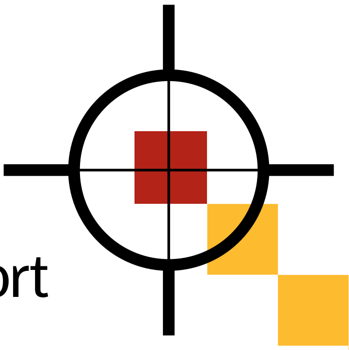
WEBSITE SECURITY THREAT REPORT



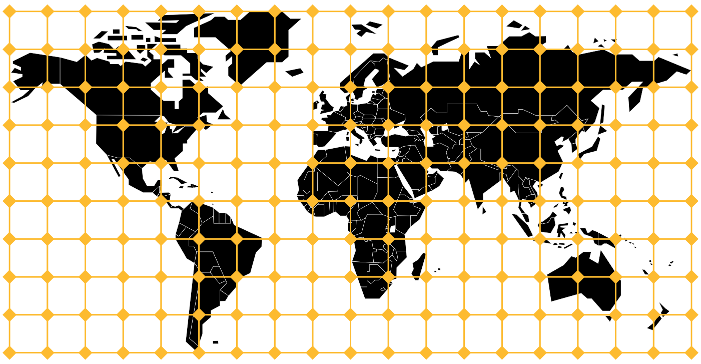
Updates from Symantec's Internet Security Threat Report

Published May 2012

Symantec.™

TABLE OF CONTENTS

FIGURES



Introduction

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network, which is made up of more than 64.6 million attack sensors and records thousands of events per second. This network monitors attack activity in more than 200 countries and territories through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, and other third-party data sources.

In addition, Symantec maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 47,662 recorded vulnerabilities (spanning more than two decades) from over 15,967 vendors representing over 40,006 products.

Spam, phishing and malware data is captured through a variety of sources, including the Symantec Probe Network, a system of more than 5 million decoy accounts; Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is able to detect new and sophisticated targeted threats before reaching customers' networks. Over 8 billion email messages and more than 1.4 billion Web requests are processed each day across 15 data centres. Symantec also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give Symantec's analysts unparalleled sources of data with which to identify, analyse, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. The result is the annual Symantec *Internet Security Threat Report*, which gives enterprises and consumers the essential information to secure their systems effectively now and into the future.

This shortened version of the report - the Website Security Threat Report – has been created to specifically focus on website security issues. You can download and read the full version of the *Internet Security Threat Report* **here**

2011 BY MONTH

MOBILE THREATS

HACKS

BOTNET TAKEDOWNS

THREAT SPECIFIC

SPAM PHISHING & 419

SOCIAL NETWORKING

JANUARY

Applications bundled with Android. Geinimi back door appear in unregulated Android marketplaces.

Scam masquerades as Indonesian Facebook app to steal login credentials.

Scammers use Serrana Flood in Brazil to solicit fake donations.

FEBRUARY

Security firm HBGary Federal hacked by Anonymous.

Android.Pjapps, another Android-based back door trojan, appears in unregulated Android marketplaces.

Spammers target unrest in Egypt and Libya with 419 scams and targeted attacks.

MARCH

Microsoft and US law enforcements take down the Rustock botnet.

Android.Rootcager appears on official Android Market.

Spammers exploit Japanese Earthquake with 419 scams, fake donation sites, and malicious attachments.

Hackers take Google's tool for removing Android.Rootcager and repackage it with a new trojan, Android.Bgserv.

Comodo Registration Authorities, InstantSSL.it and GlobalTrust.it hacked. Fake certificates for the likes of Google, Hotmail, Yahoo!, Skype, and Mozilla created.

APRIL

Sony discovers that Playstation Network has been compromised by hackers. Shuts down service while security is restored.

Iran claims another Stuxnet-style attack, called "Stars".

Malware found registering Facebook applications.

FBI awarded court order to shut down the Coreflood botnet by sending a "delete" command (included in the threats design) to compromised computers.

Spammers and FakeAV peddlers use British Royal Wedding for campaigns and SEO poisoning.

MAY

Scripting attack generates Facebook invites.

Osama bin Laden's death sparks malware and phishing attacks.

LulzSec hacking group emerges, 'in it for the "LULZ."'

Spammers found setting up their own URL shortening services.

"Tagging" spam campaign spreads across Facebook.

Facebook tokens being leaked to third parties through apps.

A free version of the popular Blackhole exploit kit released/leaked.

JUNE

LulzSec hacks Black & Berg Cybersecurity Consulting, refuses $10k previously offered as "prize".

LulzSec hacks US Senate, CIA, FBI affiliates in response to US Government declaring cyber-attacks could be perceived as an act of war.

Operation AntiSec begins, hackers are encouraged to attack government web sites, publish data found.

LulzSec finds itself the victim of an attack by TeaMp0isoN/th3j35t3r, who feels the group receives an unjust amount of attention.

A currency exchange service for the Bitcoin virtual currency is hacked.

DigiNotar certificate authority hacked, leading to the demise of the company.

JULY

Microsoft offers $250,000 reward for information leading to the arrest of the Rustock creators.

Amy Winehouse's death is used to spread Infostealer.Bancos.

AUGUST

Trojan.Badminer discovered, offloads bitcoin mining to the GPU (Graphics Processing Unit).

Phishing attacks found containing fake trust seals.

SEPTEMBER

Spammers exploit the tenth anniversary of 9/11 to harvest email addresses.

Pharmaceutical spam exploits Delhi bomb blast.

Kelihos botnet shut down by Microsoft.

OCTOBER

W32.Duqu officially discovered. May be threat Iran publicised in April.

