

GlobalSign Malware Monitoring

Protecting your website from distributing hidden malware

GLOBALSIGN WHITE PAPER

Steve Waite, Chief Marketing Officer
GMO GlobalSign Inc



www.globalsign.com

CONTENTS

Introduction..... 3

Malware Monitoring..... 3

 What is Malware..... 3

 Blacklisting..... 4

 Malware in your Environment..... 4

 HackAlert - the GlobalSign Malware Monitoring Solution..... 5

 Enterprise Malware Monitoring Solutions..... 6

Inquire about the Malware Monitoring Solution..... 6

About GlobalSign..... 7

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 and install anything!

Once infected the malware can do any assortment of nasty deeds. From corrupting data to stealing passwords to eavesdropping for credit card entry or even turning infected machines into “zombies” – unknowingly forcing them to join a zombie army responsible for massive denial of service attacks.

Such is the problem of malware distribution that search engines like Google have taken a very dim view of any website distributing malware. 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 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 web site. 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 e-mail (spam)**
- **Attacking other computers or networks (zombie attacks)**
- **Distributing more malware**

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, as 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

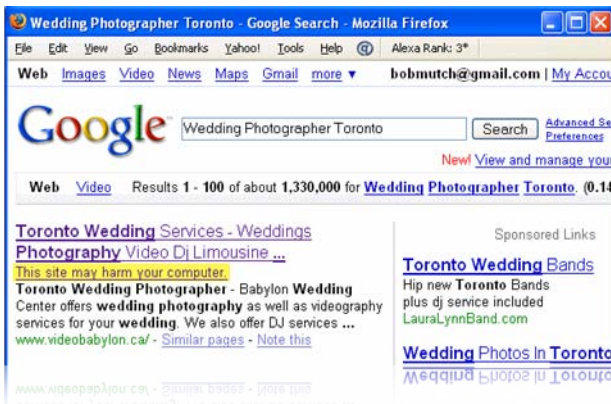
monitor keystrokes and steal passwords, listen for credit cards, steal personal information or lie dormant, waiting for the attacker to invisibly turn the infected machine into a “zombie”. Co-ordinated attacks using infected zombie machines to overload specific servers or networks have become a significant 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.

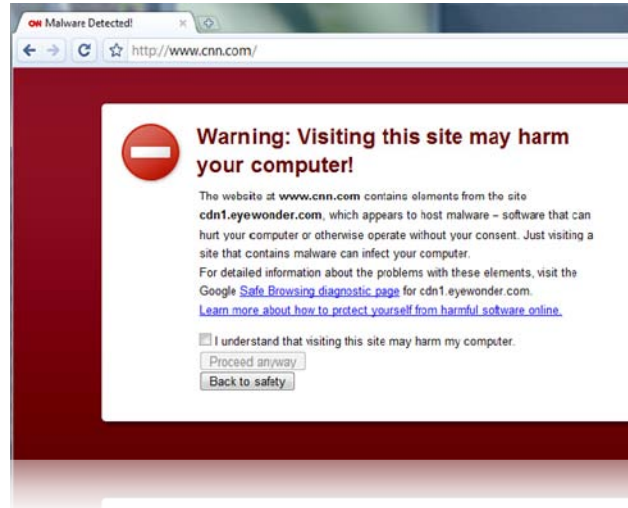
Google flagging has the greatest negative effect on websites as traffic is literally driven away from the site, due to Google posting warnings against visiting the site directly in their search results, or worse yet, removing the site from their search results altogether. This often has the effect of 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:



“Remedial time, i.e. how long it takes to have Google remove you from blacklists, is undefined and frankly

unknown. Reports in forums range from weeks to months...”



“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 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. As hackers typically seek the greatest economy of scale, attacking a hosting company’s infrastructure results 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-web-widget/?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.”

