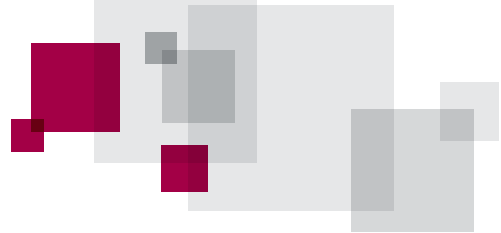


WHITE PAPER

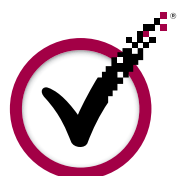
PROTECT YOUR BRAND AGAINST TODAY'S MALWARE THREATS WITH CODE SIGNING



WHITE PAPER

CONTENTS

- 1 INTRODUCTION
- 1 MALWARE: IS IT AN EPIDEMIC YET?
- 2 WHAT MAKES MALWARE SO INSIDIOUS?
- 2 UNDERSTANDING THE IMPACT OF MALWARE
- 3 CODE SIGNING: THE FIRST DEFENCE FOR LEGITIMATE SOFTWARE
- 4 ENABLING THE BENEFITS OF CODE SIGNING
- 5 IT TAKES A TRUSTED THIRD PARTY
- 5 ADDING ANOTHER LAYER OF PROTECTION
- 5 CONCLUSION
- 5 GLOSSARY
- 6 LEARN MORE
- 6 ABOUT VERISIGN





+ INTRODUCTION

Today malware is big business for cyber criminals. The availability of exploitation kits, malware-as-a-service, rogue anti-malware software (AKA “scareware”) and other tools have made it too easy for unscrupulous individuals and criminal groups to infiltrate home and business computers and networks. Faced with the increasing sophistication of these threats, even the most savvy computer users are getting infected.

It is no wonder, then, that consumers and businesses alike are skittish about anything they are asked to download from the Internet. Whether it be the latest version of a software application or a browser plug-in that enhances the user experience, users are being told to be vigilant in terms of defending themselves against downloading potentially malicious software.

The malware threat and resulting lack of confidence on the part of online users put at risk software developers and other companies that rely on software downloads. Obviously, these threats can have a major impact on profits, as fewer people purchase or download software — with relatively new and unknown brands being particularly vulnerable. Potentially even more devastating is the risk of a damaged reputation. If cyber criminals distribute malware-laden software under the guise of a legitimate brand, the damage can be lethal to the brand owner’s business.

Code signing is an industry-recommended and widely-used defence against tampering, corruption or malware infection in software code. As a powerful method, both for identifying code and for ensuring the identity of the code signer, it builds trust with anyone using the software.

This white paper discusses the malware threat, the potential impact on your business, and how to protect your company and your customers by using code signing.

+ MALWARE: IS IT AN EPIDEMIC YET?

The news on malware is not good. According to the Anti-Phishing Working Group (APWG), the number of crimeware-spreading sites and the number of unique keyloggers and malware applications reached an all-time high in the second half of 2008.¹ Microsoft further reported that the amount of malware and other unwanted software found on computers rose 43 per cent in the first half of 2008.² Google indicated that a single malware source infected over 60,000 hosts.³ Also, bot herders (criminals controlling a network of compromised computers) have taken control of 12 million new IP addresses in the first quarter of 2009, a 50 per cent increase since the last quarter of 2008.⁴

Some environments provide targets that are particularly vulnerable to malware. In the mobile environment, malicious code can spread through the network to everyone who subscribes to the provider’s wireless services. More than 400 mobile viruses have been documented to date, resulting in tens of thousands of infections worldwide.⁵

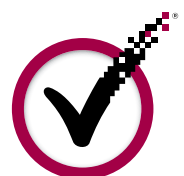
1 “Phishing Activity Trends Report, 2nd Half 2008”, APWG, 17 March 2009

2 “Microsoft: Malware Threats Up 43%”, Paul McDougall, *InformationWeek*, 3 November 2008

3 “Malware a Growing Issue: Yes, Major Impact on SEO”, Search Engine Roundtable, 5 June 2009

4 “Conficker Hype Obscures Sneaky Botnet Growth”, John Leyden, *Enterprise Security*, 6 May 2009

5 “Mobile Insights: Prevent Mobile Malware: Learn How to Protect Your Enterprise and Devices”, SearchMobileComputing.com, 30 September 2008





WHITE PAPER

As the threat continues to grow unabated, malware (e.g. Trojan horses, worms, viruses and spyware/adware) is now the tool of choice for theft, fraud, computer hijacking and other forms of nefarious activity. There are increasing signs that more people are turning to cybercrime because of current economic conditions. Online crime watchers are reporting that a number of newly unemployed technology workers are turning to theft and exploitation of sensitive data.⁶

+ WHAT MAKES MALWARE SO INSIDIOUS?

Increasingly, malware exploitation of vulnerabilities in software has become incredibly sophisticated. A perfect example is the Tigger/Syzor malware, which is, according to VeriSign iDefense, one of the most sophisticated pieces of malware that exists today. This particular software disables security products in unique ways such as posting malformed messages to windows owned by the daemon processes, sending special byte codes over named pipes, and using the products' own APIs.

