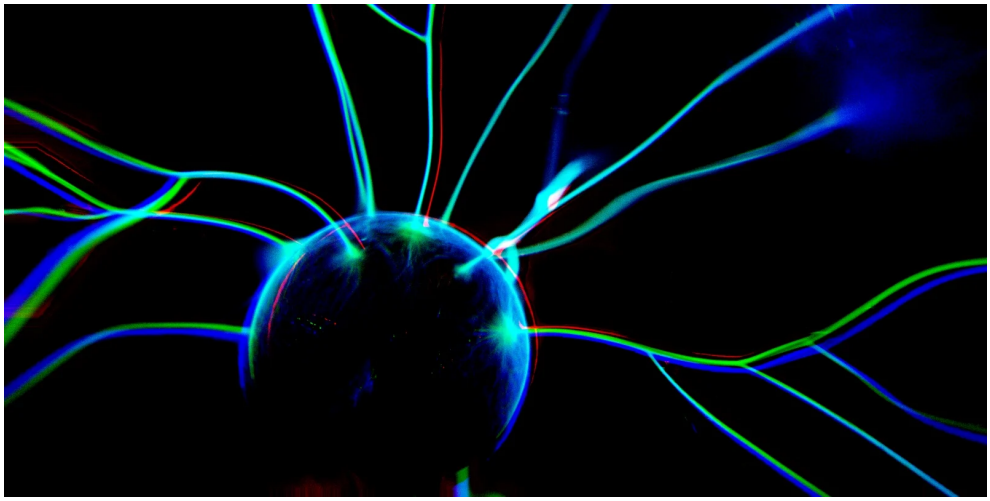
瀏覽拍賣

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** May 13, 2022 01:48 PM **0**



Microsoft says the Sysrv botnet is now exploiting vulnerabilities in the Spring Framework and WordPress to ensnare and deploy cryptomining malware on vulnerable Windows and Linux servers.

Redmond discovered a new variant (tracked as Sysrv-K) that has been upgraded with more capabilities, including scanning for unpatched WordPress and Spring deployments.

"The new variant, which we call Sysrv-K, sports additional exploits and can gain control of web servers" by exploiting various vulnerabilities, the Microsoft Security Intelligence team said (https://twitter.com/MsftSecIntel/status/1525158219206860801) in a Twitter thread.

"These vulnerabilities, which have all been addressed by security updates, include old vulnerabilities in WordPress plugins, as well as newer vulnerabilities like CVE-2022-22947."

CVE-2022-22947 is a code injection vulnerability in the Spring Cloud Gateway library that can be abused for remote code execution on unpatched hosts.

As part of these newly added capabilities, Sysrv-K scans for WordPress configuration files and their backups to steal database credentials, later used to take over the webserver.

Microsoft Security Intelligence · May 14, 2022
@MsftSecIntel
Replying to @MsftSecIntel

A new behavior observed in Sysrv-K is that it scans for WordPress configuration files and their backups to retrieve database credentials, which it uses to gain control of the web server. Sysvr-K has updated communication capabilities, including the ability to use a Telegram bot.

Microsoft Security Intelligence
@MsftSecIntel

Like older variants, Sysrv-K scans for SSH keys, IP addresses, and host names, and then attempts to connect to other systems in the network via SSH to deploy copies of itself. This could put the rest of the network at risk of becoming part of the Sysrv-K botnet.

12:57 AM · May 14, 2022

14 See latest COVID-19 info

Read 1 reply

First spotted by Alibaba Cloud (Aliyun) (https://help.aliyun.com/document_detail/196163.html) security researchers in February after being active since December 2020, this malware also landed on the radars of security researchers at Lacework Labs (https://www.lacework.com/blog/sysrv-hello-expands-infrastructure/) and Juniper Threat Labs (https://blogs.juniper.net/en-us/threat-research/sysrv-botnet-expands-and-gains-persistence) following a surge of activity in March.

As they observed, Sysrv is scanning the Internet for vulnerable Windows and Linux enterprise servers (https://www.bleepingcomputer.com/news/security/new-cryptomining-malware-builds-an-army-of-windows-linux-bots/) and it infects them with Monero (XMRig) miners and self-spreader malware payloads.

To hack its way into these web servers, the botnet exploits flaws in web apps and databases, such as PHPUnit, Apache Solar, Confluence, Laravel, JBoss, Jira, Sonatype, Oracle WebLogic, and Apache Struts.

After killing competing cryptocurrency miners and deploying its own payloads, Sysrv also auto-spreads over the network via brute force attacks using SSH private keys collected from various locations on infected servers (e.g., bash history, ssh config, and known_hosts files).

The botnet propagator component will aggressively scan the Internet for more vulnerable Windows and Linux systems to add to its army of Monero mining bots.

Sysrv fully compromises them using exploits targeting remote code injection or execution vulnerabilities that allow it to execute malicious code remotely.