1] This briefing covers data gathered from October 2004 to January 2005.

This briefing presents data and trends covering:

- Internet commerce during the 2004 holiday season
- Phishing attacks
- 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.™

TABLE OF CONTENTS

+ Summary of Key Internet Statistics

	Q4 2003	Q1 2004	Q2 2004	Q3 2004	Q4 2004
Year-over-year growth by quarter in .com registered domain names	17%	20%	23%	25%	26%
Year-over-year growth by quarter in .net registered domain names	15%	18%	20%	21%	21%
Average number of DNS Queries answered per month in each quarter	307.9 B	337.0 B	379.9 B	380.3 B	389.2 B
Total number of active VeriSign® SSL Certificates worldwide	384,006	414,092	430,243	447,621	454,621
Average number of VeriSign® Secured™ Seals Served Daily	Data Not Available	2.7 M	4.7 M	7.6 M	9.4 M
Total Amount of Settled Transactions Processed by VeriSign Payment Services	$7.71 B	$8.68 B	$8.51 B	$8.77 B	$9.65 B
Total number of Settled Transactions Processed by VeriSign Payment Services	54.19 M	58.66 M	57.45 M	61.62 M	67.79 M

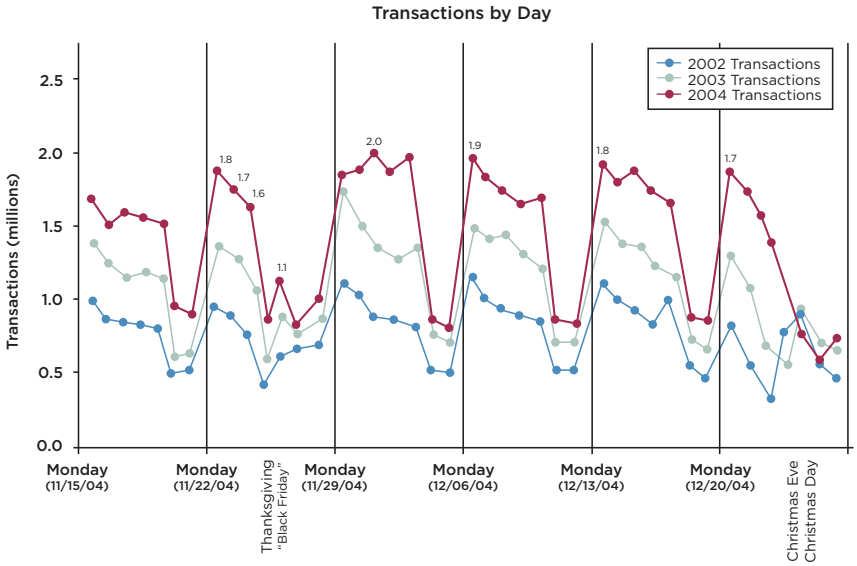
+ Internet Commerce and Fraud Trend

Key Findings

The dollar volume for holiday online commerce rose 88% in 2004 compared to 2003. VeriSign processed almost $12.0 billion in online sales between November 1st and December 31st 2004, compared to $6.4 billion during the 2003 holiday season and $4.0 billion during the 2002 holiday season during the comparable time periods.

Internet merchant transactions for holiday purchases rose 21% in 2004 compared to 2003. VeriSign processed more than 81.5 million Internet merchant transactions (all types) during the 2004 holiday season compared to 64.5 million during the same period in 2003 and 46 million during the 2002 holiday season. Average purchases per transaction decreased approximately 3% to $146 in the 2004 holiday season.

Fraud Protection Services customers identified 6% of e-commerce purchases during the 2004 holiday season as "too risky." The risk of online fraud is rising with increased transaction volume, making merchants cautious when processing online transactions. Transactions are identified as "too risky" based upon a 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 such as monitoring of the origin of payment transactions by IP address geographic location.



This chart represents all payment transactions that were processed by VeriSign Payment Services during the time periods indicated, including settled transactions.

