White paper

Malware threat landscape 2012: How to defend your business

Symantec™

Norton SECURED™ powered by VeriSign

Contents

Executive summary

Every time you or one of your employees connects to the Internet, your organisation is at risk of infection by malicious software -- malware. Some methods of connection are safer than others, but the main vectors of a malware attack are the tools most employees and customers use every day: web browsing and emails.

Hackers are constantly looking for new vulnerabilities or weaknesses in a business's website. Their malware infections or exploited vulnerabilities could risk the safety of customer information so that, before your business has time to react, your public-facing website could be blacklisted by search engines, customer trust could be compromised, and the clean-up could wreak havoc on your brand.

With today's increasingly smart malware infections and consequent online data loss, your business must do more than simply react to website security issues.

This white paper describes both today's threat landscape and how your business can establish and maintain online trust using a complementary security solution set. You'll see how to protect your customers and your reputation with SSL Certificates, alongside frequent security assessments to detect, identify and alert against potential problems.

The threat landscape: An introduction

The threat landscape is a dynamic place, and in 2011, hackers were constantly probing defences, trying to find new ways of penetrating organisations with a view to capturing data.

Attacks are delivered via a range of vectors, with a number involving increasingly sophisticated forms of social engineering, in which employees are persuaded – whether deliberately or inadvertently – to open up holes in the corporate security surface by, for example, injecting malware into the corporate network.

Meanwhile, more long-established hacking tools such as rootkits, cross-site scripting and zero-day vulnerabilities have not gone away, and hackers continue to refine and develop these attacks to stay ahead of detection tools. While the volumes of spam emails have declined over time, at least 69 percent of emails are spam, according to Symantec™'s intelligence, and they are becoming increasingly authentic, and increasingly effective at persuading recipients to click on malicious links.

In themselves, such attacks can be hard to counter, but they are often deployed in combination. For example, attackers launching the Trojan.Hydraq attack against Google in 2010 used not just one technique, but different files and combinations of attack vectors in order to compromise a network.

In the light of increasingly sophisticated malware and more online data loss, it is critical to apply patches and update your security suite solutions on a regular basis. An IT manager should take an all-round, proactive and real-time approach to website security to maintain online trust. But which infections are most dangerous to a business's online presence? This guide looks at nine of the most dangerous and common malware infections that could wreak havoc on your business.

Attack analysis

1. SQL injections

Behind many websites is an SQL database, and SQL injection attacks are often used to persuade such databases to download their information, which might contain credit card details or just crash the site. The attacks usually involve inserting malformed SQL statements into fields for which that field was not designed.

Recent high-profile examples of SQL injection attacks include Lizamoon and LulzSec. In 2010, the Lizamoon malware infected thousands of websites by prompting site users to download and install fake and useless anti-virus software. The LulzSec group claimed responsibility for a SQL injection attack on Sony's PlayStation network in 2011. As well as downloading admin details and passwords, the attack brought the network down for a month, creating losses Sony said were worth $171 million (14 billion yen).

2. Cross-site scripting (XSS) and JavaScript exploits

Cross-site scripting vulnerabilities allow attackers to bypass the client-side security systems of most web browsers. Infected sites infiltrate the user's computer, which then goes on to infect other vulnerable sites as the user browses the web. A browser cannot know that the malware script, which may originate from a site the user trusts, is in fact not to be trusted.

Scripts can access any data to which the browser has access, including passwords and cookies. Scripts can be in JavaScript, ActiveX, Flash or any other form of executable, and have affected a range of popular sites including Facebook and Twitter.

Such attacks are very common -- cross-site scripting constitutes 80 percent of all security vulnerabilities, according to research from Symantec -- and can occur whenever a website accepts user input without fully validating its generated output. It remains very common.

3. Clickjacking and social engineering

Clickjacking concatenates 'clicking' and 'hi-jacking' and is also known as UI redressing. Hackers overlay a legitimate Web page with one or more transparent or hidden pages, which include links and buttons that align with those on the legitimate page underneath. When the site visitor thinks they are clicking on a legitimate link or button, they are in fact performing actions on a hidden page.

This can then have consequences that the user never intended. Examples include social networking sites such as Twitter and Facebook, where such hidden links have led to: users making more of their profiles public than they intended; making users inadvertently follow someone on Twitter; or sharing links on Facebook.

