

Executive Summary

The VeriSign Internet Security Intelligence Briefing reports current trends in Internet growth, usage, security and online fraud. The quarterly briefing includes data and intelligence correlated from VeriSign's Internet infrastructure services, including DNS (Domain Name System), digital certificates (SSL and PKI), Managed Security Services, Payments and Fraud Protection Services.

This briefing first presents Internet commerce trends and risks since the data covers the late 2003 holiday season. The briefing updates Internet security and usage trends.

KEY FINDINGS:

Holiday online commerce dollar volume rose 59%. VeriSign processed \$6.4 billion in online sales between November 1st and December 31st, 2003 compared to \$4 billion during the 2002 holiday season.

Internet merchant transactions rose 40%.

VeriSign processed more than 64.5 million Internet merchant transactions during the 2003 holiday season compared to 46 million transactions during the same period in 2002. Average purchases per transaction rose 14% to \$152¹ in 2003.

Merchants rejected 7% of e-commerce purchases as "too risky." The risk of online fraud is rising with increased transaction volume, making merchants cautious when processing online transactions. VeriSign data reports that merchants rejected more than 7% of e-commerce purchases as too risky to fulfill. Most web merchants use a limited amount of intelligence for making risk-related transaction decisions. In this briefing, VeriSign presents a range of updated e-commerce risk data that enables e-merchants to leverage more intelligence for more accurate automated fraud detection.

Internet domain registrations continue

steady growth. The Internet continues to grow at a healthy pace, with 16% more active, registered domain names in the ".com" and 14% in the ".net" top-level domains in December 2003 over 2002.

Probes by potential attackers grew 176%.

No major threats were seen during Q4 2003, however the number of security and network events generated per device each month far exceeds previous rates, up 176% in December 2003 as compared to May 2003. VeriSign also measured a continuing pattern of growth in the number of DNS queries, up an average of 37% from July through December 2003 as compared to 2002.

VeriSign's ability to detect, investigate and resolve security issues is dramatically improving with the use of sophisticated correlation techniques on data drawn from our various services. These capabilities are illustrated in two case studies below.

¹ Average purchase price calculated off of sales and authorization transactions only, as opposed to the entire transaction pool, which includes credits and settlements.

CONTENTS

Executive Summary	1
Internet Commerce and Fraud Trends	3
Internet Security and Usage Trends	9
Two Case Study of Correlation between Fraud and Security Data	14
Conclusion	15
About the Internet Security Intelligence Briefing	16



