



Online Enemy #1: Blackhole Exploit Kit

The New Cyber Bully

The Blackhole malware exploit kit has become the Internet's most prevalent threat, striking that stomach-churning "Oh no! What did I click on?" fear into the hearts of users. Moreover, it continues to frustrate IT departments with its knack for exploiting the latest software vulnerabilities to infect otherwise well-defended systems and networks.

Blackhole has gained serious momentum and is now among the top malware-dissemination tactics employed by cybercriminals. News and analysis website Dark Reading rated Blackhole No. 2 in its list of the top 10 malware advances of 2012, second only to the Flame virus.

Blackhole stands out as a particularly effective example of an increasingly sophisticated exploit first unleashed in 2010. It is designed to elude antivirus (AV) tools, so simply running AV – the primary and perhaps only security tool used by small and medium-sized businesses (SMBs) – is not enough to stop these threats.

Developed by skilled hackers and licensed to cybercriminals around the world, Blackhole attacks endpoints like PCs, laptops and workstations by taking advantage of vulnerabilities in popular software programs developed by industry leaders like Microsoft, Google, Adobe, Oracle and Mozilla. Through such tried-and-true methods as spam, phishing, link-baiting on social media and SEO poisoning, cybercriminals trick users into compromising their own machines by clicking on infected URLs or downloading and running malicious files.

Part of the evil genius of Blackhole attacks is that when unwitting users install infected files, they have no inkling that anything bad is happening on their machine. Such incidents are called "drive-by" malware attacks, which according to estimates now account for about half of all malware infections.¹

Compromising unpatched systems with crippling, invasive malware is now among the top threats facing businesses around the globe.

Developed by skilled hackers and licensed to cybercriminals around the world, Blackhole attacks endpoints like PCs, laptops and workstations by taking advantage of vulnerabilities in popular software programs developed by industry leaders like Microsoft, Google, Adobe, Oracle and Mozilla.

Antivirus alone is no longer enough. Adequate malware defenses now require integrated patch management.

Click at Your Own Risk

Blackhole presents a complex, persistent challenge to IT security professionals.

In a kind of “hacker whack-a-mole” game, malware developers move from one set of software vulnerabilities to another as vendors plug up security holes. For years, hackers had a field day with Windows operating systems, but as Microsoft became more adept at addressing those vulnerabilities, cybercriminals looked elsewhere.

Hackers set their sights on other types of widely used software applications, such as Adobe Reader, Adobe Flash Player, Internet Explorer, Firefox and particularly Java code. And in using popular web-based services like iTunes, Skype, Facebook and Twitter as the cheese that lures users to the mousetrap, cybercriminals know exactly what buttons to push to entice users into harming their own machines.

Hackers have set their sights on widely used software applications, such as Adobe Reader, Adobe Flash Player, Internet Explorer, Firefox and particularly Java code.

For example, successful Blackhole exploit attacks came in the form of spam with fake offers of free Microsoft Windows 8 licenses² and bogus Apple iTunes invoices³ with inflated balances. Spam recipients inevitably click on links that steered them to websites hosting infected files. Clicking on disguised links triggers downloads of files with a JavaScript that scans for unpatched software and other vulnerabilities before deploying the malicious code that infects each machine.

In the Windows 8 license case, according to Help Net Security⁴, “Users who clicked the malicious link and downloaded the accompanying file were hit with a Blackhole exploit and infected with a Cridex Trojan.” The bogus iTunes invoice carried links labeled “not your order,” “cancel order” and “view/download” – all of which led to prompts that delivered viruses.

In yet another case, Facebook users received fake messages in their inboxes that they had somehow “blocked” their accounts.⁵ To unblock, users were told: “You can reactivate your account whenever you wish by logging into Facebook with your former login email address and password.” The links in the email led to compromised URLs ready to unleash Blackhole infections.

Facebook was used in yet another attack, which involved a fake email notification⁶ that someone had posted an insult on a user’s Facebook account. Clicking on links purported to lead to the comment thread instead led to a website hosting Blackhole-delivered malware.

Dark Side of SaaS

The Blackhole exploit kit is part of a recent phenomenon in malware dissemination, a sort of dark side of Software as a Service (SaaS) known as “crimeware.” Malware authors design and build the crimeware kits, and then – taking a cue from the legitimate services models – make them available through website downloads to other hackers for customization. It’s a sophisticated, efficient economy that any old-fashioned mobster would admire.

Anyone with a browser can take advantage of this “crime as a service model” to download the Blackhole kit. The sites are hosted by “hardened” servers in hidden locations. The servers are set up with sophisticated security to elude law enforcement through various means such as frequent IP address changes and traffic redirects.

Taking a page from antivirus vendors, which have used subscription-based software for more than a decade, kit developers also offer subscription licensing complete with support for updates of new exploits and malware variants. In doing so, they maximize the effectiveness of attacks. Recent versions of Blackhole cost hundreds, even thousands of dollars to purchase and maintain, but older versions of the exploit kit are available for free.⁷

Kits make it possible to customize and distribute malware, as well as manage networks of infected machines. Some kits create payloads, such as the Zeus virus, while others control web traffic, and still others focus on exploits designed specifically to identify and exploit software vulnerabilities.

