Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

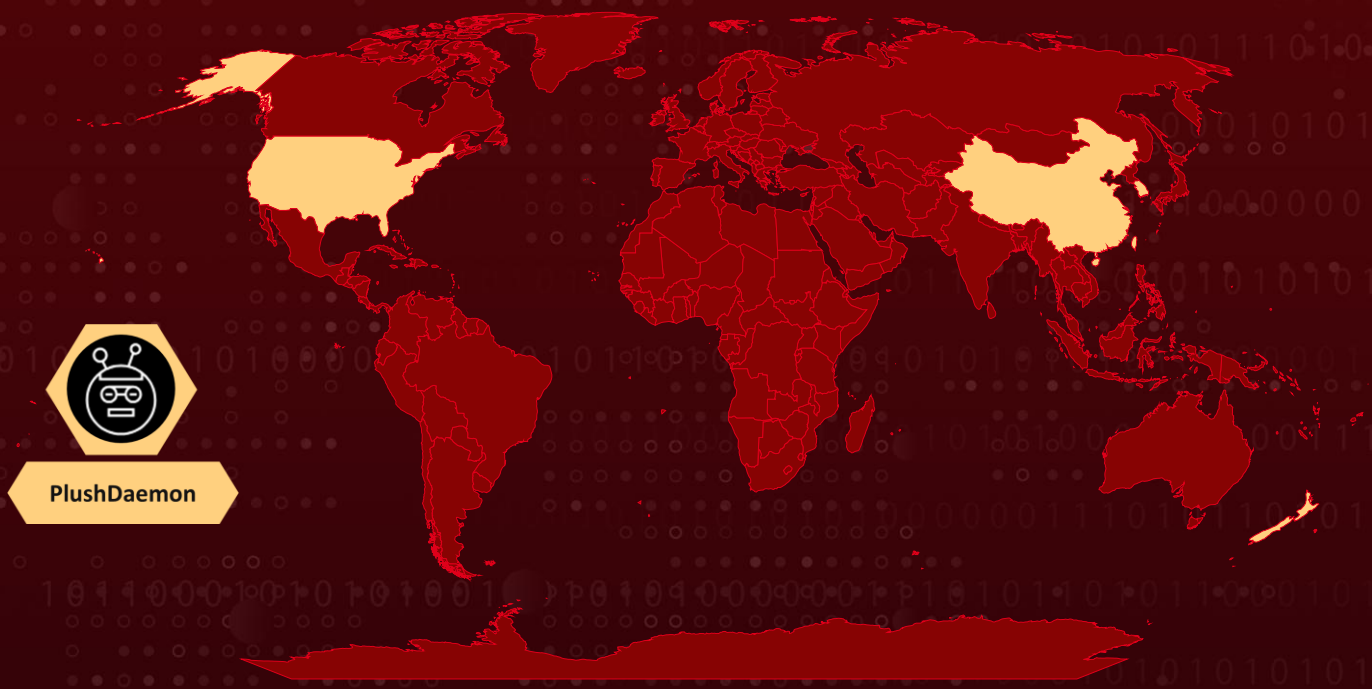
PlushDaemon's Supply Chain Heist That Shook South Korea

Date of Publication	Admiralty Code	TA Number
January 26, 2025	A1	TA2025020

Summary

Active Since: 2019
Threat Actor: PlushDaemon
Malware: SlowStepper Backdoor
Targeted Countries: South Korea, China, Taiwan, Hong Kong, United States, New Zealand
Attack: PlushDaemon, an elusive China-aligned APT group active since 2019, is making waves with its stealthy supply-chain attacks, including a bold 2023 operation targeting a South Korean VPN provider. Leveraging their custom backdoor, SlowStepper, a modular implant packed with over 30 components, the group demonstrates cutting-edge expertise in cyber espionage.

Attack Regions



Attack Details

#1 PlushDaemon, a China-aligned advanced persistent threat (APT) group active since at least 2019, orchestrated a supply-chain attack in 2023 targeting a South Korean VPN provider. The attackers replaced the legitimate VPN installer with a trojanized version, embedding their custom backdoor, SlowStepper.