Strong Growth

VeriSign data shows continued strong growth in e-commerce with dramatic increases during the holiday season in 2004. VeriSign data recorded an average of 39% greater transaction volume online as compared to 2003 and an astounding 97% when compared to 2002. Several factors could account for this increase:

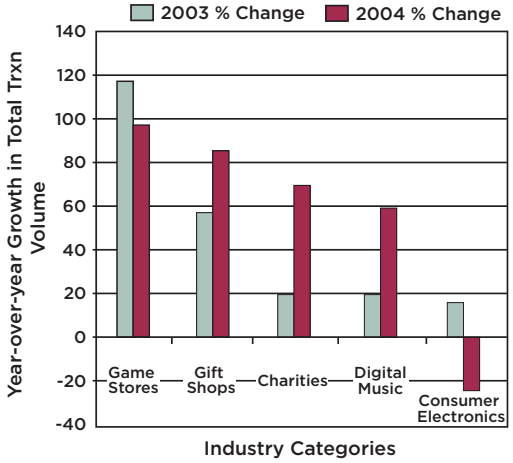
- Increasing customer confidence in shopping online
- Increased broadband and high-speed Internet access penetration across the U.S.
- Wider availability of cheaper goods online
- Greater numbers of consumers becoming less tolerant of crowded shopping malls
- An increasing number of rural consumers shopping online for goods they cannot get locally

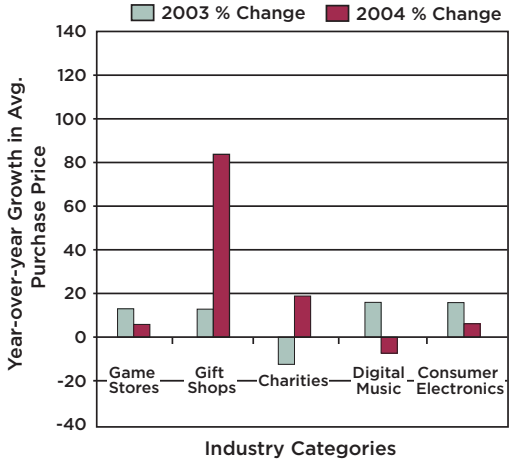
The peak shopping period is still the days around Thanksgiving. For brick-and-mortar merchants, the Friday after Thanksgiving is traditionally the biggest shopping day of the year. (This day is nicknamed "Black Friday," as it has traditionally been the day retailers' books move out of the red and into the black).

However, for Internet merchants, the Monday after Thanksgiving appears to be the biggest shopping day. For the past three years, the most transactions per day have been completed on the Monday after Thanksgiving. Mondays in general remain one of the busiest days for online holiday shopping. It is possible that consumers are going to shopping malls over the weekend to pick out what they want, and then going online to complete their purchase when they get back to their offices on Monday. VeriSign recorded an increase of over 25% growth in 2003 and over 120% growth in 2004 on each Monday after Thanksgiving, as compared to 2002. The increased growth continued up until December 20th – five days before Christmas, after which it dropped to the normal number of transactions for December.

The highest single transaction day of the season in 2004 was December 1st, with close to 2 million transactions. In past years, we recorded a decline in shopping on Christmas day and lower volume over weekends. In 2004, Christmas fell on Saturday, which compounded these two effects and lead to the lowest transaction volume on Christmas day in three years.

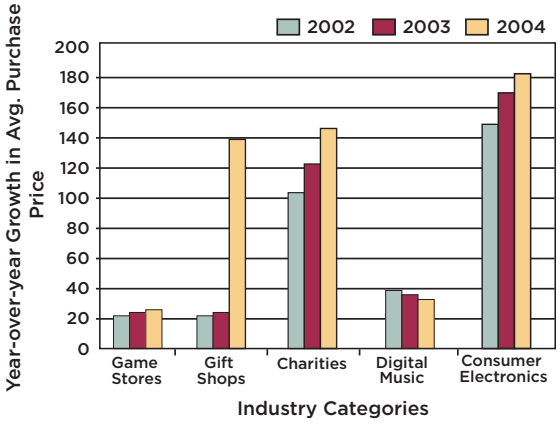
Game Stores and Gift Shops Post Highest Growth in 2004





These two charts were generated by examining the top 1000 transacting merchants of 2004 (as measured by number of settled transactions). The top 1000 merchants were then grouped into Industry categories based on popularity over the holiday season.

