CryptoPHP Backdoor Hijacks Servers with Malicious Plugins & Themes

CryptoPHP Backdoor Hijacks Servers with Malicious Plugins & Themes - Swati Khandelwal, The Hacker News.

- Published: date not stated
- Original: <https://web.archive.org/web/20160403035045/http://thehackernews.com/2014/11/cryptophp-backdoored-cms-plugins-themes.html>
- Current location: <https://web.archive.org/web/20160402192125/http://thehackernews.com/2014/11/cryptophp-backdoored-cms-plugins-themes.html>
- Preserved from: https://web.archive.org/web/20160402192125/http://thehackernews.com/2014/11/cryptophp-backdoored-cms-plugins-themes.html (live) on 2026-08-10
- Capture timestamp: 20160403035045
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

CryptoPHP Backdoor Hijacks Servers with Malicious Plugins & Themes

* *Monday, November 24, 2014* * Swati Khandelwal

Security researchers have discovered thousands of *backdoored plugins and themes* for the popular content management systems (CMS) that could be used by attackers to compromise web servers on a large scale.

The Netherlands-based security firm Fox-IT has published a whitepaper revealing a new Backdoor named ***"CryptoPHP."*** Security researchers have uncovered malicious plugins and themes for WordPress, Joomla and Drupal. However, there is a slight relief for Drupal users, as only themes are found to be infected from CryptoPHP backdoor.

In order to victimize site administrators, miscreants makes use of a simple social engineering trick. They often lured site admins to download pirated versions of commercial CMS plugins and themes for free. Once downloaded, the malicious theme or plugin included backdoor installed on the admins' server.

> *"By publishing pirated themes and plug-ins free for anyone to use instead of having to pay for them, the CryptoPHP actor is social-engineering site administrators into installing the included backdoor on their server,"* Fox-IT said in its analysis on the attack.

Once installed on a web server, the backdoor can be controlled by cyber criminals using various options such as command and control server (C&C) communication, email communication and manual control as well.

**Other capabilities of the CryptoPHP backdoor include: **

- Integration into popular content management systems like WordPress, Drupal and Joomla
- Public key encryption for communication between the compromised server and the command and control (C2) server
- An extensive infrastructure in terms of C2 domains and IP's

- Backup mechanisms in place against C2 domain takedowns in the form of email communication
- Manual control of the backdoor besides the C2 communication
- Remote updating of the list of C2 servers
- Ability to update itself

Miscreants are using CryptoPHP backdoor on compromised Web sites and Web servers for illegal Search Engine Optimization (SEO), which is also known as Black Hat SEO, researchers said in its report. It is because the compromised websites link to the websites of the attackers appear higher in search engine results.

Black hat SEO is a group of techniques and tactics that focus on maximizing search engine results with non-human interaction with the pages, thus violating search engine guidelines. These include keyword stuffing, invisible text, doorway pages, adding unrelated keywords to the page content or page swapping.

The security company has discovered 16 variants of CryptoPHP Backdoor on thousands of of backdoored plugins and themes as of 12th November 2014. First version of the backdoor was appeared on the 25th of September 2013. The exact number of websites affected by the backdoor is undetermined, but the company estimates that at least a few thousand websites or possibly more are compromised.
