Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

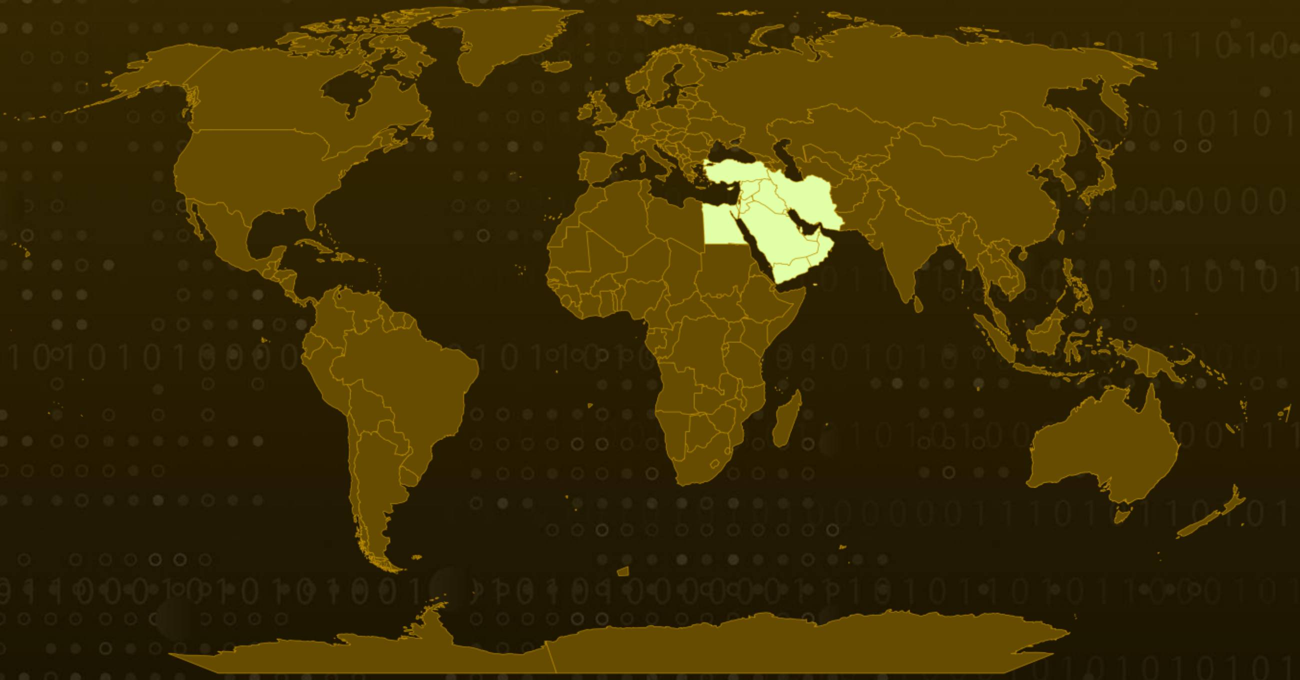
Middle East Targeted with CR4T Malware in DuneQuixote Campaign

Date of Publication	Admiralty Code	TA Number
April 22, 2024	A1	TA2024158

Summary

Attack Began: February 2024
Attack Region: Middle East
Affected Industries: Government entities
Malware: CR4T
Campaign: DuneQuixote
Attack: The DuneQuixote campaign, targeting Middle Eastern governments, introduces a new backdoor dubbed CR4T. The attack begins with a dropper available in two variants: a standard executable or DLL file and a modified installer for the legitimate tool Total Commander. These droppers serve as the initial entry points for the malicious activity associated with the CR4T backdoor.

Attack Regions



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

Attack Details

#1

The DuneQuixote campaign, discovered in February 2024, targeted Middle Eastern government institutions with the objective of deploying the CR4T backdoor. This campaign utilized two variants of droppers: a standard executable or DLL dropper and a tampered installer file for Total Commander, a legitimate program.

#2

The initial dropper, coded in Windows x64 executable using C/C++, deliberately avoids employing the Standard Template Library (STL) to minimize its footprint and evade detection. To obfuscate its behavior, it utilizes deceptive API calls, incorporating strings from Spanish poems for string comparison functions. It also constructs a framework for essential API calls using offsets of Windows API functions and decrypts critical Windows core DLL names using a simple XOR decryption algorithm.

#3

The Total Commander installer dropper mimics a legitimate installer but includes a malicious file section and modified entry point. It invalidates the installer's digital signature and employs anti-analysis measures to prevent connections to C2 resources. The malware performs various checks to detect debugging or analysis tools and decrypts the C2 server address if such conditions are met.

#4

The CR4T backdoor allows attackers to execute command lines on victim machines, enabling malicious activities like file manipulation and data exfiltration. It utilizes a PDB string and interacts with a cmd.exe process, establishing named pipes for inter-process communication. The CR4T configures a user agent for C2 communication and waits for commands from the C2 server to activate its functionality. Furthermore, a Golang version of the CR4T implant was also discovered.

#5

This version shares similar capabilities with the original C version but introduces features like scheduled tasks and persistence using COM object hijacking and C2 communications via the Telegram API. The presence of both C/C++ and Golang versions of the CR4T implant highlights the resourcefulness of threat actors, underscoring the need for robust security measures and proactive threat detection strategies.

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.

