Protecting Against Evolving Web Threats

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 several particularly dangerous types of threats: "drive-by" downloads, fake antivirus scanners, and fake video decoders (codecs).

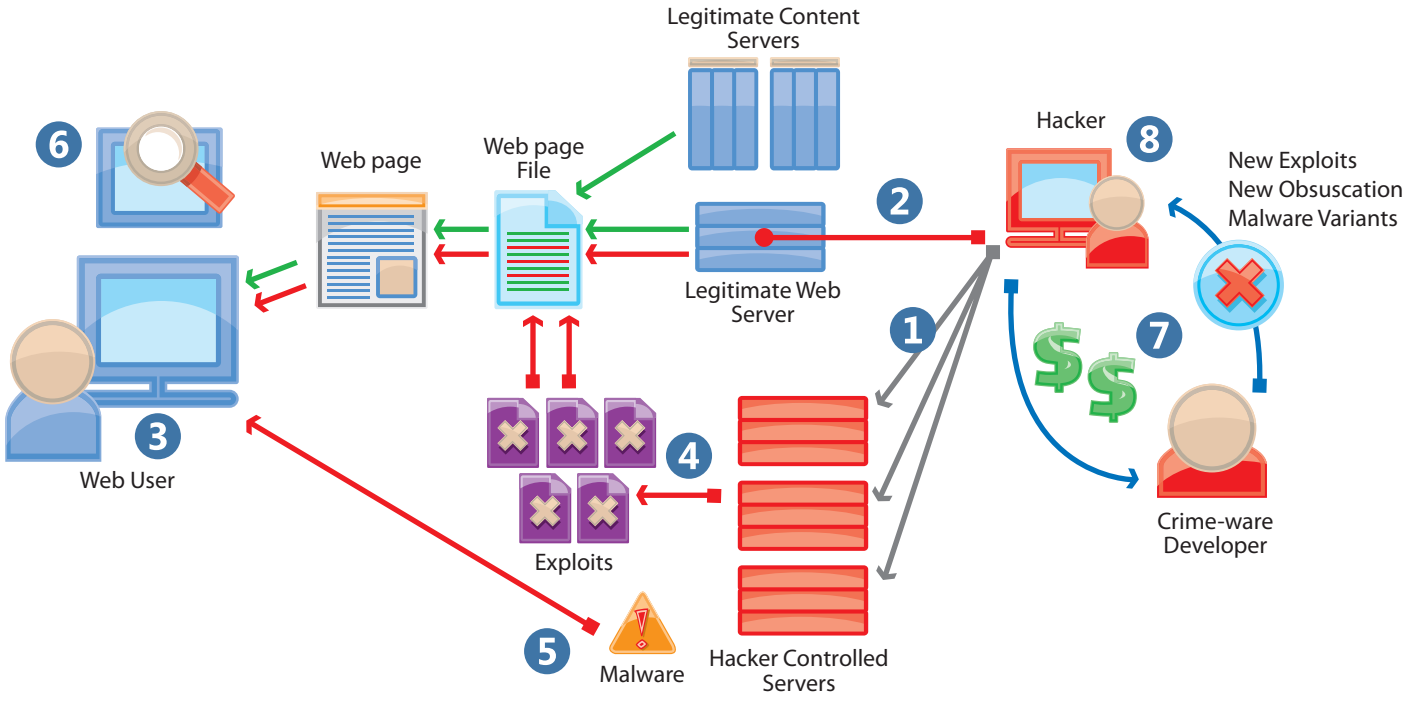
Drive-by downloads target vulnerabilities in the browser and associated helper applications – for example, Flash, Real Player, Apple's QuickTime, and Windows Media Player – to stealthily install malicious software. Notably, drive-by downloads require no user interaction to install and have become the 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.

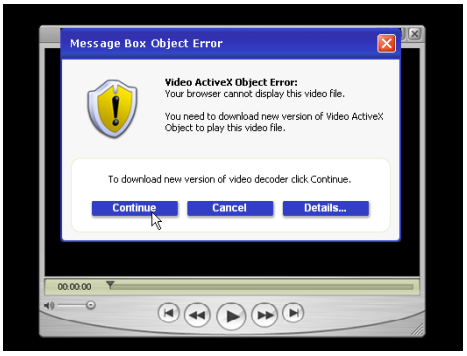
Fake antivirus scanners and fake video codecs*, on the other hand, use social engineering to deceive or scare users into voluntarily installing software

For a description of these threats, read "Growing Problems on the Web" on pg. 6.

Figure 1: Mechanics of a Drive-by Download

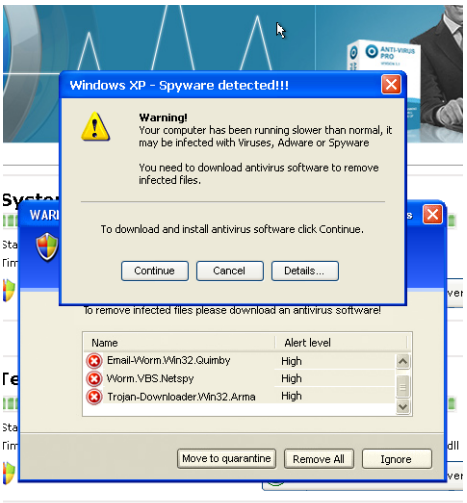
1. A crime-ware user uploads exploit codes to servers under his control.
2. Google or other search engines are used to identify potentially vulnerable servers, and automated attacks are launched.
3. A visitor arrives at the hacked site and their browser application constructs a Web page from a file containing the legitimate and malicious code.
4. The hacker code instructs the browser to download one or more exploit files from hacker controlled servers.
5. A successful exploit causes the user's computer to download and install malware without user intervention.
6. The malware can allow the hacker to steal private information, infect other computers, send spam, or engage any number of other illegitimate money-making activities.
7. The profits are used to purchase improved tools, new exploits, better obsuscation, and new malware to stay ahead of the latest signatures released by AV vendors.
8. The cycle continues - often re-infecting servers that removed the hacker code, but failed to fix the issue that allows the hacker to break-in.





