Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

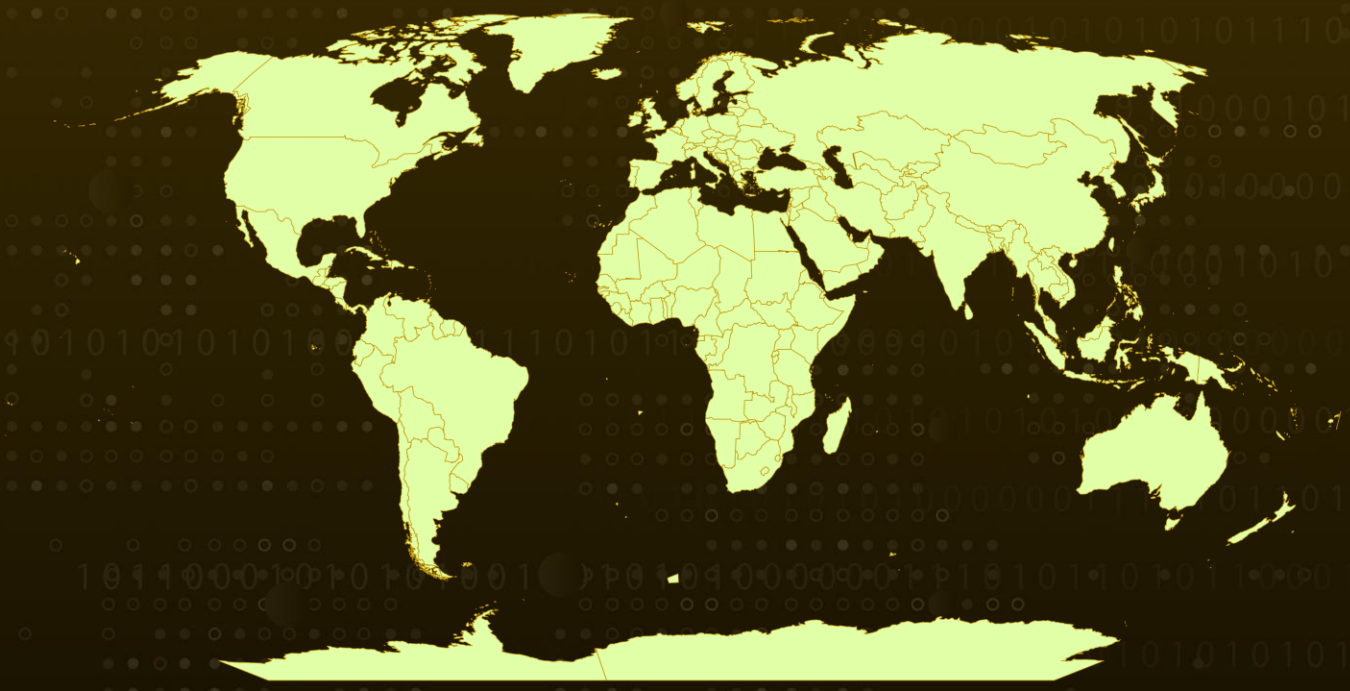
North Korean Hackers Target Crypto Users with RustBucket and KandyKorn

Date of Publication	Admiralty Code	TA Number
November 28, 2023	A1	TA2023479

Summary

First appeared: 2023
Attack Region: Worldwide
Threat Actor: North Korean threat actors
Malware: RustBucket, SwiftLoader, ObjCShellz and KandyKorn
Affected Platforms: macOS
Targeted Industries: Cryptocurrency, Financial
Attack: North Korean-aligned threat actors are targeting macOS users with two malware frameworks, RustBucket and KandyKorn, in an attempt to steal cryptocurrency.

Attack Regions



Attack Details

#1

In 2023, North Korean-aligned threat actors have been actively targeting macOS users with the goal of stealing cryptocurrency in two major malware campaigns RustBucket and KandyKorn. However, they use different techniques to achieve this goal. The RustBucket campaign involved a second-stage malware called 'SwiftLoader,' disguised as a PDF Viewer in lure documents. KandyKorn, on the other hand, targeted blockchain engineers through an elaborate multi-stage operation, using Python scripts to drop malware and a backdoor RAT named 'KandyKorn.'

