VeriSign®

Corporate Compliance & Internet Security

Autumn 2004 Update

An executive summary of current issues for Boards and Senior Management in major corporations

Contents

The information contained in this document is for guidance only. It does not necessarily reflect the views of VeriSign Inc. or any of its subsidiaries. All the information is provided without any warranty, express or implied.

Executive Summary

These reports are intended to provide senior executives in major organisations with an overview and understanding of current issues in relation to corporate compliance and Internet security. Increasingly these two areas are intertwined and organisations rely more and more on the Internet as a basic business tool. In fact many organisations under-estimate how dependent their business now is on the Internet. For example, while only 7% of UK consumer spending is via "pure" e-commerce, nearly 80% (Source:ONS) of all homes in the UK now have Internet access and over 25% now have Broadband access. And the "always-on" nature of Broadband is changing the way people use the Internet.

Today's Broadband consumer is more likely to use the Internet as an initial source of information about a product or service than any other. They are more likely to start a transaction via the Internet, even if they finish it in a more traditional manner. As a consequence, "Phishing" is increasingly a serious threat to any organisation's credibility. While the early victims were Banks, this fraud is being extended far more widely. APACS estimates that the UK banking sector has seen over £4M in losses in the last year as a result of Phishing.

According to Claritas there are over 15 million publicly available E-mail addresses in the UK that marketers can use to undertake email campaigns. So it is no surprise that hard-pressed marketing departments are turning to what is, notionally, a "free" medium in order to communicate with customers. But, sometimes this can go very badly wrong as HFC Bank found to their cost.

The Corporate Compliance and Internet Security Briefing reports current trends for Internet growth, usage, security, and online fraud. This briefing includes data and intelligence uniquely available from VeriSign's Internet infrastructure services, including Domain Name System (DNS), digital certificates (SSL and PKI), Managed Security, Payments, and Fraud Protection. Data for the report focuses on the first half of 2004.

In this briefing we are focusing on the following:

- Threat and vulnerability trends across Internet during the first half of 2004.
- New trend spotlighting phishing
- The impact of EU rules on E-mail usage
- Some best practices to improve the security posture of enterprises using the Internet.
- Data trends for Internet usage trends collected and correlated by VeriSign.

Threats and Trends

Hidden in the constant stream of email-based worms, there was a noticeable rise in attacks by multi-vector worms. These can simultaneously exploit several vulnerabilities in one attack and have a longer shelf life than single exploit worms. Another new trend was faster releases of exploit code following the public announcement of vulnerabilities, aided by tool kits for the rapid development and deployment of exploit code. Based on these trends, users should now expect exploit code to appear shortly after announcement of new vulnerabilities. Consequently, enterprises must move faster to test and install vendor patches to fix vulnerabilities before exploitation occurs.

Propagation of worms by mass email continues in popularity. The first half included many successful mass-mailers such as Novarg, MyDoom, Lovegate, and Netsky, just to name a few. VeriSign notes a new, rapidly escalating arms race of worm writers versus user education. Worm writers use increasingly clever tricks to users into opening email and associated attachments. Anti-virus software vendors are getting better at rapid deployment of vulnerability signatures. Unfortunately, zero-day attacks are a troublesome concern for enterprises. There is an increasing trend for mass mailers to include a “backdoor” code component that allows the writer or other worm writers to surreptitiously upgrade the executable. This tactic enables “Worm Wars” wherein new worms exploit backdoors left by previous worms.

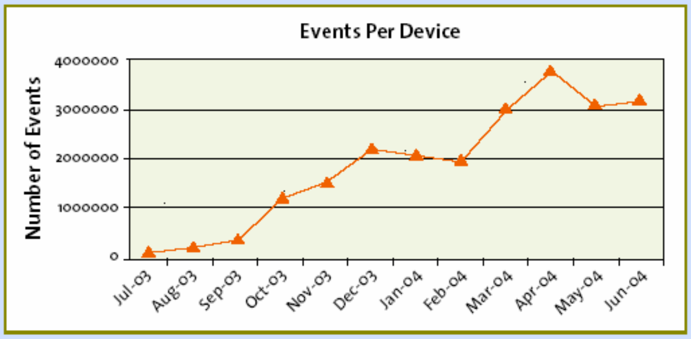
Another new trend is the improvement and rapid evolution of the multi-vector worm. Their ability to effectively exploit multiple attack vectors over time suggests the day of single-exploit worms is numbered. The most effective and potentially damaging example of this breed is called phatbot, agobot, or gaobot. Its source code is public and readily available. The resource makes it relatively easy for hackers to add new exploit code to a platform. These factors make multi-vector worms a serious threat to every enterprise.