Internet Commerce and Fraud Trends

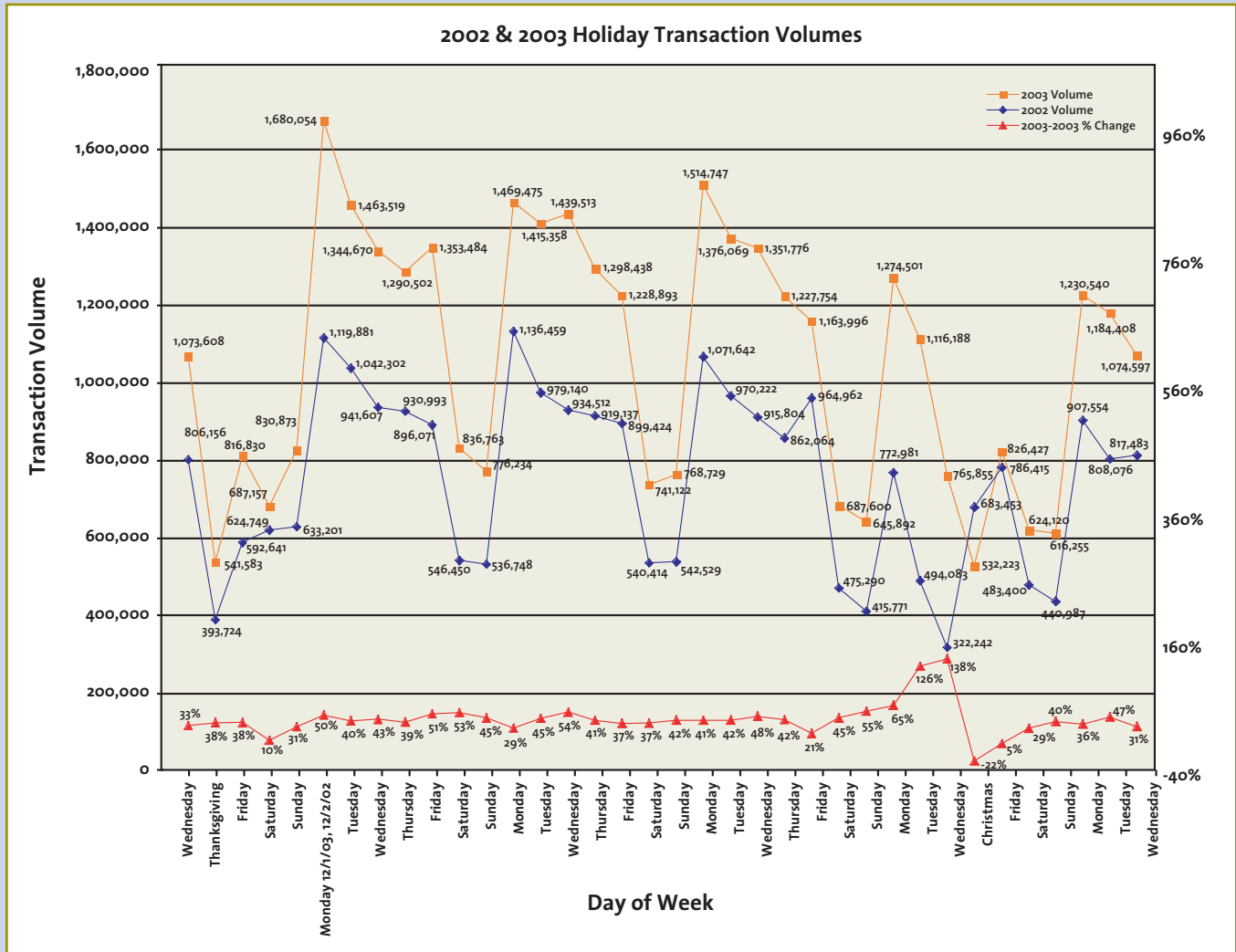


Figure 1

Continued Steady Growth: E-commerce continues steady growth with dramatic increases during the holiday shopping season in 2003. VeriSign data recorded 59% greater sales volume online than the previous year. Mondays remained the busiest transaction day for online holiday shoppers, perhaps reflecting a trend of people browsing physical shopping malls on the weekend and then going online Monday to buy products for

the lowest price. The peak-Monday pattern held up until December 22nd – just three days before Christmas. The highest single transaction day of the season was Monday, December 1st with close to 1.7 million transactions.

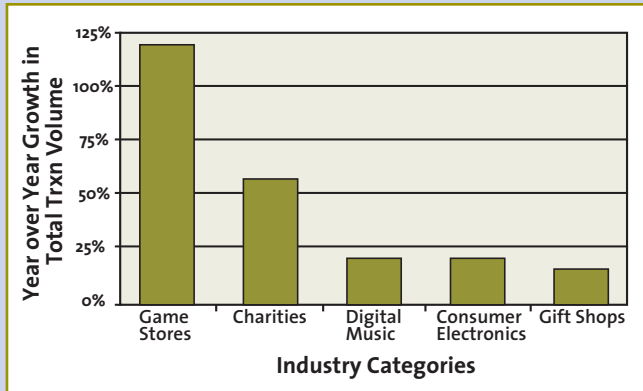


Figure 2

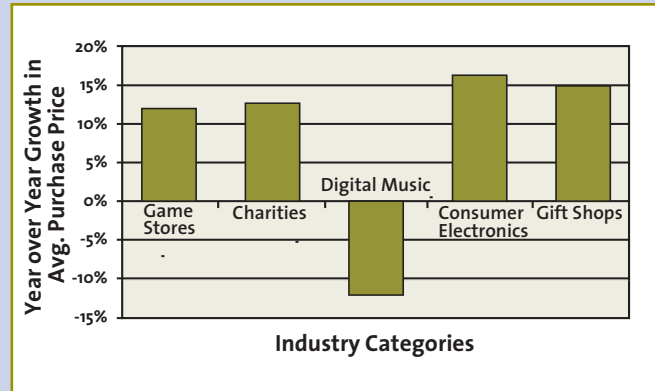


Figure 3

Video Games and Charities Post Highest Growth:

Charities and video game merchants (labeled “Game stores” in the two charts above) grew the most from 2002 to 2003. Charities saw a 55% growth in total dollar volume of donations, and 13% growth in size of average donation. Sales volume for video game merchants grew 119%, with 12% growth in average ticket size. Consumer electronics was the largest category in terms of aggregate dollar volume, but it posted a lower growth rate. Total same store dollar volume in this category grew 19%, while the average ticket size rose 16%.

Digital music was the standout anomaly. The category grew 19% in dollar volume from 2002 to 2003 but its average ticket size dropped 12%. A potential reason for the drop is a shift by consumers towards buying individual songs in lieu of bulk CDs and music broadcast subscriptions.