#2

Recent activities indicate a blending of components from these campaigns, with SwiftLoader droppers now delivering KandyKorn payloads. The KandyKorn operation involved a sophisticated five-stage attack using social engineering on Discord to distribute malicious Python applications. This included the use of SUGARLOADER, which downloaded a C2 configuration file and executed a remote access trojan (RAT) named HLOADER.

#3

In RustBucket, North Korean threat actors utilized AppleScript and Swift-based applications, such as 'Internal PDF Viewer.app,' employing specially crafted PDFs to unlock a Rust-based payload. Variants like 'SecurePDF Viewer.app' were later identified, signed and notarized by Apple, and capable of running on both Intel and Apple silicon devices.

#4

The SwiftLoader connection to KandyKorn RAT is highlighted, with overlaps found between versions of SwiftLoader and the KandyKorn operation. An analysis revealed a hardcoded URL reaching out to 'on-global.xyz' and dropping a hidden executable at '/Users/Shared/.pw.' This executable appears to interact with a C2, referencing '/Users/Shared/.pld,' which is associated with the KandyKorn RAT.

#5

The analysis establishes connections between ObjCShellz payloads and SwiftLoader stagers, indicating shared infrastructure. It suggests that RustBucket droppers and KandyKorn payloads may be part of the same infection chain. The findings emphasize the tendency of North Korean threat actors to reuse infrastructure, allowing for a broader understanding of their activities and the discovery of new indicators of compromise.

Recommendations

Enhanced Cybersecurity Measures: Implement robust cybersecurity measures, including up-to-date antivirus software, firewalls, intrusion detection systems, and secure network configurations. Regular security updates and patches for all software and operating systems should be applied promptly to mitigate vulnerabilities.

Endpoint Security: Deploy robust endpoint security solutions that include advanced threat detection capabilities. Ensure these solutions are regularly updated to recognize and mitigate emerging threats, such as RustBucket and KandyKorn.

Be careful what you click on: Don't click on links or open attachments in emails from people you don't know or trust. And be careful what you click on when you're browsing the web.

Use strong passwords and two-factor authentication (2FA): This will make it more difficult for attackers to access your cryptocurrency wallets.

Store your cryptocurrency in a secure wallet: There are two main types of cryptocurrency wallets: hot wallets and cold wallets. Hot wallets are connected to the internet, which makes them more susceptible to attack. Cold wallets are not connected to the internet, which makes them more secure. If you have a large amount of cryptocurrency, you should store it in a cold wallet.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0011 Command and Control	TA0002 Execution	TA0005 Defense Evasion
TA0003 Persistence	TA0001 Initial Access	T1059.002 AppleScript	T1059 Command and Scripting Interpreter
T1496 Resource Hijacking	T1059.006 Python	T1036.003 Rename System Utilities	T1036 Masquerading
T1204.002 Malicious File	T1566 Phishing	T1204 User Execution	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	1c817e846021bef433701a9815f906e8, 470275eaf344be97f9950c4c42a783ef, 9294648d744703cfa0456ec74d014fe4, 973225dc83f568ef6208d49fe2648fc0, 9ca5df575e5bd60035202dabd67b7af2
SHA1	060a5d189ccf3fc32a758f1e218f814f6ce81744, 09ade0cb777f4a4e0682309a4bc1d0f7d4d7a036, 26ec4630b4d1116e131c8e2002e9a3ec7494a5cf, 3c887ece654ea46b1778d3c7a8a6a7c7c7cfa61c, 43f987c15ae67b1183c4c442dc3b784faf2df090, 46ac6dc34fc164525e6f7886c8ed5a79654f3fd3, 5c93052713f317431bf232a2894658a3a4ebfad9, 62267b88fa6393bc1f1eeb778e4da6b564b7011e, 79337ccda23c67f8cfd9f43a6d3cf05fd01d1588, 884cebf1ad0e65f4da60c04bc31f62f796f90d79, 8d5d214c490eae8f61325839fcc17277e514301e, 8f6c52d7e82fbfdead3d66ad8c52b372cc9e8b18, 9f97edbc1454ef66d6095f979502d17067215a9d, a1a8a855f64a6b530f5116a3785a693d78ec09c0, ac336c5082c2606ab8c3fb023949dfc0db2064d5, be903ded39cbc8332cefd9ebbe7a66d95e9d6522, c45f514a252632cb3851fe45bed34b175370d594, c806c7006950dea6c20d3d2800fe46d9350266b6, ce3705baf097cd95f8f696f330372dd00996d29a, d28830d87fc71091f003818ef08ff0b723b3f358, e244ff1d8e66558a443610200476f98f653b8519, e275deb68cdff336cb4175819a09dbaf0e1b68f6, e68bfa72a4b4289a4cc688e81f9282b1f78ebc1f, e77270ac0ea05496dd5a2fbccba3e24eb9b863d9
IPv4	104[.]168[.]214[.]151, 142[.]11[.]209[.]144, 192[.]119[.]64[.]43, 23[.]254[.]226[.]90