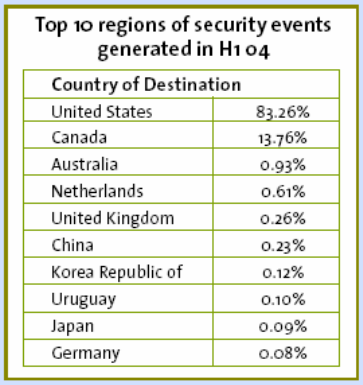
It is worth noting that quick exploitation has not followed announcements of all major vulnerabilities. For example, the complex vulnerability in Check Point Software’s Firewall-1 implementation of ISAKMP has avoided public exploitation despite the high “attraction factor” of firewalls as targets. This example suggests the cracking community cannot quickly exploit vulnerabilities that are more complex in nature.

Nevertheless, when and if more complex exploits are released, distribution network and worm toolkits will insure their fast, effective use.

.

Managed Security Service Event Statistics[1]





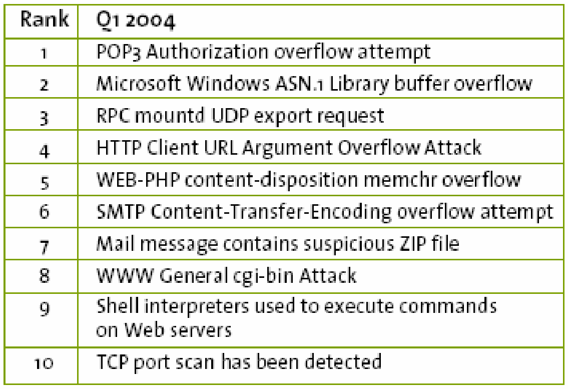
Top 10 regions of security events generated in H1 04

Country of Destination	
United States	83.26%
Canada	13.76%
Australia	0.93%
Netherlands	0.61%
United Kingdom	0.26%
China	0.23%
Korea Republic of	0.12%
Uruguay	0.10%
Japan	0.09%
Germany	0.08%

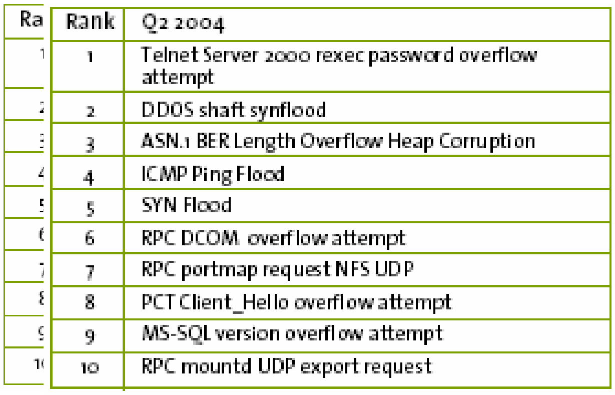
There was an increase in the aggregate number of events per device during the first half of 2004. vulnerabilities and attacks, events per device can fluctuate as Intrusion Detection System (IDS) signature vendors refine their methods of alerting for anomalies and exploits.

While the aggregate number of events continues to grow based on an increasing number of

Top Atacks



Rank	Q1 2004
1	POP3 Authorization overflow attempt
2	Microsoft Windows ASN.1 Library buffer overflow
3	RPC mountd UDP export request
4	HTTP Client URL Argument Overflow Attack
5	WEB-PHP content-disposition memchr overflow
6	SMTP Content-Transfer-Encoding overflow attempt
7	Mail message contains suspicious ZIP file
8	WWW General cgi-bin Attack
9	Shell interpreters used to execute commands on Web servers
10	TCP port scan has been detected



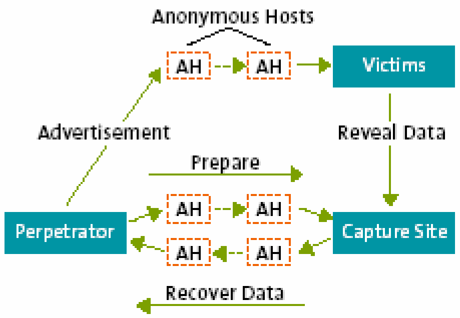
Rank	Q2 2004
1	Telnet Server 2000 rexec password overflow attempt
2	DDOS shaft synflood
3	ASN.1 BER Length Overflow Heap Corruption
4	ICMP Ping Flood
5	SYN Flood
6	RPC DCOM overflow attempt
7	RPC portmap request NFS UDP
8	PCT Client_Hello overflow attempt
9	MS-SQL version overflow attempt
10	RPC mountd UDP export request

[1] Note: In February 2004, VeriSign acquired Guardent, a recognized leader in MSS. Guardent's security consulting and managed services are integrated into VeriSign's solution portfolio. MSS historical reporting has changed to reflect the integration.

