Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

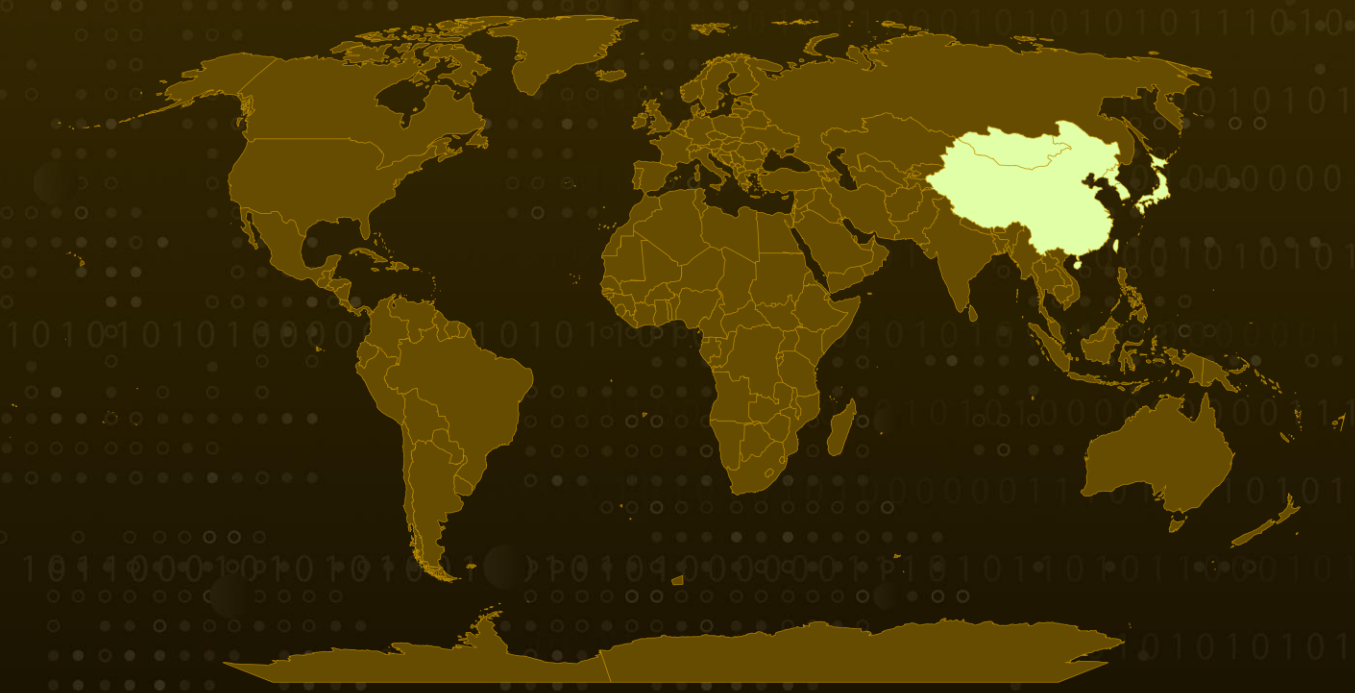
China's Cyber Espionage Targets Semiconductor Giants in East Asia

Date of Publication	Admiralty Code	TA Number
October 9, 2023	A1	TA2023404

Summary

Attack Began: August 2023
Malware: HyperBro loader, Cobalt Strike (aka Agentemis, BEACON, CobaltStrike, cobeacon), and ChargeWeapon Backdoor
Attack Region: China, Hong Kong, Macau, Japan, Mongolia, North Korea, South Korea, Taiwan, Singapore
Targeted Industry: Semiconductor
Attack: In recent cyber espionage activities, threat actors affiliated with the People's Republic of China (PRC) have targeted semiconductor companies operating in Mandarin/Chinese-speaking regions of East Asia. These attacks involve the use of a variant of the HyperBro loader to distribute Cobalt Strike beacons.

Attack Regions



Attack Details

#1 Cyber adversaries engaged in espionage within the realm of cyber espionage have focused their efforts on Mandarin/Chinese-speaking semiconductor firms located in East Asian regions, notably Taiwan, Hong Kong, and Singapore. These intrusions involve the deployment of lures themed around the Taiwan Semiconductor Manufacturing Company (TSMC) and the utilization of a variant of the HyperBro loader to distribute Cobalt Strike beacons.

