E-Guide

HACKERS OPEN MALWARE BACKDOOR IN APACHE WEBSERVERS

ComputerWeekly.com

A **NEW THREAT IS** targeting Apache webservers, which are among the most widely-used webservers in the world. Read this expert E-Guide to discover how to fight back against these hackers and secure your webserver.

HACKERS OPEN MALWARE BACKDOOR IN APACHE WEBSERVERS

Warwick Ashford

A new threat is targeting Apache webservers, which are among the most widely-used webservers in the world, according to researchers at security firms ESET and Sucuri.

The threat is a highly advanced and stealthy backdoor being used to drive traffic to malicious websites carrying Blackhole exploit packs.

Researchers have named the backdoor Linux/Cdorked.A, and have described it as the most sophisticated Apache backdoor to date.

“The Linux/Cdorked.A backdoor does not leave traces on the hard-disk other than a modified httpd file, the daemon (or service) used by Apache,” said Pierre-Marc Bureau, ESET security intelligence program manager.

“All information related to the backdoor is stored in shared memory on the server, making detection difficult and hampering analysis.”

In addition, Linux/Cdorked.A takes other steps to avoid detection, both on the compromised webserver and web browsers of computers visiting it.

Home

Hackers open malware backdoor in Apache webservers

“The backdoor’s configuration is sent by the attacker using HTTP requests that are not only obfuscated, but also not logged by Apache, reducing the likelihood of detection by conventional monitoring tools,” said Righard Zwienenberg, ESET senior researcher.

“The configuration is stored in memory, meaning no command and control information for the backdoor is visible, making forensic analysis complex,” he said.

The Blackhole exploit kit is a popular and prevalent exploit kit using zero-day and known exploits, to take control of systems when users visit a site that is comprised and infected by the Blackhole kit.

When someone visits a compromised webserver, they are not simply redirected to a malicious website and a web cookie is set in the browser so the backdoor will not send them there a second time.

The web cookie is not set on the administrator pages. The backdoor checks the visitor’s referrer field and if they are redirected to the webpage from a URL that has certain key words in it, like “admin” or “cpanel”, no malicious content is served.

ESET has called on system administrators to check their servers and verify that they are not affected by this threat.

Home

Hackers open malware backdoor in Apache webservers

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

RELATED TECHTARGET WEBSITES

TechTarget | SearchSecurity