New Trend Spotlight: Phishing

“Phishing” refers to a criminal “con” to trick Internet users into disclosing personal financial account information, username, password or other information leading to identify theft and fraud.

A phishing “con” uses email and a Web site spuriously designed to represent well known legitimate businesses, financial institutions and government agencies. According to Gartner, Phishing attacks targeted 57 million Internet users during the past year. On average, three to five percent of all individuals who received a phishing email responded and became victims to the fraud. Phishing creates huge financial and reputation and brand equity exposures for the financial institutions, e-commerce sites, hospitals and other organizations whose customers are usually the targets of such attacks.



Model of a Phishing Attack

There are three basic phases in phishing attack, Preparation, Attack, and Data Recovery.

A. During the Preparation phase the phisher will:
- Prepare the fraudulent advertisement
- Purchase or harvest victim emails
- Prepare the capture site (See definition below)

B. The Attack begins when the phisher sends a fraudulent advertisement to the victim.

C. In the Data Recovery phase, the phisher will collect the information that the victims revealed to the capture site. In order for the perpetrator to realise a profit from the phishing activity the perpetrator must make some use of the stolen credentials. In the case of stolen credit card numbers this process is known as carding. The use of the stolen credentials can start immediately after they are revealed by a victim.

In most cases a perpetrator will 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.

Capture Site
The capture site is the machine that obtains the stolen access credentials from the victims. This is almost always a Web site.
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 identity of the capture site. The most common impersonation mechanisms are spam and domain name registrations.
Recovery of Data
Since the capture site is typically located on some form of anonymous host, the perpetrator needs some means to recover the data obtained.

Phishing Advertisements are Getting Harder to Detect

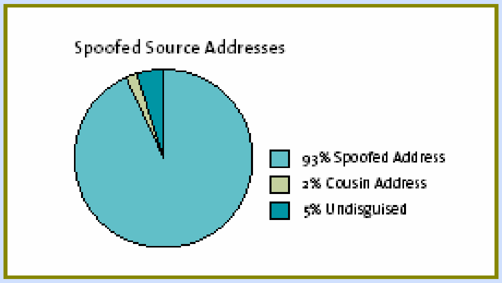
Phishers no longer send crude, misspelled emails in plain text. Phishing advertisements are now more difficult to detect because they seem like legitimate contact by known companies. Traditionally, phishers have used social engineering to register “cousin” domains, which sound similar to the company they are trying to impersonate. Lately, phishers lure victims by forging an email “from” address and using browser camouflage techniques such as floating a JavaScript window over the Address Bar to fool people into thinking they are viewing a legitimate, branded site. The phisher’s capture site thereby disguises its URL address with a legitimate site’s address. The rogue JavaScript remains installed even after leaving the phisher’s site. A phisher could easily write additional JavaScript routines to record everything sent or received through your Web browser until closing the application.

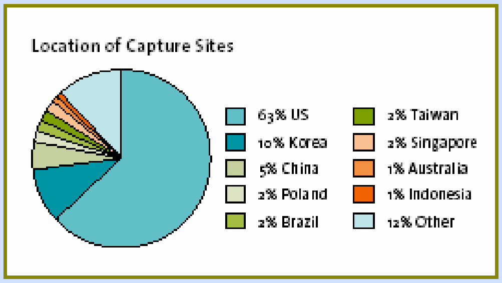
Consistent with reports from the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and, email spoofing, VeriSign found that 93% of all phishing advertisements were sent from forged or spoofed email addresses. About 5% made no attempt to hide the fraudulent "from" address with a cousin or spoofed address.

VeriSign found phishing advertisements directed users to capture sites located outside of the US 37% of the time with a concentration in: Korea, China, Poland, Brazil, Taiwan, Singapore, Australia, and Indonesia hosted multiple sites with the remaining 12% being hosted in the in the following countries:
Canada, Italy, Venezuela, Cameroon, Egypt, France, Ireland, Philippines, Seychelles, Thailand, Turkey, France, Great Britain, Japan, Latvia, Malaysia, Mexico, Netherlands, New Zealand, Norway, Pakistan, Panama, Romania, Russia, Spain, Stockholm, and UK.

What we are seeing

Sample of 490 phishing emails from the first half of 2004 targeting customers of 16 companies:





VeriSign expects the number of capture sites hosted internationally will increase because they are more difficult to shut down than domestic-hosted sites. Hurdles for closure of international capture sites include different laws, for some countries do not prohibit impersonation of an organization's Web site. Other obstacles include language barriers, different time zones, and business hours.

