GlobalSign Malware Monitoring

Protecting your website from distributing hidden malware

GLOBALSIGN WHITE PAPER

GlobalSign®

www.globalsign.com

CONTENTS

INTRODUCTION

There has been a fundamental paradigm shift in how criminals are now distributing malicious software (malware). Rather than relying on USB devices, disks and attachments to spread viruses, criminals have found it far more effective to distribute malware by "drive-by downloads". This technique takes advantage of browser vulnerabilities and zero-day exploits to plant malicious code into unsuspecting websites – code which infects anyone who visits the page, without the need to click or install anything!

Once a machine is infected, the malware can do an assortment of harm, from corrupting data to stealing passwords, to eavesdropping for credit card entry, or even turning infected machines into "zombies" – forcing them to unknowingly join a zombie army responsible for massive denial of service attacks.

Malware is such a problem that search engines like Google have taken a very negative view of any website distributing it. Once identified, infected sites are flagged as dangerous and ultimately removed from search results, which is known as blacklisting, affecting the company's reputation and years of traffic building investment.

This white paper provides an overview of what malware is and how it can affect your websites. It also explains GlobalSign's Malware Monitoring service and how this solution is essential to ensure the security of your visitors and ultimately protect the position and reputation of your company.

MALWARE MONITORING

What is Malware?

To understand the growing need for Malware Monitoring services it's important to understand the growing threat of "drive-by downloads". Drive-by downloading is a hacker technique resulting in the unauthorized download and installation (drive-by download) of unwanted malicious software (malware) onto the client PC of anyone visiting the website. It is designed to steal information from Internet users by forcing them to automatically download malware without their knowledge or consent. By using numerous techniques to:

1) **Add an invisible `iframe` to a hosted web page, invisible to the human eye**
2) **Transparently direct the visitor's browser to a server transmitting exploits designed to break the browser through known vulnerabilities**
3) **Use the now broken browser to download and install malware / viruses onto the victim's machine**

Malware is often designed for criminal, political, and/or mischievous purposes. These purposes might include:

- **Stealing financial account numbers, passwords, corporate trade secrets, or other confidential information**
- **Tricking the user into buying something that she or he doesn't need**
- **Sending junk email (spam)**
- **Attacking other computers or networks (zombie attacks)**
- **Distributing more malware**

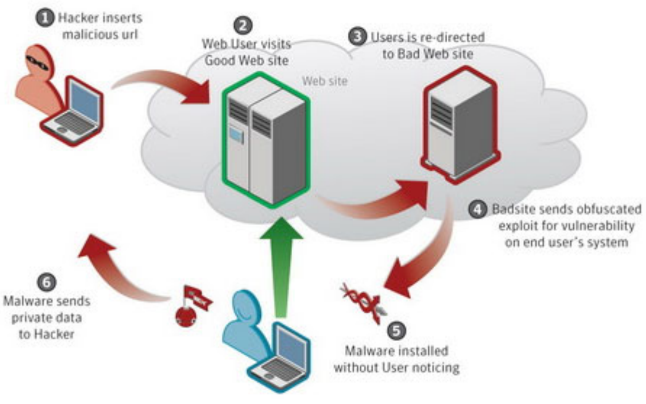

1 Hacker inserts malicious url
2 Web User visits Good Web site
Web site
3 Users is re-directed to Bad Web site
4 Badsite sends obfuscated exploit for vulnerability on end user's system
5 Malware installed without User noticing
6 Malware sends private data to Hacker

Fig 1. Example of a drive-by download

Malware includes viruses, trojans, rootkits, spam bots, spyware and other varieties (source: stopbadware.org).

Most websites are vulnerable to malicious code injection. When websites fall victim to this kind of attack, the first impact is directly against the website's visitors. The Malware installed on their PCs is designed to steal personal data, such as credit card and bank account information, or even provide the Hacker with complete control over the victim PC.

The website itself is affected as angry customers begin to complain about personal data loss. The website often quickly becomes flagged or blacklisted for hosting malicious content by organizations such as Google.