Merchants Continue Perceiving E-Commerce as Risky:

Transaction rejections during the 2003 holiday season indicate that merchants ascribed excessive risk to many e-commerce transactions. VeriSign recorded merchants rejecting on average more than 7% of the total transactions performed at their websites. This percentage represents merchants’ perception of potential fraud, not perpetration of actual fraud. While E-Commerce fraud statistics range widely on a per merchant basis, it is likely that merchants turned away a significant amount of legitimate business due to fears of potential fraud.

Merchants that deployed risk detection systems to screen customer purchases over the holiday season affected approximately 10% of their total transactions. The highly automated risk management processes leveraged by these merchants resulted in escalation of just 4% of total transaction volume for manual review.

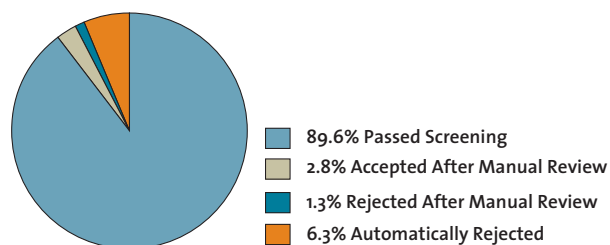
Total Breakdown of Merchant Trxns Holiday 2003

Figure 4

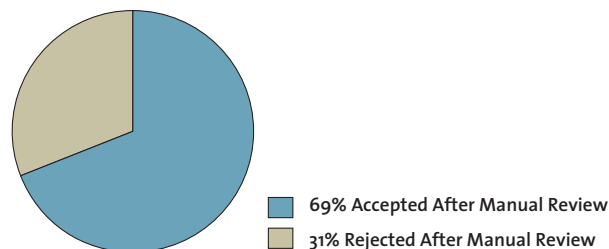
Transactions Accepted vs. Rejected After Manual Review Holiday 2003

Figure 5

Merchants Favor Automation Over Manual

Review: In scaling risk detection operations, merchants must tradeoff between increased automation and greater human oversight. Data for the holiday season 2003 displayed a tendency by merchants to favor increased automation over human oversight. Merchants automated a significant amount of their risk analysis, probably due to peak transaction volumes experienced during the holiday shopping season. Of all the rejected transactions during this period, 84% were automatically rejected by risk detection systems. Merchants eventually accepted about 70% of the transactions pulled for manual review.

The bias to reject orders with automated technologies but accept orders with human oversight may have resulted in merchants turning away a significant number of legitimate sales. Integration of automated fraud detection and fraud intelligence technologies with daily e-commerce operations can limit false-positive rejections and help capture legitimate business. Bringing a greater degree of fraud intelligence to bear on each transaction is essential to effectively managing the resources applied to risk management. Fraud intelligence is a key enabler for the overall scalability of the web as a sales channel.

Merchants Favor Simple Over Complex

Screening: Vendors of risk detection systems incorporate a wide range of data from full validation of physical addresses to geo-location screening of virtual addresses. Most merchants, however, rely on a limited set of rules for risk identification. Of frequently used screening rules, Address Verification Service and Card Security Code are most popular. About 70% of merchants using VeriSign's Fraud Protection Services limit themselves to the simple rules. This practice is likely due to a lack of familiarity with more sophisticated screening logic, or the perception that increased screening could increase the number of transactions merchants may erroneously reject or have to manually review. VeriSign predicts merchants will eventually need to leverage greater fraud intelligence as a way to improve risk detection and overall operational efficiency.

This table lists the Top 5 fraud rules merchants used to review transactions during the holiday 2003 shopping season.

Adoption of Fraud Screening Rules/Techniques

1	Address Verification Service (AVS)
2	Card Security Code (CVV2, CVC2, CID) ²
3	Card BIN number screening
4	E-Mail service provider screening
5	International order screening

² Card Security Code is a credit card verification number. It allows the Merchant to ascertain that the Shopper does have the credit card. Known as CVV2 for Visa, CVC2 for MasterCard and CID for Discover and American Express, the CSC three-digit number is typically located on the back of a credit card.

