Armed and Dangerous: The New Generation of Web-Based Viruses

Written for executives and IT professionals, this St. Bernard® white paper describes a dangerous new class of Web-borne viruses—drive-by downloads —which circumvent most existing enterprise security systems. Sobering statistics reveal just how many infected Web pages are out there, waiting to attack a Web surfer's computer. The white paper also explains how St. Bernard's unique iPrism® Web Filter hybrid solution combats these viruses at several points for superior protection.

Hackers Hijack Web Browsers in Sneak Internet Attacks

When it comes to Internet security, it's a continual shell game: Where did the hackers hide the malware this time?

Historically, hackers have hidden malware, or badware, in malicious email attachments. But as companies and individual computer users have become savvier, fewer people are opening suspicious downloads. Consequently the level of successful email-borne virus infections has dropped.

However, bad guys just never seem to give it a rest. Recently, hackers have turned to a form of stealth attack that turns your own Web browser against you.

No Safe Place: Three Ways Web-Based Viruses Infect Browsers

According to security experts, the threat from Web-based viruses is growing rapidly. During a recent scouring of URLs worldwide, Google, Inc. found that over 1 million websites were engaging in malicious downloads . Are there really so many dangerous sites out there? No, the fact is that legitimate websites themselves are under attack. Infection can occur in three ways :

- As millions of individuals and companies have discovered, websites are relatively easy to set up and deploy. However, keeping all the applications that help operate a Web portal up to date is a daunting and often neglected task. Hackers essentially have an open field to identify and exploit security weaknesses on these sites and insert some very damaging HTML code into the Web pages.
- Many website owners make money by displaying ads by third-party advertisers. Owners may also employ small third-party "widgets," or programs that, for example, count website visitors. This external content is not under the control of the website owner, and this ambiguity of ownership and responsibility can lead to security holes that hackers exploit.
- Social networking websites such as MySpace and Facebook often allow visitors to contribute content freely. If someone "contributes" malicious HTML code, all visitors to those Web pages or posts are exposed to attack.

To avoid detection, hackers change their code frequently and cloak (obfuscate) their malware in multiple layers that require several different types of troubleshooting applications to identify and neutralize them.

Drive-By Downloads Can Wreck Havoc on Millions of Computers

Regardless of how they break in, once hackers have compromised a website, they employ sophisticated automated browser infiltration tools, known as a "drive-by downloads". These bits of viral code attach to the browsers of unknowing visitors; a single visit to an infected site is all it takes.

It Could Happen to You

During a recent scouring of URLs worldwide, Google, Inc. found that over 1 million websites, most of them legitimate organizations themselves victims of virus infiltration, were engaging in malicious downloads.

The malicious code that now infects the user's browser is designed to detect vulnerabilities in the user's own computer operating system and applications in order to force a download of a whole host of malware. These deadly programs can take control of a user's computer and steal sensitive information such as banking passwords, or launch spam attacks, damage hard drives, and install additional delayed-release viruses that cause damage at a later date.

NetworkWorld noted that just last year, the websites of Al Gore's "An Inconvenient Truth" movie, the Miami Dolphins, and the MySpace profile for Alicia Keyes were infected and used to attack visitors. And these are just a few of the documented instances of seemingly safe sites corrupted to inflict damage on unsuspecting Web surfers.

In fact, to prove a point, the hacking group Cult of the Dead Cow (CDC) released a new tool, called Goolag Scan, that turned Google into an automated vulnerability scanner, scouring Web sites for sensitive information such as passwords or server vulnerabilities. According to CDC, the stunt should serve as a wake-up call for system administrators to run the tool on their own sites before attackers get around to it.

Current Methods Fail to Protect Against Web-Based Viruses

While companies and service providers that create and host websites should install protections against attacks to their Web pages, Web surfers and employers cannot afford to rely on "shoulds". Unfortunately, you also cannot rely on desktop anti-virus products like Norton and McAfee because they are not designed to examine what's happening within the Web browser.

What's needed is an easy-to-use but flexible security solution that examines browser content for hidden malicious code and keeps up with the constantly shifting Web landscape. We at St. Bernard believe the best way to do content analysis is with a gateway like the iPrism Web Filter that is specifically designed for the task, and delivers superior performance and effectiveness.

St. Bernard Pioneers Hybrid Security Solutions

Leveraging 12 years of experience and expertise delivering hardware and managed service solutions for email, instant messaging (IM), and the Web, St. Bernard has introduced a new line of unique hybrid solutions. These solutions combine the security and control of high-performance iPrism appliances with the unlimited scalability and shared global intelligence of managed services.

Melding appliance and managed service technologies offers several advantages:

- The hybrid solution maximizes value and efficiency by implementing filtering components at the best locations within your organization's IT infrastructure.
- Web security components work together seamlessly regardless of location or mode.
- A single application centralizes security management, employing a reporting system and policy framework that spans both hardware and service modalities.

Four Ways iPrism Web Filter Combats Web-Based Viruses

The iPrism Web Filter's innovative real-time detection system virtually eliminates false-positives and streamlines performance in critical high-throughput environments. Together, four technologies create a multi-layered defense against Web-based malware:

- Signatures - This technique identifies unique characteristics of a piece of malware, and compares them to a vast database of scanned files. An accurate match indicates malware, while a partial match indicates a new malware variant. The iPrism Web Filter's antivirus signature database is the largest on record, containing over 457,000 and counting pieces of identified malicious code.
- Heuristics - Heuristics are rules that describe dangerous behavior performed by malicious software. These rules are built by scanning virus files for program instructions and noting which instructions represent damaging behavior. The iPrism Web Filter's advanced heuristics technology helps limit the size of antivirus definition files and keeps ahead of virus creators.
- Emulation - Emulation creates far richer heuristics scans than conventional antivirus technologies. iPrism Web Filter antivirus engines simulate the execution of a program to see how a Windows operating system responds. This approach allows the engines to trap malicious behavior safely removed from the host operating system.
- Detection Intelligence- iPrism Web Filter antivirus engines automatically learn from the behaviors and characteristics of identified malware code to identify and block new threats often missed by other engines.

> **"As our needs have evolved, so has iPrism. First we needed URL filtering to keep our kids away from inappropriate websites. Now iPrism helps us control IM and block Web-based viruses. Next, due to new e-discovery requirements, we'll look at iPrism for our message archiving needs. St. Bernard's hybrid approach means we won't have to keep buying boxes to add capabilities, which helps us control budgets."**
>
> **— Marc Ludwig,**
> **Systems Engineer**
> **Poway Unified School District**

You can Trust St Bernard

St. Bernard is the world's only Hybrid Security solutions provider. St. Bernard offers a full suite of Hybrid Security solutions that integrate on-premises appliances with on-demand services to protect corporate networks from online threats, enforce acceptable use policies, and archive messages.

St. Bernard's suite of solutions—iPrism Web Filter, iPrism IM Filter, iPrism Email Filter, and iPrism Message Archive—deliver secure content management with the control of an appliance and scalability of a hosted service. St. Bernard's iPrism solutions prevent Internet threats such as spam, viruses, spyware and phishing from entering corporate networks across all electronic communications, including email, IM and the Web.

Established in 1995 with headquarters in San Diego, California, St. Bernard sells and supports its products directly and through solution partners worldwide. For more information, please visit http://www.stbernard.com.