Download from Trusted Sources: Only download software from trusted sources. Avoid downloading software from third-party websites or torrents, as they may contain malware or modified versions of the software.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0011 Command and Control	T1583 Acquire Infrastructure	T1583.001 Domains	T1583.002 DNS Server
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1106 Native API	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1569 System Services	T1569.002 Service Execution	T1105 Ingress Tool Transfer
T1036 Masquerading	T1027 Obfuscated Files or Information	T1027.009 Embedded Payloads	T1140 Deobfuscate/Decode Files or Information
T1546 Event Triggered Execution	T1546.015 Component Object Model Hijacking	T1053 Scheduled Task/Job	T1071 Application Layer Protocol
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	3aaf7f7f0a42a1cf0a0f6c61511978d7, 5759acc816274d38407038c091e56a5c, 606fdee74ad70f76618007d299adb0a4, 5a04d9067b8cb6bcb916b59dcf53bed3, 48c8e8cc189eef04a55ecb021f9e6111, 7b9e85afa89670f46f884bb3bce262b0, 4f29f977e786b2f7f483b47840b9c19d, 9d20cc7a02121b515fd8f16b576624ef, 4324cb72875d8a62a210690221cdc3f9, 3cc77c18b4d1629b7658afbf4175222c, 6cfec4bdcbcf7f99535ee61a0ebae5dc, c7076351095314 9fb33d06bef160821c, f3988b8aaaa8c6a9ec407cf5854b0e3b, cf4bef8537c6397ba07de7629735eb4e, 1bba771b9a32f0aada6eaee64643673a, 72c4d9bc1b59da634949c555b2a594b1, cc05c7bef5cff67bc74fda2fc96ddf7b, 0fdbe82d2c8d52ac912d698bb8b25abc, 9b991229fe1f5d8ec6543b1e5ae9beb4, 5e85dc7c6969ce2270a06184a8c8e1da, 71a8b4b8d9861bf9ac6bd4b0a60c3366, 828335d067b27444198365fac30aa6be, 84ae9222c86290bf585851191007ba23, 450e589680e812ffb732f7e889676385, 56d5589e0d6413575381b1f3c96aa245, 258b7f20db8b927087d74a9d6214919b, a4011d2e4d3d9f9fe210448dd19c9d9a, b0e19a9fd168af2f7f6cf997992b1809, 0d740972c3dff09c13a5193d19423da1, a0802a787537de1811a81d9182be9e7c, 5200fa68b6d40bb60d4f097b895516f0, abf16e31deb669017e10e2cb8cc144c8, f151be4e882352ec42a336ca6bff7e3d, f1b6aa55ba3bb645d3fde78abda984f3, 00130e1e7d628c8b5e2f9904ca959cd7, fb2b916e44abddd943015787f6a8dc35, 996c4f78a13a8831742e86c052f19c20, 4f29f977e786b2f7f483b47840b9c19d, 91472c23ef5e8b0f8dda5fa9ae9afa94, 135abd6f35721298cc656a29492be255, db786b773cd75483a122b72fdc392af6

TYPE	VALUE
Domain	Commonline[.]space, g1sea23g.commonline[.]space, tg1sea23g.commonline[.]space, telemetry.commonline[.]space, e1awq1lp.commonline[.]space, mc.commonline[.]space, userfeedsync[.]com, Service.userfeedsync[.]com, telemetry.userfeedsync[.]com

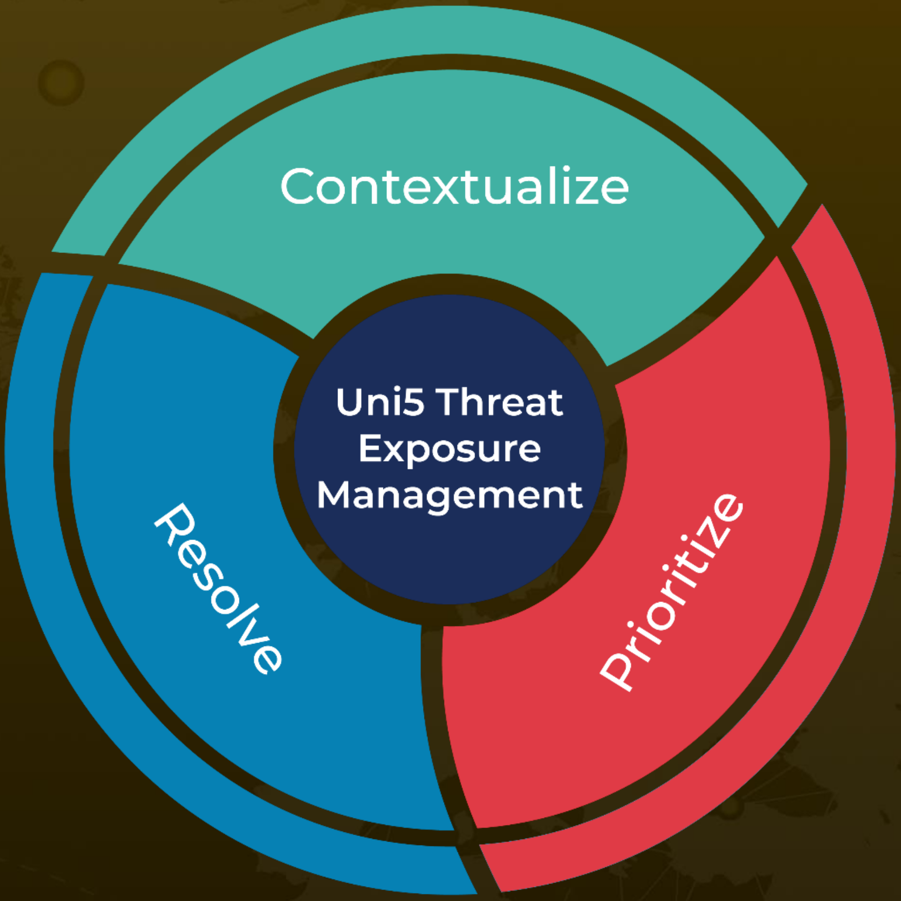
References

https://securelist.com/dunequixote/112425/

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 22, 2024 • 7:20 AM

More at www.hivepro.com