Attackers behind Blackhole exploit kit kick-off spam campaign surrounding Steve Jobs' death.

Nitro Attacks whitepaper released, detailing a targeted attack against the chemical sector.

Java becomes most exploited software, surpassing Adobe and Microsoft, according to Microsoft Security Intelligence Report, volume 11.

Libyan leader Muammar Gadhafi's death leads to spam campaign spreading malware.

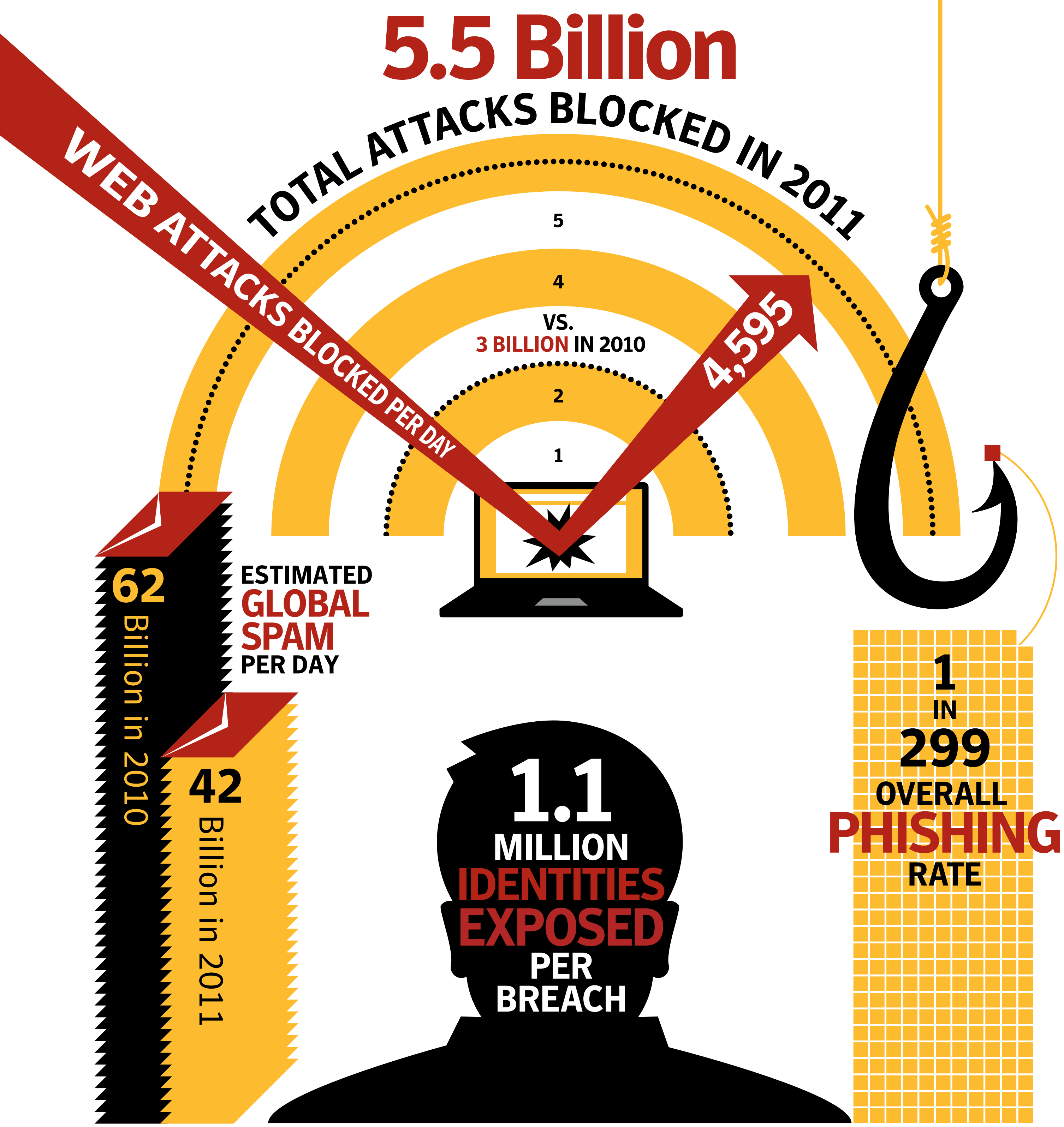
Anti-CSRF Token attacks found on Facebook.

DECEMBER

Stratfor global affairs analysis company hacked.

Spam falls to lowest levels in 3 years.

2011 IN NUMBERS



5.5 Billion

TOTAL ATTACKS BLOCKED IN 2011

VS.
3 BILLION IN 2010

WEB ATTACKS BLOCKED PER DAY

4,595

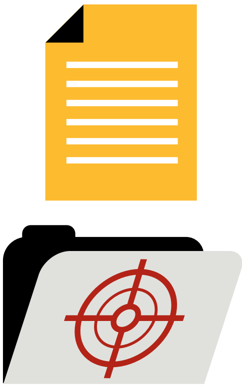
62 Billion in 2010

42 Billion in 2011

ESTIMATED
GLOBAL
SPAM
PER DAY

1.1
MILLION
IDENTITIES
EXPOSED
PER
BREACH

1
IN
299
OVERALL
PHISHING
RATE



Executive Summary

Symantec blocked more than 5.5 billion malicious attacks in 2011[1]; an increase of more than 81% from the previous year. This increase was in large part a result of a surge in polymorphic malware attacks, particularly from those found in Web attack kits and socially engineered attacks using email-borne malware. Targeted attacks exploiting zero-day vulnerabilities were potentially the most insidious of these attacks. With a targeted attack, it is almost impossible to know when you are being targeted, as by their very nature they are designed to slip under the radar and evade detection. Unlike these chronic problems, targeted attacks, politically-motivated hacktivist attacks, data breaches and attacks on Certificate Authorities made the headlines in 2011.

