Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

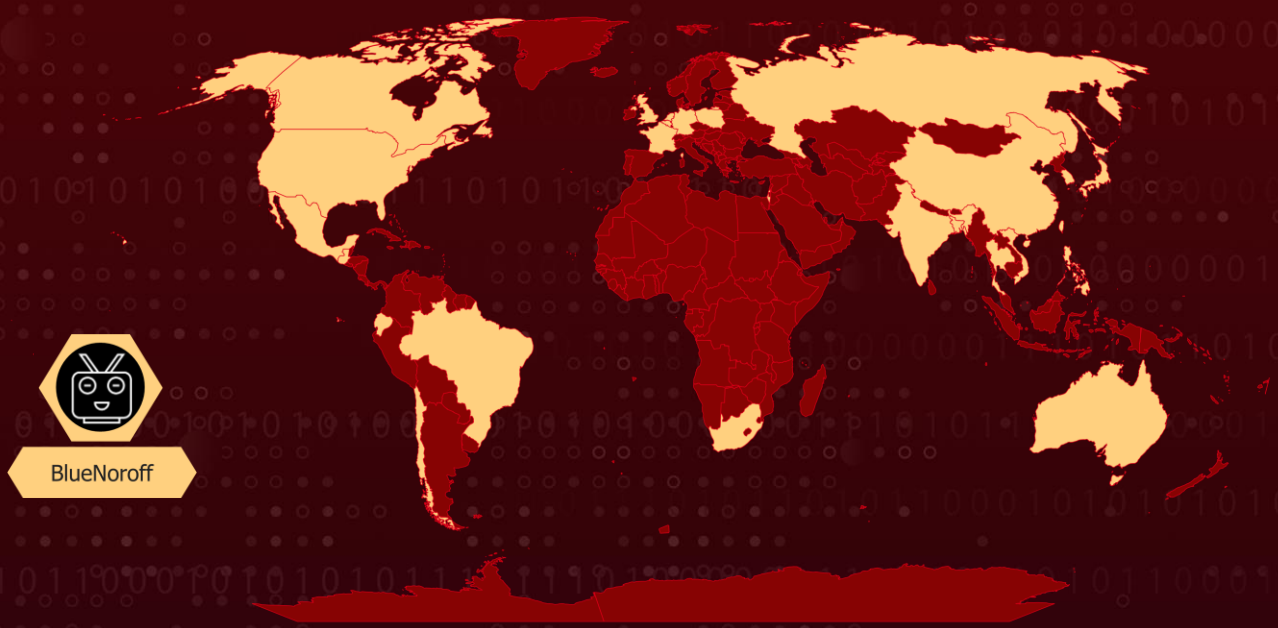
New macOS malware RustBucket attributed to North Korean group BlueNoroff

Date of Publication	Admiralty Code	TA Number
April 28, 2023	A1	TA2023204

Summary

Attack began: January 2023
Threat Actor: BlueNoroff (APT 38, Stardust Chollima, CTG-6459, Nickel Gladstone, TEMP.Hermit, T-APT-15, ATK 117, Black Alicanto, Copernicium, TA444, Sapphire Sleet)
Attack Countries: Australia, Bangladesh, Belgium, Brazil, Canada, Chile, China, Ecuador, France, Germany, Guatemala, Hong Kong, India, Israel, Japan, Mexico, Netherlands, Philippines, Poland, Russia, South Africa, South Korea, Taiwan, Thailand, UK, USA, Vietnam
Attack Industry: Aerospace, Defense, Energy, Engineering, Financial, Government, Healthcare, Media, Shipping and Logistics, Technology and BitCoin exchange
Affected OS: macOS
Malware: RustBucket
Attack: The RustBucket macOS malware family, attributed to the North Korean state-sponsored group BlueNoroff, is split into two stages, with the second stage application appearing as a legitimate PDF viewer but becoming malicious when a specific PDF is loaded.

Attack Regions



Attack Details

#1 RustBucket is a newly discovered macOS malware family . This malware family communicates with command and control (C2) servers to download and execute various payloads. The malware is believed to be attributed to a North Korean, state-sponsored threat actor known as BlueNoroff, which is thought to act as a sub-group to the well-known Lazarus Group.

#2 The malware is split into two stages. The first stage is a dropper that downloads and executes the second stage. The second stage application, named Internal PDF Viewer, looks like a legitimate Apple application and is signed with an ad-hoc signature. When launched, it acts as a functional PDF viewer. However, it only becomes malicious when a specific PDF is loaded. This PDF file is created to trigger malicious behaviors, and the application seeks out a specific blob of data within the PDF to decrypt and produce a new PDF using a hardcoded XOR key.

#3 This technique is clever because it makes analysis more difficult, especially if the C2 goes offline. It is a common technique used by malware authors to thwart analysis. Both the stage-one and stage-two components of this malware were undetected on VirusTotal until 21st April 2023.

