Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

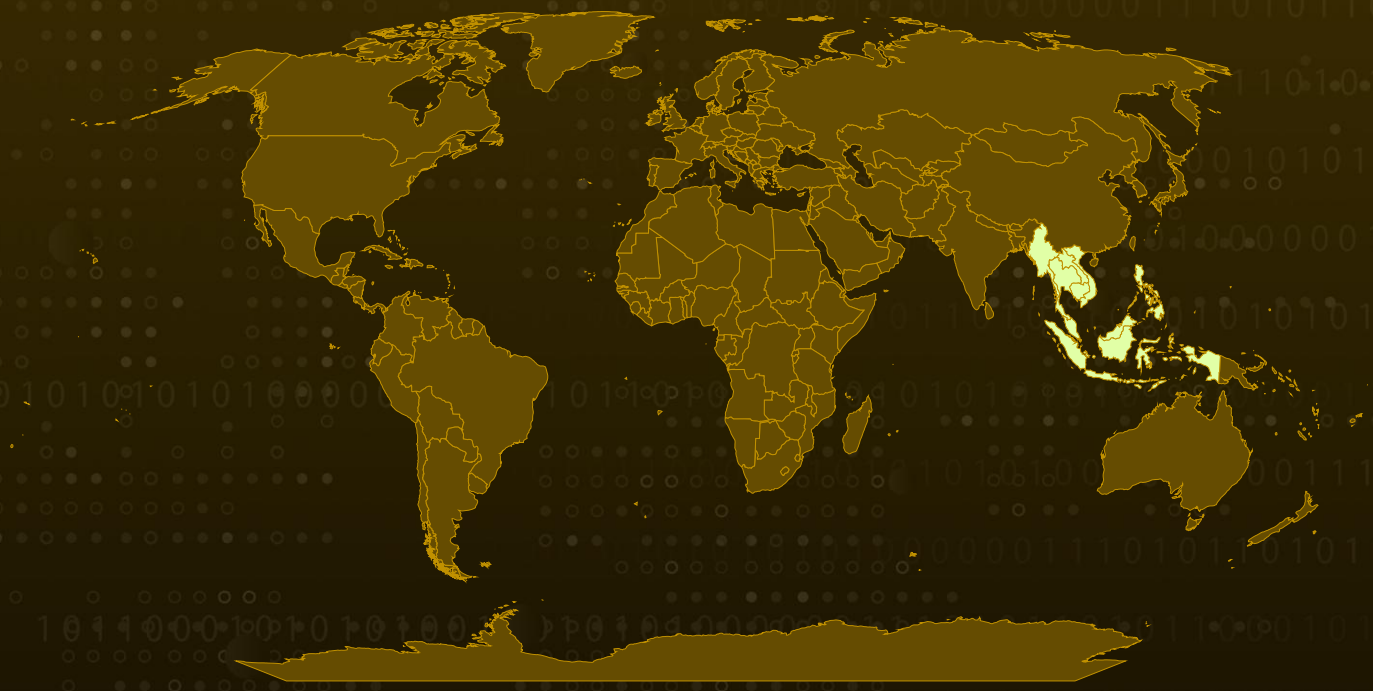
Southeast Asia Becomes a Hotspot for China-Linked Cyber Espionage

Date of Publication	Admiralty Code	TA Number
December 27, 2024	A1	TA2024476

Summary

Attack Commenced: June 2024
Malware: PlugX, Rakshasa
Targeted Countries: Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam
Targeted Industries: Government, Aviation, Telecommunication, Media
Attack: A sophisticated China-linked APT campaign targeted high-profile organizations in Southeast Asia, focusing on intelligence gathering through advanced techniques and legitimate tools to evade detection. Leveraging living-off-the-land binaries, custom malware, and secure communication proxies, the attackers demonstrated remarkable stealth and persistence.

Attack Regions



Attack Details

#1 A highly sophisticated APT operation linked to China targeted prominent organizations across Southeast Asia. The victims included government ministries, an air traffic control agency, a telecommunications provider, and a media. The primary goal was intelligence collection, achieved through advanced methods and using legitimate tools to avoid detection.