Fake codec sites deceive users into installing malware for videos that may or may not exist.

without awareness of its maliciousness – often as part of a redirect from a compromised legitimate site, and occasionally alongside a drive-by download. These fake antivirus and fake video codecs are directly correlated to infection by well known virus threats, like Vundo and Zlob.[1] One recent campaign, Antivirus XP 2008, allowed one ambitious hacker to defraud users of an estimated 5 million dollars in a single year.[2]



Fake online anti-virus or anti-spyware scanners frighten users into installing malware.

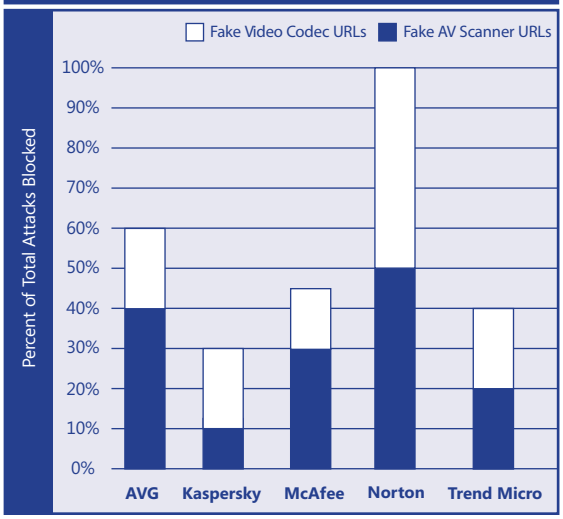
Cascadia Labs' testing focused on protection against prevalent and particularly dangerous real world Web threats that users are encountering, and how well the most recent consumer security products protect users from these threats. To determine a product's effectiveness against these drive-by downloads, Cascadia labs chose exploits from its corpus with an active payload that were in the wild just prior to and during our testing. In addition, CORE IMPACT was used to generate exploits against additional vulnerabilities that are currently being targeted by in-the-wild exploits. Likewise, fake application URLs were chosen from live samples currently in-the-wild.

Cascadia Labs tested the most recent products available from 5 companies:

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

In our testing, Symantec's Norton Internet Security 2009 blocked 100 percent of all the exploits tested. Norton's effectiveness was nearly twice that of the nearest competitor. It performed equally well against the fake AV scanner and fake video codec sites we tested, blocking every one of them. The nearest competitor only blocked 60 percent of the fake scanners and codecs and the remaining competitors blocked fewer than half.

Overall Effectiveness of Fake Application Blocking

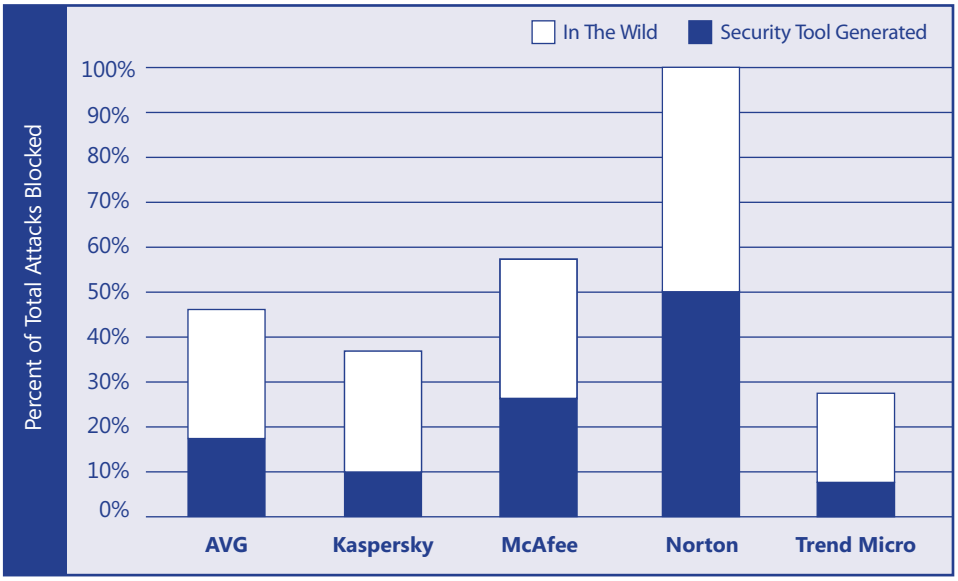


Refer to Appendix A for source data

Fighting Back – Products Use Various Techniques to Thwart Web-based Threats

Cascadia Labs tested consumer-oriented products from five vendors against a range of drive-by download URLs as well as against URLs that install fake codecs and fake security scanners. To conduct its testing, Cascadia Labs chose the "Internet Security Suite" products from each vendor; products that contain security that goes beyond mere virus detection. We found these products use a number of different techniques to combat Web-based threats such as exploit signatures, exploit heuristics, URL blacklists, intrusion

Overall Effectiveness of Drive-by Download Protection



Refer to Appendix A for source data

Cascadia Labs

prevention, browser vulnerability protection, and even traditional binary signatures as a last resort. Our testing showed that two techniques – browser vulnerability protection and intrusion protection – worked better than others.