Recommendations

- Keep software up-to-date: Make sure all macOS software is kept up-to-date with the latest security patches. This will help to prevent exploitation of known vulnerabilities by malware such as RustBucket.
- Use a reputable antivirus/anti-malware solution: Install and regularly update antivirus/anti-malware software on all macOS devices to detect and remove malware such as RustBucket.
- Be cautious of PDF files: Be cautious when opening PDF files, especially those received from unknown or untrusted sources, as they could contain RustBucket or other malware.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1082 System Information Discovery	T1071 Application Layer Protocol
T1564 Hide Artifacts	T1564.001 Hidden Files and Directories	T1518 Software Discovery	T1518.001 Security Software Discovery
T1095 Non-Application Layer Protocol	T1573 Encrypted Channel	T1547 Boot or Logon Autostart Execution	T1070 Indicator Removal
T1070.006 Timestomp	T1222 File and Directory Permissions Modification	T1553 Subvert Trust Controls	T1553.002 Code Signing
T1083 File and Directory Discovery	T1566 Phishing	T1036 Masquerading	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	dabb4372050264f389b8adcf239366860662ac52 0be69bb9836b2a266bfd9a8b93bb412b6e4ce1be e0e42ac374443500c236721341612865cd3d1eec ac08406818bbf4fe24ea04bfd72f747c89174bdb 72167ec09d62cdfb04698c3f96a6131dceb24a9c fd1cef5abe3e0c275671916a1f3a566f13489416 ca59874172660e6180af2815c3a42c85169aa0b2 d9f1392fb7ed010a0ecc4f819782c179efde9687 9121509d674091ce1f5f30e9a372b5dcf9bcd257 a1a85cba1bc4ac9f6eafc548b1454f57b4dff7e0 7a5d57c7e2b0c8ab7d60f7a7c7f4649f33fea8aa 182760cbe11fa0316abfb8b7b00b63f83159f5aa 7e69cb4f9c37fad13de85e91b5a05a816d14f490
Domains	cloud[.]dnx[.]capital deck[.]31ventures[.]info
File Path	/Users/Shared/Internal PDF Viewer.app

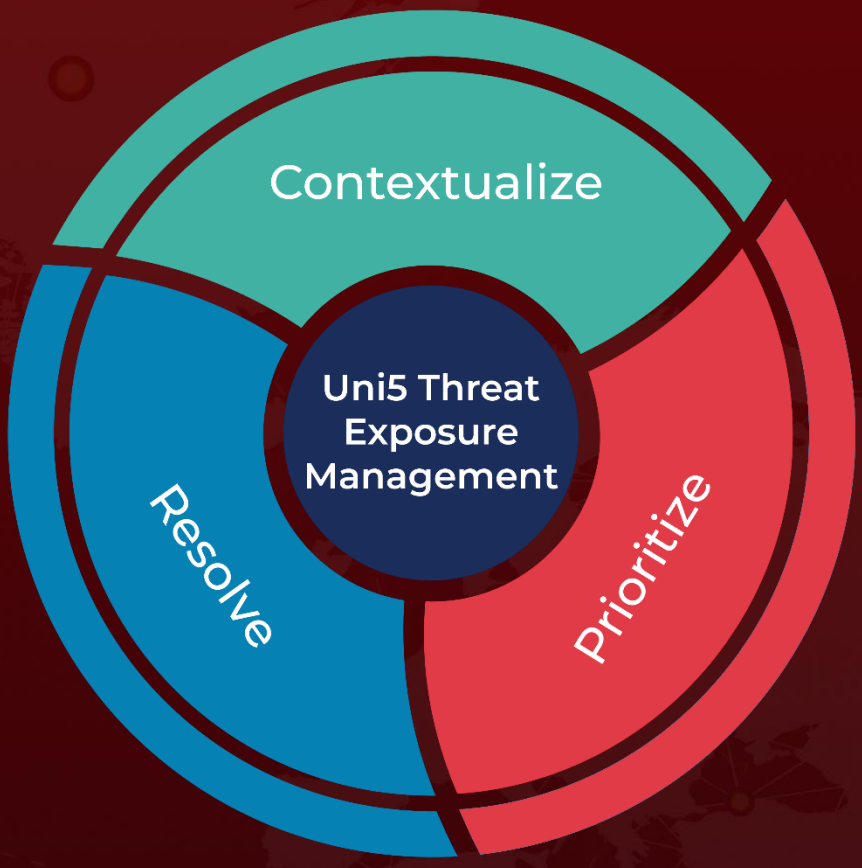
References

https://www.jamf.com/blog/bluenoroff-apt-targets-macos-rustbucket-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

April 28, 2023 • 5:00 AM

More at www.hivepro.com