Game stores saw 96% growth in total transaction volume and 4% growth in the average purchase price in 2004 as compared to 2003. Sales volumes for Gift Shops grew by 89%, and showed an amazing 83% growth in the average purchase price from 2003 to 2004. Charities recorded an increase of 71% in the total number of donations and a 19% growth in the average donation size from 2003 to 2004. Digital Music saw a 59% increase in transaction volume growth but saw a decrease of 9% in the average purchase price. Consumer Electronics saw a decrease of 27% in transactions but did record a slight increase of 6% in the average purchase price.



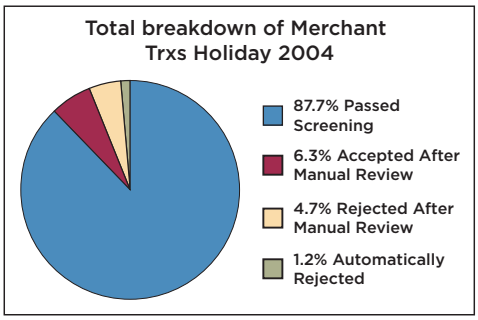
This chart represents the growth in average purchase price based on all the settled transactions of the merchants in each Industry category over the holiday season, as compared to 2003.

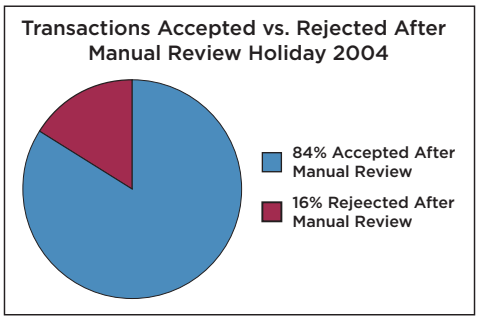
When comparing results from 2004 to those of 2003, Game Stores growth in average purchase price was weak, possibly due to increased pricing pressures in the market place as well as the short product lifecycle. This is reflected in the slow increase in the average purchase price from $22 in 2002 to $25 in 2003 and $26 in 2004. Consumer Electronics in 2003 showed a 19% growth in transactions, but in 2004 experienced a shrinkage of 27%. This could be due to the slim margins and heavy competitive market forces that are usually associated with the industry. It is possible that the brick-and-mortar companies are matching or beating online prices.

Consumer Electronics has demonstrated a steady increase in average purchase price from $147 in 2002 to $ 171 in 2003 and then $182 in 2004. Interestingly, the average purchase price in the Gift Shop category saw a significant uptake. In 2003, the average purchase price grew 12% to $24, but in 2004 the average purchase price jumped a dramatic 83%, to $140. This increase could be due to the wider selection of goods available to consumers and to an increased level of confidence in the security of online shopping due to the availability of strong fraud-protection solutions.

Charities saw their average donation increase from $107 in 2002 to $121 in 2003. In 2004, charities experienced a 19% increase in the average donation, to $150. This increase could be attributed to the widespread effort to help those affected by the Tsunami in South Asia.

Digital Music has recorded consistent declines in growth and average purchase price. In 2002 the average purchase price was $39, in 2003 it dropped to $35, and in 2004 the average purchase price was $32, a drop of 9%. This could be due to increased competition in the market place as more vendors are offering access to music downloads at a lower price.