Here is a quick description of these techniques:

- **Exploit Signatures** – The product detects specific malicious strings in the obfuscated HTML, JavaScript, or VBScript. The product analyzes the content before it is processed by the browser in a manner similar to the techniques used to detect malicious binaries with binary signatures.
- **Exploit Heuristics** – Similar to exploit signatures, but the product uses a more generic pattern that can identify key components of related types of attacks without having to match the exact signature of an attack instance.
- **URL Blacklists** – The product uses a known list of malicious URLs to block access. For most attacks, the malicious content is not stored on the compromised server. It must be downloaded from a separate server hosted on a site that the hacker owns. Once these sites are discovered, they can be blacklisted, so the browser is prevented from downloading any content from these servers.
- **Intrusion Prevention** – The product analyzes the activities of a piece of code on the network or as it is executing, and prevents it from completing malicious activities. Intrusion prevention can, for example, detect a buffer overflow in an application and prevent it, block a pop-up triggered by a fake application, or detect specific drive-by download attempts. Each product defines this capability somewhat differently.
- **Browser Vulnerability Protection** – The product monitors browser behavior for activity that would attack a known vulnerability in the browser, its plug-ins, or third-party applications. Instead of trying to stop the huge number of ever-changing exploits directly, the product instead blocks these exploits a level down by thwarting any attempt to target a known vulnerability resulting in effective protection regardless of how recent or complex an attack's obfuscation may be.
- **Binary Signatures** – As a last resort, the product can block the malicious binaries that the exploit attempts to download and execute. This approach has two flaws: the exploit has already occurred and compromised the machine by this time, and given the pace of new malware variants, it's akin to playing Russian Roulette – something will eventually get through.

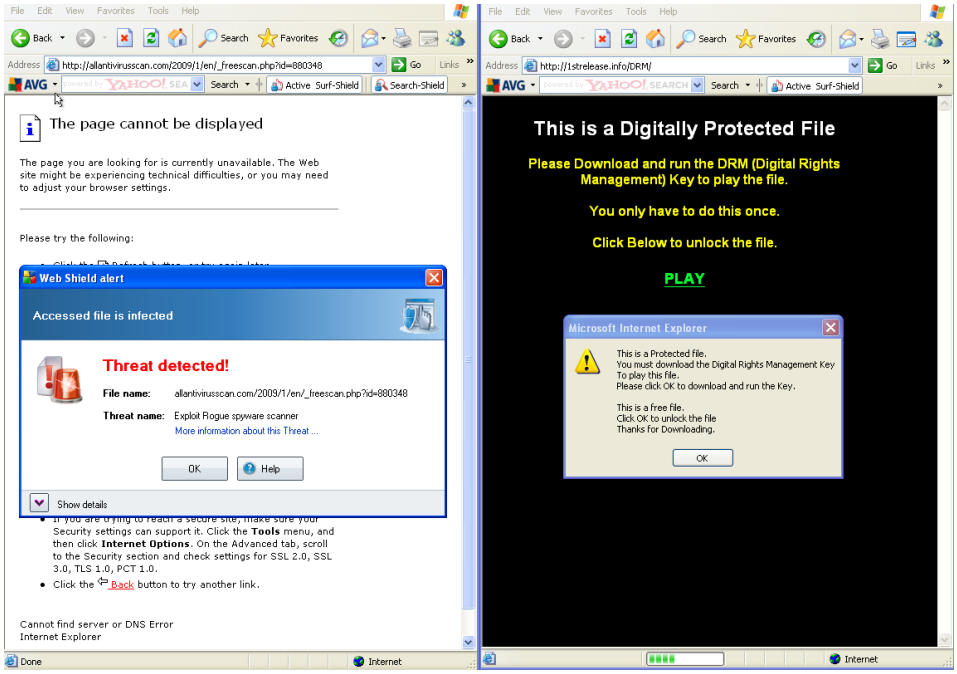
Interpreting Our Test Results

Cascadia Labs tested the products' abilities to successfully prevent the exploitation of the browser and vulnerable applications. We defined "success" for each test as completely preventing any type of compromise to the endpoint computer. We marked as failures any cases where we observed downloaded malware or crashed applications.

We chose this criterion because it reflects a conservative, safety-conscious approach. Blocking software before it can even exploit a vulnerability is preferable to permitting an exploit to occur and blocking only a subsequent download. This, in turn, is preferable to allowing a download but declaring it malicious later when it gets run. Particularly given how quickly today's malware evolves, and the challenge to antivirus vendors of keeping signatures current, we believe that eliminating the risk as far upstream as possible offers the best protection for users.

AVG Internet Security 8.0

AVG Internet Security 8.0 prevented 46 percent of the exploits and 60 percent of the fake application sites we tested it against, primarily thanks to the exploit signatures in Web Shield, its web page scanning engine. It also blocked a smaller number of exploits using heuristics aimed at detecting exploits created using specific toolkits. This component was able to detect the



AVG's Web Shield component blocked the majority of fake anti-virus sites, such as the one on the left with a generic Web Shield signature.