Malware such as Tigger installs something called a rootkit to cloak its activities. A rootkit is a malicious program designed to hide the processes and files that the attacker installs on the system. It is intended to seize control of the operating system running on the hardware.

The Tigger Trojan also logs keystrokes, gathers system information, and opens a backdoor on the compromised computer. The most alarming and unusual feature of this resourceful piece of malware is that it is the first info-stealing malware that goes to the trouble of removing other pieces of malware. Tigger removes all the rogue security software titles to project the façade of “a normally operating computer”.⁷

The Washington Post reports that Tigger claimed more than a quarter of a million victims in just a few months.⁸

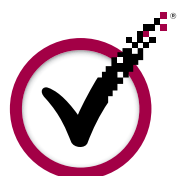
+ UNDERSTANDING THE IMPACT OF MALWARE

For computer users, businesses, service providers and software developers, the impact of malware and the resulting fear of fraud and theft can be enormous.

For instance, spyware that enables an attacker to steal a password and infiltrate a corporate network could result in dramatic financial losses, including fraud losses, theft of intellectual property, diminished brand value and lost productivity. If a data theft becomes public, customers and potential prospects could take their business to competitors where they feel that their confidential data will be safer.

Having malware identified in downloadable software or on a business's Web site could potentially ruin the reputation of the brand or business. For instance, in the current version of Google Search, if Google detects malware on a Web site it will label the site in its search results with a strong warning that the site could be harmful. Potential customers would then stay away in droves.

6 “Economic Bust, Cybercrime Boom”, Andy Greenberg, Forbes.com, 19 November 2008
7 “Tigger: The Pandora's Box Triggered”, Diyya Mohan, Bright Hub, 20 March 2009
8 “The Tigger Trojan: Icky, Sticky Stuff”, Brian Krebs, *Washington Post*, 24 February 2009





WHITE PAPER

FIGURE 1. EXAMPLE OF GOOGLE FLAGGING A POTENTIALLY MALICIOUS WEB SITE



December 2008 saw the largest jump ever in the number of sites with malicious code, reaching an all-time high of 31,173. This represents a whopping 827 per cent increase from the beginning of the year.¹⁰

—The Anti-Phishing Working Group (APWG), 17 March 2009

Once Google flags a site as being potentially harmful, cleaning the site and having it re-indexed as a “safe” site by Google takes considerable time and effort. The business typically has to file a reconsideration request with Google Webmaster Central for Google to recognise that the site is not a security risk and remove the warning.

Losses due to cybercrime are now estimated at US\$100 billion annually.⁹ Businesses can ill afford to ignore the threat of malware, least of all those that sell or provide software for download.

+ CODE SIGNING: THE FIRST DEFENCE FOR LEGITIMATE SOFTWARE

With potential customers wary of downloading software that may contain malware, developers and companies offering software for download must find a way to assure users that their software is legitimate. The best way to convey this assurance is to make it easy for users to confirm the name of the business that is publishing the software and also to confirm that the software has not been altered since it was finalised. Code signing is a widely used and industry-accepted method for doing just that. By code signing software, businesses help to protect against malware and instil confidence and trust in their brand.

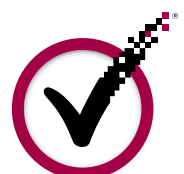
Code signing, sometimes called object signing, is a way to digitally “shrink wrap” code so that it is protected from tampering — similar to a shrink-wrapped product in a shop. By code signing software, the person downloading the software can verify that the code and its publisher have been identified by a trusted third party. Like boxed software in a shop, code signing ensures that the code has not been modified or tampered with since the code was created and signed.

This method of verification is so effective that more and more operating systems, software applications, devices and mobile networks are requiring code signing to ensure that the code will not harm or interrupt services. For instance, code signing is a requirement for any program written for the Microsoft .NET

PLATFORMS FOR CODE SIGNING

Code signing can be used for a number of platforms. In fact, digital signatures are required for many of them, otherwise the application cannot be installed or will not run:

- Microsoft® Windows® Desktop, Microsoft Windows Mobile®, and Microsoft Visual Basic for Applications (VBA) and Office
- Sun Java®
- Adobe® AIR and Adobe Shockwave
- Mac® and Mac OS X®
- Symbian™
- Qualcomm® BREW®



⁹ “Experts: Cybercrime as Destructive as Credit Crisis”, *Reuters*, 19 November 2008, eWeek.com
¹⁰ “Phishing Activity Trends Report, 2nd Half 2008”, APWG, 17 March 2009



WHITE PAPER

Framework, Kernel-Mode Driver Framework and Adobe AIR, and mobile platform certifications such as Microsoft Mobile2Market and Symbian Signed. These platforms will generate warning messages or refuse to install an application unless it is code signed by a recognised Certificate Authority (CA).