TYPE	VALUE
SHA256	2360a69e5fd7217e977123c81d3dbb60bf4763a9dae6949bc1900234f7762df1, 2ade7f8def7eceba3e8f0e5d29d0a19626bfc595aeb1ed95b7404210569c6304, 3ea2ead8f3cec030906dcbffe3efd5c5d77d5d375d4a54cca03bfe8a6cb59940, 8a8de435d71cb0b0ae6d4b15d58b7c85ce3ef8f06b24266c52b2bc49217be257, 8bfa4fe0534c0062393b6a2597c3491f7df3bf2eabfe06544c53bdf1f38db6d4, 927b3564c1cf884d2a05e1d7bd24362ce8563a1e9b85be776190ab7f8af192f6
Domains	on-global[.]xyz, swissborg[.]blog, tp-globa[.]xyz

References

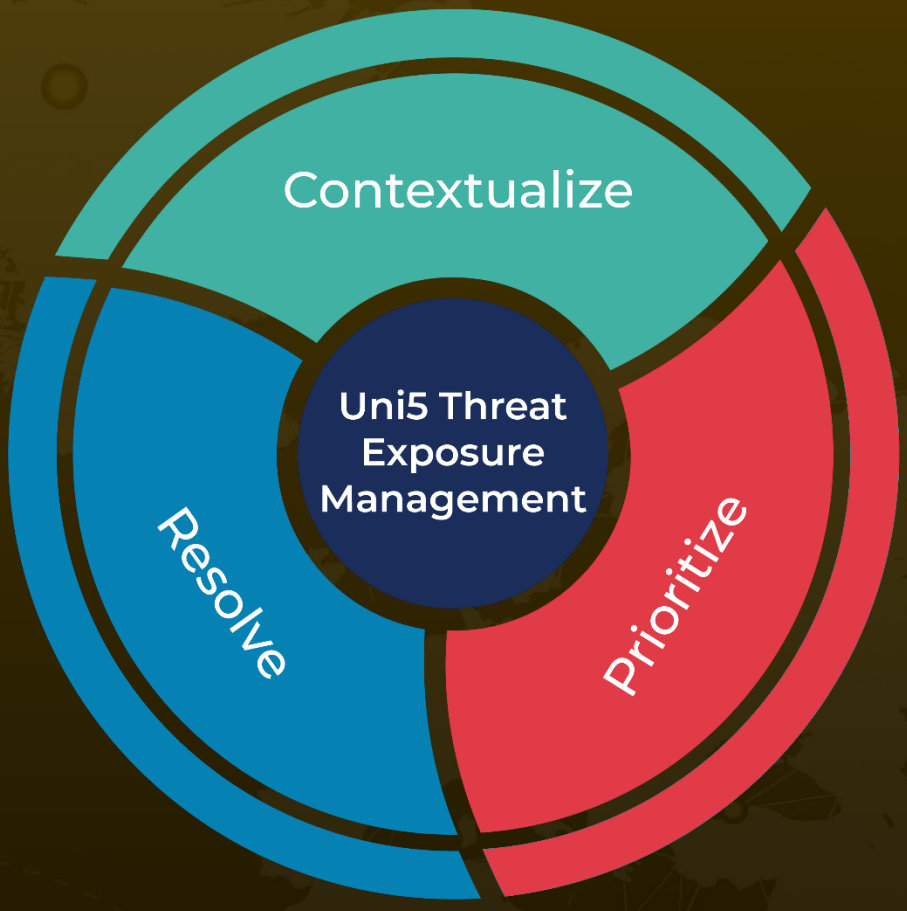
https://www.sentinelone.com/blog/dprk-crypto-theft-macos-rustbucket-droppers-pivot-to-deliver-kandykorn-payloads/

https://www.hivepro.com/threat-advisory/bluenoroff-unleashes-new-macos-malware-objcshellz/

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

November 28, 2023 • 4:30 AM

More at www.hivepro.com