Cascadia Labs

majority of fake antivirus sites using a generic "Rogue spyware scanner" signature, while fake codec sites were undetected. AVG did block the malicious software from the fake codec sites with specific signatures in its Web Shield and file scanner, Resident Shield, components.

AVG's protection was average for the products we tested. Still, we found that Web Shield lacked the ability to defend against a large number of exploits targeting third-party application vulnerabilities – a serious shortcoming in light of the large percentages of Internet users with these applications installed. It also had trouble with attacks that used newer obfuscation techniques or that used multiple obfuscation techniques. For example, AVG's signatures successfully detected a variety of obscured threats targeting Internet Explorer and Real Player vulnerabilities, but failed to block attacks from CORE IMPACT that targeted four different media players and a few other applications. The in-the-wild exploits that succeeded were common exploits using the most recent obfuscation mechanisms. AVG was able to prevent one of two exploits served from a single page in two different tests -- but in each case one exploit that employed a slightly different obfuscation method was able to compromise the machine.

AVG demonstrated poor results in blocking fake codec sites. In this it was comparable to the other products, but well behind Norton. None of the 10 sites tested were blocked, and only four of the malicious executables were detected during download by binary signatures in the Web Shield or Resident Shield components. The remaining six Trojans successfully installed without detection. It is interesting to note that six of the 10 sites tested employed a variant of a single Trojan. AVG, like Kaspersky, McAfee and Trend, only detected one of these variants with a binary signature. This result illustrates the difficulty vendors face in developing binary signatures to keep pace with the rapid evolution of malware on the web.

Fake antivirus scanners posed less of a challenge for AVG, which managed to block six of 10 sites using either a heuristic signature of URL blacklist in its Web Shield component. Among the URLs that AVG did not block, it ultimately detected two of the fake programs with binary signatures, but allowed the remaining two to be installed without complaint.

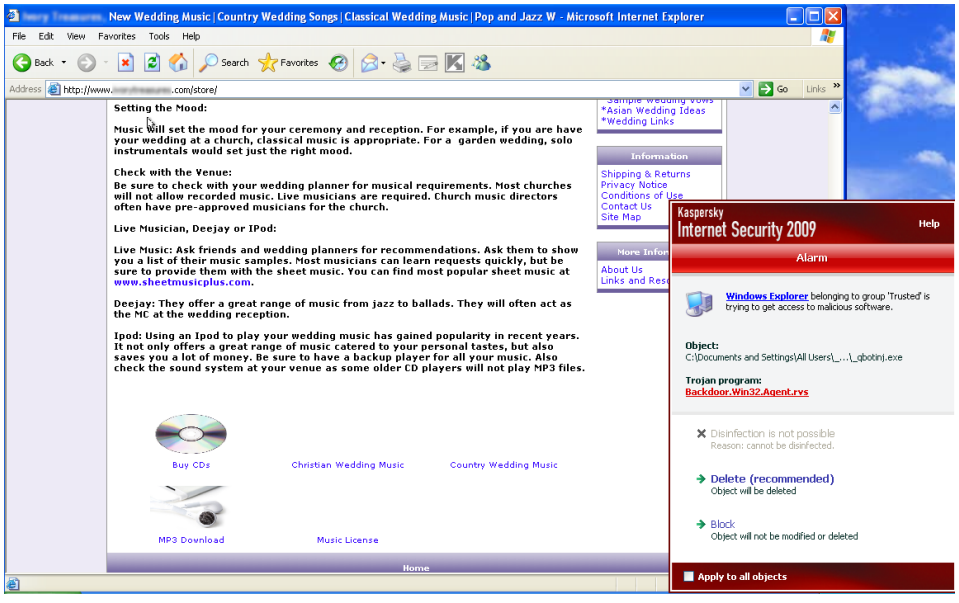
Kaspersky Internet Security 2009

Kaspersky Internet Security 2009 was one of the least effective products we tested at blocking both drive-by downloads and fake applications. In blocking 11 of the 30 exploits, we found Kaspersky relied heavily on signatures, which can miss newly obfuscated code, and that it often only blocked one portion of a multi-part attack. Kaspersky also blocked the fewest fake application sites we tested it against.

The three CORE IMPACT exploits Kaspersky detected involved the download of a malicious file by a third party application -- JetAudio, Flash, and Real Player, indicating Kaspersky relies on specific signatures for exploits contained in files processed by these applications or by the Web browser. However, the 12 exploits that evaded Kaspersky highlight the challenge in trying to keep up with a wide variety of threats using exploit signatures. Kaspersky blocked one in-the-wild exploit site containing an Apple QuickTime exploit using its firewall's intrusion prevention component. The remaining detections were made with signatures.

