Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

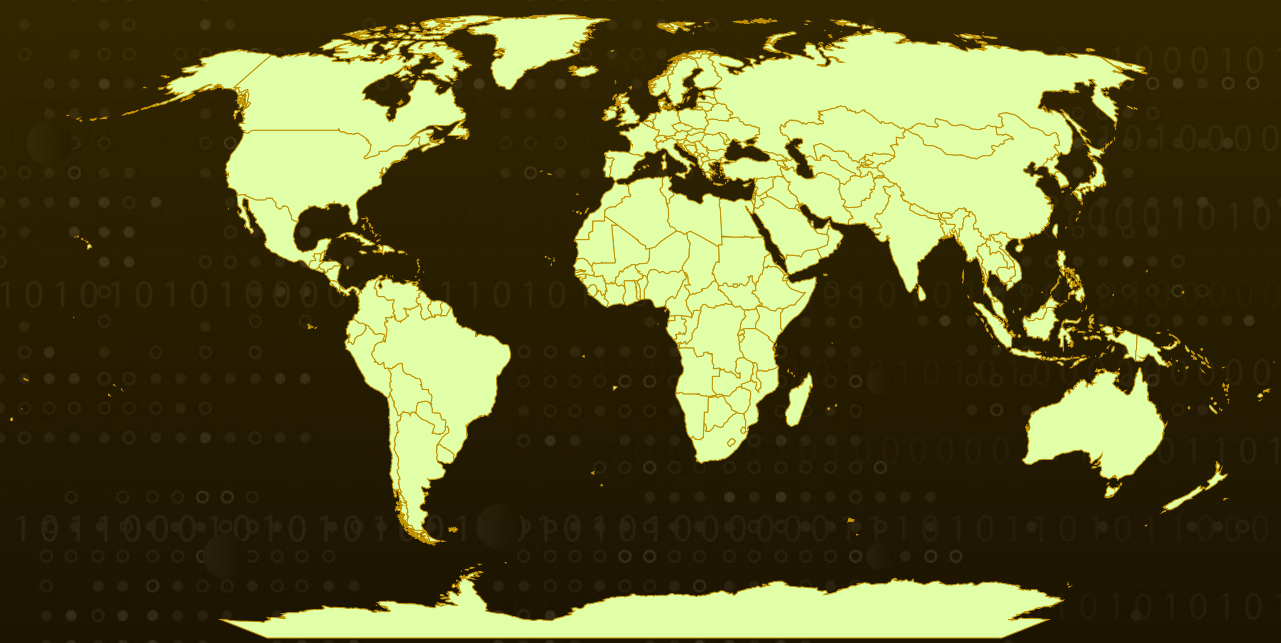
Scripted Deception: NimDoor Malware Unfolds in Fake Zoom Update

Date of Publication	Admiralty Code	TA Number
July 3, 2025	A1	TA2025205

Summary

Attack Commenced: April 2025
Targeted Countries: Worldwide
Affected Platform: macOS
Targeted Industries: Technology, Cryptocurrency
Malware: NimDoor
Attack: In a targeted cyberattack in April 2025, a North Korea-linked threat group exploited social engineering tactics to breach a macOS system. Posing as a trusted contact on Telegram, the attackers tricked the victim into running a fake “Zoom SDK update” script. This kicked off a sophisticated infection chain that dropped custom malware written in Nim and C++. Dubbed NimDoor, the malware leveraged AppleScript, encrypted communication, and clever persistence tricks to maintain access and steal sensitive information. By blending in with legitimate system tools and using deceptive names the attackers aimed to silently stay embedded for long-term surveillance and data theft.

Attack Regions



Attack Details

#1 In April 2025, a targeted cyberattack on a Web3 startup was linked to a North Korean state-backed threat group. While the early stages mirrored the group's typical social engineering playbook, the technical execution on macOS showcased new sophistication. What stood out most was the use of Nim, a rarely seen but increasingly favored programming language among threat actors, to compile multiple payloads. This added complexity helped the attackers evade detection and implement advanced capabilities like encrypted configurations, asynchronous execution, and a signal-based persistence mechanism. The malware family, dubbed NimDoor, reflects these distinct traits.