When Phishing Advertisements are Sent

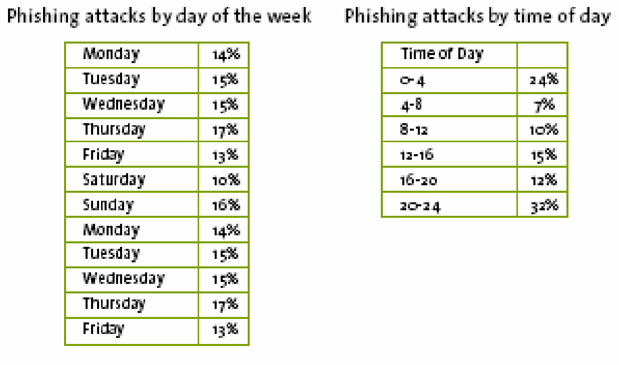
Phishing emails are sent out consistently throughout the week, although VeriSign found a spike between the hours of 9:00pm - 4:00am EST – the period when IT staffers are either on call or few in numbers.

What Enterprises Can Do

A comprehensive solution for phishing should include strategies to prevent, detect, and respond to attacks.

Prevention

Preventing fraud related to phishing attacks begins with policy, process, and education. A communications plan for safeguarding personally identifiable information begins with assessing current policies and processes, implementing educational programs for employees and end users, and developing a response plan to phishing attacks. An effective communication campaign should tell end users to stop, think, and ask when presented with a questionable email solicitation for personal information. A scam will work only if users are tricked into revealing personal information.



Phishing attacks by day of the week

Monday	14%
Tuesday	15%
Wednesday	15%
Thursday	17%
Friday	13%
Saturday	10%
Sunday	16%
Monday	14%
Tuesday	15%
Wednesday	15%
Thursday	17%
Friday	13%

Phishing attacks by time of day

Time of Day	
0-4	24%
4-8	7%
8-12	10%
12-16	15%
16-20	12%
20-24	32%

Recommended guidelines are:

Stop: Users should never reveal a credit card number unless they are making a purchase.

Think: Is it likely that a user's bank would lose their personal information? Banks never forget credit card numbers. Merchants never need a card number unless you are making a purchase.

Ask: Email that discourages discussion with other people is probably attempting to perpetrate fraud. Users should verify questionable email from a bank with a phone call to the customer service department. Bank Web sites may provide other information such as an alert for a current fraud scheme.

What's Up Next - Carding - What Happens to the Stolen Card Numbers

A criminal has no interest in stealing a credit card number unless it can be safely used to obtain cash or goods that can be easily sold. The phishing gangs who steal credit card numbers by the thousands have been equally ingenious in developing techniques that allow them to turn stolen cards into profit; this is known in hacker circles as 'carding.'

A concerning new trend is the growth of "work at home" schemes that are actually fronts for carding schemes. In this scheme, the carding gangs pose as a legitimate company that is looking for a US agent. The recruits accept money or goods and forward them to another country. As spam filtering systems have proved increasingly effective, legitimate Internet employment agencies are having to work to prevent carding gangs placing listings with them (using a stolen credit card naturally). In some cases the recruits honestly believe that they have found a genuine job right up to the moment the police arrive with a search warrant.

It is important that potential recruits understand there is no legitimate business accepting packages and forwarding them to another country and that forwarding money in this manner is in fact, a crime known as money laundering.

for VeriSign's in depth look at Internet Fraud and Carding exploits.

Cryptographic Authentication Prevents Fraud by Phishing

Cryptographic methods of authentication such as a digital signatures provide a high degree of assurance of email origination and that the contents have not been modified. Cryptographic authentication achieves the following goals:

- Reliably inform the user that an email message is genuine
- Reliably inform the user that a Web site is genuine
- Reliably inform the end user that a software download is not malicious

Cryptographic authentication is routinely used to secure e-commerce transactions via the SSL protocol and software downloads using the Authenticode protocol. VeriSign recommends that organizations allow end users to individually opt to receive mail in a secure format.

Disclosure Proof Credentials

Adoption of disclosure proof credentials is a longer-term strategy for reducing or eliminating the risk of credential disclosures. Most financial transactions are currently authenticated with static identifiers such as an account number or Social Security number. The security offered by these identifiers declines with each transaction requiring disclosure. A public key credential embedded in a smartcard or other token format allows a holder to self-authenticate with a secret key without disclosing the secret. A one-time use authenticator generated by either a token device or other trustworthy means provides an attractive alternative form of disclosure proof credential.