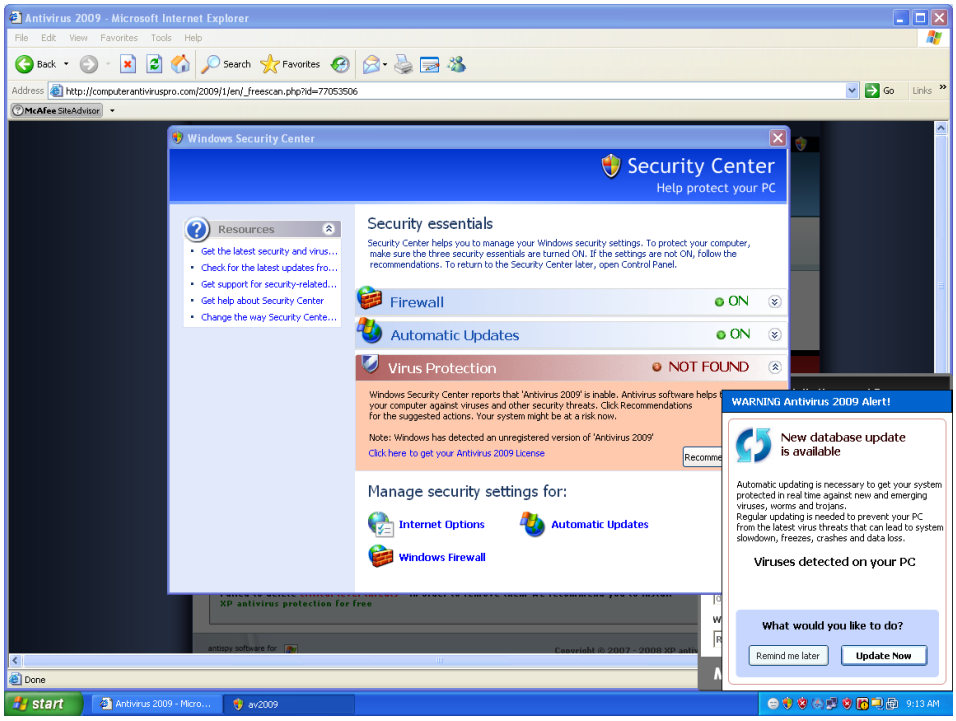
The 2009 version of Kaspersky Internet Security does include a Security Analyzer that will scan the computer for unpatched third-party applications. In our testing it only detected five of the 15 vulnerable applications we used in our testing, and it went awry and identified one vulnerable application 393 times. Once a vulnerable application is identified, it is still the user's responsibility to follow the provided link and install the patch.

Kaspersky's protection against fake application sites proved to be limited. It failed to block any of the sites, and blocked four fake codec downloads and two fake scanner downloads with its signatures. Going a step further and attempting to install the malware from the remaining 14 sites, we triggered three detections. The total blocking rate of 30 percent illustrates a clear deficiency in the protection Kaspersky currently provides against the threats we tested.



Kaspersky allowed this multi-part threat that we have seen circulating on the Web for at least 10 days to be automatically downloaded.

Kaspersky Internet Security also makes heavy use of pop-up prompts that require a user to allow or block potentially suspicious or risky activities when an application is first installed, such as accessing some system registry areas and sensitive user data. We had mixed results in following the recommended action in the prompts. When at its best, the product recommends actions that limit the damage caused by malware installed as a result of a drive-by download and alerts the user that a new process is running. This same feature, however, also resulted in blocking installation of patches for several vulnerable applications detected by the Security Analyzer. Whereas technical users may appreciate the insight and control provided by Kaspersky's prompts, the majority of users likely won't benefit because they lack the expertise to understand the very technical events presented and most users expect the software to be the expert on how to protect their system. Based on the blocked patching attempt we witnessed, following the recommended actions may actually lead to a state that is still vulnerable to exploitation.



Fake Antivirus programs, such as this one that McAfee did not detect, go to great lengths to appear legitimate on the Web and after installation.

McAfee Internet Security 2009

McAfee Internet Security 2009 blocked 57 percent of the exploit attacks we attempted with its combination of exploit signatures, intrusion prevention, and SiteAdvisor site blacklisting. While the SiteAdvisor component did rate two of the fake application sites "red," or dangerous, it and McAfee's other techniques were unable to actually block the sites. Attempting to download the malicious software on the page does result in a block. McAfee does offer an upgrade to SiteAdvisor Plus which allows blocking of red sites.

McAfee's protection against drive-by downloads consists primarily of heuristics using host based intrusion prevention (HIPS) that recognize a generic buffer overflow or a buffer overflow targeting a specific vulnerability. It missed just under half of these attacks – particularly with media player vulnerabilities, where six of eight attacks succeeded, and unlike Norton's protection, McAfee forcibly closes the browser in response to a buffer overflow detection, resulting in a degraded user experience.

McAfee's successful protection against nine in-the-wild attacks came predominantly from its signatures, while HIPS detection of Buffer Overflows was responsible for blocking only two attacks. For example, McAfee's signatures include detections of invisible links to malicious pages, malicious JavaScript and VBScript, and obfuscated exploit code for specific Internet Explorer vulnerabilities. Four of the six remaining attacks were mitigated by signature detection of the silently downloaded or installed Trojans, but two attacks completed without any detection.

McAfee's SiteAdvisor component demonstrated poor results in recognizing dangerous sites hosting fake applications. SiteAdvisor rated two sites – one codec and one scanner -- as dangerous. For the remaining 18, it marked one suspicious (yellow), 16 unknown (gray), and one safe (green). Downloading and manually installing the 20 fake applications resulted in nine detections during download and two detections on installation using binary signatures, meaning users remain seriously vulnerable to infection.