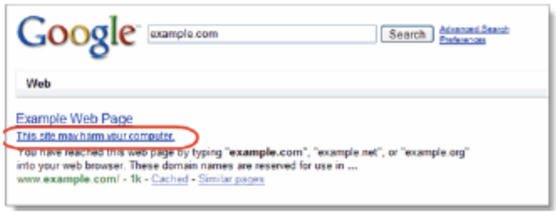
Visitors to a website can become infected by simply visiting an infected website. There is no requirement to click on any links. The malware may be designed to monitor keystrokes and steal passwords, listen for credit cards, steal personal information or lay dormant, waiting for the attacker to invisibly turn the infected machine into a "zombie". Coordinated attacks using infected zombie machines to overload specific servers or networks have become a significant problem throughout the last few years, with attacks such as Aurora (distributed denial of service attack against many major IT companies originating from China) and Operation Payback (distributed denial of service revenging against previous Wikileaks suppliers) making worldwide news.

Blacklisting

Due to the growing problem of malware distribution, Google in particular has taken a draconian view of any website distributing malware and is currently blacklisting around 9500 sites every single day.

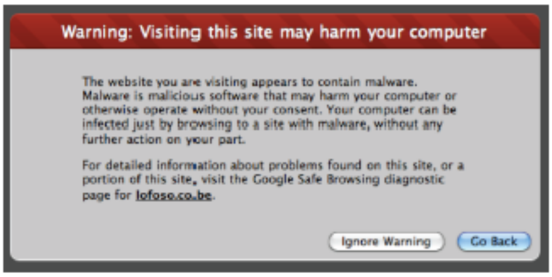
Google flagging has the greatest negative effect on websites as traffic is literally driven away from the site. Google posts warnings against visiting the site directly in their search results, or worse yet, removing the site from their search results altogether. This often has the effect of reducing a website's traffic from tens of thousands of visitors per day to almost zero.

Regardless of whether the site owners are knowingly distributing malware, a message will appear in the Google search results and also in browsers like Chrome and Firefox, warning of the potential danger of visiting the website. For example:



Example Web Page
This site may harm your computer.
You have reached this web page by typing "**example.com**", "example.net", or "example.org" into your web browser. These domain names are reserved for use in ...
www.example.com/ - 1k - Cached - Similar pages

"Remedial time, i.e. how long it takes to have Google remove you from blacklists, is undefined. Reports in forums range from weeks to months…"



Warning: Visiting this site may harm your computer

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for lofoso.co.be.

"Even major sites like cnn.com have been compromised and listed as distributing malware."

Being blacklisted also means a website owner may find their domain listed on **stopbadware.org** – a central database of infected domains referenced by hundreds of applications and service providers. For website owners blacklisting results in damage to business reputation, inevitable sharp drop in website traffic and ultimately a reduction in revenues. The remedial actions needed to be removed are slow and expensive, with no guarantees of successfully regaining rankings.

Malware in your Environment

Any company with a website is vulnerable to malware injection. Whether your company has its own dedicated servers or your websites reside in hosted space, hackers are looking for ways in.

Companies using hosted space to operate their websites need to be aware of the risk of compromise to their own infrastructure. Hackers typically seek the greatest economy of scale, attacking a hosting company's infrastructure resulting in the highest return on effort. In August 2010, malware experts identified an infection in the Network Solutions infrastructure – a widget housed on Network Solution pages. The widget took advantage of an Internet Explorer vulnerability and resulted in the Koobface malware (a virus that "phones home" for further instructions) being widely distributed. The press identified the widget as being distributed via millions of landing pages reserved for parked domains.

Source:
http://blogs.forbes.com/andygreenberg/2010/08/16/record-five-million-sites-were-likely-infected-by-hacked-webwidget/?partner=contextstory

The Network Solutions explanation suggested the malware was actually only distributed via a NetSol blog:

"Our Security Team was alerted this past weekend to a malicious code that was added to a widget housed on our small business blog, growsmartbusiness.com. This widget was used to provide small business tips on Network Solutions' under construction pages. We have removed the widget from those pages and continue to check and monitor to ensure security. The number of impacted pages that have reported publicly over the weekend are not accurate. We're still investigating the number of web pages affected.