Table 1

Deployment of Simple vs. Sophisticated Screening Holiday Season 2003

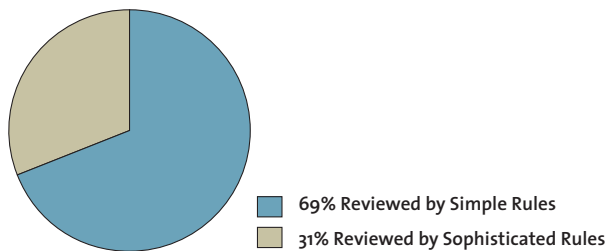


Figure 6

Impact of Customer Error On Risk Detection Holiday Season 2003

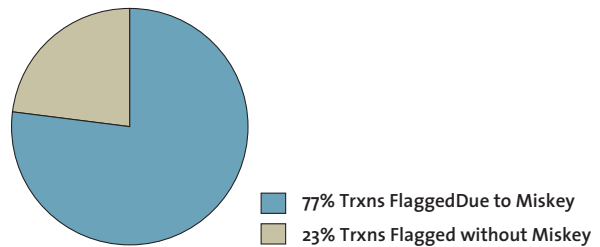


Figure 7

Data from the 2003 holiday season provides two cautionary notes to relying on simple screening methods for risk detection.

Impact of Customer Error: Transaction data suggests that 25% of e-commerce transactions flagged by a merchant's risk detection system may stem from mis-keyed or inaccurate customer information. Examples include inaccurate entry of CVV2 numbers, zip codes and credit card numbers. These inaccuracies are not always mistypes/typos. Customers may correctly type in new addresses that they have not yet updated with their bank, thereby failing AVS checks. While the risk system is correct to flag inaccurate information, the vast majority of these transactions are not fraudulent but merely indications of human checkout error. Websites that store password protected customer profiles can reduce input error, however the storage of financial information significantly raises the business's data security requirements.

Clear checkout processes can help cut this error rate but will not eliminate the problem. Customer input error will continue to drive operational inefficiencies in risk screening systems. For this reason it is important to use multiple screens on customer information in order to gain a more holistic view of the transaction. Merchants should also collect and screen information that customers do not manually input such as the customer's IP address, the number and type of products in a customer's purchase and the total checkout price.

Customer error is especially relevant given the rollout of new buyer authentication programs such as Verified by Visa and MasterCard SecureCode. Collecting accurate passwords is essential to gain liability protection from the card associations. Given the potential levels of customer input error, merchants must consider improving error handling at checkout.

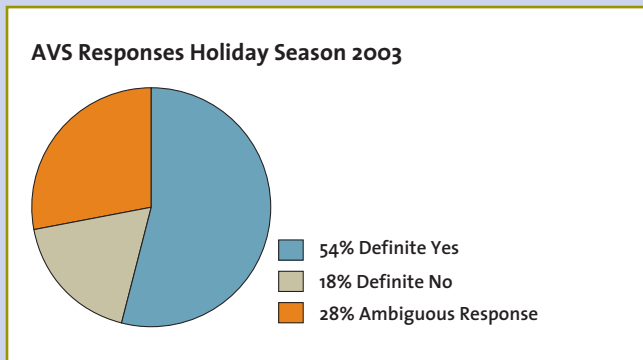


Figure 8

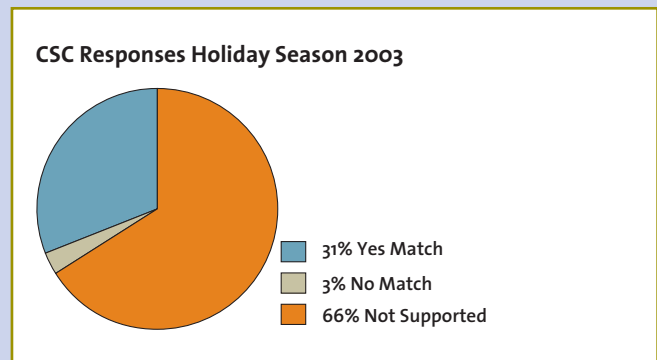


Figure 9

Limits of AVS and CSC Feedback: Address Verification Service (AVS) and Card Security Code (CSC) are security techniques merchants typically use to increase the trust in a customer transaction. AVS matches the customer's billing street address and zip code against the data on file with the issuing bank. Conceptually, only the cardholder should know the billing address. CSC matches the number strings printed on the credit card with that on file with the issuing bank. Conceptually, only the individual in possession of the card should have access to this information. Both AVS and CSC are examples of data consumers are prompted to manually input at the checkout. VeriSign's data analysis found that in 83% of web transactions, merchants used AVS as a form of risk intelligence. CSC was used in less than 40% of transactions.

AVS and CSC are helpful indicators in assessing the risk level of a transaction but are not definitive. Analysis of the feedback from these techniques showed that merchants receive an unambiguous match for AVS in just 54% of transactions, thus indicating that the purchaser correctly knows the street and zip code of the billing address. About 30% of the time merchants receive ambiguous information, such as one data element is accurate but another is not, or the issuing bank does not support AVS. With CSC, the results are less definitive. In 66% of the transactions, issuing banks do not support CSC as a card authentication method.