Norton Internet Security 2009

Norton Internet Security 2009's browser protection and intrusion prevention technology was markedly more effective than its competitors. Norton's browser protection identifies and blocks malicious code targeting underlying software vulnerabilities, which enabled it to pre-empt 100 percent of the drive-by download attacks in our tests. The ability of Norton Internet Security's intrusion prevention component to generically detect fake application page behavior led it to successfully block every one of the fake scanners and codecs we tested it against.

Norton's approach of focusing on the vulnerability that an exploit targets, rather

than relying on specific signatures that can quickly get out of date, proved highly effective in our testing. Its protection was effective against the recently developed heavily obfuscated threats that evaded the competing products, These tests include the 15 different third-party vulnerabilities listed in Table 1, and seven vulnerabilities in Internet Explorer. All of these vulnerabilities are exploited in the wild, and we are impressed that Norton provides such a breadth of protection We would expect this type of protection to maintain its effectiveness in the long term because it protects against a static vulnerability rather than trying to detect the much larger and rapidly evolving variety of code that could attack that vulnerability. Of course, this approach would be susceptible to new vulnerabilities until they were identified and addressed.

Norton's approach to drive-by downloads seems right on the mark given that hackers are continually experimenting with new obfuscation approaches and ways to attack a specific vulnerability in the browser or a susceptible third-party application. In our experience, most in-the-wild exploits use dynamic obfuscation techniques and a combination of different exploits attacking multiple points in the browser and popular third-party applications. Users may be getting better at patching Windows and the browser, but vulnerabilities in other applications often remain open. Norton's design proved excellent at addressing this real-life problem.

Norton Internet Security's intrusion prevention and Browser Protection technology detected and blocked specific fake application patterns – such as redirecting the browser and presenting several pop-ups – which

Growing Problems on the Web

Drive-by downloads are quickly evolving into the mechanism of choice for infecting PCs. They occur when a hacker uses code, known as an exploit, to take advantage of a software bug -- a "vulnerability" -- to silently install malicious software on a victim's computer. When Web users surf with a vulnerable browser or browser-integrated application, they run the risk of encountering an infected or malicious Web page that automatically downloads and installs malicious software, with no indication that they have just been infected.

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

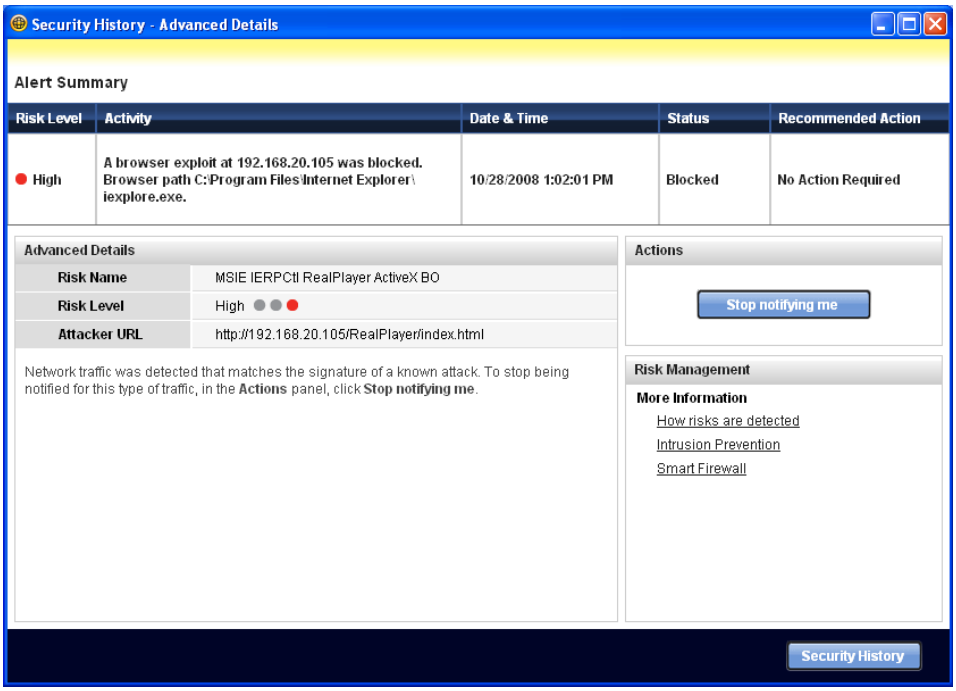
More than 630 million people reportedly use a browser that's vulnerable to a drive-by-download, and more than half of all Internet Explorer users browse with a version that is not fully patched.[4] And that's only the browser -- increasingly, exploits are targeting third-party applications such as media 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.[5] A separate study of 63,000 users reports that the in some cases more than 90 percent of the participants were using unpatched versions of browser-integrated software.[6]

Google has reported that it has identified more than 3 million drive-by-download URLs on more than 180,000 Web sites. These malicious pages appeared in 1.3 percent of search results and that number is steadily growing.[7] 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.[8] In one extreme example, a single page was found to be serving exploits targeting 22 different vulnerabilities in 18 different applications.[9]

Hackers are improving their scope and success by successfully targeting and hacking the sites of large and trusted organizations to expose trusting users to their attacks. 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

Increasingly, hackers today are deceiving users into voluntarily installing their malicious applications by offering downloads they claim to be antivirus software or video decoders (codecs). Often, though, the true purpose of these applications is to hijack the user's computer to send spam, infect other computers, steal personal information, or engage in other illegitimate activities. Our testing and other independent research show that hackers sometimes compromise legitimate sites to redirect users to these fake applications.[10]

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, a hacker can use a SQL injection attack carried out against vulnerable Web sites to inject an exploit that can expose millions of users with unpatched software 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.