#2 This modus operandi closely resembles past activities associated with state-backed Chinese threat groups linked to the People's Republic of China (PRC). While the initial vector for compromise remains undisclosed, it is conjectured to involve spear-phishing emails, a common tactic in cyber espionage operations.

#3 The threat actors behind this campaign leverage the HyperBro loader variant, utilizing a digitally signed CyberArk binary for DLL-side loading. This results in the in-memory execution of a Cobalt Strike beacon on the compromised device, providing remote access to the perpetrators. The loaded DLL decrypts bin.config, which contains XOR-encrypted Cobalt Strike shellcode.

#4 In a second iteration of the attack, the hackers utilize a compromised **Cobra DocGuard** web server to deploy an additional McAfee binary, 'mcods.exe,' and load more Cobalt Strike shellcode. This compromised server hosts a GO-based backdoor known as "ChargeWeapon," designed to enable remote access and transmit device and network information from the infected host to a Malleable C2 server under the control of the attackers.

#5 The Malleable C2 profile specifies how the beacon transforms and stores data during transactions with its C2 server, a technique employed to circumvent conventional firewall defenses. The observed operational tactics bear a striking resemblance to those employed by Chinese threat groups such as RedHotel and **APT27** (also known as Budworm or LuckyMouse).

#6 Analysis of the HyperBro Loader and the ChargeWeapon backdoor strongly suggests that they are likely operated and developed by a nation-state threat actor with PRC backing. This conclusion is drawn from factors such as observed infrastructure, malware code characteristics, and parallels with previously documented activities involving China-sponsored APTs that utilize Cobra DocGuard servers for malware delivery. These findings significantly bolster the attribution hypothesis to Chinese hackers.

Recommendations

Monitor DLL Side Loading Activities: Implement continuous monitoring for DLL side-loading activities, especially under the C:\ProgramData file path. Pay close attention to binaries like mcods.exe and vfhost.exe on Windows endpoints.

Vet Third-Party Software: Given the adversary's tactic of exploiting legitimate software in their attacks, it is crucial for organizations to thoroughly assess and monitor third-party software components, especially those integrated into critical systems. This evaluation involves scrutinizing the reputation and security practices of software providers, as well as verifying the authenticity of their digital signatures.

Application Whitelisting and Monitoring: Employ application whitelisting to prevent the execution of any unsigned executable (EXE) on Windows endpoints. Monitor and scrutinize any suspicious downloading attempts, particularly those using the Start-BitsTransfer PowerShell cmdlet.

Manage PowerShell Usage: Recognizing the increasing use of Windows PowerShell by threat actors, consider restricting or blocking its usage for regular Windows users. If blocking is not feasible, enable PowerShell module and script logging via Windows Group Policy to track and analyze PowerShell activities. Implement PowerShell Constrained Language Mode to limit the attack surface available to adversaries.

Email Security: Enhance email security measures and educates users on recognizing social engineering tactics to mitigate the risk of falling prey to phishing attacks leveraging deceptive zip file attachments.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0011** Command and Control	**T1592** Gather Victim Host Information

T1190 Exploit Public-Facing Application	**T1027** Obfuscated Files or Information	**T1105** Ingress Tool Transfer	**T1071.001** Web Protocols
T1059.001 PowerShell	**T1204.002** Malicious File	**T1047** Windows Management Instrumentation	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1036.005** Match Legitimate Name or Location	**T1140** Deobfuscate/Decode Files or Information	**T1204** User Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	12e1f50d7c9cf546c90545588bc369fa90e03f2370883e7befd87e4d50ebf0df, 7229bb62acc6feca55d05b82d2221be1ab0656431953012ebad7226adc63643b, df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348, 45e7ce7b539bfb4f780c33faa1dff523463907ec793ff5d1e94204a8a6a00ab5, df6dd612643a778dca8879538753b693df04b9cf02169d04183136a848977ce9, 3195fe1a29d0d44c0eaec805a4769d506d03493816606f58ec49416d26ce5135, ee66ebcbe872def8373a4e5ea23f14181ea04759ea83f01d2e8ff45d60c65e51, e26f8b8091bbe5c62b73f73b6c9c24c2a2670719cf24ef8772b496815c6a6ce0, e6bad7f19d3e76268a09230a123bb47d6c7238b6e007cc45c6bc51bb993e8b46, ce226bd1f53819d6654caf04a7bb4141479f01f9225ac6fba49248920e57cb25, 56f94f1df0338d254d0421e7baf17527817607a60c6f9c71108e60a12d7d6dcf
IPv4	45[.]77[.]37[.]145:8443, 45[.]32[.]33[.]17, 23[.]224[.]61[.]12