When used to overlay 'Like' buttons on Facebook, for example – a technique called 'like-jacking' – the malware persuades users to 'like' a page or product in order to receive some non-existent reward, voucher or freebie. The hackers simply want to get users to visit the page, and may get paid commission for doing so.

4. Certificate Authority attacks

Certificate Authorities (CA) are a central element of Public Key Infrastructure (PKI), which allows users to communicate securely across the Internet, and is extremely widely used. CAs are attractive targets for hackers, as false certification allows hackers to create rogue websites that appear to be trusted.

The task of the CA is to issue digital certificates that certify the ownership of a public key by the subject of the certificate. For example, the Secure Sockets Layer (SSL) mechanism used to encrypt web traffic relies on certification to verify identities. This verification of identity relies on the CA being trusted by both the certificate holder and the certificate viewer. If that trust relationship is broken, PKI cannot operate effectively.

In 2011, a well-publicised breach occurred at the Netherlands-based Certificate Authority DigiNotar, which at first signed 283 rogue certificates, and then signed a second tranche of 248 rogue certificates. This caused a huge breach of trust in the CA: its certificates were revoked, and it subsequently went out of business.

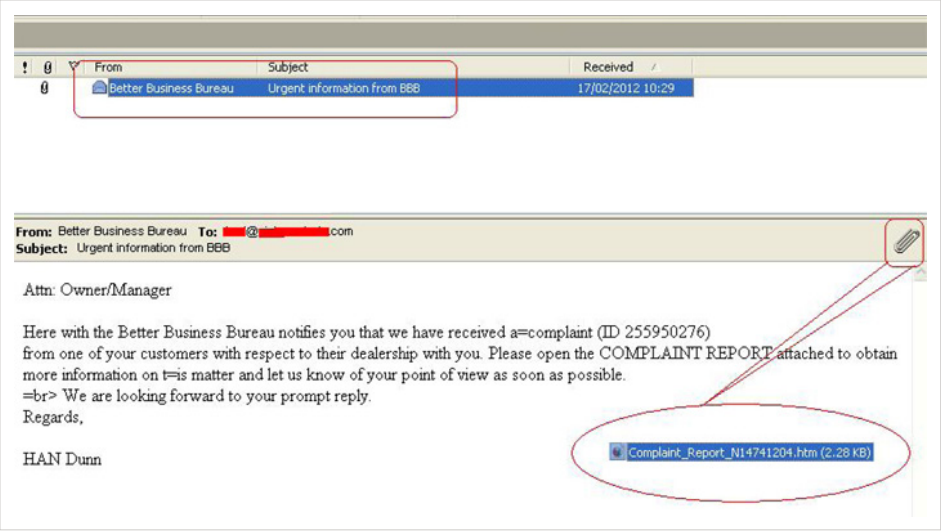
Without rigorous upkeep of the security infrastructure surrounding Certificate Authorities, CAs put their customers and the web consumer community at-large at risk. CAs must keep evolving to ensure they are ahead of the game, for their own sake as well as that of their clients. From a strategic point of view, this means they must adhere to the highest standards in terms of both infrastructure security and process best practices to ensure they stay one step ahead of these threats.

5. SEO poisoning

Hackers want to lure web users to malicious sites in order to infect their PCs with malware. One way of achieving this is with Blackhat SEO (search engine optimisation), which works by stuffing pages with keywords and links that make it appear to a search engine like a legitimate site. This 'poisoning' of the search engine's site indices results in malicious sites appearing higher up the search results in place of legitimate popular sites. If a user does not examine the link closely, they can be redirected to a site that, for example, loads up a JavaScript exploit.

6. Phishing

This infection type covers a wide range of activities, but is essentially a way of persuading users to give up personal information, especially financial information, to a supposedly trusted entity. Phishing is on the rise with increases reported every month according to intelligence reports from Symantec. Phishing can have consequences from the theft of personal data resulting in substantial personal loss, to the denial of access to email.