Merchants may often receive feedback that either confuses or provides limited insight into the risk decision process. These hurdles require maximizing the fraud intelligence brought to bear on the transaction, helping merchants make informed, accurate and profitable decisions.

International Fraud Continues to Plague

Merchants: The United States of America leads all countries in total volume as a source of fraud, but a handful of overseas countries continue to lead in rates of fraud. Indonesia is the newest country joining the Top 10. In response to the high fraud rates associated with international transactions, some merchants have chosen the revenue-limiting strategy of restricting e-commerce sales to the U.S. market. Although international transactions may present greater risk, this should not preclude abandoning international sales. Transaction approval decisions should incorporate a spectrum of fraud intelligence. Manual review and stronger intelligence play an important role in expanding the global potential of e-commerce.

Indonesia was the number one source of fraudulent transactions over the 2003 holiday season based on the ratio of fraudulent transactions to the total number of transactions in the same region. Nigeria, the top source in the last briefing dropped to second place.

**Top Countries³ By Total Volume
of Fraudulent Transactions**

Country	Ranking
USA	1
Canada	2
Indonesia	3
Israel	4
United Kingdom	5
India	6
Turkey	7
Nigeria	8
Germany	9
Malaysia	10

**Top Countries³ By Percentage
of Fraudulent Transactions**

Country	Ranking
Indonesia	1
Nigeria	2
Pakistan	3
Ghana	4
Israel	5
Egypt	6
Turkey	7
Lebanon	8
Bulgaria	9
India	10

³ Note that 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.

Table 2 & 3

Internet Security and Usage Trends

Domain name registrations continue steady growth: The number of active domain names registered in “.com” and “.net” continues to grow at a steady pace. VeriSign’s registration data indicate the count of active registered domains in these top-level domains has almost completely recovered from the dot-com downturn. The chart below

shows 2003 monthly growth in the number of registered, active domain names as compared to the same months in 2002. Domains in .com and .net together grew 13.76% in Q3 2003 and 16.14% in Q4 2003 compared to registered active domain names in 2002.

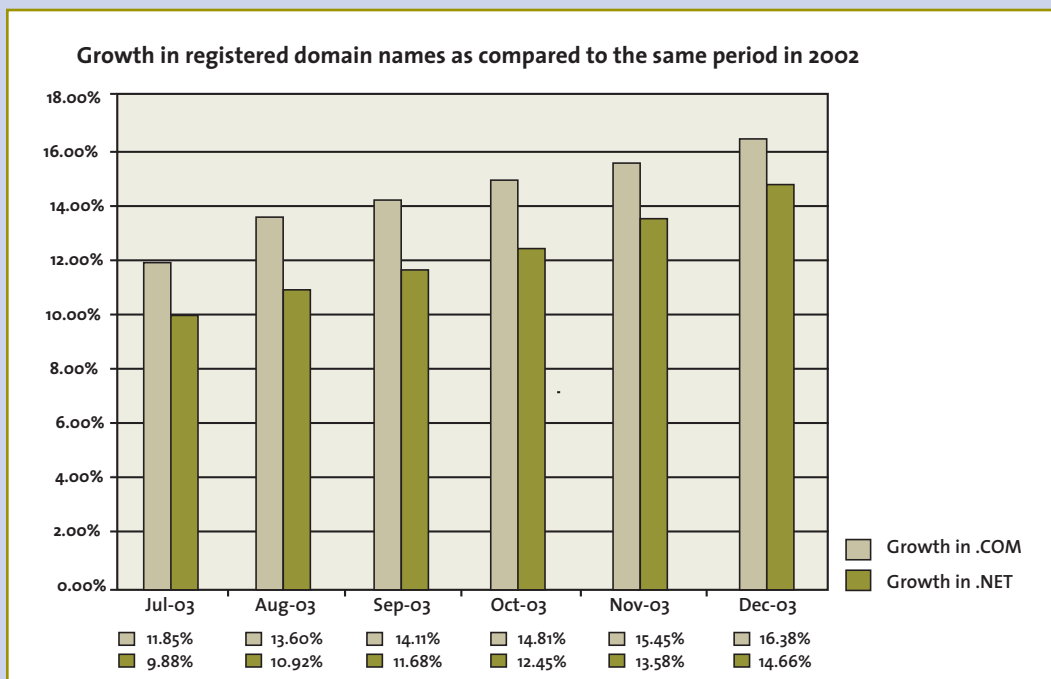


Figure 10

DNS queries: The growth in active domains corresponded with a continued increase in number of total DNS queries to the Top-Level domains and the Root domains operated by VeriSign. The term “Constellation” in Figure 11 and 12 refers to VeriSign’s global top-level domain resolution infrastructure.