#2 The attack began with a deceptive outreach over Telegram, where the victim was lured into scheduling a Zoom meeting via a legitimate-looking Calendly link. Soon after, the attacker emailed them a supposed Zoom SDK update script, which was a malicious AppleScript hosted on a spoofed domain resembling Zoom's infrastructure. This script quietly contacted a command-and-control (C2) server and pulled down additional payloads. One clever touch: the downloaded HTML file included a real Zoom redirect to maintain the illusion of legitimacy while executing the core logic in the background.

#3 The infection process was staged and modular. Two Mach-O binaries were dropped into the system's temporary directories, one compiled in C++ to deploy an encrypted payload, and the other in Nim to handle persistence. The Nim-based installer deployed two additional components, Google LLC and CoreKitAgent, both designed to maintain long-term access and avoid suspicion. By using folder paths and filenames resembling legitimate Apple software and misspelling names to trick cursory inspection, the attackers ensured their malware blended into the macOS environment.

#4 The final payload, CoreKitAgent, was the most advanced component. It was designed to operate as a persistent, event-driven backdoor using macOS's low-level kqueue mechanism. The binary was equipped to capture system signals like SIGINT and SIGTERM to reinstall itself if interrupted. Its code, controlled by a table-driven state machine, included anti-sandbox techniques like timed sleep cycles and runtime string deobfuscation. It also embedded a concealed AppleScript that beacons to its C2 every 30 seconds, fetching and executing commands silently in the background.

#5 This campaign reflects an ongoing trend, advanced threat actors are moving toward lesser-known languages like Nim to evade traditional detection methods and improve cross-platform support. By combining compiled binaries with native scripting like AppleScript and using deception at every layer, from filenames to network traffic, attackers are raising the bar for defenders. Security teams must deepen their understanding of niche languages and macOS internals to detect and analyze such threats effectively in the future.

Recommendations

- **Be Vigilant:** If someone especially over Telegram or email ends you a script or asks you to run a Zoom "update," double-check through a known, trusted channel before doing anything. Threat actors often impersonate trusted contacts to lower your guard.
- **Avoid downloading scripts or software from unknown links:** Only install Zoom updates or other software directly from official websites. Attackers often host fake update scripts on lookalike domains, hoping you'll click without verifying the source.
- **Keep an eye on your system folders and LaunchAgents:** The malware in this attack hides in folders like ~/Library/Application Support and sets up persistence through LaunchAgents. Regularly monitor these locations for unknown or suspicious files and plist entries.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0006 Credential Access	**TA0007** Discovery	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1566** Phishing	**T1566.002** Spearphishing Link	**T1059** Command and Scripting Interpreter
T1059.002 AppleScript	**T1027** Obfuscated Files or Information	**T1217** Browser Information Discovery	**T1074** Data Staged

T1055 Process Injection	**T1573** Encrypted Channel	**T1573.001** Symmetric Cryptography	**T1132** Data Encoding
T1132.001 Standard Encoding	**T1555** Credentials from Password Stores	**T1555.001** Keychain	**T1041** Exfiltration Over C2 Channel
T1140 Deobfuscate/Decode Files or Information	**T1057** Process Discovery	**T1082** System Information Discovery	**T1656** Impersonation

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	dataupload[.]store, firstfromsep[.]online, safeup[.]store, support[.]us05web-zoom[.]pro, writeup[.]live
File Paths	~/Library/Application Support/Google LLC/Google LLC, ~/Library/LaunchAgents/com.google.update.plist, ~/.ses, ~/Library/CoreKit/CoreKitAgent, ~/Library/DnsService/a, ~/Library/DnsService/netchk, /private/tmp/.config, /private/tmp/cfg, /private/var/tmp/uplex_//
SHA1	027d4020f2dd1eb473636bc112a84f0a90b6651c, 0602a5b8f089f957eeda51f81ac0f9ad4e336b87, 06566eabf54caafe36ebe94430d392b9cf3426ba, 08af4c21cd0a165695c756b6fda37016197b01e7, 16a6b0023ba3fde15bd0bba1b17a18bfa00a8f59, 1a5392102d57e9ea4dd33d3b7181d66b4d08d01d, 2c0177b302c4643c49dd7016530a4749298d964c, 2d746dda85805c79b5f6ea376f97d9b2f547da5d, 2ed2edec8ccc44292410042c730c190027b87930, 3168e996cb20bd7b4208d0864e962a4b70c5a0e7,