If you have downloaded the GrowSmartBusiness widget to your website, we recommend you delete that widget and scan your site for malware."

Source:
http://blog.networksolutions.com/2010/securityalert-malware-found-on-widget/

GLOBALSIGN'S MALWARE MONITORING SOLUTION

GlobalSign's Malware Monitoring Solution, powered by StopTheHacker, helps website owners avoid a doomsday situation by providing monitoring for malicious code injection and drive-by downloads. The solution gives due warning of an infection and sufficient details to facilitate timely removal of the injected code - protecting both customers and corporate reputation.

The non-intrusive solution crawls a website and actively analyzes the content on each page for signs of compromise. StopTheHacker uses numerous, advanced and unique techniques to ensure known and unknown malicious codes are identified quickly. Even the most advanced malware distribution techniques are efficiently identified. The service immediately notifies website owners via email if their site is infected with malicious code being used to target end users' Personal Computers with drive-by downloads.

GlobalSign's Malware Monitoring Service protects businesses and customers from the impacts of malware injection, is included with all GlobalSign Retail SSL Certificates, and provides:

- Fully automated non-intrusive scans
- Weekly, daily or hourly scans depending on SSL Certificate type purchased
- Automated email alerts should your site become blacklisted or affected by malware
- Details of injected code snippet to facilitate timely removal of malware and code-level remediation
- Cloud based Customer dashboard to fully view reports and manage website domain
- GlobalSign Trust Seal to increase visitor confidence

ENTERPRISE AND HOSTING PROVIDER MALWARE MONITORING SOLUTIONS

GlobalSign automatically bundles basic Malware Monitoring plans with its Retail SSL Certificates, but understands enterprise and hosting providers' needs may differ. No matter what size your website may be or how many domains you have, GlobalSign's Malware Monitoring Service has a solution that will work for your security requirements and budget.

INQUIRE ABOUT GLOBALSIGN'S MALWARE MONITORING SOLUTION

To Inquire about our Malware Monitoring Services, please contact us at sales@globalsign.com we would be happy to discuss your specific requirements.

For further information visit: http://www.globalsign.com/ssl/malware-scanning/

ABOUT GLOBALSIGN

GlobalSign was one of the first Certificate Authorities and has been providing digital credentialing services since 1996. It operates multi-lingual sales and technical support offices in London, Brussels, Boston, Tokyo and Shanghai.

GlobalSign has a rich history of investors, including ING Bank and Vodafone. Now part of a GMO Internet Inc group company - a public company quoted on the prestigious Tokyo Stock Exchange (TSE: 9449) whose shareholders include Yahoo! Japan, Morgan Stanley and Credit Suisse First Boston.

As leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication and Enterprise Digital ID Solutions, internal PKI & Microsoft Certificate Service root signing. Our trusted root CA Certificates are recognized by all operating systems, all major web browsers, web servers, email clients and Internet applications; as well as all mobile devices.

Accredited to the highest standards

As a WebTrust accredited public Certificate Authority, and member of the Online Trust Alliance, CAB Forum and Anti-Phishing Working Group, our core solutions allow our thousands of enterprise customers to conduct secure online transactions and data submission, and provide tamper-proof distributable code, as well as being able to bind identities to Digital Certificates for S/MIME email encryption and remote two factor authentication, such as SSL VPNs.

GlobalSign US & Canada
Tel: 1-877-775-4562
www.globalsign.com
sales-us@globalsign.com

GlobalSign EU
Tel: +32 16 891900
www.globalsign.eu
sales@globalsign.com

GlobalSign UK
Tel: +44 1622 766766
www.globalsign.co.uk
sales@globalsign.com

GlobalSign FR
Tel: +33 1 82 88 01 24
www.globalsign.fr
ventes@globalsign.com

GlobalSign DE
Tel: +49 30 8878 9310
www.globalsign.de
verkauf@globalsign.com

GlobalSign NL
Tel: +31 20 8908021
www.globalsign.nl
verkoop@globalsign.com