Norton's console provides additional details on the type of threat blocked, and in most cases what vulnerability was targeted, such as with this common Real Player exploit that all other products missed.

ultimately proved more effective than competitors' simpler blacklisting and signature based approaches. Hackers typically launch these fake application campaigns from a large number of domains and with large numbers of variants[3], which gives Norton's intrusion prevention approach an advantage over other solutions. Congratulations to Symantec for executing on a totally new approach in the battle against misleading applications.

Trend Micro Internet Security 2009

Trend Micro Internet Security 2009, with its URL blacklists, much of which is implemented in-the-cloud, blocked just eight of 30 exploits, the second worst in our testing. The Trend Micro solution performed somewhat better against the fake application sites, blocking 40 percent of them, but on the whole its protection proved to be limited. Overall, our testing raises concerns about the level of protection provided by Trend's approach and the potential for user's to be infected by prevalent Web based threats.

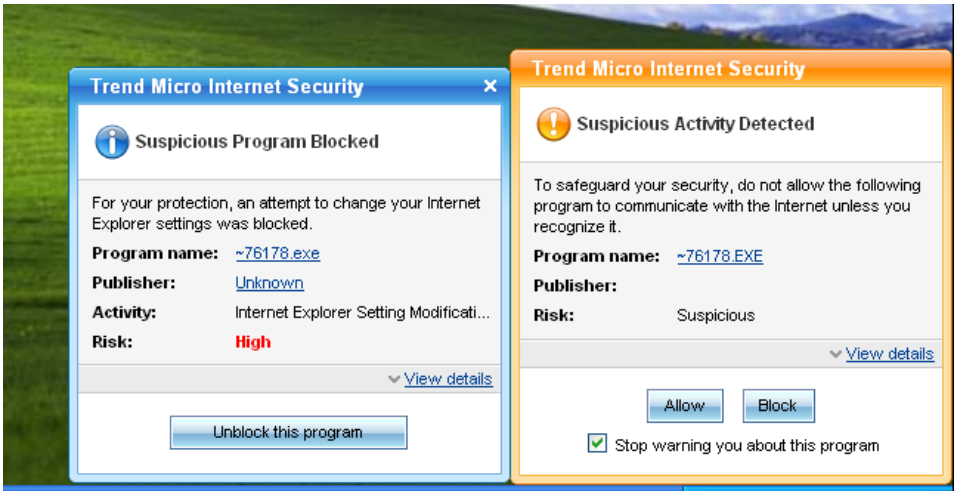
Trend's binary signatures blocked two exploits contained in files aimed at Windows Media Player and Flash, and its remote database blocked just six in-the-wild exploit URLs. We took special care during our testing to make sure the service that submits traffic to Trend Micro's remote database was performing properly and receiving appropriate responses; nevertheless, it was unable to protect against most of the drive-by downloads we tested.

Targeted Third-Party Applications

Winamp 5.12
Windows Media Player 9
(2 Vulnerabilities)
JetAudio
WinZip 10
Flash 9.0.115
Microsoft Speech API 4
Yahoo Messenger 8.1.0.249
Real Player 10.0.5
(2 Vulnerabilities)
Java Runtime 5.0u4
VLC media player
Zenturi Program Manager 1.5.0.531
Winamp 5.22

Trend's remote database successfully identified four of the 10 sites in both the fake scanner site and fake codec site testing. When we continued installing the malware that wasn't blocked, Trend identified two fake scanner applications as suspicious but failed to block them. It also flagged three fake codec performing suspicious modifications of Internet Explorer's settings but failed to prevent full installation.

Trend includes a Windows vulnerability scanning tool that assists users in maintaining an up-to-date operating system and Internet Explorer browser, but this tool does not identify vulnerable



This silently installed program from a compromised legitimate Website was downloaded, installed, and is running without detection by Trend's remote and local databases - even after a full system scan. Trend, however, is blocking it's access to other programs and the internet.

third-party applications. In our testing, each in-the-wild exploit contained a mixture of Internet Explorer and third-party application exploits, so even a fully patched version of Internet Explorer remain vulnerable to drive-by downloads if unpatched applications are also installed. Ultimately, users should be cautious on relying on Trend for real time protection from today's threats.

Drive-by Downloads - New Tricks With Old Tools

Drive-by downloads are hardly new. What is new is their scale, sophistication, and persistence -- and the use of "commercially" supported crimeware for automating and managing attacks. What used to be a nuisance concentrated in riskier parts of the Web is becoming a widespread epidemic that threatens even major sites and cautious users. A graphical presentation of how a drive-by download occurs can be found in Figure 1.

Here's how it happens. When your browser displays a single Web page, it's actually loading multiple pieces of content -- text, graphics, advertisements, interactive components -- each of which can originate literally anywhere on the Web. Hackers use that seamlessness to their advantage. By hacking a server, they can substitute one of their own files for a legitimate component. Or they can add a new, but invisible, component to an otherwise unremarkable page.