Trends in the industry point to more and more operating systems, application development platforms and mobile devices requiring signed code before allowing installation. Even when the platform does not require signed code, application users increasingly do. In a survey conducted by VeriSign, developers and software publishers indicated that code signing is becoming a requirement for partners and customers.

With the proliferation of scareware or malware masquerading as security software, anti-malware vendors are among the most diligent code signers.¹¹ However, as the threat of malware increases, all code developers should be signing their code.

+ ENABLING THE BENEFITS OF CODE SIGNING

Whether a target platform requires code signing or not, companies should seize the opportunity to instil confidence and trust in their products. Customer loyalty is more important than ever, and the best way to build a long-term relationship is to consistently deliver the assurance that your products can be trusted.

Code signing benefits everyone involved:

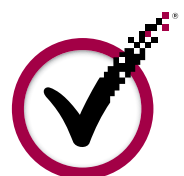
- Developers can ensure the integrity of their applications and protect their intellectual property and brand image.
- End-users can be sure that applications originate from authentic sources.
- Companies can build trust in their brands, which could help to increase downloads and revenue.
- Network operators can protect critical network resources from malicious malware attacks.
- Publishers can distribute patches and updates safely and efficiently.

+ IT TAKES A TRUSTED THIRD PARTY

Software can be signed with a trusted Certificate Authority (CA) or be self-signed or unsigned. When used externally, a self-signed certificate has little credibility and platforms do not recognise its root. Unsigned or self-signed code triggers an alert that the software publisher is unknown and that the code could be detrimental to the system. Users are unlikely to download any application that is not signed by a trusted CA.

Trust in your signed code is only as strong as the third party issuing the digital certificate. It is critical to choose a trusted third party that is recognised worldwide by consumers, businesses, network providers and software developers.

In a Code Signing Users Survey conducted by VeriSign in December 2008, software publishers and developers commented that customers increasingly say that they will not purchase unsigned products. Respondents observed that code signing makes it easier for them to distribute software over the Internet and increases customers' willingness to download code.





+ ADDING ANOTHER LAYER OF PROTECTION

Finally, businesses should protect themselves and their customers from malware by using a layered security approach. In addition to code signing, businesses should consider implementing technology such as Secure Sockets Layer (SSL) and Extended Validation (EV) SSL to encrypt sensitive information and help customers to authenticate their site.

+ CONCLUSION

Code signing allows consumers to feel comfortable about downloading software online and helps to build credibility in a business's products and brand. It is a first line of defence that helps prevent users — consumers and business users alike — from falling prey to malware and other vicious online attacks. And ultimately it protects your company's reputation, online revenue stream and the bottom line.

VeriSign® Code Signing, from the most trusted brand on the Internet, protects your brand and your intellectual property by making your applications identifiable and harder to falsify or damage. With a VeriSign certificate authenticating your code, you can rest assured that users and the majority of the platforms they are using will trust your software.

+ GLOSSARY

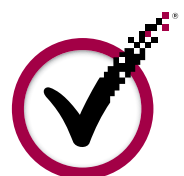
Certificate Authority (CA) — A Certificate Authority is a trusted third-party organisation that issues digital certificates, such as SSL Certificates, after verifying the information included in the certificates.

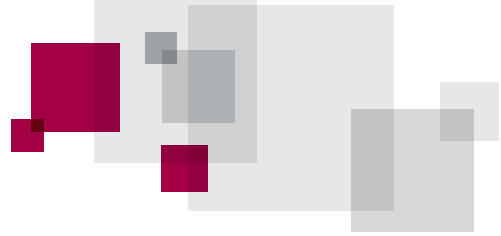
Code Signing — Code signing is a way of using digital certificates to provide explicit third-party confirmation of the authenticity of the publisher and the integrity of the application.

Encryption — Encryption is the process of scrambling a message so that only the intended audience has access to the information. SSL technology establishes a private communication channel whereby data can be encrypted during online transmission, thus protecting sensitive information from electronic eavesdropping.

Extended Validation (EV) SSL Certificate – Requires a high standard for verification of SSL Certificates, dictated by a third party, namely the CA/Browser Forum. In Microsoft Internet Explorer 7 and other popular high-security browsers, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

Secure Sockets Layer (SSL) Technology — SSL and its successor, Transport Layer Security (TLS), use cryptography to provide security for online transactions. SSL uses two keys to encrypt and decrypt data — a public key known to everyone and a private or secret key known only to the recipient of the message.





WHITE PAPER

SSL Certificate — An SSL Certificate incorporates a digital signature to bind together a public key with an identity. SSL Certificates enable encryption of sensitive information during online transactions, and in the case of organisationally validated certificates, they also serve as an endorsement of the certificate owner's identity.

+ LEARN MORE

For more information about VeriSign Code Signing solutions, please call +61 3 9674 5500 or e-mail sales@verisign.com.au.

+ ABOUT VERISIGN

VeriSign, Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day VeriSign helps companies and consumers all over the world to engage in trusted communications and commerce. Additional news and information about the company is available at www.Verisign.co.uk.

Visit us at www.Verisign.com.au for more information.

