Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

JokerSpy macOS Backdoor Attacks Japanese Cryptocurrency Exchange

Date of Publication	Admiralty Code	TA Number
June 28, 2023	A1	TA2023282

Summary

First Seen: April 2023
Malware: JokerSpy
Affected Platform: macOS
Targeted Industry: Cryptocurrency
Attack Region: Japan
Attack: An unknown cryptocurrency exchange in Japan became the target of a precise attack employing an intricate Apple macOS backdoor called JokerSpy. References to JokerSpy can be traced back to as early as April 2023.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

In June 2023, an unknown cryptocurrency exchange in Japan fell victim to a new assault aimed at deploying a backdoor named JokerSpy on Apple macOS systems. The earliest reference to JokerSpy can be traced back to April 2023. This attack resulted in the installation of Swiftbelt, an enumeration tool developed in Swift, which draws inspiration from an open-source utility called SeatBelt.

#2

JokerSpy is an advanced toolkit meticulously crafted to infiltrate macOS machines. At the core of this toolkit lies a self-signed multi-architecture binary known as xcc, specifically designed to assess FullDiskAccess and ScreenRecording permissions. Upon executing xcc, the threat actor endeavors to bypass Transparency, Consent, and Control (TCC) permissions by creating their own TCC database and attempting to replace the existing one.

#3

Another noteworthy component installed during this attack is sh.py, a Python implant employed as a conduit to deliver various post-exploitation tools, including Swiftbelt. The xcc binary, on the other hand, is launched through Bash by utilizing three distinct applications: IntelliJ IDEA, iTerm a macOS terminal emulator, and Visual Studio Code. This suggests that compromised versions of software development applications are likely employed to acquire initial access

Recommendations

Strengthen TCC permission safeguards by implementing measures to detect and prevent unauthorized manipulation of the TCC database. Regularly monitor for any attempts to create or replace the TCC database, ensuring the integrity and validity of TCC permissions.

Implement regular integrity monitoring of system directories and critical files to detect unauthorized extraction of non-native dylibs into suspicious directories. This can be achieved by utilizing macOS's built-in security measures like Gatekeeper, which provides baseline protection against known threats, effectively preventing potential exploitation.

Implement robust security measures to protect against sophisticated attacks like JokerSpy. This should include regular updates, strong access controls, permissions, and system integrity monitoring.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0040 Impact	T1496 Resource Hijacking	T1531 Account Access Removal
T1059 Command and Scripting Interpreter	T1574 Hijack Execution Flow	T1574.004 Dylib Hijacking	T1068 Exploitation for Privilege Escalation
T1548 Abuse Elevation Control Mechanism	T1564 Hide Artifacts	T1036 Masquerading	T1027 Obfuscated Files or Information
T1553 Subvert Trust Controls	T1010 Application Window Discovery	T1113 Screen Capture	T1005 Data from Local System

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	app.influmarket[.]org
SHA256	d895075057e491b34b0f8c0392b44e43ade425d19eaaacea6ef8c5c9bd3487d8,8ca86f78f0c73a46f31be366538423ea0ec58089f3880e041543d08ce11fa626,aa951c053baf011d08f3a60a10c1d09bbac32f332413db5b38b8737558a08dc1
SHA1	937a9811b3e5482eb8f96832454723d59229f945 c7d6ede0f6ac9f060ae53bb1db40a4fbe96f9ceb bd8626420ecfd1ab5f4576d83be35edecd8fa70e 370a0bb4177eeebb2a75651a8addb0477b7d610b 1ed2c5ee95ab77f8e1c1f5e2bd246589526c6362 76b790eb3bed4a625250b961a5dda86ca5cd3a11

References

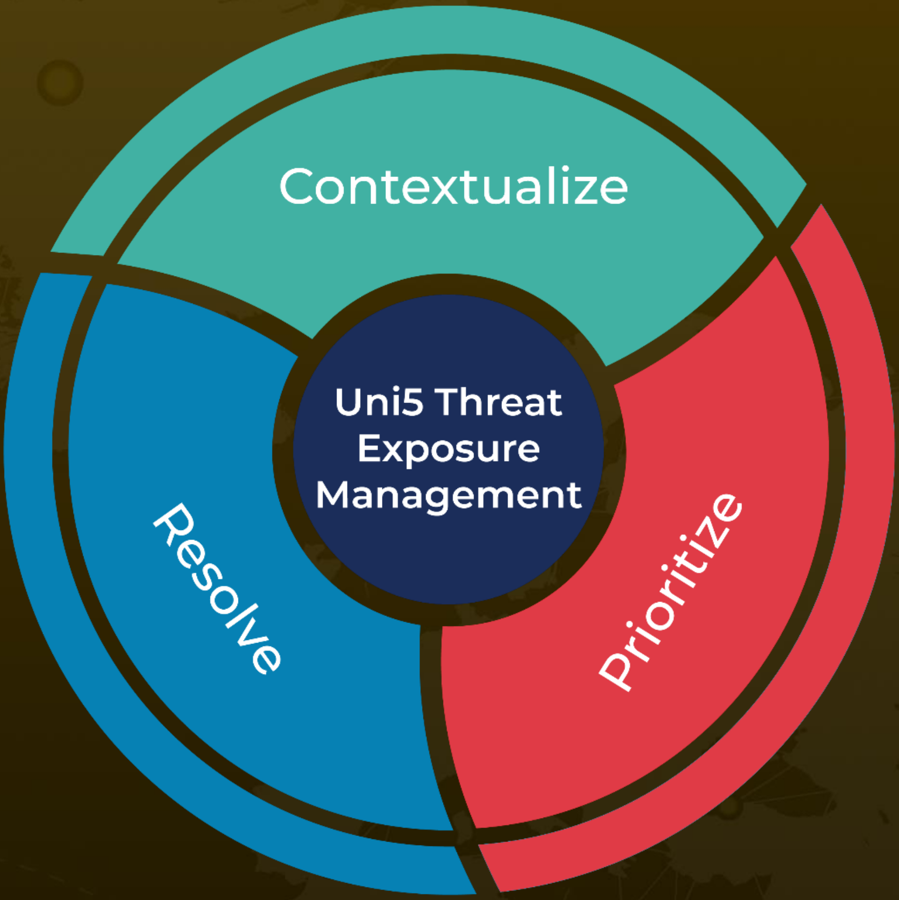
https://www.elastic.co/security-labs/inital-research-of-jokerspy

https://www.bitdefender.com/blog/labs/fragments-of-cross-platform-backdoor-hint-at-larger-mac-os-attack/

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

June 28, 2023 • 4:51 AM

More at www.hivepro.com