Sites stumble on to malware path with plugin exploit

16 December 2014, by Nancy Owano

The numbers were not pretty. Over 100,000 WordPress websites may have been infected with malware, once again proving that where there is widespread popularity, whether in operating systems or platforms or plug-ins, there is mischief. In this case, malware that compromised certain WordPress sites was inadvertently turned into a malware distribution system. Tyler Lee in *Ubergizmo* reported on the incident where sites that are infected load attack code into pages viewed by visitors. As a result, said Lee, Google has since flagged more than 11,000 domains as malicious. Tony Perez, CEO of the website security company Sucuri, in tracking how this all happened, blogged with the headline "SoakSoak Malware Compromises 100,000+ WordPress Websites" that Sunday "started with a bang" with Google flagging over 11,000 domains. "Our analysis is showing impacts in the order of 100's of thousands of WordPress specific websites. We cannot confirm the exact vector, but preliminary analysis is showing correlation with the RevSlider vulnerability," he said. The malware when decoded loads a javascript malware from the SoakSoack.ru domain.

On Monday, Daniel Cid, CTO of Sucuri, blogged that "After a bit more time investigating this issue, we were able to confirm that the attack vector is the RevSlider plugin." Some may not find it an easy flush. "The biggest issue is that the RevSlider plugin is a premium plugin, it's not something everyone can easily upgrade and that in itself becomes a disaster for website owner. Some website owners don't even know they have it as it's been packaged and bundled into their themes. We're currently remediating thousands of sites and when engaging with our clients many had no idea the plugin was even within their environment."

RevSlider is a slideshow plugin, also known as Slider Revolution. The Slider Revolution team had fixed a vulnerability previously with updates. The problem is that the old, vulnerable version of the plug-in was still being used by some sites. Dan Goodin, security editor at *Ars Technica*, said the attack "causes infected sites to load highly obfuscated attack code on every webpage." Chris Brook wrote in *Threatpost* that the malware is modifying a file in WordPress that makes it so a JavaScript file can be loaded onto every page on the site.

Graham Cluley, security blogger and researcher, gave credit to Google for its blacklisting over 11,000 domains on Sunday morning as "a quick-thinking reaction" which hopefully will make it more difficult for attackers to monetize their campaign. Stuart Dredge wrote in the *Guardian* that "affected site owners have been figuring out how to get their blogs cleaned up and back on Google. If you're one of them, this thread on the official WordPress forum may be useful." He provided the link.

ThemePunch, the company behind the slider, meanwhile, posted a clarification in the comments section on the Securi site about events: "As the developer of the Slider Revolution Responsive WordPress Plugin (referred to as "RevSlider" in this article), we would like to clarify a few things." They

said that the nature of plugins bundled in themes caused a lot of older plugin versions to linger around on the web and providing a window for malicious attacks. They said that direct buyers of their plugin were hardly affected by the exploit, as they could use the automatic update tool to keep their plugin secure.

"In February 2014, a critical vulnerability was discovered in our Slider Revolution WordPress Plugin which we immediately fixed in Version 4.2." They emphasized, "Please note !! In fact, only versions 4.1.4 or below, allow for the vulnerability and have to be updated." They said that Envato, which is the marketplace on which they are selling their products, has an article with steps to take.

APA citation: Sites stumble on to malware path with plugin exploit (2014, December 16) retrieved 24 September 2020 from https://techxplore.com/news/2014-12-sites-stumble-malware-path-plugin.html