These two charts were generated by examining the number of transactions that were processed by VeriSign Fraud Protection Services from November 1st to December 31st, 2004. Data was analyzed for transactions that were automatically accepted, rejected or marked for review. Reviewed transactions were either accepted or rejected based upon decisions made by the merchant.

Merchants Continue to Favor Automation Over Manual Review: As more and more merchants begin to enter and expand their online businesses, they must also understand the trade-off between increased automation and greater human oversight. Data for the 2004 holiday season demonstrates a tendency for merchants to favor automation over human oversight. In 2003, 90% of transactions automatically passed fraud screening. In 2004, almost 88% automatically passed fraud screening.

Merchants eventually accepted about 84% of the transactions analyzed for manual review. This is markedly higher than 70% in 2003. This significant change could be due to merchants using their human oversight as the final decision maker for accepting legitimate sales rather than relying too heavily on automated technologies. Increased fraud education in the market place in 2004, as well as a greater prevalence of fraud in 2003, might have provided the impetus for merchants to use their human oversight as the definitive decision maker, in order to more effectively avert risk.

Top Countries by Volume of Fraudulent Transactions

TOP COUNTRIES BY TOTAL VOLUME OF FRAUDULENT TRANSACTIONS	
Quartile Ranking	*Country*
4th - Highest	Romania, United States of America, Vietnam
3rd	Canada, Germany, United Kingdom
2nd	France, Hong Kong, Sweden
1st - Lowest	Turkey

The top-10-countries-of-origin ranking is derived from sorting fraudulent transactions processed by the VeriSign Fraud Protection Services during Q4 2004.The country-of-origin is determined by the 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.

Romania, the United States of America, and Vietnam are in the highest quartile ranking for total volume as a source of fraud over the 2004 holiday period. New entrants to the list are Vietnam, Romania, Hong Kong, and Sweden, while Indonesia, Israel, India, Nigeria, and Malaysia are absent when compared to the 2003 holiday period. The United States remains one of the highest-ranking sources of fraud in terms of transaction volume.

The increase in new entrants is possibly due to the continued penetration of high-speed networks into the infrastructure these countries, providing the impetus for fraudsters to exploit less protected Internet Service Providers (ISP). Also, as the Internet expands its reach globally, more merchants are willing to take additional risks and expand their businesses to increase revenue. Some merchants still choose to restrict e-commerce sales to the U.S. market, which is a strategy that limits revenue in the long run. Merchants who seek additional revenue by expanding globally should also employ an automated, intelligent fraud solution. Coupling manual review and stronger intelligence allows merchants to easily expand their e-commerce business globally, while increasing security.

Top Countries by Percentage of Fraudulent Transactions

TOP COUNTRIES BY PERCENTAGE OF FRAUDULENT TRANSACTIONS	
Quartile Ranking	*Country*
4th - Highest	Belarus, Slovenia, Vietnam
3rd	Jordan, Lithuanian, Mauritania
2nd	Croatia, Poland, Ukraine
1st - Lowest	Morocco

The top-10-countries-by-percentage-of-fraudulent-transactions ranking is derived by calculating the ratio of fraudulent transactions to the total number of transactions originating from the same region. The country-of-origin is determined by the 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.

The list for top countries by percentage of fraudulent transactions for 2004 is completely different from the equivalent list for 2003. Belarus, Slovenia, and Vietnam are in the highest quartile as a source of fraudulent transactions over the 2004 holiday period.

+ Phishing Attacks

In the July 2004 report we explain in detail how phishing attacks work. Basically there are two critical elements to every phishing attack:

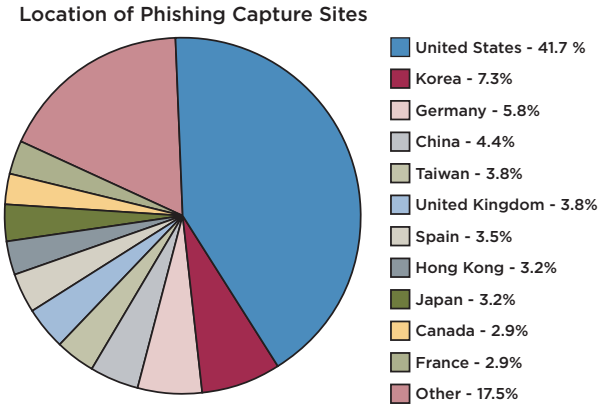
1. **Capture Site**

   The capture site is the machine that obtains the stolen access credentials from the victims. This is almost always a Web site and is typically located on some form of an anonymous host.

