Linux/CDorked FAQs

blogs.cisco.com/security/linuxcdorked-faqs

Mary Landesman May 1, 2013

Last Friday (April 26), ESET and Sucuri simultaneously blogged about the discovery of Linux/CDorked, a backdoor impacting Apache servers running cPanel. Since that announcement, there has been some confusion surrounding the exact nature of these attacks. Rather than reinvent the analysis that has already been done, this blog post is intended to clear up some of the confusion.

When did Linux/CDorked first appear?
According to Cisco TRAC analysis, the first encounter was on March 4, 2013.

How is Linux/CDorked related to DarkLeech?
The appearance of Linux/CDorked coincided with a drop in the number of DarkLeech infections, an indication the attacker(s) may be one and the same.

Unlike DarkLeech, the Linux/CDorked infections appear to be only targeting Apache servers with cPanel installed. Conversely, DarkLeech was found on servers running a variety of control panels (or not).

Why are cPanel installs being targeted?
That cPanel installs are targeted does not imply attackers are exploiting a vulnerability in cPanel to gain access. Rather, Linux/CDorked exploits the fact that cPanel doesn't use a packaging system to install Apache. This, along with some logging differences, makes it much more difficult to detect the backdoor on Apache servers running cPanel, which is key to its success.

How are attackers gaining access to the host servers?
How the attackers are gaining *root* access to begin with is a separate matter, still unresolved. Attackers may have stolen login credentials via phishing, or via a localized infection on a management system, or simply by brute-force guessing the login.

Who are the compromised hosts?
The compromised host servers observed thus far have all been smaller, less mainstream providers. This is also in contrast to DarkLeech, which netted some significantly sized host providers in those attacks.

How many websites have been affected?
While there have been thousands of encounters with Linux/CDorked injected sites, decoding the URLs reveals only a few hundred compromised sites, unlike DarkLeech, which affected thousands of innocent websites.

The size (number of impacted websites) isn't the whole story, however. The Linux/CDorked attacks appear to be in concert with local trojan Medfos infections. The Medfos family of trojans installs browser extensions which automatically redirect search results when clicked. As a result, 37% of the encounters with the Linux/CDorked injected sites have been via searches performed on Google, Bing, and Yahoo.

What exploits are involved?
The Linux/CDorked attackers are using Blackhole exploit kit v4. Hence, when a Web surfer clicks through a link to one of the sites hosted on the compromised server, the visited URL is base64 encoded before the request is handed off to the malware domain. The exploits we've observed have been a mix of known PDF and Java exploits, no zero days. Thus far, all observed malware domains (the actual redirect destination) track back to 7 unique IP addresses:

- 94.23.48.114
- 62.212.130.115
- 178.17.41.212
- 109.123.66.30
- 94.242.251.151
- 94.23.47.211
- 87.229.26.138

Reference Links:
Linux/Cdorked.A: New Apache backdoor being used in the wild to serve Blackhole
Apache Binary Backdoors on Cpanel-based servers
Malicious Apache Linux/Cdorked.A Trojan in Compromised Web Servers
Admin beware: Attack hitting Apache websites is invisible to the naked eye
Apache DarkLeech Compromises

Share: