

GOOD SITES GONE BAD

By Ryan Naraine

Security Evangelist

Kaspersky Lab, Americas



Ryan Naraine

Editor-in-Chief, Threatpost.com

Senior Security Writer, ZDNet

The Internet has matured from a network of connected dial-up modems into a valuable platform for information exchange, global commerce, and workplace productivity. The World Wide Web as we know it today is a well-oiled machine, full of sophisticated, behind-the-scenes communications between browsers, Web servers and data stored on computers. This connected maze would amaze not only most home users but also most (non-IT related) corporate professionals if they truly understood it.

Today, many people still believe that using a Web browser is much like window-shopping or going to the library in the physical world – nothing happens without the knowledge of the person. (That's what the word "browser" implies, doesn't it?). Much of what goes on behind the scenes simply escapes them because they don't actually see anything happening.

Unfortunately, this maturity and sophistication has attracted the attention of well-organized malware purveyors who are now intent on using the Web to deliver viruses, spyware, Trojans, bots, rootkits, and fake security software. The anti-malware industry refers to this covert downloading of malware, which occurs at Web sites without the user's awareness, as a "drive-by download."

Drive-by delivery is of increased appeal to cyber criminals simply because it is, in general, a more stealthy form of delivery that results in more successful attacks. It boils down simply to tricking PC users into clicking a maliciously rigged Web page or HTML document and, without warning, malware gets loaded onto the machine.

To fully understand this evolving threat – which now targets legitimate Web sites – let's take a look at how the attacks work, the techniques used to lure targets to rigged Web sites, the sophisticated exploit kits and the applications they target, the complicated maze of Web redirects, and the payloads used to conduct identity theft and computer takeover attacks. In the drive-by attack, the malicious program is automatically downloaded to your computer without your consent or even your knowledge. The attack actually occurs in two steps. The user surfs to a web site that has been rigged with code that in

turn redirects the connection to a malicious third-party server hosting exploits. These exploits can target vulnerabilities in the web browser, an unpatched browser plug-in, a vulnerable ActiveX control, or any other third-party software flaws. This chart (image below), from the Google Anti-Malware Team, shows the basic structure of a drive-by download attack. As the figure indicates, there may be any number of redirections to different sites before the exploit is actually downloaded.

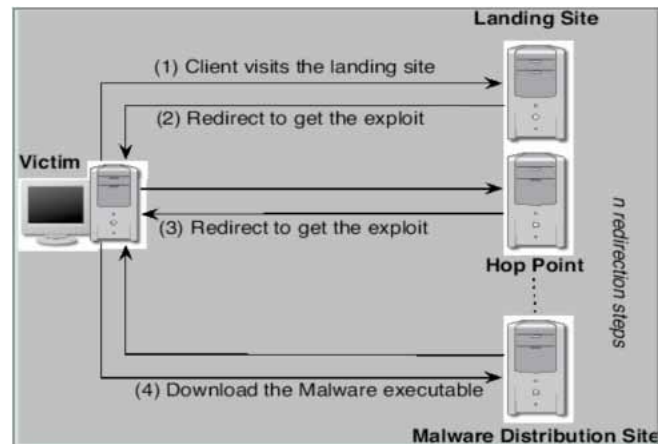


Figure 1- Basic Structure of Drive-by Download Attack

Source: Google Anti-Malware Team

According to data from Kaspersky Lab and partners in the security industry, we are in the midst of a large-scale drive-by download epidemic. Over a recent ten-month period, the Google Anti-Malware Team crawled billions of pages on the web in search of malicious activity and found more than three million URLs initiating drive-by malware downloads. "An even more troubling finding is that approximately 1.3 percent of the incoming search queries to Google's search engine returned at least one URL labeled as malicious in the results page," according to a study released by Google.

In the early days of drive-by downloads, attackers typically created malicious sites and used social engineering lures to attract visitors. This continues to be a major source of malicious

The Unpatched Desktop

The drive-by download epidemic is largely attributed to the unpatched state of the Windows ecosystem. With very few exceptions, the exploits in circulation target software vulnerabilities that are known – and for which patches are available. However, for a variety of reasons, end users are slow to apply the necessary software fixes.

Microsoft's Automatic Updates mechanism offers end users a valuable way to keep operating system vulnerabilities patched, but the same cannot be said for third-party desktop applications. Secunia, a company that tracks software vulnerabilities, estimates that about one-third of all deployed desktop applications are vulnerable to a known (patched) security issue.

The most practical approach to defending against drive-by downloads is to pay close attention to the patch-management component of defense. Specifically, users should;

- Use a patch management solution that assists with finding – and fixing – all third-party desktop applications. Secunia offers two tools – Personal Software Inspector and Network Security Inspector – that can help identify unpatched applications.
- Use a desktop browser that includes anti-phishing and anti-malware blockers. Microsoft's Internet Explorer, Mozilla Firefox, and Opera all provide security features to block malicious sites.
- Enable a firewall and apply all Microsoft operating system updates. Avoid using pirated software which has its updates disabled through WGA.

Protect Against Today's Most Pressing Threats.

Get immediate access to information on the hottest security topics facing businesses today.

- *Watch the May 19 "Real Business, Real Threats" on-demand Webinar*
- *Download the PowerPoint Presentation to share with colleagues*
- *Check out the results of our Security Survey*
- *Access the "Real Business, Real Threats" article archive*

Visit the Resource Center Now!

<http://usa.kaspersky.com/realthreats>

- Install anti-virus/anti-malware software and be sure to keep its databases updated. Make sure your anti-virus provider is using a browser traffic scanner to help pinpoint potential problems from drive-by downloads.