Detecting Phishing Attacks

VeriSign uses several services to detect potential phishing activities taking place outside an enterprise's network, including brand management services, domain name monitoring,Web crawlers and spam filters. With these tools, VeriSign can monitor the Internet for cousin ”Web sites” and other brand abuse practices.

Response - Reducing Time Between Discovery and Takedown

The longest part of an attack timeline is the interval between discovery of the phishing attack and takedown of the capture site. VeriSign believes reducing this time interval offers the best near term opportunity for stopping fraud by phishing. Tracing the source of hacker attacks such as phishing is largely a manual process. Although automated tools exist for tracing attacks within a single network connected to the Internet, communication between the networks requires human intervention. Attackers exploit the size of the Internet to conceal their traces. The trail of an attack typically involves multiple jurisdictions, time zones and languages. Most phishing attacks are hosted at sites hosted by innocent parties. Processes improving notification between the response centre and the ISPs responsible for the machines that are the source of the attack would allow the time taken before takedown occurs to be very significantly reduced.

VeriSign provides 24x7 support to take action against a phishing attack.Through close relationships with ISPs and other hosting organizations,VeriSign e-commerce fraud investigators work together to shut down phishing sites in the shortest amount of time possible.

Phishing Case Study

March 2004
The Preparation – Approximately 4:00 am PST

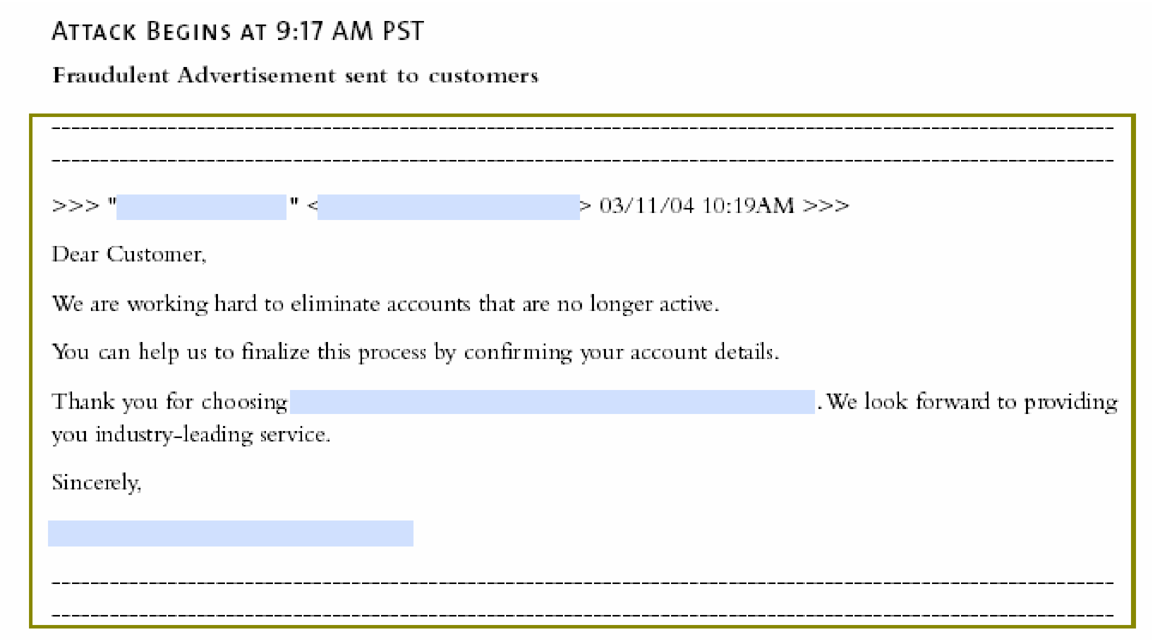
The phisher obtained access onto an anonymous host server at an ISP in Tacoma,Washington where he found an unprotected FTP share and uploaded a rootkit onto the server. From there he was able to hack into the administrative account and create new logins into the terminal services for the server, giving him free access to all hosted Web sites on the hacked server.The capture site was set up as an unlinked page off of an otherwise legitimate Web site.The phisher didn't use cousin URLs but spoofed the from address in the email. From the account he created, he used a standard PERL mailer utility to send out the fraudulent advertisements.

The time between when the phisher gained access to the anonymous host and uploaded the rootkit to mails sent is under five hours. Logging from server logs and mail server activity logs show that the scam mails were initially sent out at 9:17 AM.

The phisher then covered his tracks by deleting the mail list once the emails went out. (This prevented us from determining who he sent the fraudulent advertisement from during our investigation.)

