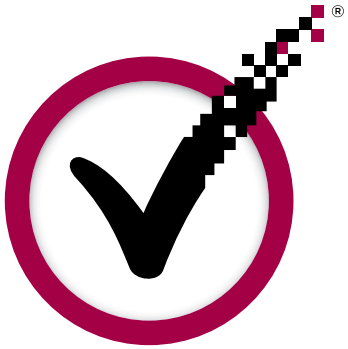


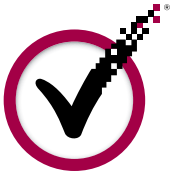
WHITE PAPER

MALWARE SECURITY REPORT: PROTECTING YOUR BUSINESS, CUSTOMERS, AND THE BOTTOM LINE

VeriSign®

WHITE PAPER

CONTENTS



WHITE PAPER

MALWARE SECURITY REPORT: PROTECTING YOUR BUSINESS, CUSTOMERS, AND THE BOTTOM LINE

MALWARE IS CRAWLING ONTO WEB SITES EVERYWHERE

This white paper will help you understand the threat from malware and how it can impact your online business. You'll learn about criminals' motivations for distributing malware through the web and how they infect web servers to make distribution possible. This paper also highlights techniques administrators can use to detect when and how attackers have compromised their web server.

Other critical malware discussion points include:

- How attackers distribute malware through web browsers rather than traditional techniques, such as infected email attachments.
- What the profit motivations are for modern criminals to infect end-user systems.
- How malware is distributed by infecting legitimate web sites.
- What tools have been developed to infect as many pages as possible
- How cybercriminals have developed attack techniques that allow malware to infect thousands of web sites at once by exploiting web site vulnerabilities.
- How attackers distribute their code through malicious advertisements to infect the most-popular, often well-secured, web sites.

WHAT IS MALWARE?

Malware is a general term for malicious software, and it is a growing problem on the Internet. Hackers install malware by exploiting security weaknesses on your web server to gain access to your web site. Malware includes everything from adware, which displays unwanted pop-up advertisements, to Trojan horses, which can help criminals steal confidential information, like online banking credentials.

Malware is increasingly distributed through web browsers. This tactic has become more common in recent years, as email filtering made it more difficult for attackers to distribute their programs through email spam. Additionally, as firewalls have become more prevalent in the workplace and at home, malware can no longer easily spread from system to system over a network. Through the web, there are opportunities for hackers to penetrate your company's web site and use it as a host to spread malware to your customers.

Malware code is not easily detectable and may infect consumers' computers when they simply browse your web site. This is known as "drive-by" malware, and users are largely (or completely) unaware that their systems have become compromised with this type of attack—making it a particularly insidious problem. Hackers use drive-by malware to spread viruses, hijack computers, or steal sensitive data, such as credit card numbers or other personal information.

How drive-by malware works, and are small web sites at risk?

Drive-by malware downloads itself onto a user's system without their consent. Cybercriminals exploit browser and/or plug—in vulnerabilities to deliver the malware by hiding it within a web page as an invisible element (e.g., an iframe or obfuscated javascript) or by embedding it in an image (e.g., a flash or PDF file) that can be unknowingly delivered from the web site to the visitor's system.

Any web site is at risk. Small sites can be more vulnerable because they are less likely to have the resources and expertise needed to detect and rapidly respond to attacks. Malware may infect your customers' computers when they simply browse your site. Targeting web sites with low traffic allows hackers to avoid detection longer and cause more damage.

THE ANATOMY OF MALWARE ATTACKS

To infect a computer through a web browser, an attacker must accomplish two tasks. First, they must find a way to connect with the victim. Next, the attacker must install malware on the victim's computer. Both of these steps can occur quickly and without the victim's knowledge, depending on the attacker's tactics.

One way for an attacker to make a victim's browser execute their malicious code is to simply ask the victim to visit a web site that is infected with malware. Of course, most victims will not visit a site if told it is infected, so the attacker must mask the nefarious intent of the web site. Sophisticated attackers use the latest delivery mechanisms, and often send malware-infected messages over social networks, such as Facebook, or through instant messaging systems. While these methods have proved successful to a degree, they still rely on tempting a user to visit a particular web site.

Other attackers choose to target web sites that potential victims will visit on their own. To do this, an attacker compromises the targeted web site and inserts a small piece of HTML code that links back to their server. This code can be loaded from any location, including a completely different web site. Each time a user visits a web site compromised in this manner, the attacker's code has the chance to infect their system with malware.