TYPE	VALUE
SHA1	5b16e9d6e92be2124ba496bf82d38fb35681c7ad, 7c04225a62b953e1268653f637b569a3b2eb06f8, 945fcd3e08854a081c04c06eeb95ad6e0d9cdc19, a25c06e8545666d6d2a88c8da300cf3383149d5a, c9540dee9bdb28894332c5a74f696b4f94e4680c, e227e2e4a6ffb7280dfe7618be20514823d3e4f5, ee3795f6418fc0cacbe884a8eb803498c2b5776f, 023a15ac687e2d2e187d03e9976a89ef5f6c1617, bb72ca0e19a95c48a9ee4fd658958a0ae2af44b6, 4743d5202dbe565721d75f7fb1eca43266a652d4, 1e76f497051829fa804e72b9d14f44da5a531df8, 79f37e0b728de2c5a4bfe8fcf292941d54e121b8

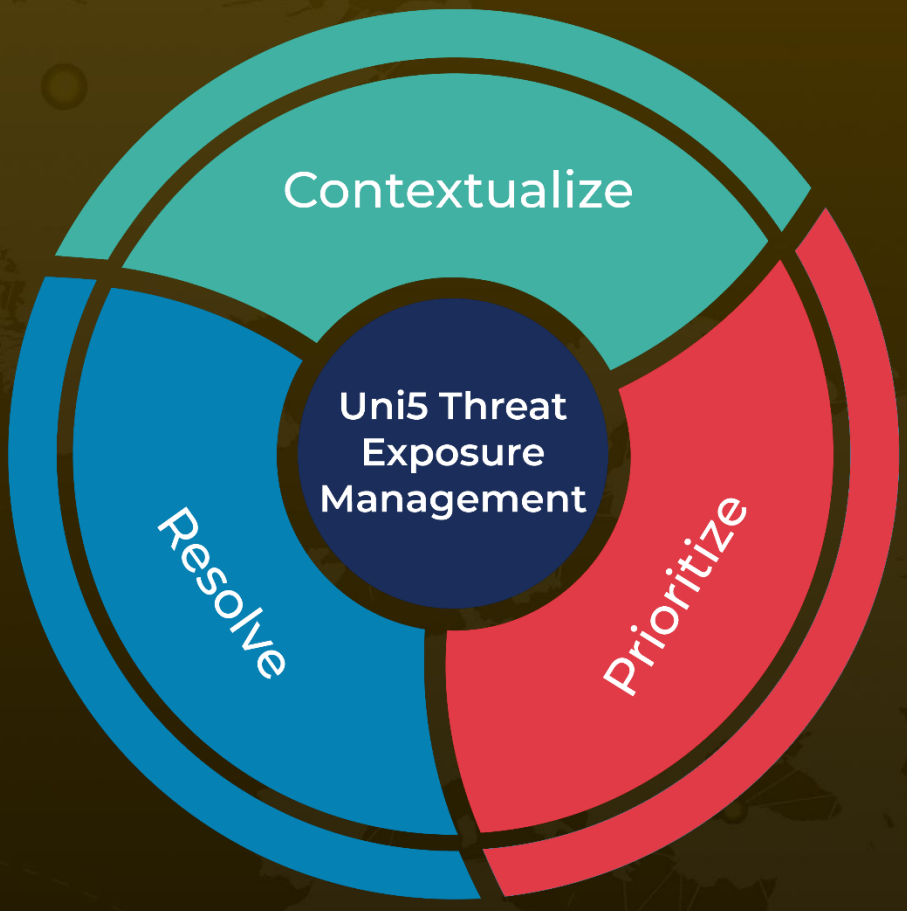
References

https://www.sentinelone.com/labs/macos-nimdoor-dprk-threat-actors-target-web3-and-crypto-platforms-with-nim-based-malware/

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

July 3, 2025 • 7:40 AM

More at www.hivepro.com