Certificate Authorities And Transport Layer Security (TLS) V1.0 Are Targeted As SSL Use Increases

High-profile hacks of Certificate Authorities, providers of Secure Sockets layer (SSL) Certificates, threatened the systems that underpin trust in the internet itself. However, SSL technology wasn't the weak link in the DigiNotar breach and other similar hacks; instead, these attacks highlighted the need for organisations in the Certificate Authority supply chain to harden their infrastructures and adopt stronger security procedures and policies. A malware dependent exploit concept against TLS 1.0 highlighted the need for the SSL ecosystem to upgrade to newer versions of TLS, such as TLS 1.2 or higher.

Website owners recognised the need to adopt SSL more broadly to combat Man-In-The-Middle (MITM) attacks, notably for securing non-transactional pages, as exemplified by Facebook, Google, Microsoft, and Twitter adoption of Always On SSL[2].

Certificate Authorities Under Attack

Certificate Authorities (CAs), which issue SSL certificates that help encrypt and authenticate websites and other online services, saw an unprecedented number of attacks in 2011.

Notable examples of attacks against CAs in 2011 included:

MARCH

1 An attack compromised the access credentials of a Comodo partner in Italy and used the partner's privileges to generate fraudulent SSL certificates[3].

MAY

2 It was reported that another Comodo partner was hacked: ComodoBR in Brazil[4].

JUNE

3 StartCom, the CA operating StartSSL was attacked unsuccessfully in June[5].

4 Diginotar was hacked in June. But no certificates were issued at first[6].

JULY

5 An internal audit discovered an intrusion within DigiNotar's infrastructure indicating compromise of their cryptographic keys. Fraudulent certificates are issued as a result of the DigiNotar hack for Google, Mozilla add-ons, Microsoft Update and others[7].

AUGUST

6 Fraudulent certificates from the DigiNotar compromise are discovered in the wild. Hacker (dubbed ComodoHacker) claims credit for Comodo and DigiNotar attacks and claims to have attacked other certificate authorities as well. Hacker claims to be from Iran.

SEPTEMBER

7 Security researchers demonstrate "Browser Exploit Against SSL/TLS" (BEAST for short)[8], a technique to take advantage of a vulnerability in the encryption technology of TLS 1.0, a standard used by Browsers, Servers and Certificate Authorities.

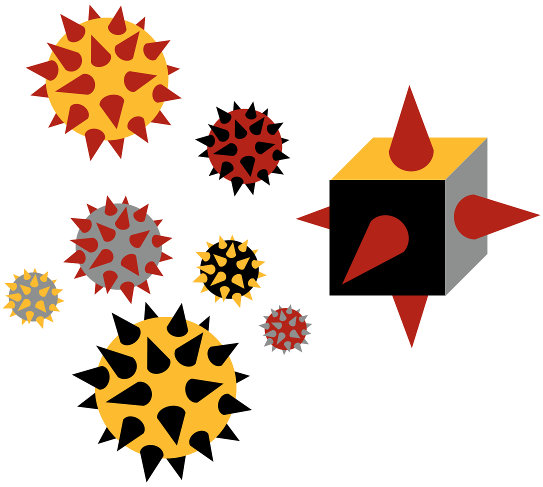
8 GlobalSign attacked, although the Certificate Authority was not breached, their web server was compromised[9], but nothing else[10]. ComodoHacker claims credit for this attack as well.

9 Dutch government and other Diginotar customers suddenly had to replace all Diginotar certificates as the major Web browser vendors removed Diginotar from their trusted root stores[11]. DigiNotar files for bankruptcy.

NOVEMBER

10 Digicert Sdn. Bhd. (Digicert Malaysia) an intermediate certificate authority that chained up to Entrust (and is no relation to the well-known CA, Digicert Inc.) issued certificates with weak private keys and without appropriate usage extensions or revocation information. As a result Microsoft, Google and Mozilla removed the Digicert Malaysia roots from their trusted root stores[12]. This was not as the result of a hacking attack; this was a result of poor security practices by Digicert Sdn. Bhd.

These attacks have demonstrated that not all CAs are created equal. These attacks raise the stakes for Certificate Authorities and require a consistently high level of security across the industry. For business users, they underline the importance of choosing a trustworthy, well-secured Certificate Authority. Lastly, consumers should be using modern up-to-date browsers and become more diligent about checking to verify that sites they visit are using SSL issued by a major trusted CA and we have included some advice in the best practices section at the end of this report.



Malicious Code Trends

Malware In 2011

By analysing malicious code we can determine which threats types and attack vectors are being employed. The endpoint is often the last line of defense, but it can often be the first-line of defense against attacks that spread using USB storage devices, insecure network connections and compromised, infected websites. Symantec's cloud-based technology and reputation systems can also help to identify and block new and emerging attacks that haven't been seen before, such as new targeted attacks employing previously unknown zero-day exploits. Analysis of malware activity trends both in the cloud and at the endpoint can help to shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers.

Corresponding to their large internet populations, the United States, China and India remained the top sources for overall malicious activity. The overall average proportion of attacks originating from the United States increased by one percentage point compared with 2010, while the same figure for China saw a decrease by approximately 10 percentage points compared with 2010.

The United States was the number one source of all activities, except for malicious code and spam zombies, where India took first place. Around 12.6% of bot activity originated in the USA as did 33.5% of web-based attacks, 16.7 % of network attacks and 48.5% of phishing websites.

