

Protecting Against Evolving Web Threats

Summary Report

Executive Summary

Throughout 2008, the increasing frequency and sophistication of Web-based threats has driven security software companies to harden their defenses. In our tests of leading consumer-oriented security suites, we found vast differences in how well different products protected against one of the major infection vectors today - the "drive-by" download. These attacks are enabled by commercially supported "crime-ware" and target vulnerabilities in browsers and associated third-party applications, for example, Flash, Real Player, Apple's QuickTime, and Windows Media Player. Notably, drive-by downloads require no user interaction to install and have become the hacker's infection vector of choice. The code that delivers these threats is obfuscated to make it effectively indecipherable, often attacking multiple points in the browser and popular third-party applications, and they are delivered through chains of redirects hidden in invisible Web page features. The end result is a cocktail that thwarts many protection approaches.

To determine a product's effectiveness against these drive-by downloads, Cascadia labs chose exploits from its corpus with an active payload that were in the wild during our testing. In addition, CORE IMPACT was used to generate exploits against additional vulnerabilities that are currently being targeted at a lower frequency by in-the-wild exploits. In our testing, Symantec's Norton Internet Security 2009 completely blocked 100 percent of the in-the-wild exploits, and exploits from commercial and open source security tools - nearly twice the effectiveness of the nearest competitor.

We set out to test the level of security that these consumer products provided

A Growing Problem

Recent studies shows that the number of exploitable Internet users is enormous, that the number of attacks is growing rapidly, and that even legitimate sites are increasingly being hacked and exposing visitors to malicious code.

More than 630 million people reportedly use a browser that's vulnerable to a drive-by-download, and that over half of all Internet Explorer users having a version that does not have all of the available patches installed.¹ And that's only the browser - increasingly, exploits are targeting third-party applications and browser plug-ins such as media players and ActiveX controls. The Symantec Internet Security Threat Report XIII, documents that 239 browser plug-in vulnerabilities were reported in the second half of 2007.² Google has reported that it has identified more than 3 million drive-bydownload URLs on over 180,000 Web sites. These malicious pages appeared in 1.3 percent of search results and that numbers are steadily growing.³ Data collected by ScanSafe from January to June 2008 shows a 278 percent increase in malware from hacked Web sites, along with a 212 percent increase in the attacks used to upload code to Web sites.⁴ In one extreme example, a single page was found to be serving exploits targeting 22 different vulnerabilities in 18 different applications.⁵

Hackers are also successfully targeting the sites of large and trusted organizations. In early June a section of the Web site for one of the world's largest main-stream retailers was compromised, and the chat page for a Western European government site was briefly found to be performing drive-by downloads.

Exploits are proliferating largely because economics encourage it. Today's hackers are often profit-driven and have access to sophisticated tools that make large-scale break-ins easy. For example, SQL injection attacks carried out against vulnerable Web sites can expose millions of users with unpatched browsers to dangers when they simply visit the hacked sites. With threats so commonplace and fast-evolving, it's more important than ever for client security software to reliably thwart exploit attempts.

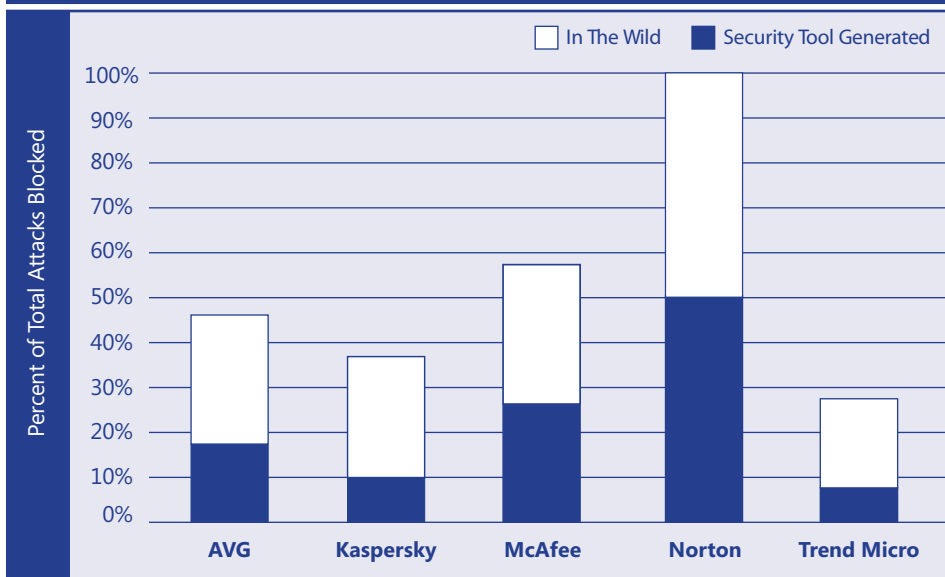
against the changing threat landscape using Web-pages compromised by crime-ware, such as MPack, Neosploit, and WebAttacker, and that exploit varying OS, browser, browser-plug-ins, and third party applications. We also used the security tool, CORE IMPACT, which allows us to generate Webpages hosting specific exploits for less-commonly targeted third party applications.