#2 The campaign began with extensive reconnaissance. The attackers employed open-source tools like Dismap and NBTScan to analyze network structures and locate vulnerabilities. Public utilities, such as FastReverseProxy (FRP), exposed internal servers to external networks, facilitating deeper infiltration.

#3 On May 27, 2024, the attackers executed a PowerShell command to modify the registry and disable Remote UAC filtering, thereby elevating privileges for remote administrative access. For payload delivery, the attackers leveraged Impacket, executing commands through Windows Management Instrumentation (WMI).

#4 A keylogger masquerading as ChromeUpdate.exe was uploaded to intercept credentials. By May 28, they had established persistence by creating registry entries and scheduled tasks, disguising malicious files as legitimate .NET framework components.

#5 The campaign heavily relied on living-off-the-land binaries (LOLBins) like PowerShell, Reg.exe, and WMI to blend malicious activities with legitimate processes. Tools such as Stowaway and Rakshasa enabled secure command-and-control (C2) communications, while the versatile remote access Trojan PlugX (Korplug) expanded their capabilities. Throughout the campaign, the attackers demonstrated persistence and precision, exfiltrating valuable intelligence over several months.

Recommendations

Enhance Network Visibility and Monitoring: Use IDS tools to monitor for unusual activity and network scans, such as those conducted by Dismap and NBTScan. Ensure critical systems are segmented from less sensitive ones to limit lateral movement in case of a breach.

Code and System Hardening: Harden systems and networks and deploy code to minimize vulnerabilities. Use code analysis and penetration testing tools to identify and address any weak points in software or websites.

Use Application Whitelisting: Implement application whitelisting to prevent unauthorized or malicious software from running on your systems, allowing only trusted applications to execute.

Zero Trust Architecture: Implement a Zero Trust security model, where all users and devices are continuously authenticated and verified, regardless of their location within the network.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery	**TA0009** Collection
TA0011 Command and Control	**TA0010** Exfiltration	**TA0043** Reconnaissance	**TA0042** Resource Development
T1595 Active Scanning	**T1595.002** Vulnerability Scanning	**T1590** Gather Victim Network Information	**T1590.006** Network Security Appliances
T1190 Exploit Public-Facing Application	**T1059** Command and Scripting Interpreter	**T1059.001** PowerShell	**T1059.003** Windows Command Shell
T1112 Modify Registry	**T1053.005** Scheduled Task	**T1047** Windows Management Instrumentation	**T1105** Ingress Tool Transfer
T1588.002 Tool	**T1588** Obtain Capabilities	**T1218** System Binary Proxy Execution	**T1027** Obfuscated Files or Information
T1056.001 Keylogging	**T1082** System Information Discovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	45[.]123[.]188[.]180, 198[.]244[.]237[.]131
IPv4:PORT	38[.]60[.]146[.]78[:]443, 118[.]107[.]219[.]66[:]443
SHA256	d312b0e1968beae5a2ff3be2d8efc6d1bfdab3b1aec6faf8eafa295c47230194, 33cb9f06338a9ea17107abbdc478071bbe097f80a835bbac462c4bb17cd0b798, 8b6d081be732743aa6f6bccfb68b3f21878aa36723c1311f50406d752aacc9fa, 89707a5bf9862a9effb1618a1a285a8d027fb343f6103f4bc68f736889f0a86e, 9fe3ff51443c41fe0be01a55a3a5fbfb261bcf63b3b0cd67f65a2c00a6d52ff3, e6cecba25abd092bfccba825298edecd2fdee6c428d9ae85399fabc54355e31f, 779b4a5f53d3128ab53dd8e13c362d6d077c3eb4987f878d7ef3416c801ef0dd, e9572549b2f35f32861ffc9be160e9c8f86e4d9d3dd43c3727f0df4dc2acc944, e0f3b8028a2969e280efdd770978a54181fc242dd26cbf0a22e922f1e6a1b951, b7472c6f6cba47ec85fa147c78f3a7a40a4fc5913fe41654ab499a7b1bd4ea2e, 3e4d86c4e1d463b99478f960c9c00f7d11cd0d1fb8dd2948e8340b7bc3550904, fb603072418da9150673ac9826a46a2b2462c8fc0afeacb2034ecb2b7d666001, 340e872c814d221989ca2cb93819b9ad307572851b5b3f8bfcf791ff08e0e677, 80c3effc8f017b26c549bed8ba82097a6be7a59e383dd35adc917bf661e0a754, 9b1794a1c8c59631d95178c7c4e2f5917b84864b342b4cfdab8f0990c3dbf5d2, ca0eeb4b71d4124dec785a9492970e9b1cfaa4cab0e8ca4486fc14b2e256d7f7,

