Hackers hammer SpringShell vulnerability in attempt to install cryptominers

Getty Images

reader comments

13 with 9 posters participating

Share this story

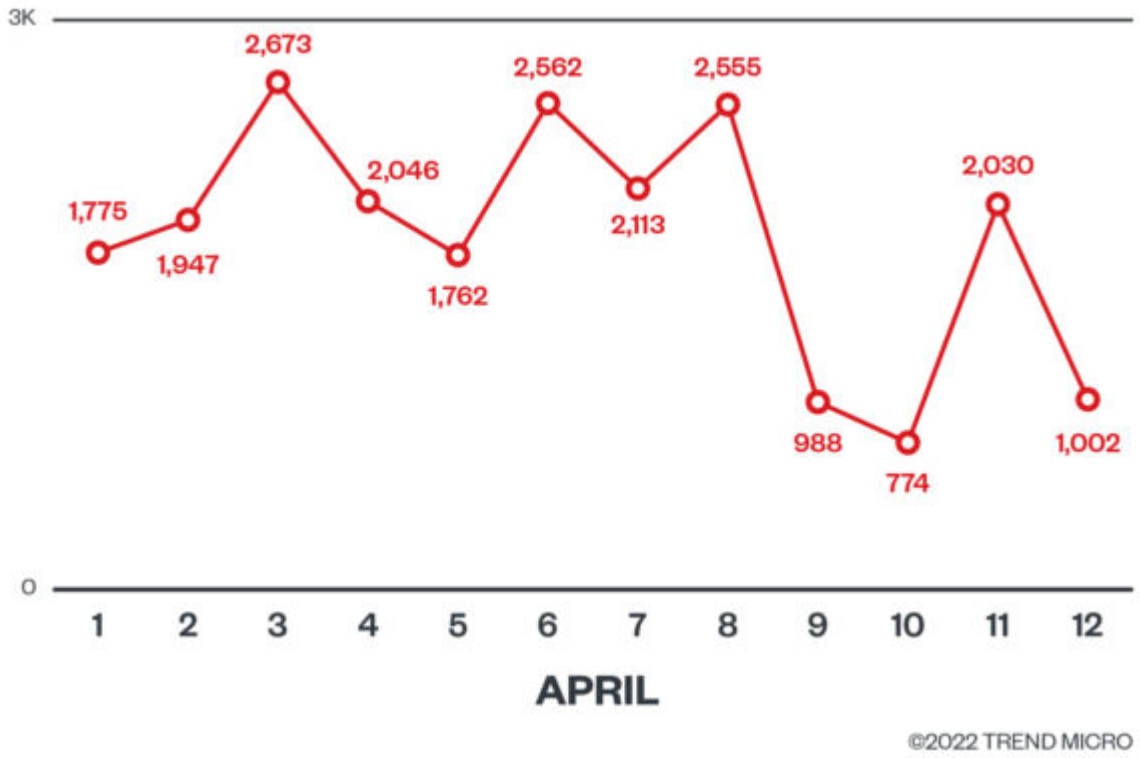
Malicious hackers have been hammering servers with attacks that exploit the recently discovered SpringShell vulnerability in an attempt to install cryptomining malware, researchers said.

SpringShell came to light late last month when a researcher demonstrated how it could be used to remotely execute malicious code on servers that run the Spring model-view-controller or WebFlux applications on top of Java Development

Kit versions 9 or higher. Spring is the most widely used Java framework for developing enterprise-level applications in Java. The framework is part of a sprawling ecosystem that provides tools for things like cloud, data, and security apps.

Earlier this month, security firm Trend Micro said it began detecting attempts. From April 1 to April 12, company researchers detected an average of roughly 700 attempts per day to exploit the vulnerability to install cryptomining software. By running the malware on powerful enterprise servers, criminals can mine Bitcoin or other types of digital cash using the resources and electricity of an unwitting victim.

The number of exploit attempts peaked on April 3 at almost 3,000.



Trend Micro

The hackers first sent commands that were designed to discern if the vulnerable servers were running Windows or Linux. Then they ran exploit code that tried to install a type of

interface known as a web shell, which allows a remote user to run commands using a Web-based window.

The URI corresponding to the encoded exploit looked like this, with the web shell being “zbc0fb.jsp” and parameters w and l standing for the Windows and Linux payloads, which are Base64-encoded.

```
/zbc0fb.jsp?w=powershell.exe+-NonI+-W+Hidden+-NoP+-Exec+Bypass+-Enc+ &l=echo+
```

A powershell script then tried to download the cryptocurrency miner and execute it. Trend redacted the script in the following snippet:

```
$cc="http://"
$sys=-join ([char[]](48..57+97..122) | Get-Random -Count (Get-Random (6..12)))
$dst="$env:AppData\$sys.exe"
```

The execution flow looked like this:

1. *The firewall is turned off using the netsh utility.*
2. *Other known cryptocurrency miners such as kthreaddi, sysrv, and sysrv012 are stopped or killed.*
3. *Other running processes listening on ports 3333, 4444, 5555, 7777, and 9000 are stopped.*
4. *If the process kthreaddk does not exist, the cryptocurrency miner downloads a binary, sys.exe, from 194[.]145[.]227[.]21 to C:\Users\\AppData\Roaming\.exe.*
5. *The cryptocurrency miner then starts the process with a hidden window to avoid having the user observe visual hints of the process being executed.*
6. *A scheduled task with the name “BrowserUpdate” is created*

> *later, running every minute. In addition, the Windows run key is modified to run the binary sys.exe.*

Trend Micro researchers don’t know how many, if any, of the exploit attempts were successful. Earlier this month, company researchers said they had also uncovered attempts to exploit SpringShell to install the Mirai botnet. Anyone running the Spring model-view-controller or WebFlux applications on the JDK version 9 or higher should patch the flaw as soon as practical. https://arstechnica.com/?p=1850048