Website Malware

Drive-by attacks continue to be a challenge for consumers and businesses. They are responsible for hundreds of millions of attempted infections every year. This happens when users visit a website that is host to malware. It can happen when they click on a link in an email or a link from social networking site or they can visit a legitimate website that has, itself, been infected.

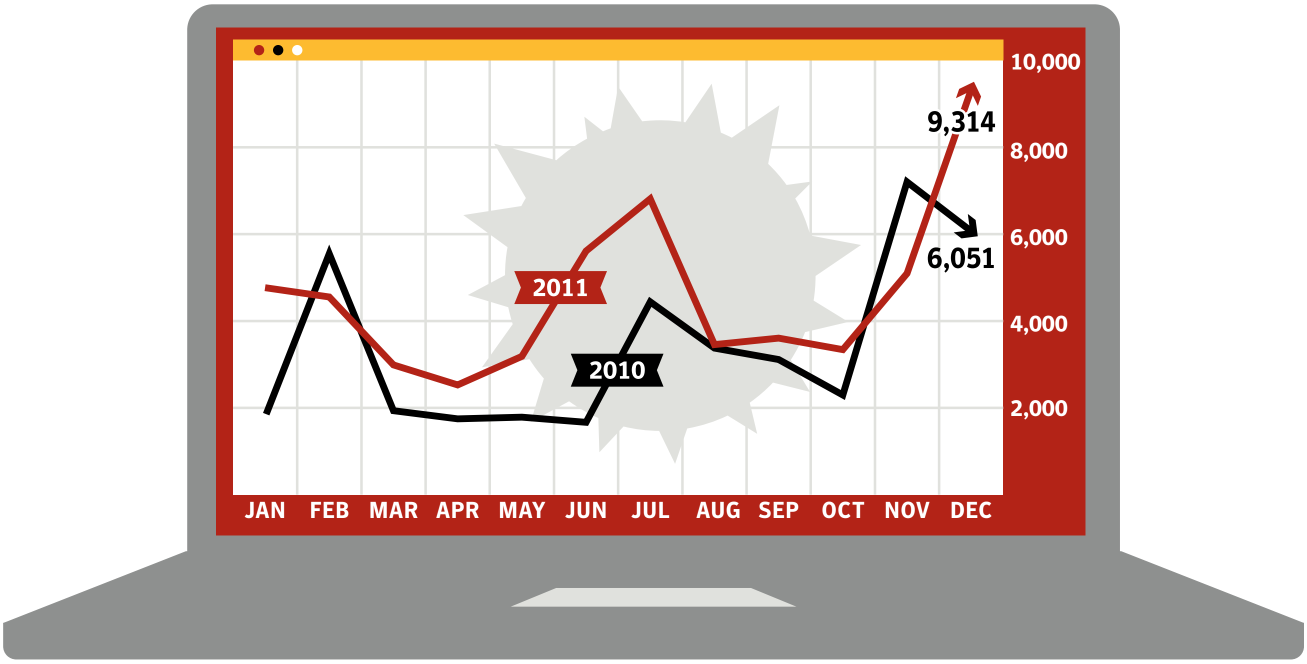
Attackers keep changing their technique and they have become very sophisticated. Badly-spelled, implausible email has been replaced by techniques such as 'clickjacking' or 'likejacking' where a user visits a website to watch a tempting video and the attackers use that click to post a comment to all the user's friends on Facebook, thereby enticing them to click on the same malicious link.

As result, Facebook has implemented a 'Clickjacking Domain Reputation System' that has eliminated the bulk of clickjacking attacks by asking a user to confirm a Like before it posts, if the domain is considered untrusted.

Based on Norton Safe Web[13] data – Symantec technology that scans the Web looking for websites hosting malware – we've determined that 61% of malicious sites are actually regular Web sites that have been compromised and infected with malicious code.

Figure 1

Average Number Of Malicious Web Sites Identified Per Day, 2011



Source: Symantec.cloud

Dangerous Web Sites

Figure 2

Most Dangerous Web Site Categories, 2011

Rank	Top-10 Most Frequently Exploited Categories Of Web Sites	% Of Total Number Of Infected Web Sites
1	**Blogs/Web Communications**	**19.8%**
2	**Hosting/Personal hosted sites**	**15.6%**
3	**Business/ Economy**	**10.0%**
4	**Shopping**	**7.7%**
5	**Education/ Reference**	**6.9%**
6	**Technology Computer & Internet**	**6.9%**
7	**Entertainment & Music**	**3.8%**
8	**Automotive**	**3.8%**
9	**Health & Medicine**	**2.7%**
10	**Pornography**	**2.4%**

Source: Symantec

It is interesting to note that Web sites hosting adult/pornographic content are not in the top five, but ranked tenth. The full list can be seen in figure 2.

Moreover, religious and ideological sites were found to have triple the average number of threats per infected site than adult/pornographic sites. We hypothesise that this is because pornographic website owners already make money from the internet and, as a result, have a vested interest in keeping their sites malware-free – it's not good for repeat business.

In 2011, the Symantec VeriSign website malware scanning service[14] scanned over 8.2 Billion URLs for malware infection and approximately 1 in 156 unique websites were found to contain malware. Websites with vulnerabilities are more risk of malware infection and Symantec began offering its SSL customers a website vulnerability assessment scan from October 2011. Between October and the end of the year, Symantec identified that 35.8% of websites had at least one vulnerability and 25.3% had a least one critical vulnerability.