Discovery – 9:42 am PST

VeriSign became aware of the scam email at 9:42 AM (25 minutes after attack launched). After analyzing a copy of the email, our fraud team initiated action.We clicked on the link, confirmed that it was a scam, and determined where the capture site was hosted.
We found that clicking on the link took the victim to a site that looked like the login page. No matter what data was entered for username and password, the phisher's site then took the victim to the page below that collected further information.



ATTACK BEGINS AT 9:17 AM PST

Fraudulent Advertisement sent to customers

>>> "[redacted]" <[redacted]> 03/11/04 10:19AM >>>

Dear Customer,

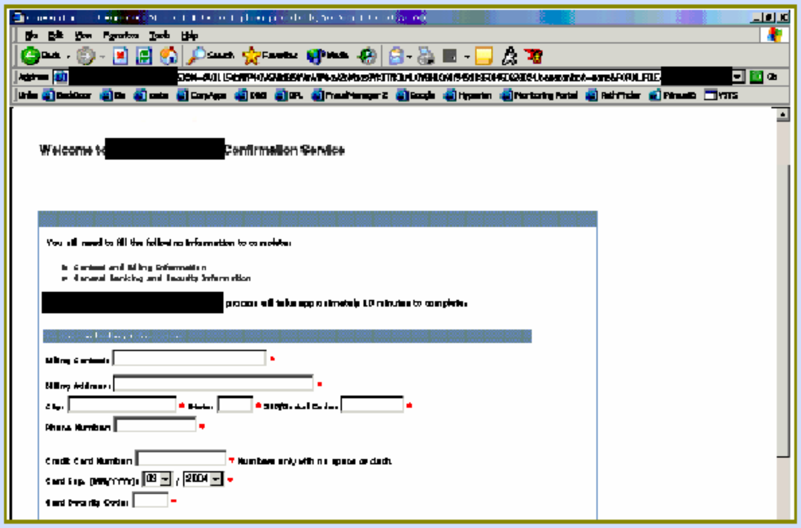
We are working hard to eliminate accounts that are no longer active.

You can help us to finalize this process by confirming your account details.

Thank you for choosing [redacted]. We look forward to providing you industry-leading service.

Sincerely,

[redacted]



[redacted]

Welcome to [redacted] Confirmation Service

You will need to fill the following information to complete:

- Contact and Billing Information
- General Banking and Security Information

[redacted] process will take approximately 10 minutes to complete.

Billing Contact: *

Billing Address: *

City: * State: * Zip/Postal Code: *

Phone Number: *

Credit Card Number: * Numbers only with no space or dash.

Card Exp. (MM/YYYY): 08 / 2004 *

Card Security Code: *

A separate resource investigated the mail itself, starting with the Internet headers.These are easy enough for the phisher to spoof, but it still gives a good starting point for further investigation.

The Take-Down – 9:47 am PST

We contact the ISP in Tacoma through their listed ARIN “abuse@” contacts but only got voice mail.

Leveraging our extensive database of contacts, our next attempt to contact them got us to a live person.We let them know that they may have a server been compromised, and that they are hosting a scam page. By 9:47 AM (five minutes after VeriSign became aware of the attack) the scam page is taken down.

We were able to get the site down so quickly in part because the site was domestic and because of the quick response of our fraud team.

Investigation

Within an hour of getting the site taken down, we had a copy of the scam site payload in our hands for forensics.We also had the FTP logs to give us details of where and when the phisher started this from. FTP logs show that he accessed the servers from three separate IP’s, two from Romania and one from Spain. This particular site was light weight and basically just harvested data and sent it to a free email account. We immediately initiated contact with the email provider in orderto get the mail account shut down.[2]

[2] Portions of the Phishing Case study were edited to protect customer identity

EU Rules Impact Email Usage

From December of 2003 all organisations in the EU have been required to comply with Electronic Communications Directive as well as the Data Protection Directive. The former was incorporated into the Electronic Communications Regulations, while the latter was incorporated into the Data Protection Act 1998.

Briefly, the former makes spam illegal throughout the EU, while the latter provides individuals with a level of protection regarding the use of their personal data.

There is some evidence that these are both having an impact on the level of email use for promotional purposes in the UK. Once recent study suggested that spam originating within the UK has now dropped to negligible proportions. The same study also found that nearly half FTSE 100 companies now have procedural rules regarding the use of email for promotional/marketing purposes. The need for these rules was recently highlighted by a major UK Bank:

HFC Bank undertook an email to a small section of its customer base – some 2400 people. Unfortunately, ALL the email addresses of the recipients were in the “To” field – rather than being “BCC’d”. This meant that everyone could see both the email address and, because of the email content, know that they were an HFC customer.