Mounting an Effective Defense

Product versions tested: September - October, 2008.

- AVG Internet Security 8.0
- Kaspersky Internet Security 2009
- McAfee Internet Security 2009
- Norton Internet Security 2009
- Trend Micro Internet Security 2009

Overall Effectiveness of Drive-by Download Protection



Refer to Appendix A for source data

In our tests, five leading security products showed wide variation in how effectively they provided comprehensive protection against exploits. The varied results reflect products' different technical mechanisms for providing protection. Traditionally, security products have taken one or both of two approaches: use blacklists of known-dangerous Web pages and sites, and check for signatures or patterns that can detect known-malicious downloads or Web pages with suspicious characteristics, such as obfuscated JavaScript code. Some products also include host intrusion prevention capabilities that can, for example, detect a buffer overflow in an application, which often provides an indication that an exploit is being attempted. These traditional techniques proved only minimally to moderately effective against 30 exploits drawn both from real-world malicious sites and testing tool generated attacks we selected.

Norton Internet Security 2009's Browser Protection and Intrusion Prevention technology led to markedly better effectiveness. Norton identifies and generically blocks malicious code targeting the underlying software vulnerabilities, which enabled it to

preempt 100 percent of attacks. By focusing on the vulnerability that the exploit is targeting, our testing shows Symantec is able to provide more effective protection against constantly changing attacks without relying on traditional pattern based AV updates. We expect this type of protection to be more effective in the long-term, because it focuses on providing protection for a static vulnerability rather than detecting the dynamically generated code attacking that vulnerability.

The next most effective product, from McAfee, prevented only 57 percent of the same set of exploits. McAfee's blocking is due primarily to a mixture of specific and generic exploit signatures, and generic buffer-overflow detection, the latter feature specifically preventing one in-the-wild and four CORE IMPACT based attacks. AVG's blocking, 46% of our threats, comes from its signature-based Web Shield component, which identifies specific exploits and those generated by common hacker kits, but often lacked signatures for the most recent attacks. Kaspersky's signatures blocked 37 percent of the exploits we tested with, though we found it often only blocked one portion of a multi-part attack and

like AVG lacked signatures for the most recent obfuscation techniques. Trend's local and remote databases blocked just 27 percent of all the exploits we tested with. Its local signature set was only able to block two CORE IMPACT tests using files to deliver the exploits to Flash and Real Player, while its in-the-wild threat blocking came exclusively by a remote URL blacklist that intercepts and blocks the browser's attempt to access harmful URLs. In our in-the-wild tests, the remote database prevented only 40% of drive-by downloads. Overall, our testing raises concerns about the level of protection provided by the competing approaches used by the competing products and the potential for users to be infected by prevalent Web based threats.

The 30 exploits we tested with included in-the-wild drive-by downloads (which were live for at least 24 hours) and attacks we tested and deployed using CORE IMPACT. We selected exploits that are representative of vulnerabilities exploited in the wild, such as browser version, third party application, plug-in or ActiveX control. Additional details on the current state of drive-by downloads, how we tested, and how the products fared, can be found in our full-length report at http://www.cascadialabs.com/reports/WebThreats09_Full.pdf

The Verdict

It is clear that new approaches are required to combat drive-by downloads. Our testing shows that Symantec has developed a solution with its Norton Internet Security 2009 product that is more effective against a wide variety of these attacks. ▲

Appendix A - Total Attacks Blocked by Type

Drive-by Downloads	AVG	Kaspersky	McAfee	Norton	Trend Micro	Total Attacks
In-the-Wild	60%	53%	60%	100%	40%	15
CORE IMPACT	33%	20%	53%	100%	13%	15
Overall	46%	37%	57%	100%	27%	30

References

1. S Frei, T Dubendorfer, G Ollmann, M May, Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the "insecurity iceberg", July 01, 2008, <http://www.techzoom.net/publications/insecurity-iceberg/index.en>
2. Symantec Global Internet Security Threat Report, Volume XIII, April 2008, pg 6. <http://www.symantec.com/business/theme.jsp?themeid=threatreport>
3. N Provos, P Mavrommatis, M A Rajab, F Monrose, Google Technical Report provos-2008a, All Your iFRAMEs Point to Us, February 4th, 2008. <http://research.google.com/archive/provos-2008a.pdf>
4. ScanSafe Global Threat Report, June 2008. http://www.scansafe.com/_data/assets/pdf_file/8277/gtr_June2008.pdf
5. Exploit kit with 22 exploits and updated obfuscation techniques, October 22, 2008. <http://realsecurity.wordpress.com/2008/10/22/a-exploit-kit-with-22-exploits-and-new-obfuscation-techniques/>



Independent evaluations of technology products

Contact: info@cascadialabs.com
www.cascadialabs.com



This comparative review, conducted independently by Cascadia Labs in September and October of 2008, was sponsored by Symantec Corporation. Cascadia Labs aims to provide objective, impartial analysis of each product based on hands-on testing in its security lab.