TYPE	VALUE
URLs	hxxp[://]38[.]54[.]119[.]239:443/jquery-3.3.1.min[.]js, hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcvsocfg[.]dll, hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/mcods[.]exe, hxxp[://]154[.]93[.]7[.]99:8090/CDGServer3/images/zh/bin[.]config
File Path	c:\programdata\mcvsocfg[.]dll, c:\programdata\mcods[.]exe, c:\programdata\bin[.]config, c:\Users\xdd\Desktop\今天\0.直接装载 \VFTRACE\Release\VFTRACE.pdb

References

https://blog.eclecticiq.com/chinese-state-sponsored-cyber-espionage-activity-targeting-semiconductor-industry-in-east-asia

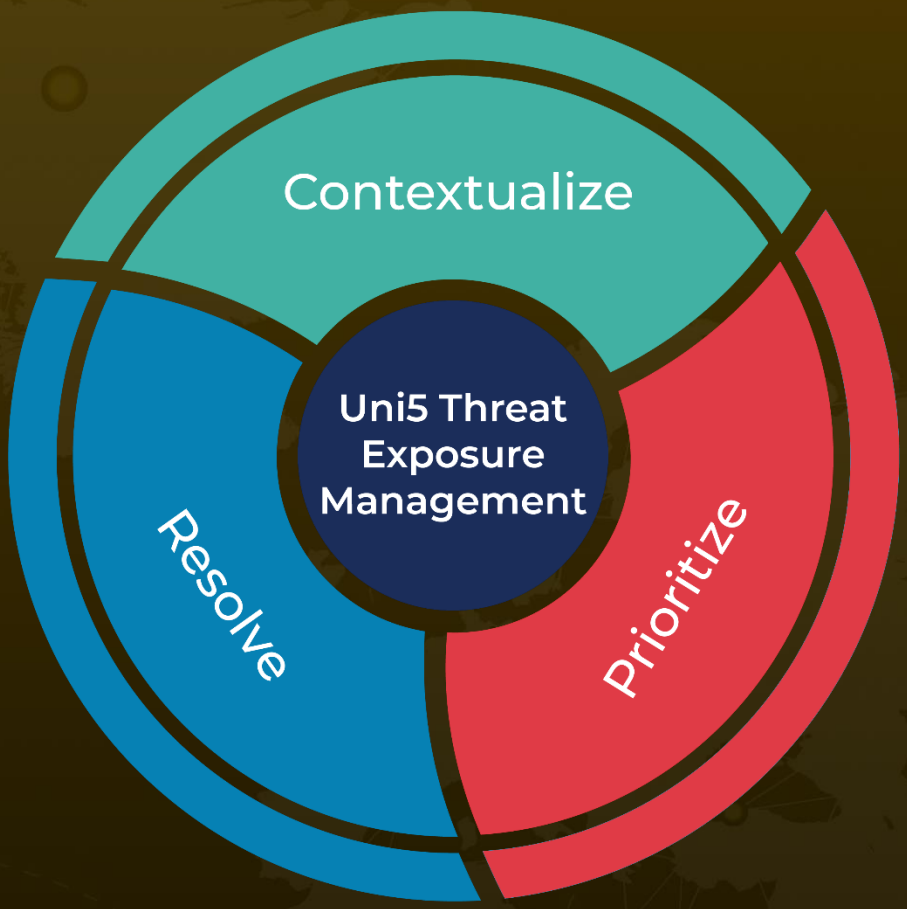
https://www.hivepro.com/budworm-attackers-return-with-new-espionage-strikes-against-the-united-states/

https://www.hivepro.com/carderbee-apt-strikes-hong-kong-with-supply-chain-attack/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 9, 2023 . 9:30 PM

More at www.hivepro.com