TYPE	VALUE
SHA256	d7b85b92fb185272b89a7ff27424bff22a5a6542f6bde9838482aa9f87979828, fa6de0d0bc9d83a3942aa8b3a12a5924dc662bec32cb3c2f212a0a0c0a4ebc7a, 10029f14f2718362144b0e9b660994e8fb944af9ce9fcff04925f8b0615bb509, aa096f18e712ac0604e18d16441b672fcb393de9edf3ff4393519c48ab26a158, 386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd

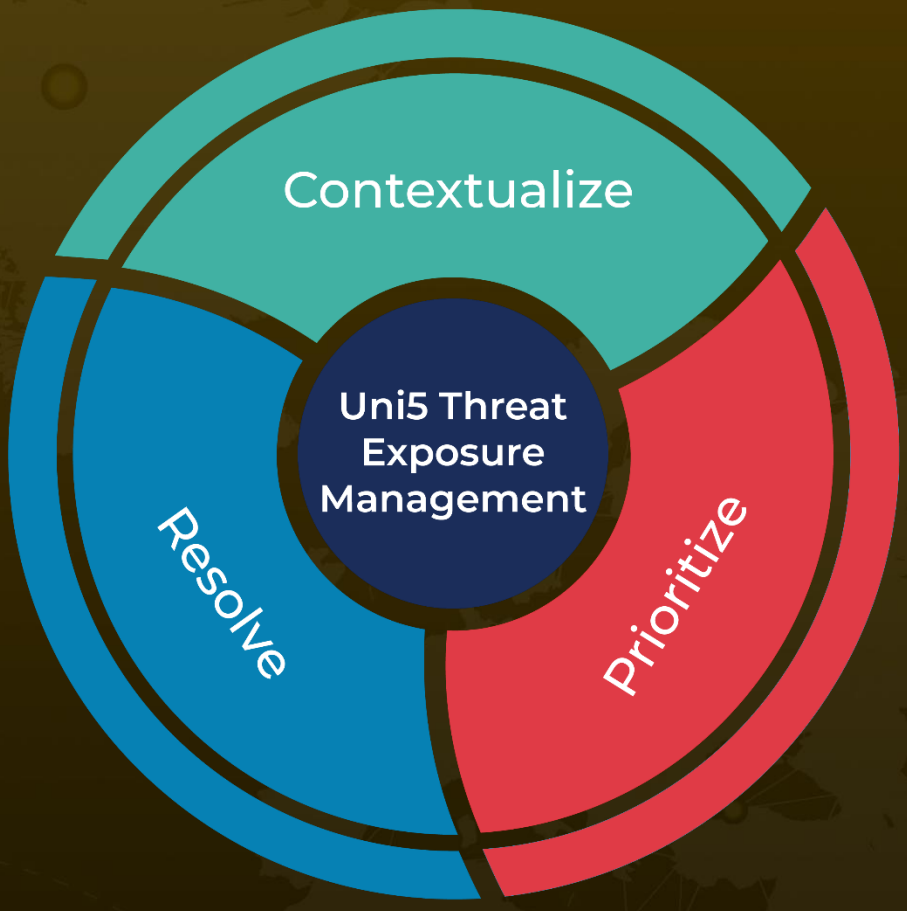
References

https://www.security.com/threat-intelligence/china-southeast-asia-espionage

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

December 27, 2024 • 7:00 AM

More at www.hivepro.com