Common types of malware delivery mechanisms:

- **Software updates:** Malware posts invitations inside social media sites, inviting users to view a video. The link tries to trick users into believing they need to update their current software to view the video. The software offered is malicious.
- **Banner ads:** Sometimes called "malvertising," unsuspecting users click on a banner ad that then attempts to install malicious code on the user's computer. Alternatively, the ad directs users to a web site that instructs them to download a PDF with heavily-obscured malicious code, or they are instructed to divulge payment details to download a PDF properly.
- **Downloadable documents:** Users are enticed into opening a recognizable program, such as Microsoft Word or Excel, that contains a preinstalled Trojan horse.
- **Man-in-the-middle:** Users may think they are communicating with a web site they trust. In reality, a cybercriminal is collecting the data users share with the site, such as login and password. Or, a criminal can hijack a session, and keep it open after users think it has been closed. The criminal can then conduct their malicious transactions. If the user was banking, the criminal can transfer funds. If the user was shopping, a criminal can access and steal the credit card number used in the transaction.
- **Keyloggers:** Users are tricked into downloading keylogger software using any of the techniques mentioned above. The keylogger then monitors specific actions, such as mouse operations or keyboard strokes, and takes screenshots in order to capture personal banking or credit card information.

THE MALWARE BUSINESS MODEL

How do attackers use malware to turn a profit? They can use infected computers to generate income in many ways. One of the simplest is through advertising. Just as many of the web sites generate income by displaying ads, malware can display ads that result in payments to the cybercriminal.

Alternatively, extortion is used. A large network of infected computers can be very powerful, and some attackers use this threat to extract payments from web site owners. A group of computers controlled by one attacker, known as a "botnet," can send a large amount of network traffic to a single web site, which can result in a denial of service (DoS) attack. The criminals then contact the web site owner and demand a payment to stop the attack.

Criminals also frequently use infected computers to gather valuable user information, such as credentials for online banking. This type of malware, known as an infostealer or banking Trojan, is one of the most sophisticated and stealthy forms of malware. The criminals can then use the private information for their own malicious schemes or sell it to a third-party who then uses it to make a profit.

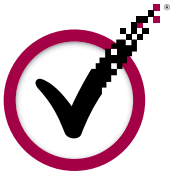
What is blacklisting, and why is it important to avoid?

Because of the potential damage caused by malware, Google, Yahoo, Bing and other search engines place any web site found with malware on a blocked list, or "blacklist." Once blacklisted, the search engine issues a warning to potential visitors that the site is unsafe or excludes it from search results altogether. No matter how much search engine optimization you do, if your web site is blacklisted the impact to your business could be devastating. This blacklisting can occur without warning, is often done without your knowledge, and is very difficult to reverse. Taking the proper measures to prevent search engine blacklisting is critical to the long-term success of any web site.

VERISIGN CONTINUES ITS LEADERSHIP IN ONLINE SECURITY

VeriSign was the first-to-market with a commercial SSL solution in the mid-1990's. It is the leading provider of SSL Certificates, and VeriSign is the most recognized Internet security brand in the world today. Cultivated over many years, this reputation has been developed with both consumers and online businesses through industry leadership and the application of state-of-the-art technology into its leading SSL solutions.

In addition to the peace-of-mind that comes with selecting a proven SSL Certificate, VeriSign has continued to address its customers' needs by constantly augmenting its SSL offerings with support for new standards and integration with complementary technologies and solutions. VeriSign continues this heritage by providing daily web site malware scanning with its SSL solutions to ensure that your web site, your valuable brand, and your customers' confidential information are protected from an ever-changing Internet threat environment.



CONCLUSION

Online sales and services have experienced tremendous growth over the past decade. However, the increasing use of the Internet in everyday life has also brought a rise in nefarious activity. Malware is becoming more pervasive and jeopardizes the growth of e-commerce by fostering fears of compromised personal information. This leads to trepidation and sub-optimal results for online businesses. There needs to be an effective means to combat the use of malware if e-commerce is to reach its full potential.

VeriSign provides a comprehensive trust solution for your online business success by combining premium SSL Certificates with innovative functionality to ensure that your public-facing web sites are regularly monitored for malware. Combined with the VeriSign seal, the world's #1 trust mark, VeriSign helps you give your customers peace of mind when they interact with you online. If you want to ensure that consumers view your web site as a trusted place to conduct e-commerce, VeriSign SSL Certificates are the right choice.

ABOUT VERISIGN

VeriSign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.

Visit us at www.VeriSign.com for more information.

00028754 06-23-2010