2. **Advertisement**

   It is unlikely that victims will discover a phishing attack site by chance so advertising the capture site is usually required. The advertisement usually impersonates the true identity of the site that the capture site resembles. The most common impersonation mechanisms are spam and domain name registrations.

In most cases, perpetrators use a series of anonymous hosts to avoid identification. It is equally important for the perpetrator to conceal the creation of the capture site, the source of phishing spam, and the recovery of encrypted data. In reviewing some 350 phishing attacks over Q4 2004, The VeriSign® Phishing Response Service team discovered that the capture sites for these attacks were distributed geographically over 37 countries. This distribution makes it extremely difficult to limit the harm some of these phishing attacks can incur, as capture-site shut-down may take a long time. It requires bridging foreign policies, language, and business practices. It also requires strong foreign alliances with ISPs and law enforcement agencies.



This chart depicts the location of the capture sites in 350 phishing attacks reviewed in Q4 2004 by the VeriSign Phishing Response team.

58% of the capture sites are located outside of the US which is higher than the 37% reported for the first half of 2004 in the July 2004 Internet Security Intelligence Briefing. This is exactly as VeriSign expected, given that shutting down capture sites hosted in foreign countries is far more difficult than those hosted domestically. However, the United States still continues to host the highest number of phishing capture sites. 11 countries hosted more than 82% of the capture sites, with the remaining capture sites being hosted in 26 countries.

+ Threats and Trends

New security threats continue to increase in volume at a staggering pace. In reviewing Q4 2004, VeriSign observed a record number of new exploits, worms, and viruses, often appearing on public networks within days or hours of the release of proof-of-concept exploit code.

Fortunately for all potential victims, exploits of late have relied on users having to "click here." The most far reaching and damaging worms during the past few years, worms like Code Red, Blaster, Slammer and Sasser have all been able to propagate on their own, without user interaction. These worms targeted vulnerabilities in applications left running and exposed on perimeter servers, though they were almost always successful in finding their way inside corporate firewalls via mobile users, laptop-carrying consultants, or poor demilitarized zone (DMZ) design. "Click-here"-based attacks exploit vulnerabilities within a desktop system, an area inside the corporate firewall, and are therefore historically considered difficult for an attacker to penetrate. While we have seen click-here style trojans for many years, this past quarter gave rise to a record number of new variants.

Users are inundated with pop-up windows, spam, and Instant Messenger links, all prompting click-through for some type of reward, while in reality they are prompting infection. To date, these attacks have largely resulted in more spam, but worse, phishers have used these same techniques to install keystroke loggers, and it is possible that a doomsday worm, set to go off at a future date, could be installed using such methods.

Hostile and compromised advertisement banners represent another point of entry for such trojans and are a much more challenging problem to address. To date the Internet community has been largely effective at self policing banner ads, however this solution does not provide 100% coverage, nor does it address zero-day infections. Anti-virus firms work around the clock to keep desktop systems protected against these click-here trojans, and while effective on the corporate front, un-protected home users are still highly vulnerable to attack.

In addition, an increasing variety of devices are being targeted for attack. Bluetooth phones, Web-cams, printers, and other networked hardware are all being used as platforms for various forms of malware. Organizations and home users need to consider these devices, as well as handhelds, game-systems, security-systems, and anything IP-enabled, as part of their normal security policy. User education and vigilant, preferably layered anti-virus protection are the strongest defenses against such threats.