Email-Borne Malware

The number of malicious emails as a proportion of total email traffic increased in 2011. Large companies saw the greatest rise, with 1 in 205.1 emails being identified as malicious for large enterprises with more than 2,500 employees. For small to medium-sized businesses with up to 250 employees, 1 in 267.9 emails were identified as malicious.

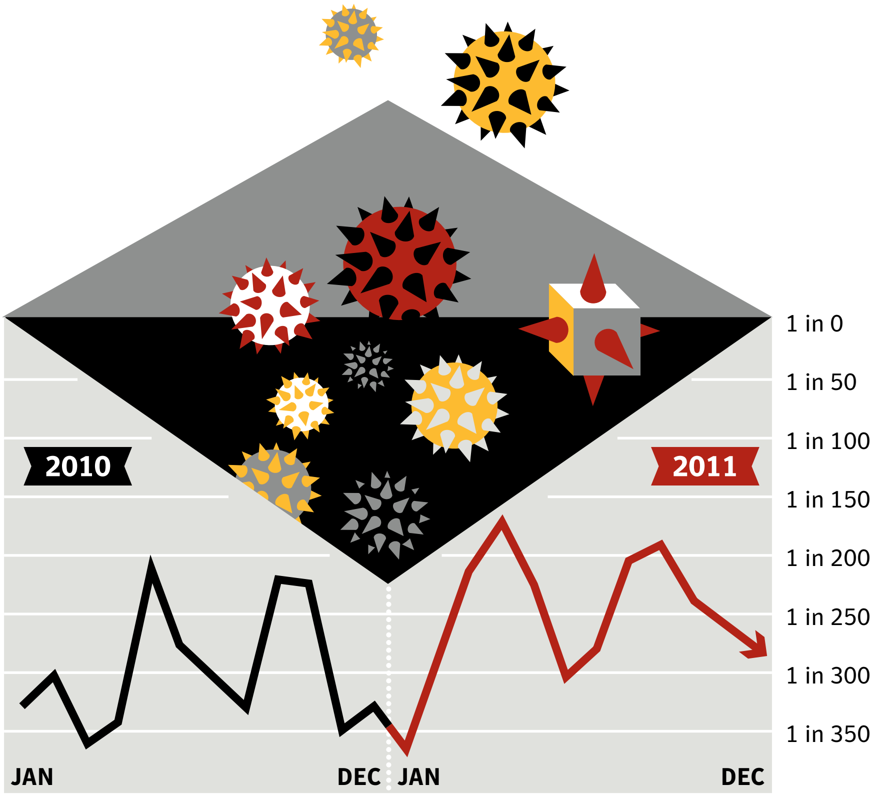
Criminals disguise the malware hidden in many of these emails using a range of different attachment types, such as PDF files and Microsoft Office documents. Many of these data file attachments include malicious code that takes advantage of vulnerabilities in the parent applications, and at least two of these attacks have exploited zero-day vulnerabilities in Adobe Reader.

Malware authors rely on social engineering to make their infected attachments more clickable. For example, recent attacks appeared to be messages sent from well-known courier and parcel delivery companies regarding failed deliveries. In another example, emails purporting to contain attachments of scanned images sent from network-attached scanners and photocopiers. The old guidance about not clicking on unknown attachments is, unfortunately, still relevant.

Moreover, further analysis revealed that 39.1% of email-borne malware comprised hyperlinks that referenced malicious code, rather than malware contained in an attachment. This is an escalation on the 23.7% figure in 2010, and a further indication that cybercriminals are attempting to circumvent security countermeasures by changing the vector of attacks from purely email-based, to using the Web.

Figure 3

Ratio Of Malware In Email Traffic, 2011



Source: Symantec.cloud

Exploiting The Web: Attack Toolkits, Rootkits And Social Networking Threats

Attack toolkits, which allow criminals to create new malware and assemble an entire attack without having to write the software from scratch, account for nearly two-thirds (61%) of all threat activity on malicious websites. As these kits become more widespread, robust and easier to use, this number is expected to climb. New exploits are quickly incorporated into attack kits. Each new toolkit version released during the year is accompanied with increased malicious Web attack activity. As a new version emerges that incorporates new exploit functionality, we see an increased use of it in the wild, making as much use of the new exploits until potential victims have patched their systems. For example, the number of attacks using the Blackhole toolkit, which was very active in 2010, dropped to a few hundred attacks per day in the middle of 2011, but re-emerged with newer versions generating hundreds of thousands of infection attempts per day towards the end of the year.

On average, attack toolkits contain around 10 different exploits, mostly focusing on browser independent plug-in vulnerabilities like Adobe Flash Player, Adobe Reader and Java. Popular kits can be updated every few days and each update may trigger a wave of new attacks.

They are relatively easy to find and sold on the underground black market and web forums. Prices range from $40 to $4,000.

Attackers Are Using Web Attack Toolkits In Two Main Ways:

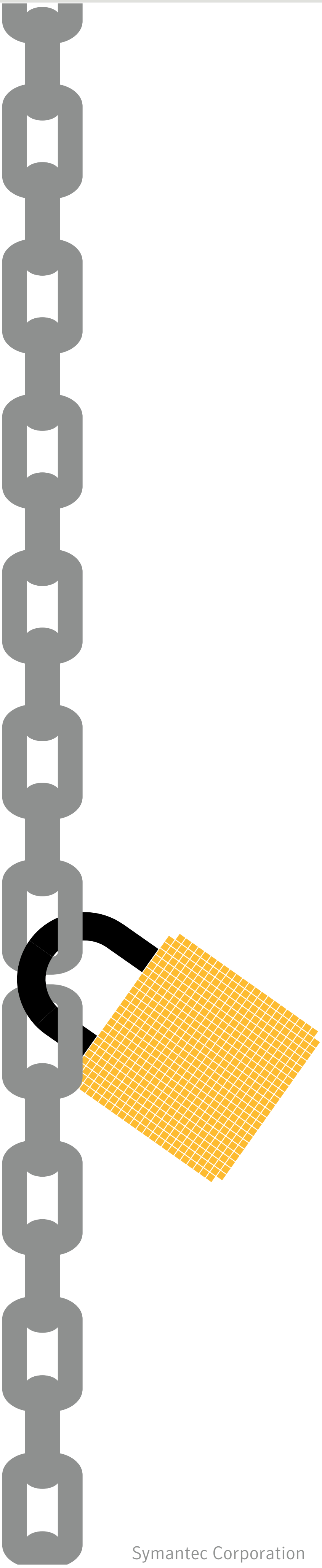
1 **Targeted attacks**. The attacker selects a type of user he would like to target. The toolkit creates emails, IMs, blog posts to entice the target audience to the infected content. Typically, this will be a link to a malicious website that will install the malware on the victim's system.

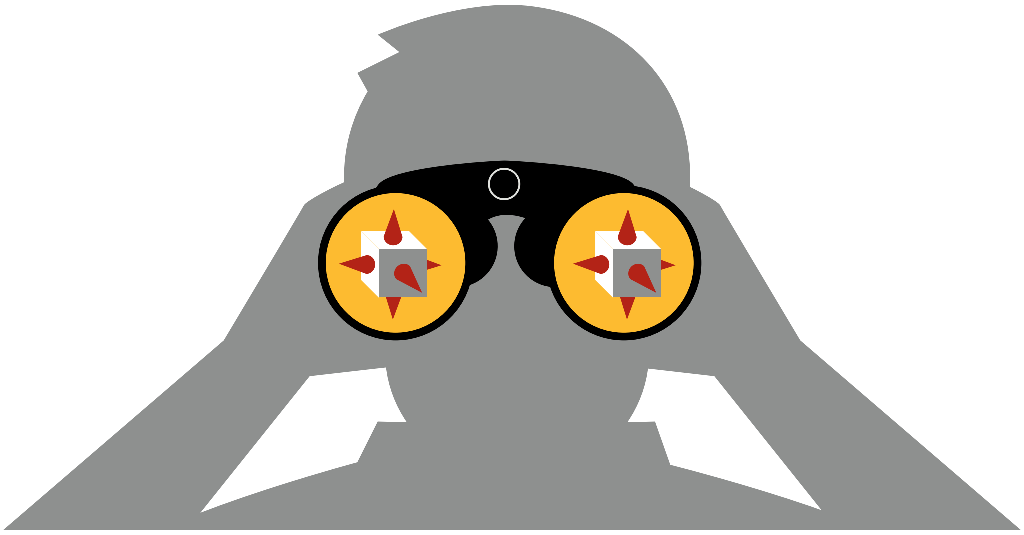
2 **Broadcast attacks.** The attacker starts by targeting a broad range of websites using SQL injection, web software, or server exploitation. The objective is to insert a link from an infected website to a malicious site that will infect visitors. Once successful, each subsequent visitor will be attacked.

Building Trust And Securing The Weakest Links

Law-abiding users have a vested interest in building a secure, reliable, trustworthy Internet. The latest developments show that the battle for end-users' trust is still going on:

- **Always On SSL**. Online Trust Alliance[15] endorses Always On SSL, a new approach to implementing SSL across a website. Companies like Facebook[16], Google, PayPal, and Twitter[17] are offering users the option of persistent SSL encryption and authentication across all the pages of their services (not just login pages). Not only does this mitigate man-in-the-middle attacks like Firesheep[18], but it also offers end-to-end security that can help secure every Web page that visitors to the site use, not just the pages used for logging-in and for financial transactions.
- **Extended Validation SSL Certificates.** EV SSL Certificates offer the highest level of authentication and trigger browsers to give users a very visible indicator that the user is on a secured site by turning the address bar green. This is valuable protection against a range of online attacks. A Symantec sponsored consumer survey of internet shoppers in Europe, the US and Australia showed the SSL EV green bar increases the feeling of security for most (60%) shoppers[19]. Conversely, in a US online consumer study, 90% of respondents would not continue a transaction if they see a browser warning page, indicating the absence of a secure connection[20].
- **Baseline Requirements for SSL/TLS Certificates.** The CA/Browser Forum released "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", the first international baseline standard for the operation of Certification Authorities (CAs) issuing SSL/TLS digital certificates natively trusted in browser software. The new baseline standard was announced in December 2011 and goes into effect July 1, 2012.
- **Code signing certificates and private key security.** High profile thefts of code signing private keys highlighted the need for companies to secure and protect their private keys if they hold digital certificates[21]. Stealing code signing keys enables hackers to use those certificates to digitally sign malware and that can help to make attacks using that malware much harder to recognise. That is exactly what happened with the Stuxnet and Duqu attacks.
- **DNSSEC.** This technology is gaining momentum as a method of preserving the integrity of the domain name system (DNS). However, it is not a panacea for all online security needs, it does not provide website identity authentication nor does it provide encryption. DNSSEC should be used in conjunction with Secure Sockets Layer (SSL) technology and other security mechanisms.
- **Legal requirements.** Many countries, including the EU Member States[22] and the United States (46 states)[23] have at least sectoral data breach notification legislation, which means that companies must notify authorities and, where appropriate, affected individuals if their data is affected by a data breach. As well as a spur to encourage other territories with less regulation, these requirements can reassure users that in the event of a breach they will be quickly notified and will be able take some action to mitigate against potential impact, including changing account passwords.