#2 SlowStepper is a sophisticated implant featuring over 30 components, developed using C++, Python, and Go, showcasing the group's technical expertise. The group primarily engages in cyberespionage against targets in China, Taiwan, Hong Kong, South Korea, the United States, and New Zealand.

#3 PlushDaemon gains initial access through two primary methods: compromising legitimate software updates (notably those of Chinese applications) and exploiting vulnerabilities in web servers. In May 2024, PlushDaemon compromised the VPN installer from the South Korean firm IPany, deploying malware onto victims' devices.

#4 The attack chain begins with the execution of the installer, which establishes persistence on the host system. It then triggers a loader responsible for executing shellcode to load another DLL. This DLL extracts two additional files, ultimately sideloading a malicious DLL to deploy the SlowStepper implant.

#5 SlowStepper has been under development since January 2019, with its latest version, 0.2.12, compiled in June 2024. The version used in the IPany VPN supply-chain compromise, identified as 0.2.10 Lite, retains hundreds of functions, highlighting its modular and adaptable nature.

Recommendations

Implement Strict Software Integrity Checks: Verify the authenticity of all software updates and installers by using cryptographic signatures and validating them against known sources.

Enhance Vendor Security Assessments: Conduct thorough security evaluations of third-party vendors and partners to ensure their systems and processes meet robust security standards.

Implement Network Segmentation: Limit lateral movement by isolating critical systems and services from general network access. Strengthen VPN security by regularly auditing and patching VPN software to address known vulnerabilities and prevent exploitation.

Utilize Micro-Segmentation for High-Risk Systems: Go beyond traditional network segmentation by applying micro-segmentation to critical systems and high-value assets. This granular approach limits the spread of attacks by creating isolated zones within the network, making it harder for attackers to move laterally.

Implement One-Time Software Installation Tokens: Use time-limited, one-time tokens for software installations or updates, ensuring that even if an attacker compromises the installer, the installation process will only be valid for a brief window, reducing the window of opportunity for exploitation.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1583.001** Domains	**T1583.004** Server	**T1608** Stage Capabilities
T1608.001 Upload Malware	**T1608.002** Upload Tool	**T1588** Obtain Capabilities	**T1588.001** Malware
T1588.002 Tool	**T1588.003** Code Signing Certificates	**T1588.005** Exploits	**T1659** Content Injection
T1190 Exploit Public-Facing Application	**T1195** Supply Chain Compromise	**T1195.002** Compromise Software Supply Chain	**T1059** Command and Scripting Interpreter
T1059.003 Windows Command Shell	**T1059.006** Python	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder

T1547.004 Winlogon Helper DLL	**T1574** Hijack Execution Flow	**T1574.002** DLL Side-Loading	**T1222** File and Directory Permissions Modification
T1222.001 Windows File and Directory Permissions Modification	**T1070** Indicator Removal	**T1070.004** File Deletion	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1112** Modify Registry	**T1027** Obfuscated Files or Information	**T1027.007** Dynamic API Resolution
T1027.009 Embedded Payloads	**T1027.013** Encrypted/Encoded File	**T1553** Subvert Trust Controls	**T1553.002** Code Signing
T1217 Browser Bookmark Discovery	**T1083** File and Directory Discovery	**T1120** Peripheral Device Discovery	**T1057** Process Discovery
T1012 Query Registry	**T1518** Software Discovery	**T1082** System Information Discovery	**T1614** System Location Discovery
T1016 System Network Configuration Discovery	**T1016.002** Wi-Fi Discovery	**T1033** System Owner/User Discovery	**T1560** Archive Collected Data
T1560.002 Archive via Library	**T1123** Audio Capture	**T1005** Data from Local System	**T1074.001** Local Data Staging
T1113 Screen Capture	**T1125** Video Capture	**T1071.004** DNS	**T1132.001** Standard Encoding
T1573.001 Symmetric Cryptography	**T1008** Fallback Channels	**T1105** Ingress Tool Transfer	**T1104** Multi-Stage Channels
T1095 Non-Application Layer Protocol	**T1090** Proxy	**T1219** Remote Access Software	**T1020** Automated Exfiltration
T1041 Exfiltration Over C2 Channel	**T1583** Acquire Infrastructure		