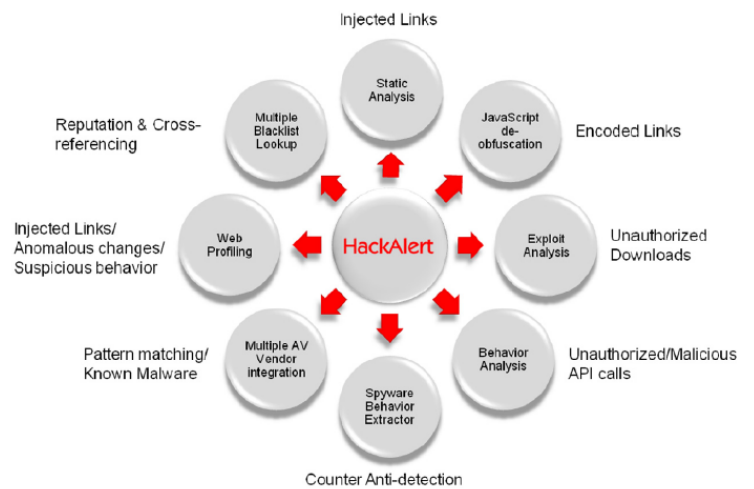
Source: <http://blog.networksolutions.com/2010/security-alert-malware-found-on-widget/>

HackAlert - the GlobalSign Malware Monitoring Solution

HackAlert helps website owners avoid a doomsday situation by providing monitoring for malicious code injection and drive-by-downloads by giving due warning of an infection and sufficient details to facilitate timely removal of the injected code - protecting both customers and corporate reputation.

The solution crawls a website and actively analyzes the content on each page for signs of compromise. HackAlert uses numerous unique techniques to ensure malicious code is identified quickly and even the most advanced malware distribution techniques are efficiently identified.

HackAlert’s detection technologies include the following:



The cloud-based Malware Monitoring detection service immediately notifies website owners if their site is infected with malicious code being used to target end-user’s Personal Computers with Drive-by Downloads. Delivered as a hosted Software Service (SaaS), HackAlert protects businesses and customers from the impacts of Malware Injection. Features include:

- **Identifies drive-by downloads and zero-day malware threats hidden in websites and online advertisements**
- **Optimizes multiple analysis techniques to detect malware drive-by downloads targeting end-users before the website is flagged by search engines as malicious**
- **Protects your clients and customers from malware injection and malicious advertising (malvertising)**
- **Deploys globally distributed crawler and analyzer agents for non-intrusive 24x7x365 drive-by download monitoring**
- **Identifies active malware downloads as well as links to dormant malware before the website is flagged by search engines such as Google**
- **Displays injected code snippets to facilitate immediate malware removal and code-level remediation**

- **Reports injected page, malware source, browser vulnerability being exploited and drive-by download destination**

scans per hour for as many as 5000 unique pages. No matter what size your website may be, GlobalSign HackAlert has a plan that will work for your security requirements and budget.

Enterprise Malware Monitoring Solutions

GlobalSign automatically bundles basic Malware Monitoring plans with SSL Certificates and the Managed SSL platform. To benefit from more robust malware monitoring, we have developed a number of Enterprise specific deployment plans.

GlobalSign Enterprise Malware Monitoring plans are designed to provide varying levels of alert protection based on identification technologies, website size (i.e. number of pages), scan frequency and management tools needed. Malware Monitoring is available for any number of “sites” (FQDNs or subdomains) and can cover up to 4

INQUIRE ABOUT THE MALWARE MONITORING SOLUTION

To inquire about Malware Monitoring for your enterprise, please contact us at www.globalsign.com. We would be happy to discuss your specific requirements.

ABOUT GLOBALSIGN

GlobalSign was one of the first Certification 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 a leader in public trust services, GlobalSign Certificates include SSL, Code Signing, Adobe CDS Digital IDs, Email & Authentication, Enterprise Digital Solutions, internal PKI & Microsoft Certificate Service root signing. Its 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, 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