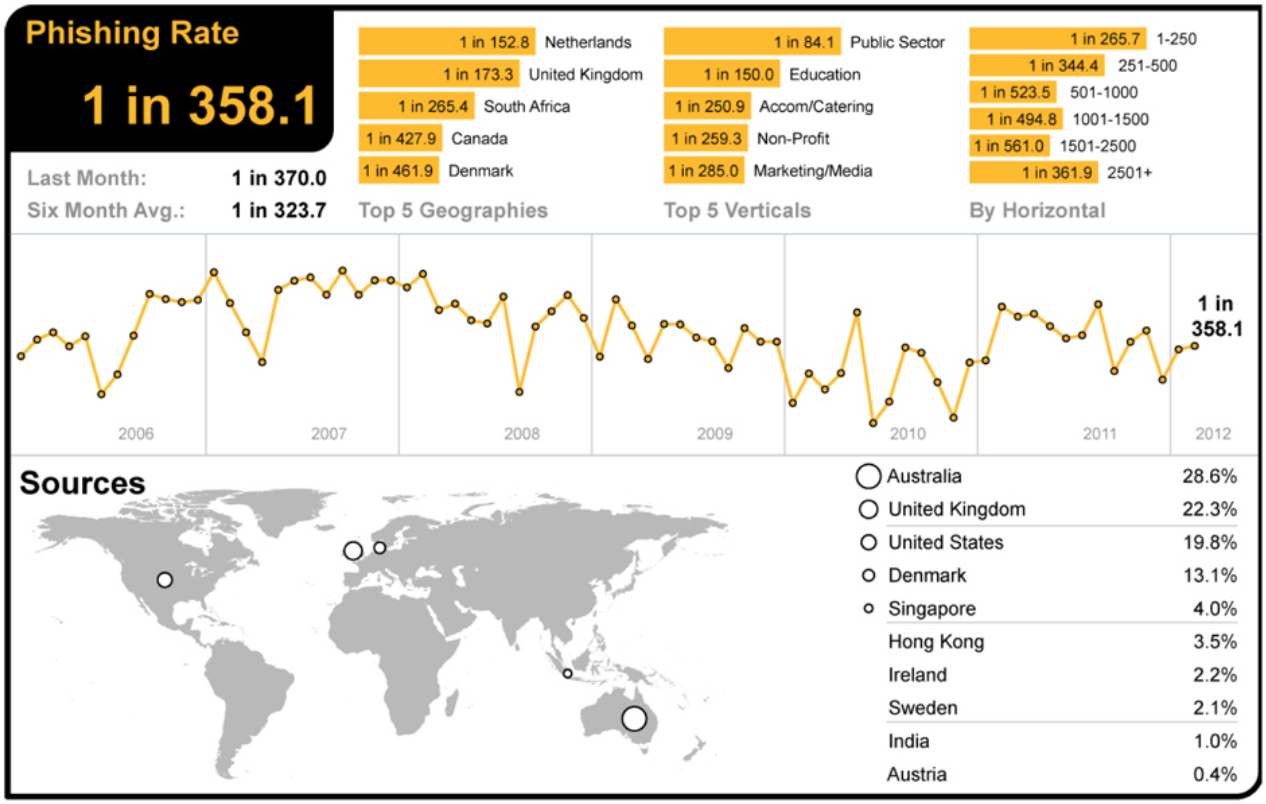
This phishing example is a faked email from the Better Business Bureau, a well-known US b2b mediation and arbitration service.

Examples include emails purporting to come from popular websites, auction sites and online payment processors, the government, or even a company's internal IT administrators. Such emails look legitimate, although they are unlikely to include personal details and might be addressed to 'Dear <insert name of bank> Customer'. This generic greeting might be followed by a warning, which says your account security might have been compromised. It may ask you to then click on a link to provide your password or PIN to verify your identity. Clicking on the link will lead to a malicious site, which could infect the user's machine and even steal their login details.