The latter category includes Blackhole, several versions of which have been released since 2010. Believed to be the creation of notorious Russian hackers, Blackhole-based threats have become so pervasive that even if the kit's authors were caught and stopped, the threat would continue to exist and grow. Once unleashed, Blackhole-based threats have kept spreading and evolving to evade capture.

Christopher Boyd, Senior Threat Researcher for ThreatTrack Security, says Blackhole is extremely risky because it changes its function frequently, depending on the type of cyber-threat it creates. The kit makes it very easy to effectively carry out an attack, often capitalizing on prominent brands such as Facebook and Skype to do its work, he says.

Blackhole presents a complex, persistent challenge to IT security professionals.

Making matters worse, Blackhole is spawning new malware variants, as hackers continue to improve on their craft. A newer strain of Blackhole dubbed "Cool" has started making the rounds, allowing hackers to remotely exploit vulnerabilities for drive-by attacks. The tool also scans browsers and operating systems to detect vulnerable plug-ins.

How to Fight Back

As clever and innovative as malware developers are, they are not invincible. But it takes the right tools to fight them.

As vulnerabilities come to light, developers of targeted applications typically are quick to react by sending the necessary patches to users. The problem is users often ignore them because their IT departments have told them to do so. IT and security professionals have long instructed users repeatedly not to click on links even from known sources (to combat phishing and other socially engineered tactics), or have even restricted users from installing updates themselves by limiting administrative rights on endpoint machines. These are good practices, but they create a conundrum: While users are protected from clicking disguised links, they may also be ignoring legitimate update prompts that

would protect them against the problems caused by the treacherous links.

Fortunately, IT departments can effectively address the issue. The answer lies in implementing automated, centralized software patching so that users don't have to be interrupted in their work – or have the option to ignore the prompts – to run a patch or update. In leveraging automation, IT departments stand to effectively boost their defenses against Blackhole and similar exploit attacks.

To be sure, AV prevents the majority of malware infections, but it is only one component of a truly comprehensive security strategy. Just as a homeowner cannot stop home invaders by locking the doors and leaving the windows open, an IT network needs more than one security tool to shore up its defenses.

Automated patch management systems are the surest way to meet the daunting challenge of deploying and applying dozens, possibly hundreds, of patches each year. Patch management systems can be set to conduct regularly scheduled software and network audits to identify potential problems and assess vulnerabilities. This gives IT departments the insights they need to keep networks secure and regulation-compliant. Patch management is a quick, efficient way to address software patches and updates, and as such it is essential to fighting off threats such as the Blackhole exploit kit.

Consequently, businesses and organizations need to demand more from their security solutions, particularly their AV. VIPRE Business Premium offers users integrated patch management that automatically patches vulnerable machines while detecting, preventing and remediating malware. With VIPRE, there is no need to deploy a second solution. Patching is managed easily from a single, comprehensive console ideal for SMBs and larger organizations like educational institutions, healthcare providers and government agencies.

The benefits of this approach are significant: For one thing, an organization no longer must rely on individual users for patches and updates. Second, combining patch management with AV provides a layered approach to network security that enables IT departments to more proactively address the top threat their users now face online.

Conclusion

Each day seems to bring news of another Blackhole-related attack. Such attacks are bound to continue now that crimeware has made it easier than ever for hackers to customize cyber-attacks. Any organization looking to avoid becoming the next victim needs to assess its security infrastructure and – if it hasn't already done so – move fast to implement automated patch management alongside its AV solution. It is the only approach that is sure to keep such attacks at bay.

About VIPRE Business Premium

VIPRE Business Premium is the small-footprint antivirus with integrated patch management, a groundbreaking feature that automatically patches unpatched machines. VIPRE Business Premium also includes Mobile Device Management, Mac support, a firewall, bad website blocking and anti-phishing.

Protect against the number one cause of PC infections now. Download your free 30-day trial of VIPRE Business Premium at www.ThreatTrackSecurity.com/VIPRE.

¹Spam Fighter News, Drive-by Downloads Observed in Over 50% of Malware Assaults, February 2012
<http://www.spamfighter.com/News-17370-Drive-by-Downloads-Observed-in-Over-50-of-Malware-Assaults.htm>

²GFI Labs, Bogus Windows License Spam is in the Wild, October, 2012
<http://www.gfi.com/blog/bogus-windows-license-spam-is-in-the-wild/>

³GFI Labs, GFI Labs Email Roundup for the week, November, 2012
<http://www.gfi.com/blog/gfi-labs-email-roundup-for-the-week-2/>

⁴Help Net Security, Blackhole exploits lead a black month for malware, November 2012
http://www.net-security.org/malware_news.php?id=2326

⁵GFI Labs, This Spam Gives Recipients a Second Chance, October 2012
<http://www.gfi.com/blog/this-spam-gives-recipients-a-second-chance/>

⁶NBCNEWS.com Facebook scam insults, then infects you, October 2012

⁷V3, Blackhole exploit tool traced to Russia, December 2012
<http://www.v3.co.uk/v3-uk/news/2228859/blackhole-exploit-tool-traced-to-russia>

⁸Computer Weekly, Cyber criminals target Skype, Facebook and Windows users, November 2012
<http://www.computerweekly.com/news/2240171783/Cyber-criminals-target-Skype-Facebook-and-Windows-users>

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. ThreatTrack Security, Inc is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, ThreatTrack Security, Inc makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. ThreatTrack Security, Inc makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.