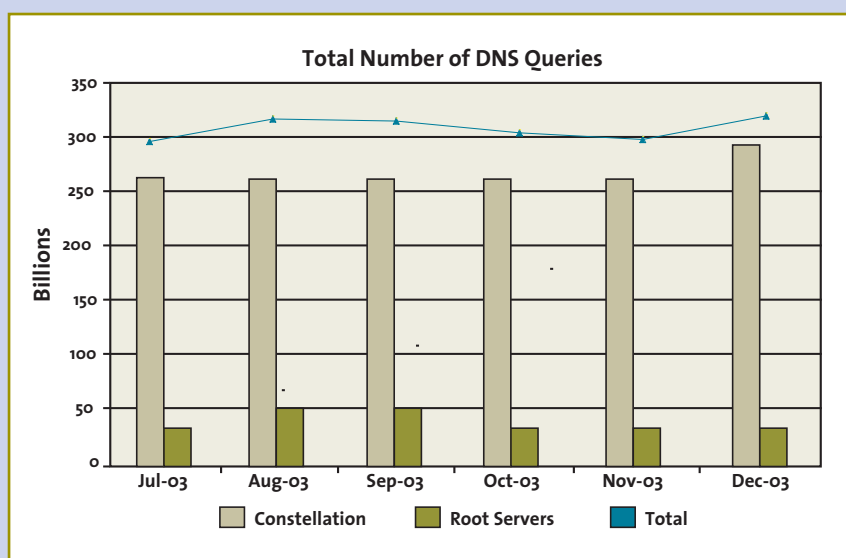


Figure 11

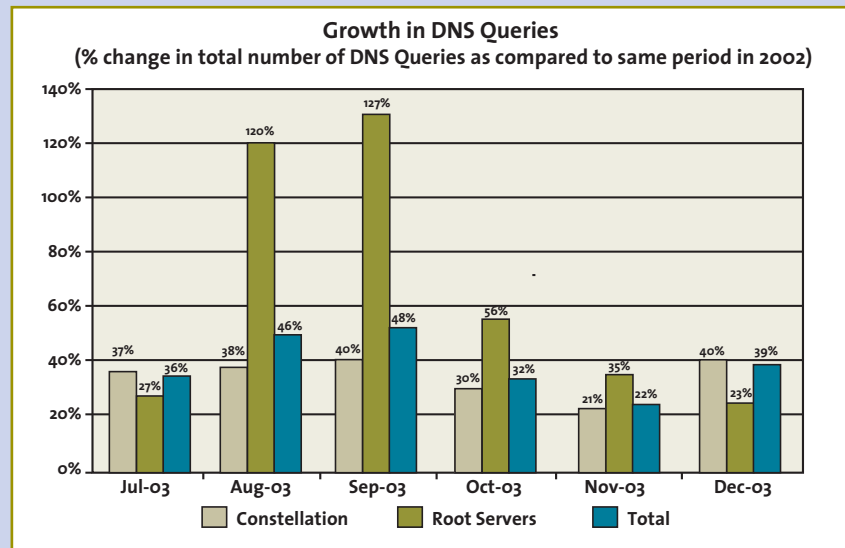


Figure 12

Comparing the number of queries in 2003 to 2002, VeriSign recorded a marked increase targeting Root servers in August and September (noted in the Oct. 2003 Internet Security Intelligence Briefing). VeriSign then reported the increase was largely due to the SoBig.F virus and other threats during that period. The chart above shows the number of queries declined rapidly by 77% as the virus expired. Nevertheless, the overall number of DNS queries continued to grow in 2003 at an average rate of 37% as compared to the same period in 2002.

Some of this traffic is natural growth as more domains become active. Some traffic is obviously due to mis-configurations and such. However, a large amount of new traffic is from potentially malicious activities. This latter type of traffic is driven by the two characteristics possessed by many viruses/worms. The first is a tendency to rely on e-mail for threat propagation; the second is a need to “call-home” for updates. Both of these characteristics depend on DNS infrastructure to resolve a domain name to an IP address.

VeriSign also measured a drop in the total percentage of e-mail based queries vs. other DNS queries from highs in August and September to a steady average of approximately 14%.

DNS Query Type	Sept 03	Oct 03	Nov 03	Dec 03
E-Mail	20%	14%	13%	14%
Other (A, NS, PTR, etc.)	80%	86%	87%	86%

Table 3

SSL Certificates: The number of issued and renewed SSL certificates continued to grow in 2003. This growth reflects an increased demand for security of Internet communications and transactions.

