McAfee Labs – W32/Vulcanbot FAQ

What is W32/Vulcanbot?

W32/Vulcanbot is Trojan malware that causes infected machines to connect to a botnet with command and control systems located around the globe that are accessed predominantly from IP addresses inside Vietnam. The resulting botnet was used to launch distributed denial of service attacks against blogs that cover politics and human rights in Vietnam.

McAfee Labs found this malware during its investigation into the Operation Aurora attack that hit Google and at least 20 other companies, learning that it found its way onto computers inside a subset of companies targeted by Aurora.

McAfee added detection of this malware in January, around the same time we provided protection for Operation Aurora related malware.

What are its attributes?

W32/Vulcanbot is a common piece of Trojan malware that caused the infected machines to join a network of compromised PCs.

The malware was disguised as a keyboard driver for Vietnamese character support on Windows. The attackers sent the malware to targeted individuals in e-mail attachments, sending them to a legitimate website, Vietnamese Professionals Society. The website was infected with malware that downloaded itself onto users' machines upon connection.

Communication may be made with remote hosts over port 80, 2120, 8585 or other random high TCP ports.

How does W32/Vulcanbot differ from other botnets? From Operation Aurora?

W32/Vulcanbot is a relatively unsophisticated piece of Trojan malware that caused the infected machines to join a network of compromised PCs. The resulting botnet was used to launch distributed denial of service attacks against Vietnamese human rights websites. This is in contrast to Operation Aurora, in which the overall attack was extremely sophisticated and the desired result was intellectual property theft, achieved via browser exploitation and targeted malware.

Even though we found that a subset of the companies in Operation Aurora were infected with W32/Vulcanbot, our analysis leads us to believe that the two attacks are unrelated.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

How can I protect myself?

McAfee anti-malware and web security software have included protection for W32/Vulcanbot since January, about the time that we did so for Operation Aurora.

Consumers.

1. Make sure that you have the latest version of McAfee anti-malware and web security software, including McAfee AntiVirus Plus, Internet Security, Total Protection, and SiteAdvisor.

Enterprises.

1. Ensure that your McAfee anti-malware software is up to date with the latest DAT file.
2. Run a full system scan on your system if yourDAT is earlier than 5870.
3. Enable Artemis – McAfee’s real-time file reputation engine, which protects against known, new, and emerging threats – on your endpoint products. If you do not know how to do this, please visit the McAfee Corporate Knowledge Base to access a video tutorial.
4. Enable TrustedSource – McAfee’s real-time web, email, and network reputation engine, which protects against malicious or suspicious websites, IPs, domains, and senders – on your web security products.

Am I protected with McAfee products?

McAfee releases updated virus definition files (DATs) as necessary to combat the latest malware, including W32/Vulcanbot. Protection against W32/Vulcanbot was released with the McAfee DAT file versions 5870 and later. McAfee Web Gateway products also protect customers from connecting to malicious websites associated with W32/Vulcanbot malware.

Am I infected? What should I be looking for?

McAfee anti-malware and web security software can detect W32/Vulcanbot malware. If you don’t have the latest DAT files (5870 or later) or still want to check, you should update to the latest DAT release and run a full system scan.

Closely monitor your client network traffic and firewall logs in order to track down infected hosts. Note that computers trying to connect to known malicious websites or trying to connect to websites at regular intervals are likely to be infected with this or another Trojan.

If I've been infected, what should I do?

Consumer:

- Make sure that you have the latest version of McAfee anti-malware and web security software, including McAfee AntiVirus Plus, Internet Security, Total Protection, and SiteAdvisor.
- If your software is not up-to-date, you should update it and run a full system scan.

Enterprise:

- Ensure that your McAfee anti-malware software is up to date with the latest DAT file.
- Run a full system scan on your system if your DAT is earlier than 5870.
- Let our incident response team help you. If you fear you may have been compromised by this or other attacks, contact McAfee Foundstone.

What other resources can I leverage?

Researchers at McAfee Labs are delivering behavioral and content signatures, web security, IPS, and IP security updates, product configuration suggestions, and advice on a continuous basis on the McAfee Labs blog.

Learn more specifics about W32/Vulcanbot and other malware at the McAfee Labs Threat Library.

McAfee Global Threat Intelligence offers the most comprehensive protection in the market. With visibility across all key threat vectors – file, web, email, and network – and a view into the latest vulnerabilities across the IT industry, we correlate real-world data collected from millions of sensors around the globe and deliver real-time protection via your suite of McAfee security products. Learn more.

Additional Information:

- W32/Vulcanbot - http://vil.nai.com/vil/content/v_254209.htm
- Vietnamese Speakers Targeted In Cyberattack - http://siblog.mcafee.com/cto/vietnamese-speakers-targeted-in-cyberattack/
- The Chilling Effects of Malware - http://googleonlinesecurity.blogspot.com/2010/03/chilling-effects-of-malware.html