Hive Pro

THREAT ADVISORY

Chinese state-sponsored threat group APT41 targets U.S. critical organizations using two Zero-Days	TA2022051
Threat Level RED	**Published Date –** Mar 09, 2022

A China state-sponsored threat group known as APT41 is observed compromising at least six U.S. state governments networks in a threat campaign beginning from May 2021. APT41 is a well-known Chinese state-sponsored espionage outfit that targets companies in both the public and commercial sectors and engages in financially motivated behavior for personal benefit.

The threat group exploited two zero-day vulnerabilities, including one in the USAHerds program (CVE-2021-44207) and the now-famous zero-day in Log4j (CVE-2021-44228). After exploiting Log4Shell the actor deployed a new iteration of a modular C++ backdoor known as KEYPLUG on Linux systems. During the attacks, an in-memory dropper dubbed StealthVector was also spotted, which is coordinated to execute the next-stage payload, as well as sophisticated post-compromise tools like DEADEYE. During the espionage operation, adversaries stole personally identifying information from the organizations compromised.

The Mitre TTPs commonly used by APT41 are::
TA0001: Initial Access
TA0007: Discovery
TA0040: Impact
TA0009: Collection
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
TA0042: Resource Development
TA0002: Execution
TA0008: Lateral Movement
TA0006: Credential Access
TA0029: Privilege Escalation
T1071.001: Application Layer Protocol: Web Protocols
T1071.002: Application Layer Protocol: File Transfer Protocols
T1071.004: Application Layer Protocol: DNS
T1560.001: Archive Collected Data: Archive via Utility
T1197: BITS Jobs
T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1110.002: Brute Force: Password Cracking
T1059.001: Command and Scripting Interpreter: PowerShell
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1059.004: Command and Scripting Interpreter: Unix Shell
T1136.001: Create Account: Local Account
T1543.003: Create or Modify System Process: Windows Service
T1486: Data Encrypted for Impact
T1005: Data from Local System
T1568.002: Dynamic Resolution: Domain Generation Algorithms
T1546.008: Event Triggered Execution: Accessibility Features
T1480.001: Execution Guardrails: Environmental Keying

T1190: Exploit Public-Facing Application
T1203: Exploitation for Client Execution
T1133: External Remote Services
T1083: File and Directory Discovery
T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
T1574.002: Hijack Execution Flow: DLL Side-Loading
T1574.006: Hijack Execution Flow: Dynamic Linker Hijacking
T1070.001: Indicator Removal on Host: Clear Windows Event Logs
T1070.003: Indicator Removal on Host: Clear Command History
T1070.004: Indicator Removal on Host: File Deletion
T1105: Ingress Tool Transfer
T1056.001: Input Capture: Keylogging
T1036.004: Masquerading: Masquerade Task or Service
T1036.005: Masquerading: Match Legitimate Name or Location
T1112: Modify Registry
T1104: Multi-Stage Channels
T1046: Network Service Scanning
T1135: Network Share Discovery
T1027: Obfuscated Files or Information
T1588.002: Obtain Capabilities: Tool
T1003.001: OS Credential Dumping: LSASS Memory
T1566.001: Phishing: Spearphishing Attachment
T1542.003: Pre-OS Boot: Bootkit
T1055: Process Injection
T1090: Proxy
T1021.001: Remote Services: Remote Desktop Protocol
T1021.002: Remote Services: SMB/Windows Admin Shares
T1496: Resource Hijacking
T1014: Rootkit
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.001: Signed Binary Proxy Execution: Compiled HTML File
T1218.011: Signed Binary Proxy Execution: Rundll32
T1553.002: Subvert Trust Controls: Code Signing
T1195.002: Supply Chain Compromise: Compromise Software Supply Chain
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery
T1033: System Owner/User Discovery
T1569.002: System Services: Service Execution
T1078: Valid Accounts
T1102.001: Web Service: Dead Drop Resolver
T1047: Windows Management Instrumentation

Actor Details

Name	Known As	Origin	Target Locations	Target sectors
APT41	Double Dragon, TG-2633, Bronze Atlas , Red Kelpie, Blackfly, Earth Baku, SparklingGoblin, Grayfly	China	Australia, Bahrain, Brazil, Canada, Chile, Denmark, Finland, France, Georgia, Hong Kong, India, Indonesia, Italy, Japan, Malaysia, Mexico, Myanmar, Netherlands, Pakistan, Philippines, Poland, Qatar, Saudi Arabia, Singapore, South Korea, South Africa, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	Construction, Defense, Education, Energy, Financial, Government, Healthcare, High-Tech, Hospitality, Manufacturing, Media, Oil and gas, Petrochemical, Pharmaceutical, Retail, Telecommunications, Transportation, Online video game companies

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Versions	Affected CPE	Vulnerability Name	CWE
CVE-2021-44207	Acclaimsystems: usaherds	cpe:2.3:a:acclaimsystems:usaherds:*:*:*:*:*:*:*:*	Acclaim USAHERDS code execution	CWE-798
CVE-2021-44228	Apache log4j versions 2.0 to 2.14.1	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Apache Log4j remote code execution	CWE-20 CWE-400 CWE-502

Indicators of Compromise (IoCs)

Type	Value
MD5	900ca3ee85dfc109baeed4888ccb5d39, B82456963d04f44e83442b6393face47, 49f1daea8a115dd6fce51a1328d863cf, B108b28138b93ec4822e165b82e41c7a, 143278845a3f5276a1dd5860e7488313
SHA1	355b3ff61db44d18003537be8496eb03536e300f, 996aa691bbc1250b571a2f5423a5d5e2da8317e6, E85427af661fe5e853c8c9398dc46ddde50e2241, 7056b044f97e3e349e3e0183311bb44b0bc3464f, 6f6b51e6c88e5252a2a117ca1cfb57934930166b
SHA256	e024ccc4c72eb5813cc2b6db7975e4750337a1cc619d7339b21fdbb32d93fd85, d7e8cc6c19ceebf0e125c9f18b50167c0ee65294b3fce179fdab560e3e8e0192, ebf28e56ae5873102b51da2cc49cbbe43192ca2f318c4dfc874448d9b85ebd00, 062a7399100454c7a523a938293bef7ddb0bc10636ed402be5f9797d8cc3c57e, a4647fcb35c79f26354c34452e4a03a1e4e338a80b2c29db97bba4088a208ad0
IPs	103[.]238[.]225[.]37, 182[.]239[.]92[.]31, 194[.]195[.]125[.], 194[.]156[.]98[.]12, 54[.]248[.]110[.]45, 45[.]153[.]231[.]31, 185[.]118[.]167[.]40, 104[.]18[.]6[.]251, 104[.]18[.]7[.]251, 20[.]121[.]42[.]11, 34[.]139[.]13[.]46, 54[.]80[.]67[.]241, 149[.]28[.]15[.]152, 18[.]118[.]56[.]237, 107[.]172[.]210[.]69, 172[.]104[.]206[.]48, 67[.]205[.]132[.]162

Type	Value
URLs	cdn[.]ns[.]time12[.]cf, east[.]winsproxy[.]com, afdentry[.]workstation[.]eu[.]org, ns1[.]entrydns[.]eu[.]org, subnet[.]milli-seconds[.]com, work[.]viewdns[.]ml, work[.]queryip[.]cf, microsoftfile[.]com, down-flash[.]com, libxqagv[.]ns[.]dns3[.]cf

Patch Link

https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.15.0/
https://logging.apache.org/log4j/2.x/manual/migration.html
https://github.com/apache/logging-log4j2/pull/607/files

References

https://www.mandiant.com/resources/apt41-us-state-governments