Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

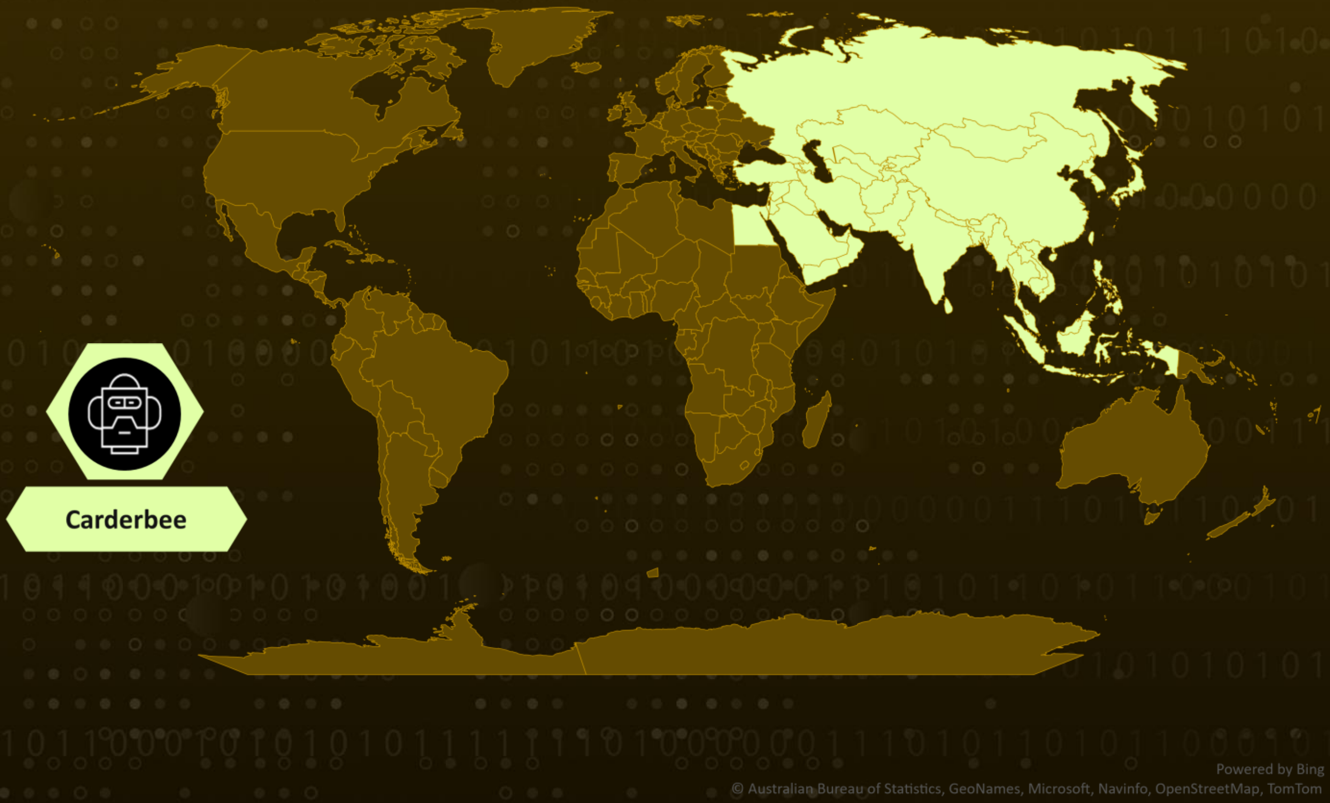
Carderbee APT Strikes Hong Kong with Supply Chain Attack

Date of Publication	Admiralty Code	TA Number
August 23, 2023	A1	TA2023342

Summary

Attack Began: April 2023
Malware: PlugX (aka Korplug)
Threat Actor: Carderbee
Attack Region: Asia
Attack: The Carderbee advanced persistent threat (APT) group executed a supply chain attack by exploiting the legitimate Cobra DocGuard software. Their objective was to deploy the PlugX backdoor onto targeted organizations primarily situated in Hong Kong.

Attack Regions


Carderbee
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The Carderbee advanced persistent threat (APT) group executed a supply chain attack by exploiting the legitimate Cobra DocGuard software. Their objective was to deploy the PlugX backdoor, also known as Korplug, onto targeted organizations primarily situated in Hong Kong. However, some victims were in other Asian regions as well. Notably, the PlugX backdoor has been utilized by several APT groups, such as Space Pirates, Mustang Panda, Budworm, and SparklingGoblin, throughout the latter half of 2022 and the initial half of 2023.

#2 Carderbee employs a modified version of a legitimate program named EsafeNet Cobra DocGuard Client to deliver the PlugX backdoor, also known as Korplug, onto victim networks. During this attack, Carderbee utilized malware that was signed using a valid Microsoft certificate known as the "Microsoft Windows Hardware Compatibility Publisher." This specific downloader was used to implant the PlugX backdoor onto targeted systems.

#3 The malevolent DLL introduced by Carderbee contains both x64 and x86 drivers, which are instrumental in establishing the necessary Windows services and registry entries for sustained presence within the system. Ultimately, PlugX is injected into the genuine 'svchost.exe' (Service Host) process within the Windows system, effectively evading detection by antivirus mechanisms.

Recommendations

Vet Third-Party Software: Considering the Carderbee APT group's exploitation of legitimate software for their attacks, it is essential for organizations to diligently vet and monitor third-party software components, particularly those employed in critical systems. This process entails assessing the reputation and security practices of software providers, along with evaluating the authenticity of their digital signatures.

