Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

The Dangers of macOS Ransomware: A Closer Look at KeRanger, FileCoder, MacRansom, and EvilQuest

Date of Publication	Admiralty Code	TA Number
January 6, 2023	A1	TA2023011

Summary

First appeared: 2016
Attack Region: Worldwide
Affected OS: macOS
Attack: Malicious behavior posed by macOS ransomware families KeRanger, FileCoder, MacRansom, and EvilQuest

Attack Regions

Attack Details

#1

MacOS ransomware typically spreads through user-assisted methods such as downloading and running fake or trojanized applications. It can also arrive as a second-stage payload dropped or downloaded by other malware or as part of a supply chain attack. When it infects a device, it typically follows a process of gaining access, executing, encrypting the victim's files, and then sending a ransom message. There are several known families of macOS ransomware, which include KeRanger, FileCoder, MacRansom, and EvilQuest.

#2

KeRanger is a ransomware that was discovered in 2016. It was distributed through a compromised version of the popular BitTorrent client Transmission. FileCoder is another ransomware that was discovered in 2018. It was distributed through malicious advertisements on websites. MacRansom is a ransomware that was discovered in 2019. It is distributed through malicious email attachments. EvilQuest is a ransomware that was discovered in 2020. It is distributed through malicious apps that are available for download on the internet.

#3

The techniques used by various strains of macOS ransomware include file enumeration, anti-analysis techniques, persistence, and encryption. For file enumeration, FileCoder and MacRansom use the "find" utility to search for files to encrypt, while KeRanger and EvilQuest use library functions to get a list of files. To evade analysis, KeRanger, MacRansom, and EvilQuest employ hardware-based checks or use specific code.

#4

For persistence, EvilQuest can create both Launch Agent and Launch Daemon files, while MacRansom typically creates a Launch Agent file. In terms of encryption, FileCoder uses the ZIP utility to encrypt files, KeRanger uses AES encryption in Cipher block chaining (CBC) mode and the mbedtls library, MacRansom uses a symmetric algorithm, and EvilQuest uses a custom symmetric key encryption routine. In addition to these techniques, EvilQuest has been observed to exhibit other behavior such as file infection, keylogging, stealing information, disabling security solutions, and in-memory execution.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
TA0010 Exfiltration	T1204 User Execution	T1204.002 Malicious File	T1059 Command and Scripting Interpreter
T1059.002 AppleScript	T1569 System Services	T1569.001 Launchctl	T1543 Create or Modify System Process
T1543.001 Launch Agent	T1543.004 Launch Daemon	T1554 Compromise Client Software Binary	T1548 Abuse Elevation Control Mechanism
T1548.003 Sudo and Sudo Caching	T1140 Deobfuscate/Decode Files or Information	T1222 File and Directory Permissions Modification	T1222.002 Linux and Mac File and Directory Permissions Modification

T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1070 Indicator Removal	T1070.004 File Deletion
T1070.006 Timestomp	T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1083 File and Directory Discovery
T1057 Process Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery	T1082 System Information Discovery
T1033 System Owner/User Discovery	T1005 Data from Local System	T1071 Application Layer Protocol	T1071.001 Web Protocols
T1132 Data Encoding	T1132.002 Non-Standard Encoding	T1105 Ingress Tool Transfer	T1041 Exfiltration Over C2 Channel
T1486 Data Encrypted for Impact			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	b34738e181a6119f23e930476ae949fc0c7c4ded6efa003019fa946c4e5b287a bcdb0ca7c51e9de4cf6c5c346fd28a4ed28e692319177c8a94c86dc676ee8e48 617f7301fd67e8b5d8ad42d4e94e02cb313fe5ad51770ef93323c6115e52fe98 d19b903adbd0f8c119d0d8f25b194bdd24b737357a517f23ca5cdc6c75b35038 31b6adb633cff2a0f34cefd2a218097f3a9a8176c9363cc70fe41fe02af810b9

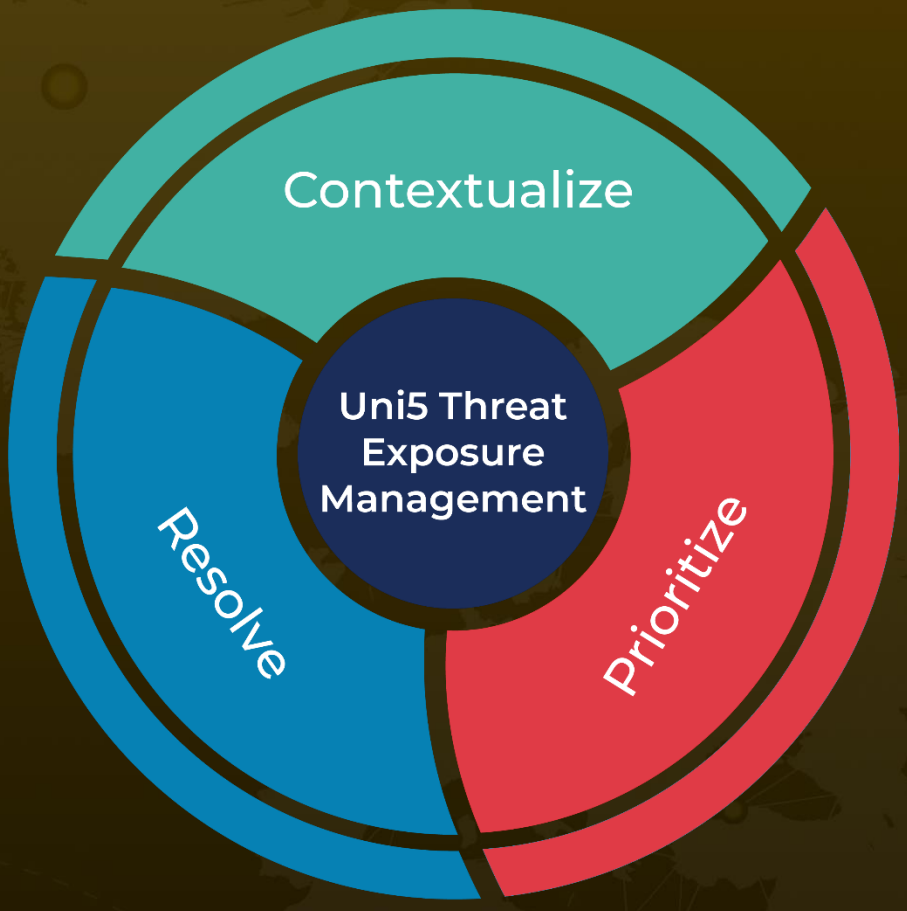
References

https://www.microsoft.com/en-us/security/blog/2023/01/05/unraveling-the-techniques-of-mac-ransomware/

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 6, 2023 . 4:30 AM

More at www.hivepro.com