Once a hacker controls what a browser retrieves, he can configure a server to respond with data that takes advantage of a vulnerability in the browser or a third-party application. The browser retrieves that little bit of malicious code -- the exploit -- which effectively "escapes from" the browser and then can perform most any task on the computer. Typically, what it does next is silently download and install software that will begin running immediately or the next time the computer starts up. Exploits aren't always easy to detect. Among other problems, the code that delivers them may be obfuscated to make it effectively indecipherable and these obfuscation methods are regularly updated to stay a step ahead of a vendor's signatures. Obfuscation itself doesn't necessarily indicate maliciousness since Web developers sometimes use it to deter others from examining their legitimate code, and even if a product blocks one type of threat, another threat in the same mix might find its way through.

How do sites get hacked in the first place? They may have Web servers with inadequate security, unpatched vulnerabilities, or poorly written code that makes them easy targets for techniques like SQL injection attacks. And hacking is no longer a one-off operation. Hackers are scaling up and optimizing their attacks by operating in loosely affiliated gangs and automating the process using software that's commercially supported on the black market. Tools with names like MPack, Icepack, Neosploit, WebAttacker, and Nuclear can contain graphical user interfaces and be designed for use by non-experts, so common criminals can make an occupation out of Web-based crime. It's estimated that there may be as many as 68,000 of these kits in circulation,[11] and the most sophisticated kits automate all processes of the infection cycle – from server break-in to code injection and obfuscation. Some tools even offer a 12-month paid subscription, which provides new exploits to stay a step ahead of security vendors, releasing new versions that work around security vendors' signature updates.

Malware authors make it difficult to shut down their activity by using the distributed nature of the Internet to their advantage. They may launch their campaigns using several or dozens of servers, often hosted in places like China or Russia where they are difficult to pursue. And they often serve exploits from multiple servers simultaneously, so that even if some are shut down or cleaned up, others will survive. The result is an escalating arms race, where security vendors must move quickly to keep pace with a criminal economy that continues to evolve in pursuit of profits.

How We Tested - Sample Exploits & Attacks

The 30 exploits we tested with included in-the-wild drive-by downloads (which were live for at least 24 hours) and attacks we deployed using CORE IMPACT. We selected representative exploits that target different browser versions, third-party application, plug-in, or ActiveX controls. Table 1 lists the specific applications exploited using CORE IMPACT. In-the-wild exploits targeting Apple QuickTime, Adobe Reader, and Real Player [11] were also tested. The in-the-wild exploits were drawn from real-world Web pages compromised by crimeware, such as MPack, Neosploit, and WebAttacker. CORE IMPACT was used to provide Web pages hosting specific exploits documented in-the-wild for less-commonly targeted third-party applications. The fake application sites were all drawn from in-the-wild threats and were selected from a pool of more than 1,000 URLs to obtain samples distinct in their domain, appearance, behavior, and in the type of malicious software they delivered.

Cascadia Labs performed all testing using Microsoft Windows XP Service Pack 2 with no patches, the appropriate third party applications installed, and the most recent signature updates for each product that corresponds to when an in-the-wild threat was identified for testing. Each product was tested using the default settings recommended during installation. Successful exploitation of a vulnerable application by an in-the-wild threat or a CORE IMPACT-hosted Web page was confirmed on an unprotected PC prior to testing any product. Cascadia Labs maintains proprietary tools that allow the capture and 100 percent repeatable replays of

in-the-wild drive-by downloads and fake applications in order to ensure that all products are tested against an identical threat.

The Verdict

It is clear that new approaches are required to combat drive-by downloads and fake applications that use social engineering to infect users. Our testing shows that Symantec has developed a solution within its Norton Internet Security 2009 product that is more effective against a wide variety of both 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**
Fake Applications						
Fake Codecs	40%	40%	30%	100%	40%	10
Fake Antivirus	80%	20%	60%	100%	40%	10
Overall	**60%**	**30%**	**45%**	**100%**	**40%**	**20**

References

1. Symantec Corp, "Misleading Applications – What you need to know", http://www.symantec.com/norton/theme.jsp?themeid=mislead
2. J Markoff, "Antiviral 'Scareware' Just One More Intruder", October 19, 2008, http://www.nytimes.com/2008/10/30/technology/internet/30virus.html?ref=technology
3. D Danchev, "Localized Fake Security Software", Danch Danchev's Blog – Mind Streams of Information Security Knowledge, April 14, 2008. http://ddanchev.blogspot.com/2008/04/localized-fake-security-software.html
4. 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
5. Symantec Global Internet Security Threat Report, Volume XIII, April 2008, pg 6. http://www.symantec.com/business/theme.jsp?themeid=threatreport
6. S Dunn, "Unpatched software abounds on user systems", Windows Secrets, September 6, 2007. http://windowssecrets.com/2007/09/06/01-Unpatched-software-abounds-on-user-systems.
7. 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.
8. ScanSafe Global Threat Report, June 2008. http://www.scansafe.com/__data/assets/pdf_file/8277/gtr_June2008.pdf
9. Real Security, "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/.
10. C Boyd, "BandJammer - Hacking A Myspace Music Profile Near You" blog.Spywareguide, http://blog.spywareguide.com/2007/10/bandjammer_hacking_a_myspace_m.html.
11. Cyber crime tool kits go on sale. September 4, 2007. http://news.bbc.co.uk/2/hi/technology/6976308.stm.

Cascadia Labs

Independent evaluations of technology products

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

symantec™

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.