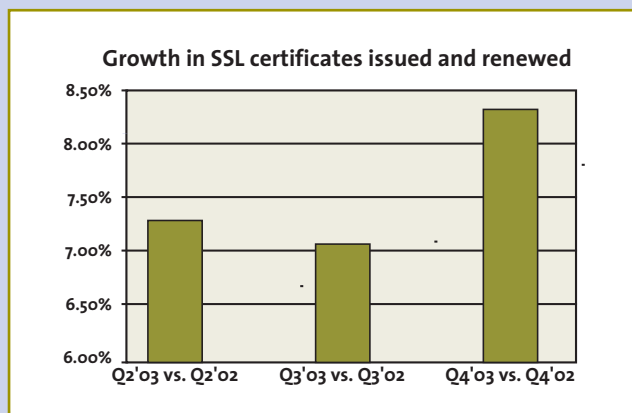


Figure 13

The United States and Japan continue with the largest growth.

**New SSL certificates issued
by region for the period of Q4'03**

United States	51.38%
Japan	15.04%
Great Britain	5.96%
Canada	3.71%
France	2.54%
Netherlands	2.18%
Brazil	1.70%
Germany	1.63%
Australia	1.59%
Sweden	1.38%

Table 4

Security remains a great concern with a dramatic rise in 2003 of security-related events generated per managed security device. Event growth was an astounding 176% in December 2003 as compared to May 2003. Events for managed devices – even finely tuned devices – are persistently rising despite the death of SoBig.F and some of the more severe threats of the third quarter. The rise of nuisance traffic mostly stems from malicious reconnaissance such as scans and probes for security vulnerabilities and un-monitored open ports.

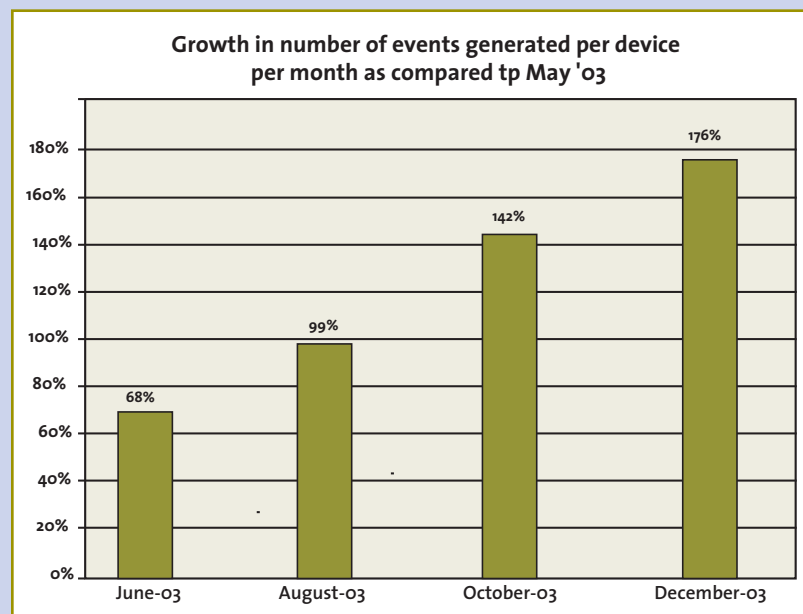


Figure 15

United States continues as the top source for most potential threats. The North American continent accounts for 96% of all potential threats monitored by VeriSign.

Top 10 Regions for Security Events generated in Q4 '03

1	United States	90.21%
2	Canada	5.89%
3	India	1.10%
4	Netherlands	0.62%
5	Australia	0.43%
6	United Kingdom	0.40%
7	China	0.18%
8	Germany	0.14%
9	Uruguay	0.12%
10	Japan	0.10%

Table 5

Two Case Studies of Correlation between Fraud and Security Data

In the October 2003 Internet Security Intelligence Briefing, we reported a 47% correlation between VeriSign fraud data and sources of security attacks. Analysis of the fraud data with VeriSign's security events data revealed parity between the two data sets. When combined, the correlated data provided an effective and efficient way to isolate potentially malicious traffic. The critical element is the IP address of confirmed (or potentially) malicious and fraudulent activity. Each incident analyzed by VeriSign begins with the sharing of IP addresses. Analysis of these data by the skilled Monitoring and Analysis (M&A) team in VeriSign's Security Operation Center follow best practices to further investigate the correlation, proactively enabling our customers to further secure and potentially prevent future disasters.

CASE 1: IP ADDRESS REGISTERED TO UKRAINIAN ISP⁴

In late November 2003, the Payments Fraud Protection team at VeriSign identified a series of fraudulent credit card transactions originating from an IP address registered to a Ukrainian ISP. The perpetrators attempted to siphon funds from stolen credit cards into a Ukrainian bank. This scheme, known as a "credit back" is common to organized criminal groups in the region. The Payments Fraud Protection team blocked all transactions and then traced the criminal group's activity back to 48 compromised IP addresses.

