Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

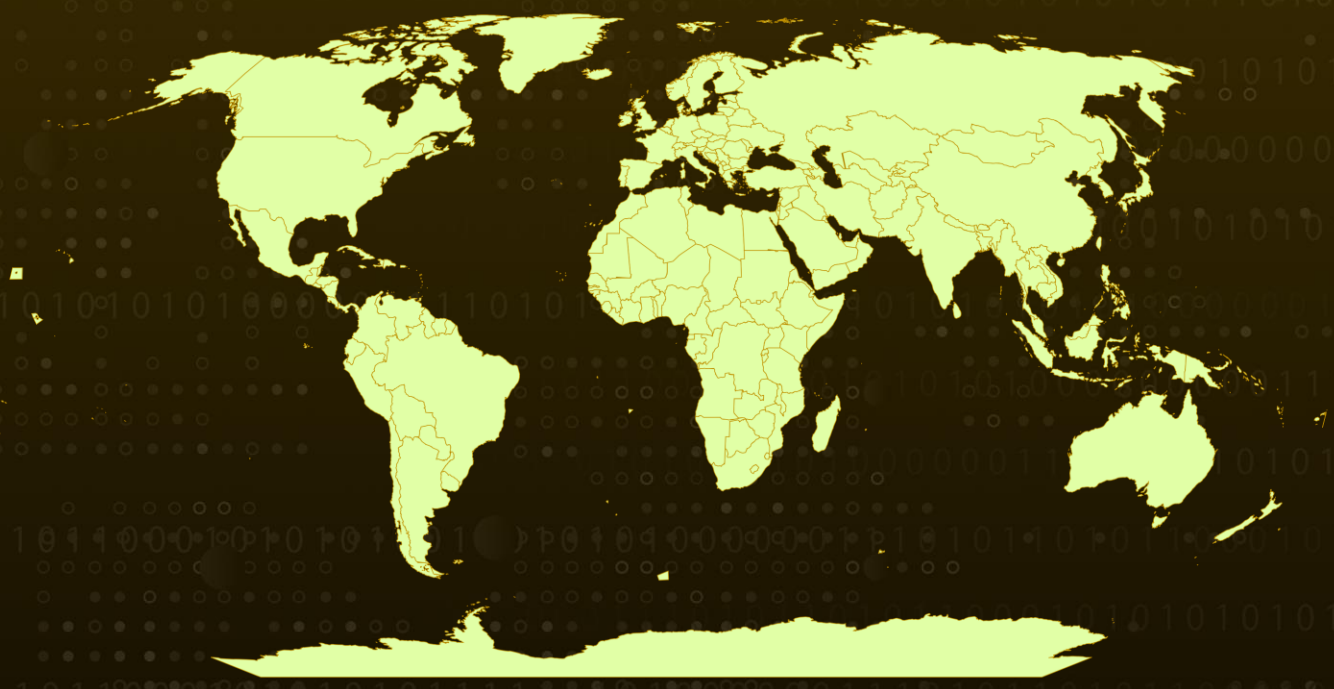
New Backdoor Masquerading as a Software Update Agent, Targets macOS

Date of Publication	Admiralty Code	TA Number
February 13, 2024	A1	TA2024056

Summary

Attack Discovered: November 2023
Attack Region: Worldwide
Malware: RustDoor
Attack: Apple macOS users are currently being targeted by a newly discovered Rust-based backdoor known as RustDoor. This backdoor masquerades as an update for Microsoft Visual Studio and is designed to target both Intel and Arm architectures. RustDoor is equipped with various commands, enabling it to collect and upload files, as well as extract information from the compromised endpoint.

Attack Regions



Attack Details

#1 A new backdoor named RustDoor has been identified, specifically targeting Mac OS users. This backdoor disguises itself as a Visual Studio update, and the discovered files are distributed as FAT binaries containing Mach-O files for both x86_64 Intel and ARM architectures.

#2 RustDoor has been observed in multiple iterations with slight variations, suggesting continuous development efforts. The earliest detected sample of RustDoor dates back to November 2, 2023. While Variant Zero lacks an Apple script and an embedded configuration, it still functions as a backdoor. It includes a diverse set of commands, enabling it to collect and transmit files and extract information about the compromised endpoint.

#3 The utilization of Rust in the source code of the files can pose challenges for security researchers in analyzing and identifying malicious code. Notably, a variant detected on November 22, 2023, appears to be a test version, as indicated by the embedded plist file (test.plist). This variant configuration lacks a field for leveraging LaunchAgents for persistence.

#4 The second variant of the malware, identified on November 30, 2023, exhibits a slightly larger size compared to its predecessor. It incorporates a sophisticated JSON configuration and features an embedded Apple script designed for data exfiltration.

#5 The script is employed to extract documents with specific extensions and sizes from the Documents and Desktop folders, along with user notes stored in SQLITE format. Strings containing targeted extensions were detected within the binaries. Subsequently, the extracted files are compressed into a ZIP archive and transmitted to the C2 server.

#6 The artifacts and IoCs indicate a potential association of RustDoor with the BlackBasta and (ALPHV/BlackCat) ransomware operators. Notably, three out of the four command and control servers were previously linked to Windows client ransomware campaigns.