Indicators of Compromise (IOCs)

TYPE	VALUE
File Name	AutoMsg.dll, lregdll.dll, OldLJM.dll, svcghost.exe, main.dll, IPanyVPNsetup .exe
URL	hxxps[:]//ipany[.]kr/download/IPanyVPNsetup[.]zip
IPv4	202[.]189[.]8[.]72, 47[.]96[.]17[.]237, 202[.]105[.]1[.]187, 47[.]74[.]159[.]166, 8[.]130[.]87[.]195, 47[.]108[.]162[.]218, 47[.]113[.]200[.]18, 47[.]104[.]138[.]190, 120[.]24[.]193[.]58, 202[.]189[.]8[.]87, 202[.]189[.]8[.]69, 202[.]189[.]8[.]193, 47[.]92[.]6[.]64
SHA1	a8ae42884a8edfa17e9d67ae5bebe7d196c3a7bf, 2db60f0adef14f4ab3573f8309e6fb135f67ed7d, 846c025f696da1f6808b9101757c005109f3cf3d, ad4f0428fc9290791d550eeddf171aff046c4c2c, 401571851a7cf71783a4cb902db81084f0a97f85, 068fd2d209c0bbb0c6fc14e88d63f92441163233

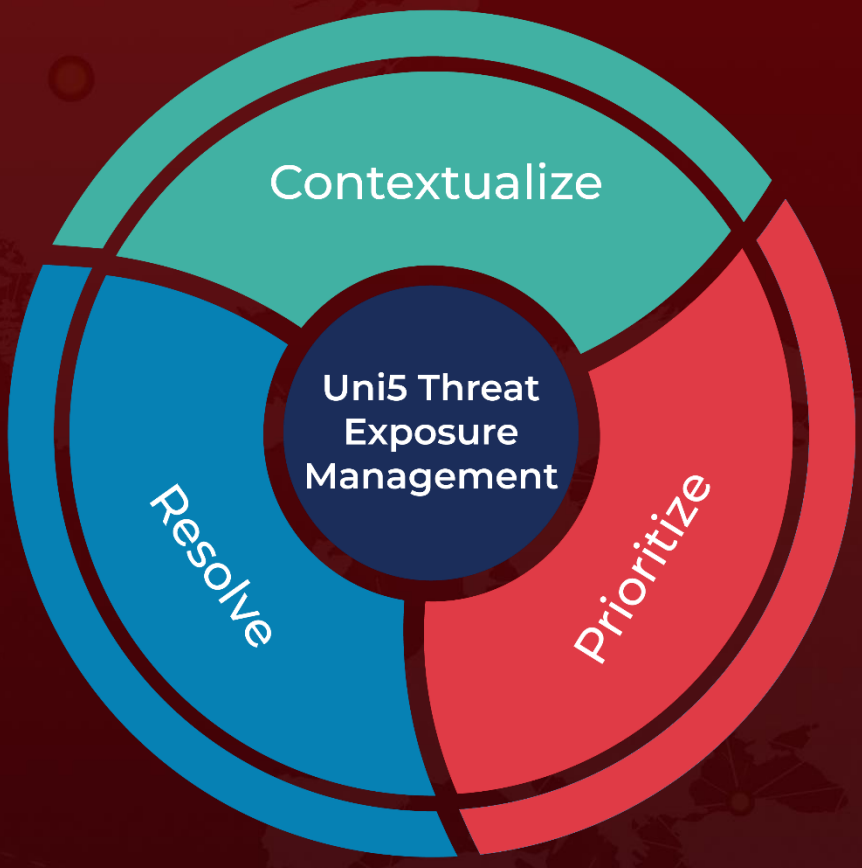
References

https://www.welivesecurity.com/en/eset-research/plushdaemon-compromises-supply-chain-korean-vpn-service/

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

January 26, 2025 . 8:30 PM

More at www.hivepro.com