Conventional passwords are becoming obsolete

One of the more alarming trends seen this quarter is that conventional passwords (eight characters or less in length, regardless of the complexity), are now considered short, and no longer secure. Worms capable of carrying out dictionary and brute-force attacks are becoming more common, as well as a new style of attack, known as the pre-computation attack. With the advent of faster CPUs, along with cheap storage, attackers have now computed all possible eight character passwords, hashed them, and store them for convenience on a DVD. Even complex passwords like 1l0veY0u, can now simply be looked up from their hash. Several Web sites will even recover a password for you based on the hash.

Fortunately, there are other options. Using long passwords or "pass phrases" is a simple and effective solution. Using a password like, "I love my house on the main street" is not only easy to remember, but computationally secure. One-time passwords are another useful alternative and should be considered seriously.

TOP 10 REGIONS OF SECURITY EVENTS GENERATED IN Q4 2004

Source Country	*Percentage of the Top 10 regions of Security Events Generated*
United States	79.28%
Canada	5.65%
Korea	2.48%
United Kingdom	2.36%
Russia	1.82%
Germany	1.52%
Israel	1.47%
Japan	1.43%
India	1.35%

Security Events are measured by the number of alerts generated by security devices that are monitored and managed through VeriSign® Managed Security Services (MSS). VeriSign MSS manages intrusion detection systems, intrusion prevention systems, and firewalls that reside either at the perimeter or inside the customers' network.

The United States and Canada are once again the primary sources of security events generated. These two countries have consistently remained at the top since Q4 2003. Compared with the top ten in Q4 2003, new regions in Q4 2004 are Taiwan, Korea, Russia, and Israel. The regions that dropped off the Q4 2003 list are The Netherlands, Australia, China, and Uruguay. Interestingly, China, France, and Italy were among the top regions for Q3 2004 and have since been replaced by Taiwan, Israel, and India.

In comparing the top regions of security events generated and the top regions in which phishing capture sites are located, one cannot help but notice how closely the two lists match.

Top Attacks seen during Q4 2004

RANK	OCTOBER 2004	NOVEMBER 2004	DECEMBER 2004
1	NNTP article post without path attempt	NNTP article post without path attempt	Netscape NSS SSLv2 library Client Hello with pad challenge length overflow attempt
2	Netscape NSS SSLv2 library Client Hello with pad challenge length overflow attempt	Netscape NSS SSLv2 library Client Hello with pad challenge length overflow attempt	NNTP article post without path attempt
3	Microsoft SSLv3 library invalid Client Hello attempt	Microsoft SSLv3 library invalid Client Hello attempt	Microsoft SSLv3 library invalid Client Hello attempt
4	MS-SQL version overflow attempt	RPC portmap request NFS UDP	Half-open SYN attack
5	Netscape NSS SSLv2 library Client Hello challenge length overflow attempt	MS-SQL version overflow attempt	Netscape NSS SSLv2 library Client Hello challenge length overflow attempt
6	RPC portmap request NFS UDP	MS-PCT Client Hello overflow attempt	RPC portmap request NFS UDP
7	ICMP Ping Flood	Netscape NSS SSLv2 library Client Hello challenge length overflow attempt	MS-PCT Client Hello overflow attempt
8	NNTP version overflow attempt	RPC mountd UDP unmount request	MS-SQL version overflow attempt
9	MS-SQL stack based overflow attempt	RPC mountd UDP export request	ICMP Ping Flood
10	Port Zero traffic detected	NNTP version overflow attempt	RPC mountd UDP unmount request

This table shows the unique signatures that were triggered by VeriSign customers' intrusion detection systems that VeriSign Managed Security Services has under management.

Application and network reconnaissance remain a steady source of security events as can be seen by the Half-open SYN attack, Port Zero traffic detected and ICMP Ping Flood.

Both humans and worms continue to scan for systems which are un-patched for common exploits, contributing a large percentage of the total security events volume. These vulnerabilities tend to cluster around a few major themes: RPC, SSL, and SQL vulnerabilities.