Recommendations

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Always ensure to download software from trusted and reputable sources to minimize the risk of inadvertently installing malware or malicious programs on your system.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration	TA0011 Command and Control
T1036 Masquerading	T1059 Command and Scripting Interpreter	T1059.002 AppleScript	T1082 System Information Discovery
T1647 Plist File Modification	T1053 Scheduled Task/Job	T1053.003 Cron	T1543 Create or Modify System Process
T1543.001 Launch Agent	T1005 Data from Local System	T1566 Phishing	T1560 Archive Collected Data
T1041 Exfiltration Over C2 Channel			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	6dd3a3e4951d34446fe1a5c7cdf39754, 90a517c3dab8ceccf5f1a4c0f4932b1f, b67bba781e5cf006bd170a0850a9f2d0, f5774aca722e0624daf67a2da5ec6967, 52a9d67745f153465fac434546007d3a, 30b27b765878385161ca1ee71726a5c6, 1dbc26447c1eaa9076e65285c92f7859, 05a8583f36599b5bc93fa3c349e89434, 5d0c62da036bbe375cb10659de1929e3, 68e0facbf541a2c014301346682ef9ca, b2bdd1d32983c35b3b1520d83d89d197, 5fcc12eaba8185f9d0ddecafae8fd2d1, 97cd4fc94c59121f903f2081df1c9981, 28bdd46d8609512f95f1f1b93c79d277, 3e23308d074d8bd4ffdb5e21e3aa8f22, 088779125434ad77f846731af2ed6781, b67f6e534d5cca654813bd9e94a125b9, cf54cba05efee9e389e090b3fd63f89b, 44fcf7253bcf0102811e50a4810c4e41, 690a097b0eea384b02e013c1c0410189, 186be45570f13f94b8de82c98eaa8f4f, 3c780bcfb37a1dfae5b29a9e7784cbf5, 925239817d59672f61b8332f690c6dd6, 9c6b7f388abec945120d95d892314ea7, 85cd1afbc026ffdfe4cd3eec038c3185, 6aaba581bcef3ac97ea98ece724b9092, bcbbf7a5f7ccff1932922ae73f6c65b7, bde0e001229884404529773b68bb3da0, 795f0c68528519ea292f3eb1bd8c632e, bc394c859fc379900f5648441b33e5fd, 0fe0212fc5dc82bd7b9a8b5d5b338d22, 835ebf367e769eeaaef78ac5743a47ca, Bdd4972e570e069471a4721d76bb5efb
Domains	https[:]//sarkerrentacars[.]com/zshrc, https[:]//turkishfurniture[.]blog/Previewers, http[:]//linksammosupply[.]com/zshrc2, http[:]//linksammosupply[.]com/VisualStudioUpdaterLs2, http[:]//linksammosupply[.]com/VisualStudioUpdater, maconlineoffice[.]com, https://serviceicloud[.]com

TYPE	VALUE
IP	193.29.13[.]167, 88.214.26[.]22

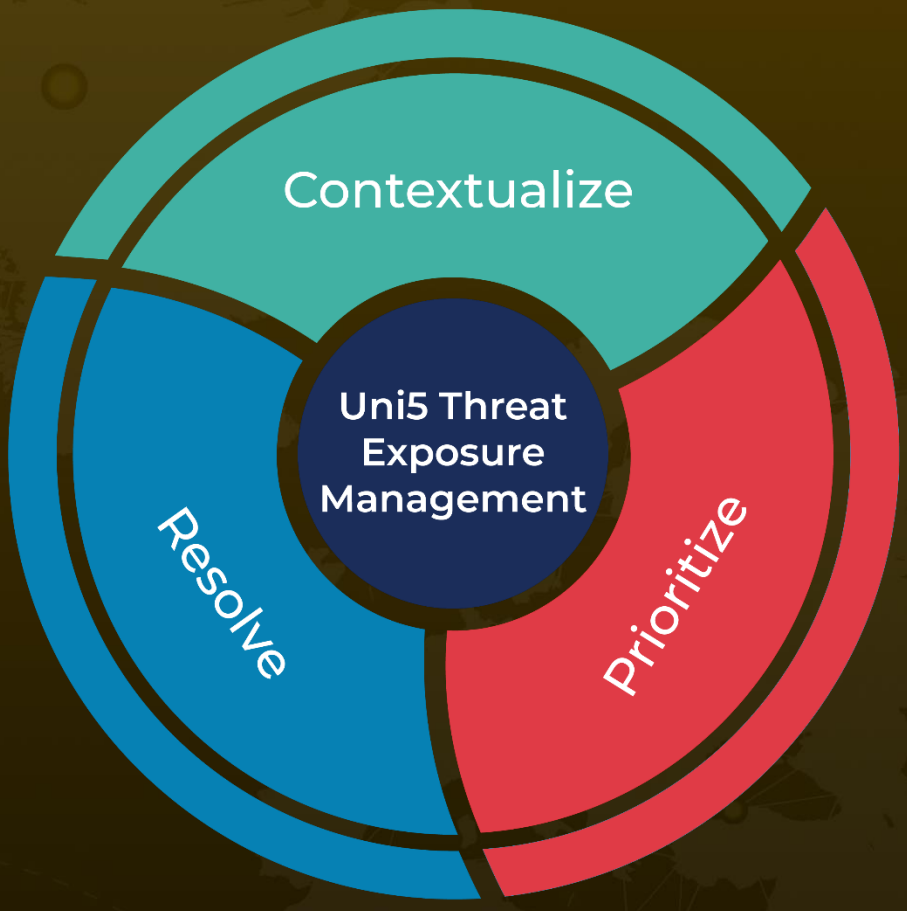
References

https://www.bitdefender.com/blog/labs/new-macos-backdoor-written-in-rust-shows-possible-link-with-windows-ransomware-group/

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

February 13, 2024 • 4:40 AM

More at www.hivepro.com