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

White Paper

Protect Your Brand Against Today's Malware Threats with Code Signing

Symantec™

Norton™ SECURED
powered by VeriSign

Protect Your Brand Against Today Malware Threats with Code Signing

CONTENTS

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 savviest computer users are getting infected.

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

The malware threat and resulting lack of confidence on the part of online users puts software developers and other companies that rely on software downloads at risk. 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 defense against tampering, corruption, or malware infection in software code. As a powerful method to both identify code and assure 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 both reached all-time new heights in the second half of 2008.[1] Microsoft further reported that the amount of malware and other unwanted software found on computers rose 43 percent in the first half of 2008.[2] Google indicated that a single malware source infected over 60,000 hosts.[3] And 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 percent increase since the last quarter of 2008.[4]

Some environments provide particularly vulnerable targets for 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, March 17, 2009
[2] "Microsoft: Malware Threats Up 43%," Paul McDougall, InformationWeek, November 3, 2008
[3] "Malware a Growing Issue: Yes, Major Impact on SEO," Search Engine Roundtable, June 5, 2009
[4] "Conficker Hype Obscures Sneaky Botnet Growth," John Leyden, Enterprise Security, May 6, 2009
[5] "Mobile Insights: Prevent Mobile Malware: Learn How to Protect Your Enterprise and Devices," SearchMobileComputing.com, Sept. 30, 2008

As the malware threat continues to grow unabated, malware such as Trojan horses, worms, viruses, and spyware/adware is now the tool of choice for theft, fraud, computer hijacking, and other forms of nefarious activity. And there are increasing signs that more people are turning to cyber crime because of the current economic conditions. Online crime watchers are reporting that a portion 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 Symantec 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 like Tigger installs something called a rootkit to cloak its activities. A rootkit is a malicious program designed to hide the processes and files 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 enables a backdoor on the compromised computer. The most scary and unique feature of this resourceful piece of malware is that it's 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-million victims in the span of 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 their confidential data is safer.

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

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

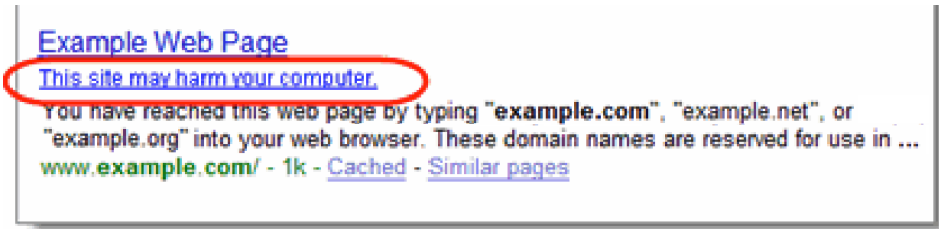

Figure 1. Example of Google flagging a potentially malicious website

Once Google flags a site as potentially harmful, purifying the site and having it reindexed as a "safe" site by Google takes considerable time and effort. The business typically has to file a reconsideration request with Google Webmaster Central to have Google recognize that the site is not a security risk and remove the warning.

Losses due to cyber crime are now estimated at $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.

> 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 percent increase from the beginning of the year.[10]
>
> —The Anti-Phishing Working Group (APWG), March 17, 2009

Code Signing: The First Defense 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 publishing the software and that the software hasn't been altered since it was finalized. Code signing is a widely used and industry-accepted method to do just that. By code signing software, businesses help protect against malware and instill 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 on a store shelf. 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 store, 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 Framework, Kernel-Mode Driver Framework, Adobe AIR, and mobile platform certifications such

[9] "Experts: Cyber-Crime as Destructive as Credit Crisis," Reuters, November, 19, 2008, eWeek.com
[10] "Phishing Activity Trends Report, 2nd Half 2008," APWG, March 17, 2009

as Microsoft Mobile2Market and Symbian Signed. These platforms will generate warning messages or refuse to install an application unless it's code signed by a recognized Certificate Authority (CA).

Trends in the industry point to more and more operating systems, application development platforms, and mobile devices requiring signed code before installation. Even when the platform doesn't require signed code, application users increasingly do. In a survey conducted by Symantec, 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, antimalware vendors are among the most diligent code signers.[11] However, as the threat of malware increases, all code developers should be signing their code.

In a Code Signing Users Survey conducted by Symantec in December 2008, software publishers and developers commented that customers increasingly say they won't 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.

Enabling the Benefits of Code Signing

Whether a target platform requires code signing or not, companies should seize the opportunity to instill 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 product 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 originated from authentic sources
- Companies can build trust in their brands, which could help increase downloads and revenue
- Network operators can protect critical network resources from malicious malware attacks
- Publishers can safely and efficiently distribute patches and updates

It Takes a Trusted Third Party

Software can be signed with a trusted CA, self-signed, or unsigned. When used externally, a self-signed certificate has little credibility and platforms do not recognize 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.

Platforms For Code Signing

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

- Microsoft® Authenticode, Microsoft Office, Microsoft Windows Mobile, and Microsoft Visual Basic® for Applications (VBA)
- Sun® Java
- Adobe® AIR and Adobe Shockwave
- Windows Mobile
- Symbian

Glossary

Certificate Authority (CA)
A CA is a trusted third-party organization 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.

[11] "Threat Research & Response Blog," Microsoft Malware Protection Center, November 6, 2008

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

Adding Another Layer of Protection

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

Conclusion

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

Symantec™ 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 Symantec Certificate authenticating your code, you can rest assured that users and the majority of the platforms they are using will trust your software.

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 where data can be encrypted during online transmission, 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, the CA/Browser Forum. In Microsoft Internet Explorer 7 and other popular high security browsers, websites 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.

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 organizationally validated certificates, also serve as an attestation of the certificate owner's identity.

Learn More

For more information about Symantec Code Signing solutions, please call 1 (866) 893-6565 or 1 (650) 426-5112 (option 3) or email isales@vsymantec.com

More Information

Visit our website

http://go.symantec.com/code-signing

To speak with a Product Specialist in the U.S.

Call 1 (866) 893-6565 or 1 (650) 426-5112

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

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.

Symantec World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
1 (800) 721 3934
www.symantec.com

Symantec™

Norton™ SECURED
powered by VeriSign