Conclusion: What's Ahead In 2012

A wise man once said, 'Never make predictions, especially about the future'. Well, this report has looked back at 2011 but in the conclusion we'd like to take a hesitant peak into the future, projecting the trends we have seen into 2012 and beyond.

- Targeted attacks and APTs will continue to be a serious issue and the frequency and sophistication of these attacks will increase.
- Techniques and exploits developed for targeted attacks will trickle down to the broader underground economy and be used to make regular malware more dangerous.
- Malware authors and spammers will increase their use of social networking sites still further.
- The CA/Browser Forum[24] will release additional security standards for companies issuing digital certificates to secure the internet trust model against possible future attacks.
- Consumerisation and cloud computing will continue to evolve, perhaps changing the way we do business and forcing IT departments to adapt and find new ways to protect end users and corporate systems.
- Malware authors will continue to explore ways to attack mobile phones and tablets and, as they find something effective and money-making, they will exploit it ruthlessly.
- In 2011, malicious code targeting Macs was in wider circulation as Mac users were exposed to websites that were able to drop trojans. This trend is expected to continue through 2012 as attack code exploiting Macs becomes more integrated with the wider web-attack toolkits.
- While external threats will continue to multiply, the insider threat will also create headlines, as employees act intentionally – and unintentionally – to leak or steal valuable data.
- The foundation for the next Stuxnet-like APT attack may have already been laid. Indeed Duqu may have been the first tremors of a new earthquake, but it may take longer for the aftershock to reach the public domain.

Best Practice Guidelines For Businesses

Employ Defence-In-Depth Strategies:

Emphasise multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.

Monitor For Network Threat, Vulnerabilities And Brand Abuse.

Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious Web site reporting.

Antivirus On Endpoints Is Not Enough:

On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits.

Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

- Endpoint intrusion prevention that protects against unpatched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
- Browser protection for protection against obfuscated Web-based attacks;
- Consider cloud-based malware prevention to provide proactive protection against unknown threats;
- File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
- Behavioral prevention capabilities that look at the behaviour of applications and malware and prevent malware;
- Application control settings that can prevent applications and browser plug-ins from downloading unauthorised malicious content;
- Device control settings that prevent and limit the types of USB devices to be used.

Secure Your Websites Against MITM Attacks And Malware Infection:

Avoid compromising your trusted relationship with your customers by:

- Implementing Always On SSL;
- Scanning your website daily for malware;
- Setting the secure flag for all session cookies;
- Regularly assessing your website for vulnerabilities;
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users;
- Displaying recognized trust marks in highly visible locations on your website to inspire trust and show customers your commitment to their security.

Make sure to get your digital certificates from an established,trustworthy certificate authority who demonstrates excellent security practices. Protect your private keys: Implement strong security practices to secure and protect your private keys, especially if you use digital certificates. Symantec recommends that organizations:

- Use separate Test Signing and Release Signing infrastructures,
- Store keys in secure, tamper-proof, cryptographic hardware devices, and
- Implement physical security to protect your assets from theft.

Use Encryption To Protect Sensitive Data:

Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organisation.

Use Data Loss Prevention To Help Prevent Data Breaches:

Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organisation over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.

Implement A Removable Media Policy.

Where practical, restrict unauthorised devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Update Your Security Countermeasures Frequently And Rapidly:

With more than 403 million unique variants of malware detected by Symantec in 2011, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.

Be Aggressive On Your Updating And Patching:

Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure.

Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organisation.

Enforce An Effective Password Policy.

Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

Restrict Email Attachments:

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.

Ensure That You Have Infection And Incident Response Procedures In Place:

- Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
- Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
- Isolate infected computers to prevent the risk of further infection within the organisation;
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
- Perform a forensic analysis on any infected computers and restore those using trusted media.

Educate Users On The Changed Threat Landscape:

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
- Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
- Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;

- Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
- Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
- Only download software (if allowed) from corporate shares or directly from the vendors Web site;
- If Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.
- Advise users to make sure they are using a modern browser and operating system and to keep their systems current with security updates.
- Instruct users to look for a green browser address bar, HTTPS, and trust marks on any websites where they login or share any personal information.

Best Practice Guidelines For Consumers

Protect Yourself:

Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:

- Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;
- Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
- Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;
- Browser protection to protect against obfuscated Web-based attacks;
- Reputation-based tools that check the reputation and trust of a file and Web site before downloading; URL reputation and safety ratings for Web sites found through search engines.
- Consider options for implementing cross-platform parental controls, such as Norton Online Family[25].

Keep Up To Date:

Keep virus definitions and security content updated at least daily if not hourly. By deploying the latest virus definitions, you can protect your computer against the latest viruses and malware known to be spreading in the wild. Update your operating system, Web browser, browser plug-ins, and applications to the latest updated versions using the automatic updating capability of your programs, if available. Running out-of-date versions can put you at risk from being exploited by Web-based attacks.

Know What You Are Doing:

Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.

- Downloading “free,” “cracked” or “pirated” versions of software can also contain malware or include social engineering attacks that include programs that try to trick you into thinking your computer is infected and getting you to pay money to have it removed.
- Be careful which Web sites you visit on the Web. While malware can still come from mainstream Web sites, it can easily come from less reputable Web sites sharing pornography, gambling and stolen software.
- Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.

Use An Effective Password Policy:

- Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or Web sites. Use complex passwords (upper/lowercase and punctuation) or passphrases.

Think Before You Click:

Never view, open, or execute any email attachment unless you expect it and trust the sender. Even from trusted users, be suspicious.

