

Malware Attacks on Websites: Answering the Why and How

If your website has suffered a malware attack in the past, or if you have heard about this emerging threat for websites, you may be asking yourself two questions: (1) Why are websites being attacked? and (2) How do these attacks occur? This article will answer both questions for you.

Executive Summary:

- Hackers are targeting innocent, legitimate websites with drive-by-download malware attacks in order to propagate viruses.
- Drive-by-downloads do not require any user interaction other than loading an infected web page.
- A website that suffers a malware attack may infect all visitors with a virus.
- Google, Yahoo, Firefox, Internet Explorer, Norton, and McAfee all blacklist websites that are found to be serving malware.
- Websites can suffer losses of revenue, traffic, and reputation.
- Websites can face potential liability issues from infecting users.
- Malware attacks can occur in many different ways, including vulnerable web applications, compromised web server, compromised admin credentials, malvertising, and third-party widgets.
- Websites need anti-malware tools to protect themselves from malware attacks.

Why Are Websites Being Targeted for Malware Attacks?

The simple answer is that malware attacks on websites are the best way for hackers to distribute viruses. In the past, viruses used to spread via email attachments, or by coaxing users to download and install a malicious file.

These have all become less effective and/or too cumbersome for the hackers over time. The preferred method of distributing viruses these days is by **drive-by-downloads** from legitimate websites.

A drive-by-download occurs when a user visits a web page and malicious code is automatically and silently downloaded and installed on the user's computer, without any interaction with the user required. Once the virus is on the user's PC, the hackers have remote access to the computer and can steal sensitive information such as banking passwords, send out spam or install more malicious executables over time.

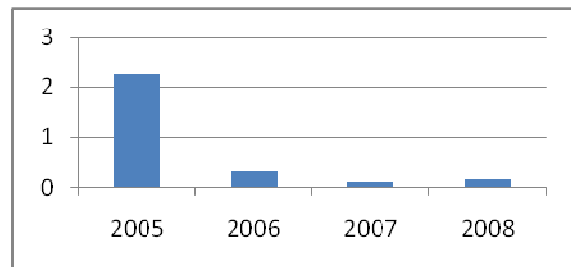


Figure 1 - Emails with Infected Attachments, 2005-2008 (Percent of total emails)

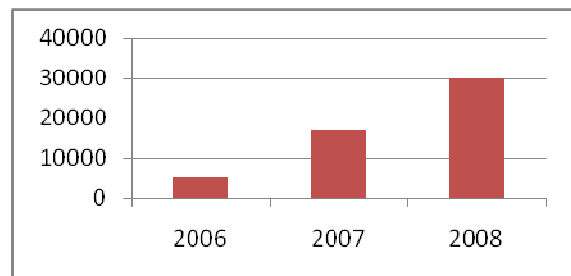


Figure 2 - Malware-infected web pages discovered daily, 2006-2008

From the data above [1][2], one can observe that emails with infected attachments have **declined 94% since 2005**, while malware-infected web pages have **increased by 600% since 2006**.

According to published reports, 77% of drive-by-downloads are occurring on legitimate websites [3]. From the hacker's point of view, it is easier to tap into a legitimate website's existing user base than try to lure users over to a malicious website that they themselves have set up. Therefore, the hackers now target innocent, legitimate websites for virus distribution.

The impact on websites of this behavior is enormous. If undetected, the website will now infect any visitors with a virus. This can severely damage the website's reputation with its existing and potential customers, as well as create liability issues. Furthermore, search engines, browsers, and security companies are now blacklisting websites that are found to be serving malware drive-by-downloads. Google, Yahoo, Firefox, Internet Explorer, Norton, and McAfee all blacklist legitimate sites that have been infected with malware. The blacklisting has an immediate impact on the website's traffic and revenues, as well as heightens the damage to a website's brand and reputation.



Figure 3 - Google flags a website that is discovered to be serving malware

How Do Malware Attacks Occur?

There are many different ways in which a website can suffer a malware attack. Here is a (non-exhaustive) list of how these attacks can occur:

Vulnerable web applications

One way in which hackers can compromise a website is via attacks against vulnerable web applications running on the site. For example, the attackers identify websites that are running vulnerable versions of blogging or content management software, shopping cart applications, or discussion forum software. Poor input sanitization or output escaping result in SQL injection or cross-site-scripting (XSS) vulnerabilities in these web applications [5]. The attackers exploit the vulnerabilities in these web applications in order to plant malicious code onto the website. For example, in a SQL injection attack, the hackers send database commands into form fields (like login or comment forms) instead of legitimate user input. The database commands are constructed in a way that they trick the web application into executing the commands and planting malicious code into the database. If the web application calls on the database to generate dynamic web pages (for example, calling the database to generate parts of the header or footer), the malicious code planted in the database could be presented to users, resulting in infections.

