Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

BlueNoroff Unleashes New macOS Malware ObjCShellz

Date of Publication	Admiralty Code	TA Number
November 8, 2023	A1	TA2023450

Summary

First appeared: May 31, 2023
Attack Region: Worldwide
Affected Platform: macOS
Threat Actor: BlueNorOff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet, TAG-71)
Malware: ObjCShellz, RustBucket
Targted Industries: Cryptocurrency, Financial
Attack: A new macOS malware variant linked to the financially motivated BlueNoroff APT group, named "ObjCShellz," featuring remote shell capabilities and suspicious domain communication. The malware, written in Objective-C, serves as a late-stage tool within multi-stage RustBucket campaign, maintaining functionality and potentially evading detection.

Attack Regions

Attack Details

#1 A new macOS malware variant linked to the BlueNoroff group, known for financially motivated cyberattacks. This malware, named "ObjCShellz," shares similarities with the RustBucket campaign and was discovered communicating with a suspicious domain, swissborg[.]blog. The malicious domain resembles legitimate crypto-related sites, a tactic commonly used by BlueNoroff to blend in with network activity.

#2 The malware, written in Objective-C, operates as a remote shell, enabling attackers to execute commands on compromised systems. It communicates with its command-and-control server using a POST request, providing information about the victim's macOS version. Despite its simplicity, the malware fulfills its intended functionality, serving as a late-stage tool for attackers within multi-stage malware campaigns.

#3 The malware's main function initializes periodic network requests through a timer to ensure continuous operation, indicating its potential use in ongoing attacks. The malware was undetected by antivirus solutions at the time of analysis, suggesting an attempt to evade detection.

#4 The malicious domain, swissborg[.]blog, was registered in 2023 and points to an IP address previously associated with BlueNoroff's activities. The analysis uncovered submissions to VirusTotal from countries like Japan and the US, indicating potential global distribution.

#5 While this malware's design is relatively straightforward, its operational capabilities support attackers in their objectives. Additionally, the FBI linked BlueNorOff and Lazarus Group, another North Korean hacker collective, to a significant crypto heist involving the Axie Infinity's Ronin network bridge. The hackers made off with a substantial amount of Ethereum and USDC tokens, underlining the group's sophisticated and financially motivated cyber activities.

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: Use endpoint security solutions that can detect and prevent the execution of malicious files and scripts. These solutions can help stop malware like Lu0Bot from infecting endpoints.

Monitoring and Threat Detection: Employ advanced threat detection tools and continuously monitor networks for unusual or suspicious activities. This includes monitoring network traffic for any communication with domains resembling legitimate sites and identifying potentially malicious payloads.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0010 Exfiltration	TA0011 Command and Control	TA0002 Execution
TA0040 Impact	TA0042 Resource Development	T1583 Acquire Infrastructure	T1583.001 Domains
T1059 Command and Scripting Interpreter	T1204 User Execution	T1204.001 Malicious Link	T1588.001 Malware
T1588 Obtain Capabilities	T1020 Automated Exfiltration	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	104.168.214[.]151
SHA1	588d84953ae992c5de61d3774ce86e710ed42d29, 677b119edfa1335b6eb9b7307b034bee512dbc1a, 79337ccda23c67f8cfd9f43a6d3cf05fd01d1588, 8dc95be0cf52c64e3d6c519e356b0c3f0d729bd4, bc33f1a6c345e0452056ec08d25611b85c350b2e, e2af7a895aef936c2761289acafe564b4dc7ba4e
URLs	http://swissborg.blog/ghjk/yuio, http://swissborg.blog/qwertyuiop/asdfghjkl, http://swissborg.blog/tx/10299301992/hash, http://swissborg.blog/zxcv/bnm
Domains	blockfi[.]loans, cryptyk[.]info, gumi-cryptos[.]loan, swissborg[.]blog
Hostname	asset[.]crypto-ecosystem[.]world, bico[.]tokentracking[.]info, cnbc[.]crypto-ecosystem[.]world, crypto[.]blockchainworld[.]info, daiwa[.]azure-defender[.]cloud, defi[.]smart-contracts[.]blog, docs[.]panteracapital[.]ventures, internal-server[.]nextera[.]capital, internal[.]daiwa[.]ventures, recent[.]bico-news[.]blog, exceptions[.]coinbase[.]expublic[.]linkpc[.]net, google[.]coinbase[.]expublic[.]linkpc[.]net, coinbase[.]expublic[.]linkpc[.]net

References

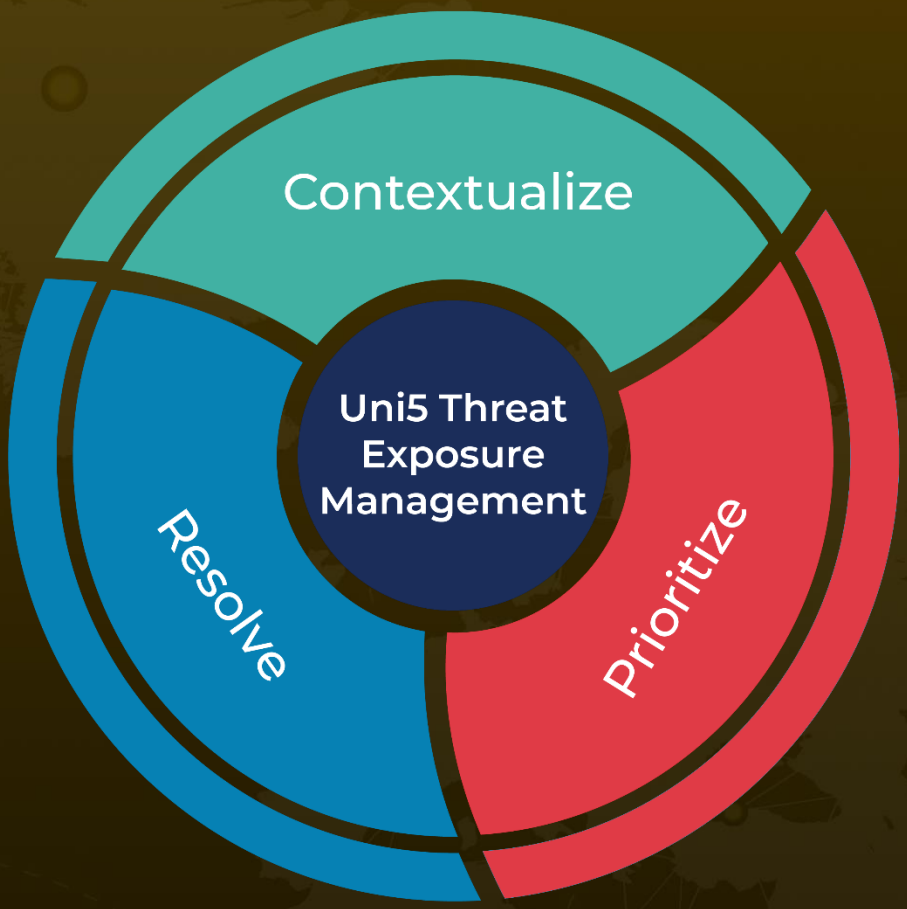
https://www.jamf.com/blog/bluenoroff-strikes-again-with-new-macos-malware/

https://www.hivepro.com/new-macos-malware-rustbucket-attributed-to-north-korean-group-bluenoroff/

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 8, 2023 • 4:30 AM

More at www.hivepro.com