- Be cautious when clicking on URLs in emails, social media programs even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using previews or plug-ins.
- Do not click on links in social media applications with catchy titles or phrases even from friends. If you do click on the URL, you may end up "liking it" and sending it to all of your friends even by clicking anywhere on the page. Close or quit your browser instead.
- Use a Web browser URL reputation solution that shows the reputation and safety rating of Web sites from searches. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
- Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor's Web site.

Guard Your Personal Data:

Limit the amount of personal information you make publicly available on the Internet (including and especially via social networks) as it may be harvested and used in malicious activities such as targeted attacks and phishing scams.

- Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.
- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.
- Look for the green browser address bar, HTTPS, and recognisable trust marks when you visit websites where you login or share any personal information.
- Configure your home Wi-Fi network for strong authentication and always require a unique password for access to it.

More Information

- Symantec.cloud Global Threats: http://www.symanteccloud.com/en/gb/globalthreats/
- Symantec Security Response: http://www.symantec.com/security_response/
- Internet Security Threat Report Resource Page: http://www.symantec.com/threatreport/
- Norton Threat Explorer: http://us.norton.com/security_response/threatexplorer/
- Norton Cybercrime Index: http://us.norton.com/cybercrimeindex/

Endnotes

1 NB. This figure includes attack data from Symantec.cloud for the first time. Excluding these figures for comparison with 2010, the total figure would be 5.1 billion attacks.

2 https://otalliance.org/resources/AOSSL/index.html

3 Certificate Authority hacks (Comodohacker), breaches & trust revocations in 2011: Comodo (2 RAs hacked)
https://www-secure.symantec.com/connect/blogs/how-avoid-fraudulent-ssl
http://www.thetechherald.com/articlesInstantSSL-it-named-as-source-of-Comodo-breach-by-attacker/13145/

4 http://www.theregister.co.uk/2011/05/24/comodo_reseller_hacked/

5 StartCom attacked,
http://www.internet-security.ca/internet-security-news-archives-031security-firm-start-sslsuffered-a-security-attack.html
http://www.informationweek.com/news/security/attacks/231601037

6 http://www.theregister.co.uk/2011/09/06/diginotar_audit_damning_fail/

7 DigiNotar breached & put out of business,
https://www-secure.symantec.com/connect/blogs/why-your-ca-matters
https://www-secure.symantec.com/connect/blogs/diginotar-ssl-breach-update
http://www.arnnet.com.au/article/399812/comodo_hacker_claims_credit_diginotar_attack/
http://arstechnica.com/security/news/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached.ars
http://www.darkreading.com/authentication/167901072/security/attacks-breaches/231600865/comodo-hacker-takes-credit-for-massive-diginotar-hack.html
http://www.pcworld.com/businesscenter/article/239534/comodo_hacker_claims_credit_for_diginotar_attack.html

8 Attacks & Academic proof of concept demos: BEAST
(http://blog.ivanristic.com/2011/10/mitigating-the-beast-attack-on-tls.html)
and TLS 1.1/1.2, THC-SSL-DOS, LinkedIn SSL Cookie Vulnerability
http://www.wtfuzz.com/blogs linkedin-ssl-cookie-vulnerability/

9 http://www.itproportal.com/2011/09/13/globalsign-hack-was-isolated-server-business-resumes/

10 http://www.theregister.co.uk/2011/09/07/globalsign_suspends_ssl_cert_biz/

11 http://www.pcworld.com/businesscenter/article/239639/dutch_government_struggles_to_deal_with_diginotar_hack.html

12 http://www.theregister.co.uk/2011/11/03/certificate_authority_banished/

13 For more information on Norton Safe Web, please visit http://safeweb.norton.com

14 For more information on the Symantec website vulnerability assessment service:
http://www.symantec.com/theme.jsp?themeid=ssl-resources

15 https://otalliance.org/resources/AOSSL/index.html

16 http://blog.facebook.com/blog.php?post=486790652130

17 http://blog.twitter.com/2011/03/making-twitter-more-secure-https.html

18 http://www.symantec.com/connect/blogs/launch-always-ssl-and-firesheep-attacks-page

19 Symantec-sponsored consumer web survey of internet shoppers in the UK, France, Germany, Benelux, the US, and Australia in December 2010 and January 2011 (Study conducted March 2011).

20 http://www.symantec.com/about/news/release/article.jsp?prid=20111129_01

21 http://www.symantec.com/connect/blogs/protecting-digital-certificates-everyone-s-responsibility/

22 http://www.enisa.europa.eu/act/it/library/deliverables/dbn/at_download/fullReport

23 http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/

24 http://www.cabforum.org/

25 For more information about Norton Online Family, please visit https://onlinefamily.norton.com/

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com

For specific country offices and contact numbers,
please visit our website.
For product information in the UK.,
Call 0800 032 2101 or +44 (0) 208 6000 740

Symantec UK

Symantec (UK) Limited. 350 Brook Drive, Green Park,
Reading, Berkshire, RG2 6UH, UK.
www.symantec.co.uk

NO WARRANTY. Symantec makes this document available AS-IS, and makes no warranty as to its accuracy or use. The information contained in this document may include inaccuracies or typographical errors and may not reflect the most current developments, and Symantec does not represent, warrant, or guarantee that it is complete, accurate, or up-to-date, nor does Symantec offer any certification or guarantee with respect to any opinions expressed herein or any references provided. Changing circumstances may change the accuracy of the content herein. Opinions presented in this document reflect judgment at the time of publication and are subject to change. Any use of the information contained in this document is at the risk of the user. Symantec assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. Symantec reserves the right to make changes at any time without prior notice.