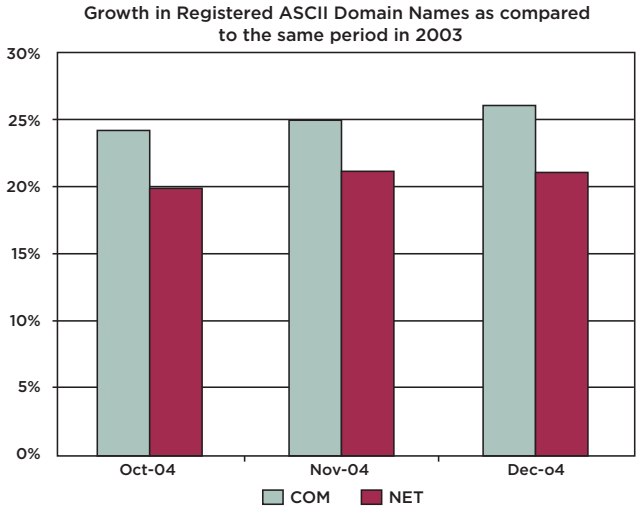
In addition to reconnaissance, most security events are being generated by worm propagation attempts, such as "MS-SQL version overflow" attempt and "MS-PCT Client Hello overflow" attempt. During Q4 2004, VeriSign counted over 680,000 "MS-SQL version overflow" attempts and over 375,000 "MS-PCT Client Hello overflow" attempts.

Also, there are many Unix attacks that are still being attempted against the previous Netscape SSL, Sun RPC, and NNTP vulnerabilities. This shows that once exploit codes are available, they remain a constant threat against un-patched systems. Therefore, one has to remain diligent when providing Internet access to legacy systems or when performing backup recovery, which may revert to an un-patched system.

+ Internet Usage and Security

Growth in Domain Name Registration

In 2004, the .com top-level domain grew (for the year) over 25% and the .net top-level domain grew over 20%, showing continued strong demand and usage of these domains.



This chart depicts the growth in Q4 2004 of the total number of ASCII domain names registered in the .com and .net top-level domains as compared to Q4 2003.

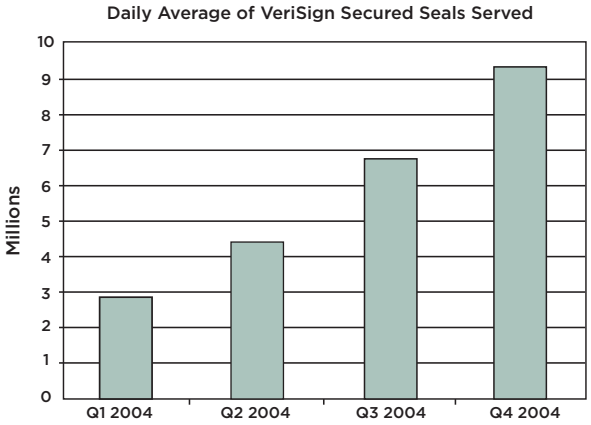
In operating the generic Top-level Domain Registries (gTLD) for .com and .net, VeriSign processes more than 14 billion queries, on average, each day. Domain names ending in .com represent the largest percentage of domains in the world; approximately 40 million domains currently end in .com. While .net domains currently number around 5 million, a significant portion of the Internet relies on .net, making it one of the world's most valuable communications networks.

Growth in SSL Certificates

The number of active VeriSign® SSL Certificates worldwide continues to grow, with more than 15% growth in 2004 over 2003.

