Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

Budworm Attackers Return with New Espionage Strikes Against the United States

Date of Publication	Admiralty code	TA Number
October 14, 2022	A1	TA2022225

Summary

The Budworm espionage group exploited Log4j vulnerabilities to jeopardize the Apache Tomcat service by integrating several custom and publicly available tools to exfiltrate sensitive information.

CVEs

CVE	NAME	PATCH
CVE-2021-44228	Apache Log4j remote code execution	✓
CVE-2021-45105	Apache Log4j denial of service	✓

Actor Map

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0008** Lateral Movement	**TA0011** Command and Control
T1059 Command and Scripting Interpreter	**T1053** Scheduled Task/Job	**T1053.002** At	**T1078** Valid Accounts
T1036 Masquerading	**T1190** Exploit Public-Facing Application	**T1105** Ingress Tool Transfer	**T1003** OS Credential Dumping
T1574 Hijack Execution Flow	**T1543** Create or Modify System Process	**T1210** Exploitation of Remote Services	**T1574.002** DLL Side-Loading

Technical Details

#1 The Budworm, also identified as APT27, leveraged Log4j vulnerabilities to compromise the Apache Tomcat service on servers and install web shells. The attackers employed Vultr and Telstra Virtual Private Servers (VPS) as command-and-control (C2) servers.

#2 The HyperBro malware family remains the primary payload of the advisories. On occasion, attackers employed the PlugX/Korplug Trojan as a payload. The HyberBro malware was installed via the endpoint privilege management software CyberArk Viewfinity. The HyperBro backdoor was loaded using its HyperBro loader in some instances.

#3 Further, publicly available tools were Cobalt Strike, which was used to install shellcode on a victim machine; LaZagne, which was used to dump credentials; and IOX, which is a proxy and port-forwarding tool. Additionally, Fast Reverse Proxy (FRP) and Fscan were all utilized in the recent attack.

Actor Detail

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Budworm (Emissary Panda,APT 27,LuckyMouse,Bronze Union,TG-3390,TEMP.Hippo,Group 35,ATK 15,Iron Tiger,Earth Smilodon,Red Phoenix ,ZipToken)	China	Australia, Canada, China, Germany, Hong Kong, India, Iran, Iraq, Israel, Japan, Jordan, Kuwait, Lebanon, Mongolia, Oman, Palestine, Philippines, Qatar, Russia, Saudi Arabia, South Korea, Spain, Syria, Taiwan, Thailand, Tibet, Turkey, UK, United Arab Emirates, USA, Yemen	Aerospace, Aviation, Defense, Education, Embassies, Government, Manufacturing, Technology, Think Tanks, Telecommunications,
	MOTIVE		
	Information theft and espionage		

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	5aecbb6c073b0cf1ad1c6803fa1bfaa6eca2ec4311e165f25d5f7f0b3fe001db,779ae012ede492b321fd86df70f7c9da94251440ebe5ec3feee84a432f432478,ab949af896b6a6d986aed6096c36c4f323f650ccccfc7ea49004ba919d1bfa46,bebce37572ea2856663383215a013f8115c1f81da0f2bf1233c959955c494032,27c2a9608ce80a443c87a0a2947864df7d4491cfa85608c6a6b6680ec0277f9d,42b603fffd4766fa22f6e10884e7fa43f449d515cfa20a18f0d07a6d4c370962,0d46907320ab55d98966389f41441aa0341a7db829cd166748d8929d466c9fba,620e401b2b7727a6c7ebc37ee1f7d8e1742d7121c1f4ea350a43d460ef9bdc4c,c8aea84abb476ab536198a36df53b37be3d987a9ce58cb06e93cac7d2bfb3703,233bb85dbeba6923153340850169769 5a66b7790e751925231d64bddf80bbf91,d610547c718fcca7c5c7e02c6821e9909333daf6376a1096edf21f9355754f29,5c2d05bfc9b6d4fc7aea32312c62180564fac9f65b0867e824d81051e5fc34fd,ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56,3d7dc77ded4022a92a32db9e10dbc67fbcc80854a281c3cc0f00b6cbd2bfd112,48e81b1c5cc0005cc58b99cefe1b6087c841e952bb06db5a5a6441e92e40bed6
IPV4	139.180.146[.]101 45.77.46[.]54 139.168.200[.].123 207.148.76[.]235
URLs	http[:]//setting.101888gg.com/jquery-3.3.1.min[.]js http[:]//207.148.76.235/jquery-3.3.1.min[.]js

Patch Links

https://logging.apache.org/log4j/2.x/security.html

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/budworm-espionage-us-state

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

October 14, 2022 . 5:55 AM

More at www.hivepro.com