Enhance Certificate Management and Behavioral Analysis: Reinforce the management of digital certificates and code-signing processes, encompassing regular monitoring, updates, and swift revocation of compromised certificates. Furthermore, employ behavioral analysis techniques to identify malware activity that could potentially bypass traditional signature-based antivirus solutions. Vigilantly monitoring for unusual behavior can effectively unveil previously unseen threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1129 Shared Modules	T1543.003 Windows Service	T1547.008 LSASS Driver	T1027 Obfuscated Files or Information
T1036 Masquerading	T1070.004 File Deletion	T1112 Modify Registry	T1056 Input Capture
T1012 Query Registry	T1018 Remote System Discovery	T1082 System Information Discovery	T1518.001 Security Software Discovery
T1071 Application Layer Protocol	T1095 Non-Application Layer Protocol	T1105 Ingress Tool Transfer	T1573 Encrypted Channel

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622, 19a6a404605be964ab87905d59402e2890460709a1d9038c66b3fbeedc1a2343, 1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d, 2400d8e66c652f4f8a13c99a5ffb67cb5c0510144b30e93122b1809b58614936, 2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4, 47b660bbaacb2a602640b5e2c589a3adc620a0bfc9f0ecfb8d813a803d7b75e2, 5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7, 7e6d0f14302662f52e4379eb5b69a3749d8597e8f61266aeda74611258972a3d,

TYPE	VALUE
SHA256	85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af, 8bd40da84c8fa5f6f8e058ae7e36e1023aca1b9a9c83797049340a77080da76f, 8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f, 9e96f70ce312f2638a99cfbd3820e85798c0103c7dc06fe0182523e3bf1e2805, 9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c, b5159f8ae16deda7aa5d55100a0eac6e5dacd1f6502689b543513a742353d1ea, b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510, b84f68ab098ce43f9cb363d0a20a2267e7130078d3d2d8408bfb32bbca95ca37, f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97
IPv4	45.76.179[.]209, 104.238.151[.]104
URLs	hxxp://111.231.100[.]228:8888/CDGServer3/UpgradeService2, hxxp://103.151.28[.]11:8090/CDGServer3/UpgradeService2
Domains	cdn.stream-amazon[.]com, cdn.ofo[.]ac, gobay[.]info, tjj.active-microsoft[.]com, githubassets.akamaixed[.]net, ms-g9-sites-prod-cdn.akamaixed[.]net, ms-f7-sites-prod-cdn.akamaixed[.]net

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse

https://www.hivepro.com/a-deep-dive-into-space-pirates-unconventional-cyber-arsenal/

https://www.hivepro.com/mustang-panda-apt-targets-europe-with-customized-plugx-malware/

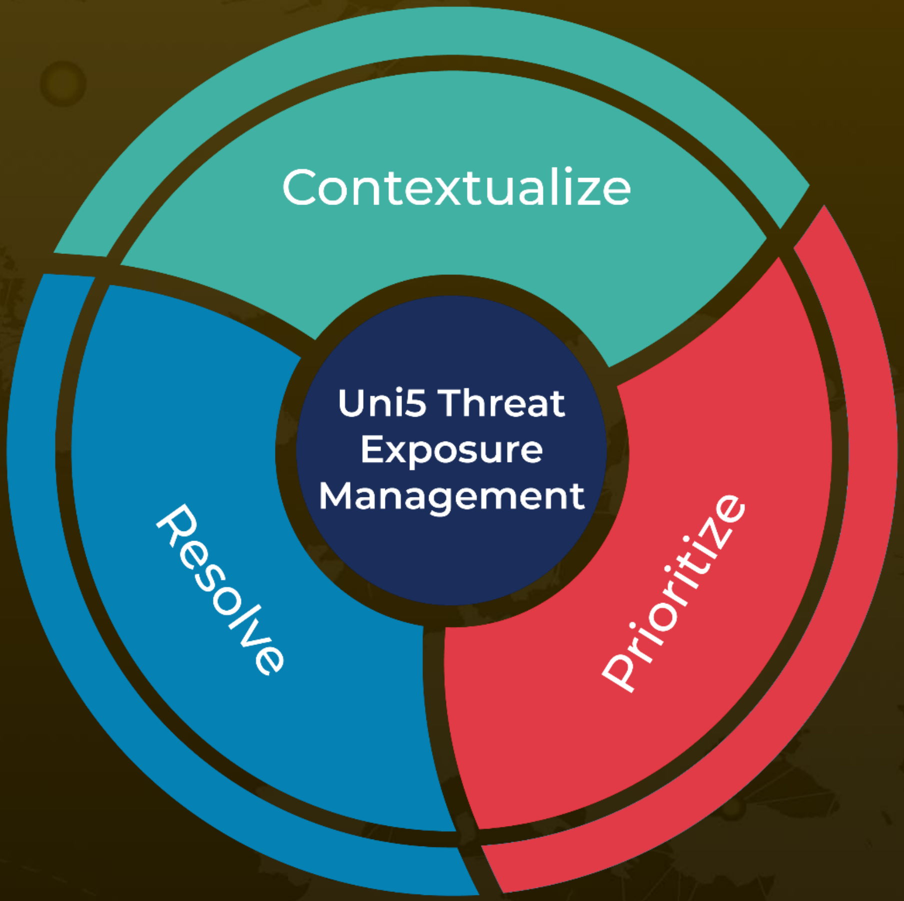
https://www.hivepro.com/budworm-attackers-return-with-new-espionage-strikes-against-the-united-states/

https://www.hivepro.com/sparklinggoblin-revamps-sidewalk-backdoor-for-linux-variant/

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

August 23, 2023 • 6:30 AM

More at www.hivepro.com