7. Malvertisements

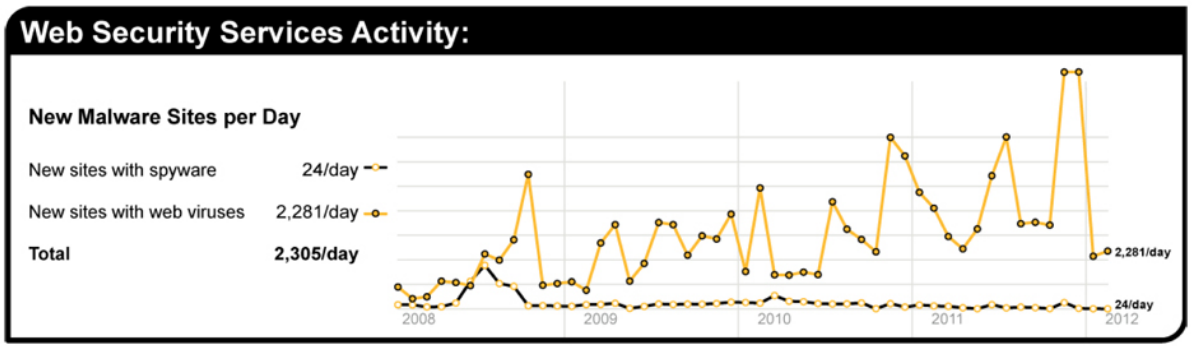
This malware consists of pop-up windows that look like advertisements, especially those warning of the possibility of the user's computer being infected, but which invite users to click on them. If a user is alarmed enough to click on this so-called 'scareware', the site to which they are directed may attempt to infect their machine or extract money from the user for removing non-existent threats from their PC.

One exploit used malvertisements on Facebook. When the user clicked on a malicious advertisement, they were redirected to a sites containing malware. The technologies that enable this behaviour are primarily JavaScript and ActiveX, which are



Global phishing rate in February 2012.

enabled in browser settings to allow for advanced web interactivity such as pop-ups or add-ons. However, a hacker can exploit vulnerabilities in the code, taking advantage of these settings to install and run malware that will erase important data, or capture sensitive information.



The chart above shows the increase in the number of new spyware and adware websites blocked each day on average during February compared with the equivalent number of web-based malware websites blocked each day.

8. Advanced persistent threats (APTs)

APT refers not so much to a particular type of technology or threat but the perpetrators of threats. In other words, an APT emanates from a group, consisting of hackers or even a government, which directs threats towards another entity, whether a company or country.

Stuxnet is an example of an APT. This worm was the first of its kind to be targeted very specifically at industrial control systems, in particular those manufactured by Siemens for controlling Iran's uranium enrichment infrastructure.

9. Cookie misuse

Cookies are small text files used to identify users of websites and initially designed to make life more convenient by reducing the need to log-on to a site each visit, and help visitors navigate by providing continuity both during and across browsing sessions. For example, by identifying you as a previous visitor, they allow such parameters as your native language and other preferences to be retained.

Convenience comes at a price, however, as the transmission of cookies over the network as plain text allows them to be captured and misused. They can identify the user and, as a result, web users have become suspicious of cookies, and of sharing personal data with websites. However, many sites cannot be accessed without cookies, so they are now generally accepted as necessary.

How to defend your business against threats

To counteract these dangerous infections that form the malware threat landscape, the key is to understand the weaknesses they exploit. However, because hackers use multiple methodologies to penetrate security defences, a single security solution is not enough.

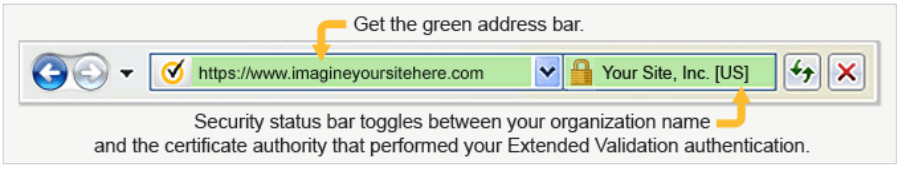
Instead, your approach to security must be multi-layered. Such an approach will need to include end-user education about the various ways in which hackers use social engineering as a way to persuade users to click on malicious links or respond to bogus emails. They need to understand the basics of click-jacking, SEO poisoning, malvertisements and phishing, as a key line of defence. This helps to make end users more aware of the threats that exist, and how to spot a dangerous email, link or website if they encounter one.

But there is not a one-size-fits-all solution to keeping your public-facing website and online information safe, and even the most IT-savvy employee could be fooled by a hacker. A business should employ many different solutions to fight malware, from both sustained to real-time protection, using both a proactive and a reactive defence.

