Hive Pro

THREAT ADVISORY

Chinese APT group targets financial institutions in the campaign “Operation Cache Panda”

TA2022040

Threat Level RED

Published Date – Feb 23, 2022

Chinese threat actor APT10 conducted a series of large-scale supply chain attacks that exclusively targeted the financial software systems of Taiwanese financial institutions from the end of November 2021 until the middle of February 2022. The actor is well-known for the attacks on Japanese automakers, British managed service providers, US-based aerospace and defense corporations, and South Korean missile defense systems.

The current attack targeting Taiwan was codenamed "Operation Cache Panda" and started with exploitation of a web service vulnerability in the security software system management interface. First, the attacker uploaded the ASPXCSharp WebShell commonly used by Chinese hackers to control the website host, and then began to use the well-known penetration tool Impacket to scan intranet computers, trying to implant the DotNet backdoor program on a large scale, and intending to steal the hacked unit data. The attackers then utilized a method known as reflected code loading to execute malicious code on local systems and install a version of the Quasar RAT that provided persistent remote access to the affected system via reverse RDP tunnels. Quasar RAT features include capturing screenshots, recording webcam, editing registry, keylogging, and stealing passwords.

The Mitre TTPs used by APT10 in the current attack are:
TA0002: Execution
TA0007: Discovery
TA0005: Defense Evasion
TA0003: Persistence
TA0004: Privilege Escalation
TA0008: Lateral Movement
T1620: Reflective Code Loading
T1569.002: System Services: Service Execution
T1047: Windows Management Instrumentation
T1021.001: Remote Services: Remote Desktop Protocol
T1505.003: Server Software Component: Web Shell
T1082: System Information Discovery
T1518.001: Software Discovery: Security Software Discovery
T1543.003: Create or Modify System Process: Windows Service
T1055: Process Injection
T1027: Obfuscated Files or Information
T1480: Execution Guardrails
T1562.001: Impair Defenses: Disable or Modify Tools

The other TTPs commonly used by APT10 are:
TA0042: Resource Development
TA0001: Initial Access
TA0006: Credential Access
TA0009: Collection
TA0011: Command and Control[

T1087.002: Account Discovery: Domain Account
T1583.001: Acquire Infrastructure: Domains
T1560: Archive Collected Data
T1560.001: Archive via Utility
T1119: Automated Collection
T1059.001: Command and Scripting Interpreter: PowerShell
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1005: Data from Local System
T1039: Data from Network Shared Drive
T1074.001: Data Staged: Local Data Staging
T1074.002: Data Staged: Remote Data Staging
T1140: Deobfuscate/Decode Files or Information
T1568.001: Dynamic Resolution: Fast Flux DNS
T1190: Exploit Public-Facing Application
T1210: Exploitation of Remote Services
T1083: File and Directory Discovery
T1574.001: Hijack Execution Flow: DLL Search Order Hijacking
T1574.002: Hijack Execution Flow: DLL Side-Loading
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: Masquerading
T1036.003: Rename System Utilities
T1036.005: Match Legitimate Name or Location
T1106: Native API
T1046: Network Service Scanning
T1588.002: Obtain Capabilities: Tool
T1003.002: OS Credential Dumping: Security Account Manager
T1003.003: OS Credential Dumping: NTDS
T1003.004: OS Credential Dumping: LSA Secrets
T1566.001: Phishing: Spearphishing Attachment
T1055.012: Process Injection: Process Hollowing
T1090.002: Proxy: External Proxy
T1021.004: Remote Services: SSH
T1018: Remote System Discovery
T1053.005: Scheduled Task/Job: Scheduled Task
T1218.004: Signed Binary Proxy Execution: InstallUtil
T1553.002: Subvert Trust Controls: Code Signing
T1016: System Network Configuration Discovery
T1049: System Network Connections Discovery
T1199: Trusted Relationship
T1204.002: User Execution: Malicious File
T1078: Valid Accounts
T1047: Windows Management Instrumentation

Actor Details

Name	Target Locations	Target sectors	Motive
APT10 (Stone Panda, APT 10 , menuPass, Red Apollo, CVNX, Potassium, Hogfish, Happyyongzi, Cicada, Bronze Riverside, CTG-5938, ATK 41, TA429, ITG01)	Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Japan, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.	Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, Pharmaceutical, Telecommunications and MSPs.	Information theft and espionage

Indicators of Compromise (IoCs)

Type	Value
Domain	43[.]245[.]196[.]124 43[.]245[.]196[.]123 43[.]245[.]196[.]122 43[.]245[.]196[.]121 43[.]245[.]196[.]120
MD5	375270077E842624BCE08C368CDC62F9 EEADD95725DE21D269933881A8E8B21A 03B88FD80414EDEABAAA6BB55D1D09FC F1726539E5CF68EBB2124262E695C65E 7D12FA8EEBBD401390F2A5046FF2B4BB 0724AC34E997354CA9FB06D57AF4E29B A991AC3EB2D5C66DA1BECF002C19B9E6 2949C999C785AA1CA4673FC7FAE58A73 D506ED774089BA11D515F28087DC3E21 9F1BF77452A896B8055D3EA2EF6A6A65 8CE271DA8A84CD3D42552547A8BBAF5B 165758BA40B3CC965D98C1FDE2D56798 ADC84F8C72E65EC85E051FE7CC419332
SHA-1	D42BF66485218F2ED76A8B1D63AF417FD2A82C8B 4ECFC1A89B50CD8DC1B9424C3EFCF63E257525AA 6E6C399BDA3C1F06ADE71053FDDD8FBEFA15029C 4ECFC1A89B50CD8DC1B9424C3EFCF63E257525AA 6E6C399BDA3C1F06ADE71053FDDD8FBEFA15029C EC30990EFD04B15926F2F9DB59F3BFDFEC413C23 7D8EDEDB3104FEE9A422FC4E97B1969DC31C4E66 CE2925BCD3188D3CB6F8BB67CD9D3F2D72FDDC05 BD6069BE81C70E918CF95BBDB30765A90A07FD98 333D9A94DC1A95D3C773BDE232D1BC2756C10518 6B47C2DEE1788017043B456C27E22193537B7A26 49E803BEAA4230E69A216B91757E35840D0C8683 A9541DEB16FFB41B6B4744D409597F9C62F7110E B6626AE6ED2F24FB82E262A2B766F2E5FD7E5230 7CB09DC4BC7DD68D6AACE7A9628634248F18EBA5

References

https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525
https://medium.com/cycraft/supply-chain-attack-targeting-taiwan-financial-sector-bae2f0962934