Total number of Active VeriSign SSL Certificates Worldwide	2004			
	Q1	*Q2*	*Q3*	*Q4*
	414,092	430,243	447,133	454,621

Continued Dramatic Growth in Secured Seals Served

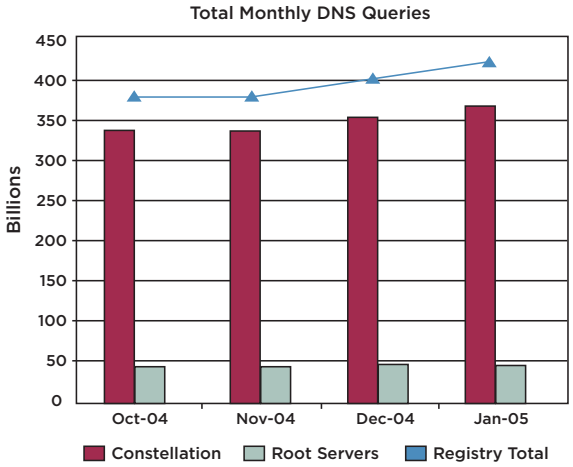


This chart represents the average number of unique visitors that access a web page displaying a VeriSign Secured Seal on a daily basis, within any ten day period.

There is a continued dramatic increase in the number of verifications of secure sites, reaching well above 9 million verifications per day in Q4 2004, indicating a continued strong demand among Web site operators for the endorsement implied by the VeriSign Secured Seal and the increasing behavior of online shoppers to conduct transactions only with secured Web sites.

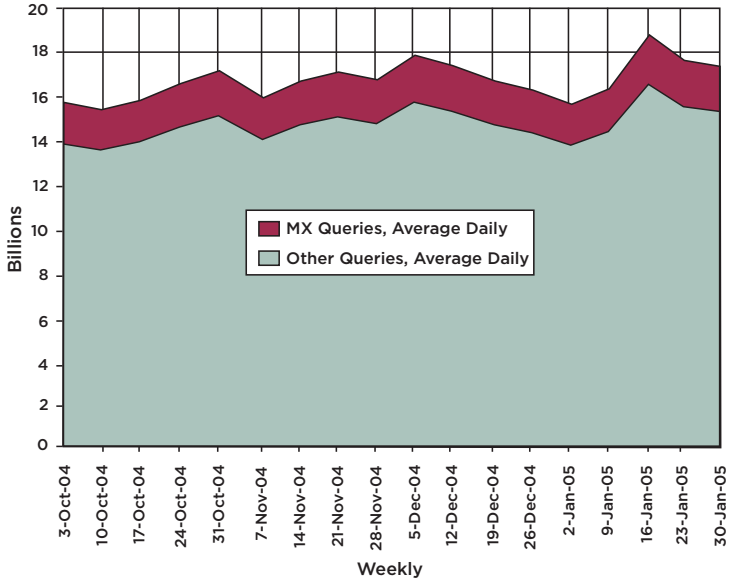
Continued steady growth in DNS Queries

The total number of Domain Name System queries answered by the entire generic Top Level Domain constellation, in Q4 2004 fluctuated between 380 and 400 billion queries per month. This is higher than in July 2004 by about 30 billion queries and is an astonishing 80 billion queries more than what was answered in December 2003. This clearly indicates that there is a continued healthy growth in Internet usage.



The chart above depicts the total number of DNS queries (for .com and .net) answered by the entire gTLD constellation (15 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 3 Internet Root Servers managed by VeriSign.

DNS Queries by Type (Email vs. all others)



This chart depicts the distribution of the total number of DNS queries on a daily basis by type.

The number of email-based DNS queries (MX query type) continues to track all the other types of DNS queries evenly, at roughly 13%. This is much lower than the 19-24% range reported for Q3 2004, but in line with the 14% reported for Q4 2003. This drop in email-based DNS queries over the fourth quarter of each year (2003 and 2004) may be attributed to the holidays (and some company shutdowns) reducing the amount of business email.

The noticeable increase in the total number of queries around December 5th 2004 and January 16th 2005 was due to a domain misconfiguration by a third-party for a few hundred domains, which resulted in the extra traffic to the VeriSign DNS Service.

+ 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 13 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 127,000 customers. Over 37% 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/internet-security-briefing.html

02/05