Sustained, proactive security

A secure and trusted site helps to attract more customers and gives them the confidence to complete their transactions. Your customers will look for trustworthy signs, such as seeing your organisation's name highlighted in green in the address bar. This green bar is a clear and widely recognised sign of a legitimate website and denotes the use of highly secure Extended Validation (EV) SSL Certificates.

Secure Socket Layer (SSL) technology enables the encryption of sensitive online information, such as log-ins and personal details. A Certificate Authority (CA) establishes your site's credentials by verifying unique information about your business. Providing a more rigorously audited authentication method, EV SSL Certificates are a strong line of defence and allow customers to use your website with confidence. A leading and trusted CA, Symantec offers EV SSL Certificates as a highly reliable choice for website security.



The green address bar is a clear and widely recognised sign of a legitimate website and denotes the use of highly secure Extended Validation (EV) SSL Certificates.

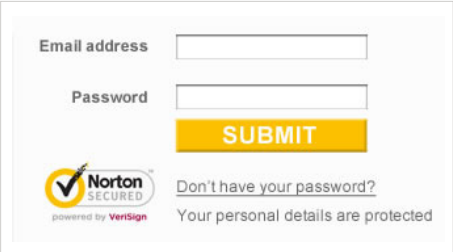
In addition to strong SSL encryption, you can give your potential customers peace of mind that it is safe to transact with you before they even click on your site. With concerns around clickjacking and SEO poisoning, your users will look for assurance and validity even in search results. By providing a visual cue such as a trust seal in popular search engines, shopping pages, or any part of your website where customers need assurance, your business will ease potential worries over the safety. According to Symantec research, customers identify with these seals in search, with 65% of consumers agreeing that a website displaying the Norton™ Secured seal is safe to browse and won't include a virus.

Real-time, proactive security

A typical website – from the simplest blog to an online shop – may have thousands of potential vulnerabilities that shift as the site changes. From a technology standpoint, real-time defences can quickly identify potential entry points through which a website's functionality or data can be damaged, downloaded or manipulated. An automated scan and report of a site's vulnerabilities and possible threats to it can act as a complement to your existing protection.

A vulnerability assessment system should be able to identify commonly-targeted weaknesses on your website and report on them. The system should, for example, be able to warn about entry points targeted in cross-site scripting and SQL injection. Vulnerability reports should categorise the issues based on type and risk, and propose corrective actions. This helps you quickly identify and remedy critical safety issues, making it easier to secure your website. Symantec provides a free Vulnerability Assessment tool with its Premium SSL Certificates.

Malware scanning is another way to help protect your site in real-time, alerting you if your website becomes infected with malicious software. Malicious code, such as that inserted by cross-site scripting, can be hidden in the source code of your website and can be difficult to detect without line-by-line analysis. It also can result in your site being blacklisted or excluded by search engines.



According to Symantec research, customers identify with these seals in search, with 65% of consumers agreeing that a website displaying the Norton™ Secured seal is safe to browse and won't include a virus.

This protection should be deployed in addition to traditional anti-malware software, which focuses on the end point -- the desktop. Most scanning solutions are designed to protect employees from downloading or installing malware rather than protecting the company's website from distributing malware. Symantec's web site malware scanning service, also included with its SSL Certificates, looks at your public Web pages on a daily basis, providing a list of infected pages and notification of the code causing the problem, so that you can then apply a suitable remedy to your site.

Conclusion

With an all-round approach to website security, your business can establish and maintain online trust while keeping the hackers away. With worldwide IT spending in 2011 topping $3.7 trillion , maintaining your online reputation is of paramount importance. By using a complementary service set such as SSL encryption, seal-in-search, vulnerability assessment and malware scanning, you can detect, identify, alert and defend against potential problems, protecting your customers and your reputation.

The additional levels of reassurance and trust that such a service set creates will allow visitors to your website to click with confidence, which in turn increases conversions and improves your business results.

More information

Visit our website

www.verisign.co.uk

To speak with a product specialist

Call 0800 032 2101 or +44 (0) 208 6000 740

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations 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.

Symantec (UK) Limited

350 Brook Drive, GreenPark
Reading, Berkshire
RG2 6UH, United Kingdom