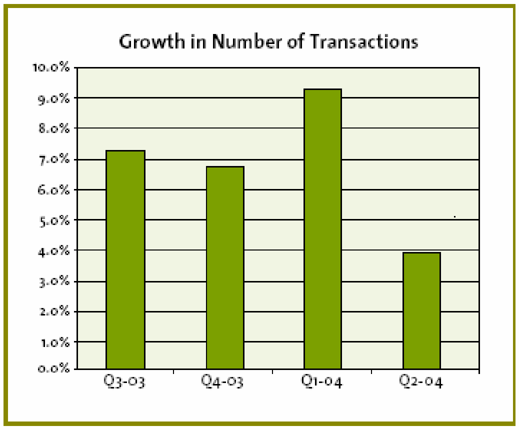
This not only presented a potential security breach – it also breached the Data Protection Act on at least two grounds – which HFC were forced to admit. Email addresses ARE personal data and should NOT be published without permission. The net result was that HFC ended up paying out over £100,000 as compensation to its customers.

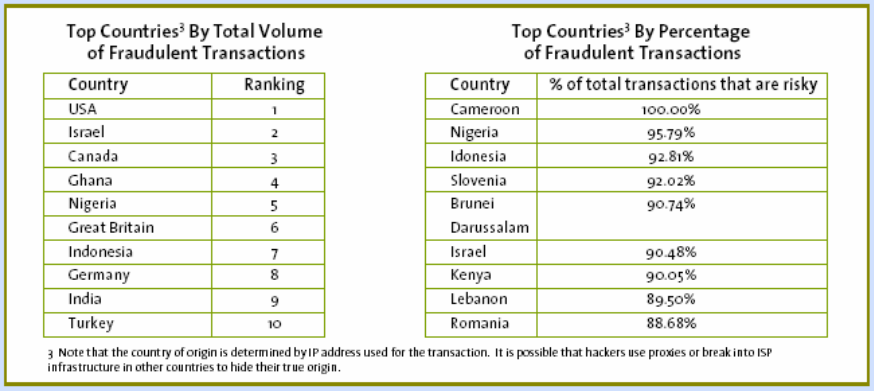
The reality is that very few companies are likely to find the law used against them by the authorities. Instead, what is happening is that customers are increasingly aware of their rights and are making life very difficult for organisations that ride over their rights.
Errors, such as the case above highlight how vital good staff training is at all levels in order to ensure that valuable technology tools do not expose an organisation to corporate compliance issues.

Data Trends for Internet Usage

Internet Commerce and Fraud

In tracking the growth of over 600 merchants over the past 12 months, data correlated by VeriSign indicates steady growth in Internet commerce. Despite slightly slower growth rates in the second quarter of 2004,VeriSign recorded overall quarter over quarter growth in the number of transactions each merchant processed. Additionally, the total dollars transacted by each merchant increased an average of 13.2% over the past 12 months.





Top Countries[3] By Total Volume of Fraudulent Transactions

Country	Ranking
USA	1
Israel	2
Canada	3
Ghana	4
Nigeria	5
Great Britain	6
Indonesia	7
Germany	8
India	9
Turkey	10

Top Countries[3] By Percentage of Fraudulent Transactions

Country	% of total transactions that are risky
Cameroon	100.00%
Nigeria	95.79%
Idonesia	92.81%
Slovenia	92.02%
Brunei Darussalam	90.74%
Israel	90.48%
Kenya	90.05%
Lebanon	89.50%
Romania	88.68%

[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.

Top Countries by Volume of Fraudulent Transactions

There was some ranking variation of countries for volume of fraudulent transactions during the first half of 04 as compared to the last briefing. The United States continued to dominate the list with Australia, Italy, and France taking their place as newcomers on the list.

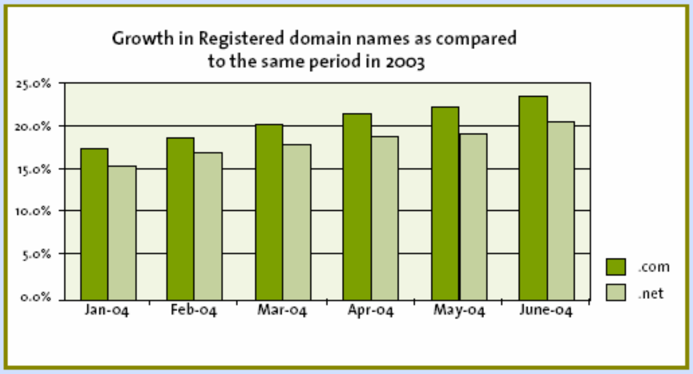
Top Countries by Percentage of Fraudulent Transactions

More than half of the countries with highest rates of originating fraudulent transactions stayed on the list for H1 04.The chart below shows the top 10 countries for fraudulent transactions.