According to a report published by Google in 2007 [4], applications that accepted user generated content were particularly susceptible to malware attacks. Web bulletin boards or online poll applications that allowed users to post anonymous comments would be exploited

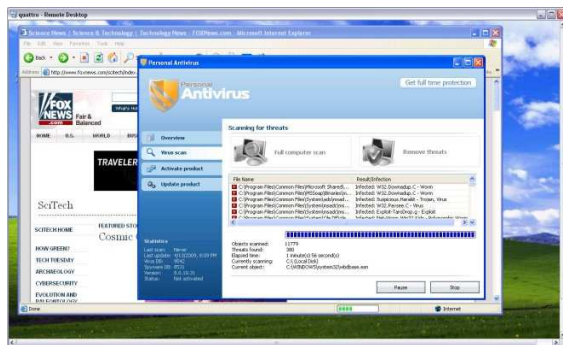


Figure 5 - Example of a malvertising pop-up imitating anti-virus software [7]

Third-party widgets and mash-ups

Modern web pages are pretty complex. In order to offer the best user experiences, as well as to manage the operations of their website, businesses often include widgets from third parties onto their web pages. Examples include the e-commerce payment buttons, poll widgets, social applications (such as reviews), traffic counters, and analytics packages. Any of these third-party widgets could be potential sources of malware infections. We spoke with one developer who found a free traffic counter and included it in his company's website. The counter was in fact injecting malicious code into every page of the website and causing visitors of the site to get infected. Clearly, websites must only source in content via widgets and mash-ups from third parties whom they trust.

However, suppose that Website A trusts Website B, and Website A uses a widget provided by Website B on every page of their site. Even though Website B is a legitimate and trusted source, there is some risk that Website B may get compromised by attackers, who are able to inject malicious content into the widgets provided by Website B to others. Now, even though Website A has performed some due diligence and has verified that Website B is a trusted third party, Website A is still being

infected because it is sourcing in malicious content from Website B's compromised servers.

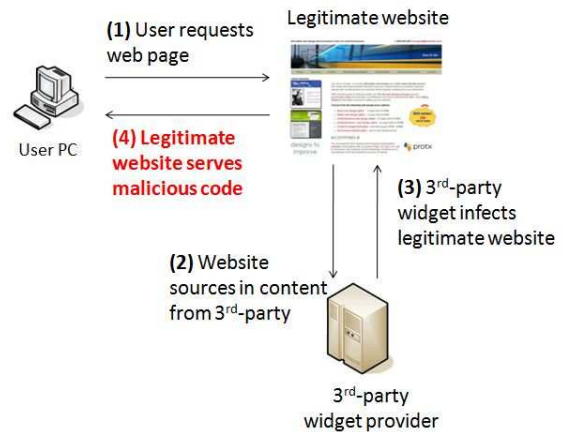
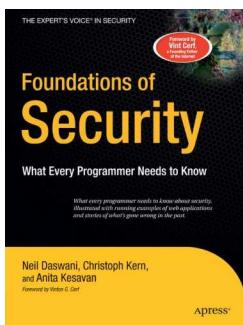


Figure 6 – Third-party Widgets Can Infect Legitimate Sites

Hopefully, this article provided you with some more information about why websites are being targeted for malware attacks, and how the attacks actually occur. Dasient’s WAM (Web Anti-Malware) solution is designed to protect websites from the rampant problem of malware attacks, and with the knowledge that there are many different attack vectors that could result in an infection.

About Dasient

Dasient was founded by ex-Google engineers and product managers from the security and web server teams. One of Dasient's co-founders, Dr. Neil Daswani, has published the book "Foundations of Security: What Every Programmer Needs to Know," which has become standard issue for new engineers at Google.



ISBN: 1590597842

Dasient is backed by some of the most influential angel investors in security and software, including the founders/investors in Verisign, Citrix, XenSource, VA Linux, and Tumbleweed Security.

Dasient is located in Silicon Valley, CA.

References

- [1] Sophos Security Threat Report 2009
- [2] Microsoft Security Intelligence Report, Vol. 6
- [3] WebSense Security Labs, State of Internet Security, Q3-Q4 2008
- [4] Niels Provos, Dean McNamee, et al. "The Ghost in the Browser: Analysis of Web-Based Malware"
- [5] Neil Daswani, Christoph Kern, Anita Kesavan; "Foundations of Security: What Every Programmer Needs to Know"
- [6] Wesley Fryer, "Hacked Wordpress footer.php" (<http://www.flickr.com/photos/wfryer/2850567461/>)
- [7] Dancho Danchev, "Scareware pops-up at Fox News" (<http://blogs.zdnet.com/>)
- [8] Bandit Defense blog post, "Using a hacked Wordpress site to pwn the web server" (<http://blog.banditdefense.com/>)