This resulting case data was shared with the VeriSign M&A team for correlation with security events data. One IP address had more than 2,200 hits with security events/MSS data collected during this same timeframe. The associated attack patterns indicated that several VeriSign customer infrastructures were being probed/scanned via established, common ports. Data showed attempts were being made to gain access to the customers' networks via the most commonly used ports. The perpetrator first attempted to discover which ports were allowing traffic through the firewall and

then used that knowledge for deeper network penetration. VeriSign analysts quickly determined activity from the IP address was highly suspicious. The use of these ports (53 and 113) is not suspicious by itself, but traffic patterns became critically suspect when paired with a known fraud source that was also confirmed as a source of potentially malicious activity. VeriSign found that the source was attempting to use a DNS port to gain access and change DNS records on our customers' internal DNS server. The targeted MSS customers were immediately contacted and steps were taken to cleanse and further harden their DNS servers.

CASE 2: IP ADDRESS REGISTERED TO THE U.S. GOVERNMENT⁴

In mid-December 2003, the Payments Fraud Protection team identified a broad scale carding attack. Carding is a common brute force attack method in the payments world where criminals use merchant websites to validate active credit cards. The Payments Fraud Protection team isolated the attack as originating from three IP addresses, which were then reported to the M&A team for further research. These addresses were registered to a department of the U.S. government. VeriSign's Managed Security services monitoring and correlation engines recorded more than 14,000 communications to and from one of these three IP addresses during the same time period. All this traffic traversed web related port (80), yet analysts were unable to bring up valid web traffic associated to these IP addresses. This anomaly raised the threat profile associated with these IP addresses to critically suspect. Firewall logs for the targeted customers confirmed that the firewalls had allowed inbound web traffic from these critically suspect IP addresses. VeriSign immediately alerted the targeted MSS customers of the situation. The government agency was unaware of why any business traffic would be directed from these addresses and is currently researching the situation.

⁴ In order to protect the identity of the entity involved, VeriSign is not prepared to offer the unique IP address involved.

Thousands of probing events take place every day over the Internet. While the activity described in Case 2 may prove to be non-malicious, the IP address was engaged in questionable activity. VeriSign's ability to share data between its Fraud Protection and Managed Security Services teams allows significant focus during investigations of terabytes of noisy data. VeriSign regularly sees extraordinarily large volumes of events that exhibit similar patterns. Attacks typically begin with reconnaissance, including port scans, probes and such to find open ports that are un-monitored, or have unusually high volumes of traffic. Perpetrators prefer the associated anonymity and do not want to be singled out. Without the addition and strategic placement of Intrusion

Detection Systems (IDS), the next logical steps of an attack are not as likely to be visible, as they would typically traverse trusted ports. The IP addresses in Case 2 did not trigger any IDS signatures. So even with properly configured firewalls and IDSs, it is impossible to see all attacks. These case studies show that correlation of intelligence from multiple critical infrastructure assets enables faster detection and isolation of suspect events – many of which would have normally fallen below the radar. This correlation allows the analysis of vast amounts of data unique to VeriSign and assembly of evidence that leads to faster understanding and resolution of security problems.

Conclusion

Data collected and analyzed for the 2003 holiday season revealed a period of steady growth in Internet usage and dramatic growth in e-commerce. The data also demonstrated that there is no room for complacency, as the number of events generated by security devices and fraud rates continues to increase.

About the Internet Security Intelligence Briefing

This Briefing is primarily based on data and intelligence from VeriSign's critical Internet infrastructure services, including:

Domain Name System (DNS) – 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). Globally, there are 13 Internet root servers that contain the authoritative name server information for every top-level domain (e.g., .com, .net, .us, .uk). VeriSign operates two of these root servers. The .com and .net domains are supported by 13 name servers, which are operated by VeriSign worldwide. These VeriSign name servers resolve more than 10 billion domain name queries everyday.

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 more than 390,000 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' premises logs security related information. These logs are then aggregated in VeriSign Secure Data Centers, normalized, correlated, and analyzed by VeriSign's ISAAC (Intelligent Security Analysis and Correlation) platform. Further detailed analysis is then carried out by VeriSign Security Research Analysts.

Payments and Fraud Protection Services –

VeriSign provides online Payment and Fraud Protection services to more than 100,000 customers. Over 30% of North American e-commerce payments are processed through VeriSign.

For more information e-mail securitybriefing@verisign.com.