Internet Usage and Security

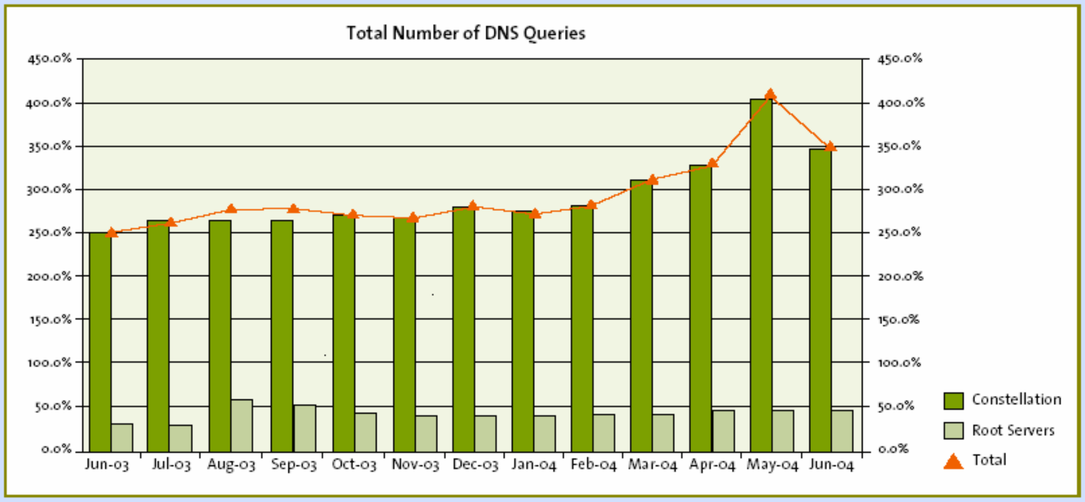
Domain Name Registration

The growth in active registered domain names in .com and .net remain strong compared to the same period in 2003. Both .com and .net top-level domains continued to exhibit strong growth as compared to the previous year.

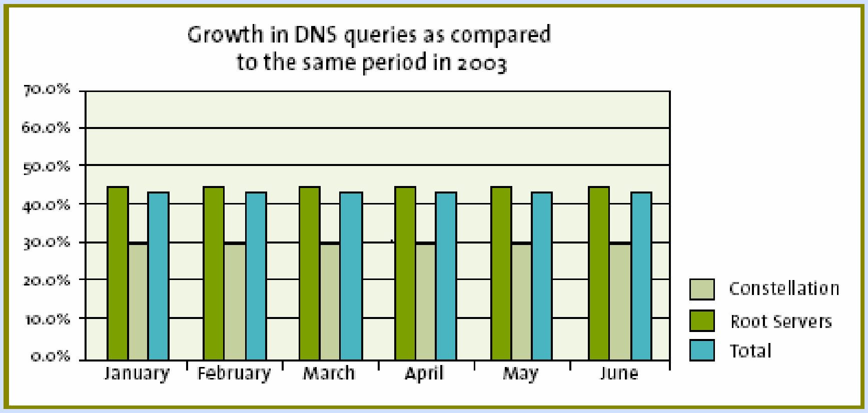


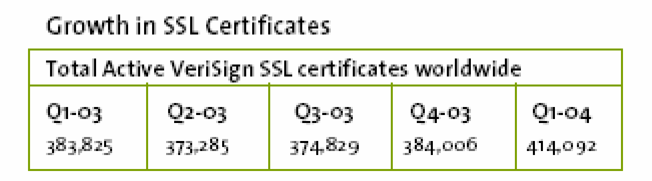
DNS Queries

The total number of Domain Name System queries grew to more than 400 billion per month during the first half of 2004.



The growth in the number of DNS queries during the first quarter of 2004 reflected a similar range as reported in the January 2004 Briefing.





Growth in SSL Certificates

Total Active VeriSign SSL certificates worldwide				
Q1-03	Q2-03	Q3-03	Q4-03	Q1-04
383,825	373,285	374,829	384,006	414,092

During the first quarter of 2004 the growth in SSL certificates continues to grow world wide.

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) – 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 10 billion resolutions 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 over 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' 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 100,000 customers. Over 30% of North American e-commerce payments are processed through VeriSign.

For more information email securitybriefing@verisign.com.