Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

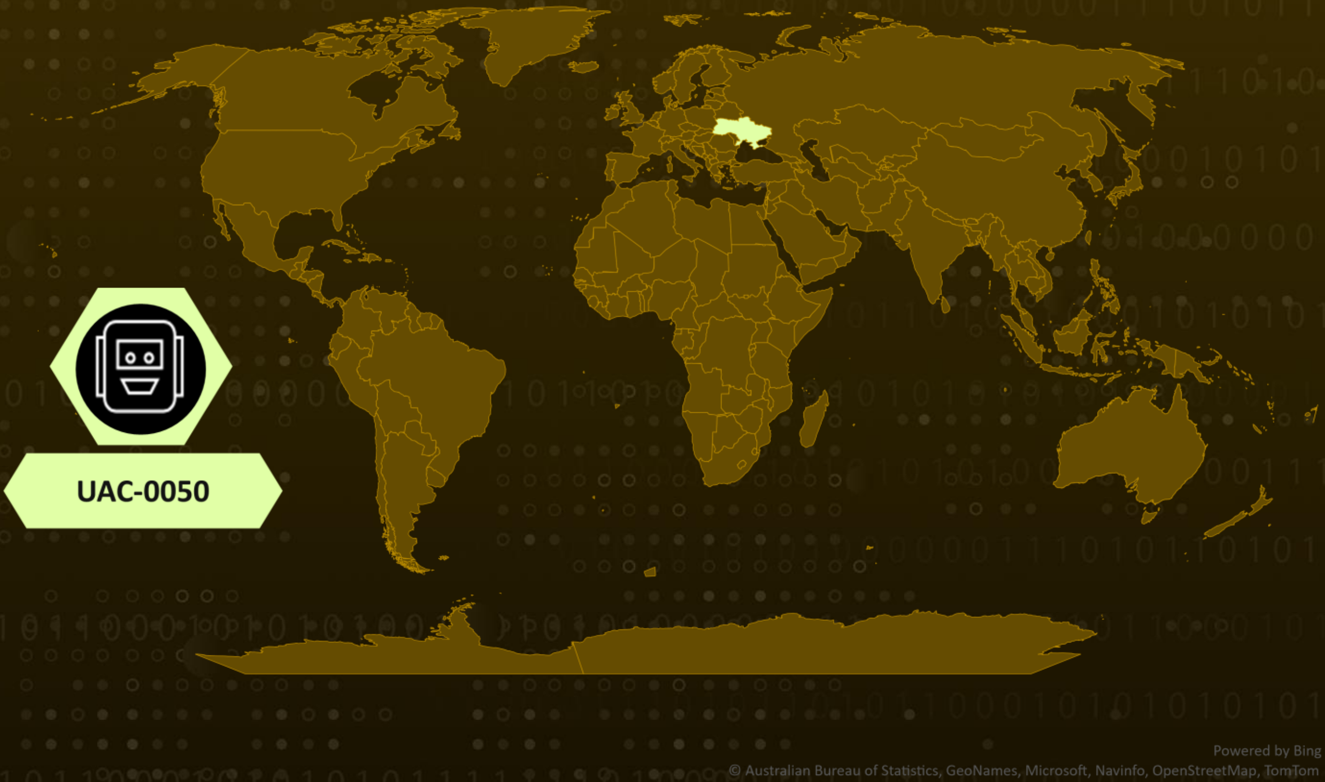
Decoding UAC-0050's Cyber Espionage Playbook

Date of Publication	Admiralty Code	TA Number
January 05, 2024	A1	TA2024006

Summary

Attack Began: December 2023
Threat Actor: UAC-0050
Malware: Remcos RAT
Affected Platform: Windows
Attack Region: Ukraine
Targeted Sector: Government
Attack: UAC-0050, a threat actor focused on Ukraine, is using new tactics to spread the Remcos RAT. In their latest move, UAC-0050 shows advanced adaptability by cleverly avoiding detection through a hidden data transfer method and outsmarting EDR systems.

Attack Regions


UAC-0050
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The entity known as UAC-0050 is currently targeting Ukraine, employing innovative strategies to spread the Remcos RAT while skillfully avoiding detection mechanisms implemented by security software. Remcos, marketed as a proprietary remote control and surveillance tool by Breaking Security, serves as the focal point for UAC-0050's cyber-espionage activities.

#2 Active since 2020, UAC-0050 has a history of directing its efforts toward Ukrainian and Polish entities through social engineering campaigns. These campaigns involve impersonating legitimate organizations to trick recipients into opening malicious attachments.

#3 In their latest operational iteration, the UAC-0050 group has cleverly integrated a pipe method for interprocess communication, providing a covert channel for data transfer that adeptly evades detection by EDR and antivirus systems, highlighting their advanced adaptability.

#4 The attack sequence begins with the acquisition of information about antivirus products installed on the target computer. Subsequently, an HTML application is retrieved and executed from a remote server. Upon execution, a PowerShell script is triggered to download a malicious payload (word_update.exe) from a server.

#5 The execution of word_update.exe, in turn, initiates cmd.exe and facilitates the exchange of malicious data through a pipe. This series of events culminates in the launch of explorer.exe with the deployment of the malicious Remcos RAT version 4.9.2 Pro, capable of harvesting system data, cookies, and login information from web browsers.

Recommendations

User Training and Awareness: Conduct regular training sessions to educate users on recognizing and avoiding social engineering tactics, particularly those used by UAC-0050. Encourage a cautious approach when opening email attachments, especially if they appear suspicious or come from unfamiliar sources.

Anomaly Detection: Implement anomaly detection algorithms to identify deviations from normal network behavior. This includes monitoring network traffic, system logs, and user activities for any unusual patterns.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1566 Phishing	T1059 Command and Scripting Interpreter	T1007 System Service Discovery
T1059.001 PowerShell	T1547 Boot or Logon Autostart Execution	T1216 System Script Proxy Execution	T1027 Obfuscated Files or Information
T1555 Credentials from Password Stores	T1547.001 Registry Run Keys / Startup Folder	T1041 Exfiltration Over C2 Channel	T1204 User Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	56154fedaa70a3e58b7262b7c344d30a, 9b777d69b018701ec5ad19ae3f06553f, 74865c6c290488bd5552aa905c02666c, 7c05cfed156f152139a6b1f0d48b5cc1, 7c05cfed156f152139a6b1f0d48b5cc1, 0b2d0eb5af93a3355244e1319e3de9da, 7f87d36c989a11edf0de9af392891d89, f5ee6aa31c950dfe55972e50e02201d3, 5c734bb1e41fab9c7b2dabd06e27bc7b, 1c3e1e0319dc6aa24166d5e2aaaec675, 818beece85ecd90d413782dd51d939b1, 8158b43f745e0e7a519458b0150e1b61, f71ef85824f906856cb3d2205058bdd2, 8bebea01d914a3c3a2d876417f7d1d54, b1f8484ee01a7730938210ea6e851888

TYPE	VALUE
File Names	6.hta, ofer.docx, word_update.exe, fmTask_dbg.exe
IPv4	194[.]87.31[.]229, 46[.]249.58[.]40
Domains	cluster00<X>[.]ovh[.]net, new-tech-savvy[.]com/6.hta, new-tech-savvy[.]com/5[.]hta, new-tech-savvy[.]com/algo[.]hta, new-tech-savvy[.]com/shablon[.]hta, new-tech-savvy[.]com/word_update[.]exe, new-tech-savvy[.]com/zayava[.]docx, new-tech-savvy[.]com/ofer[.]docx

References

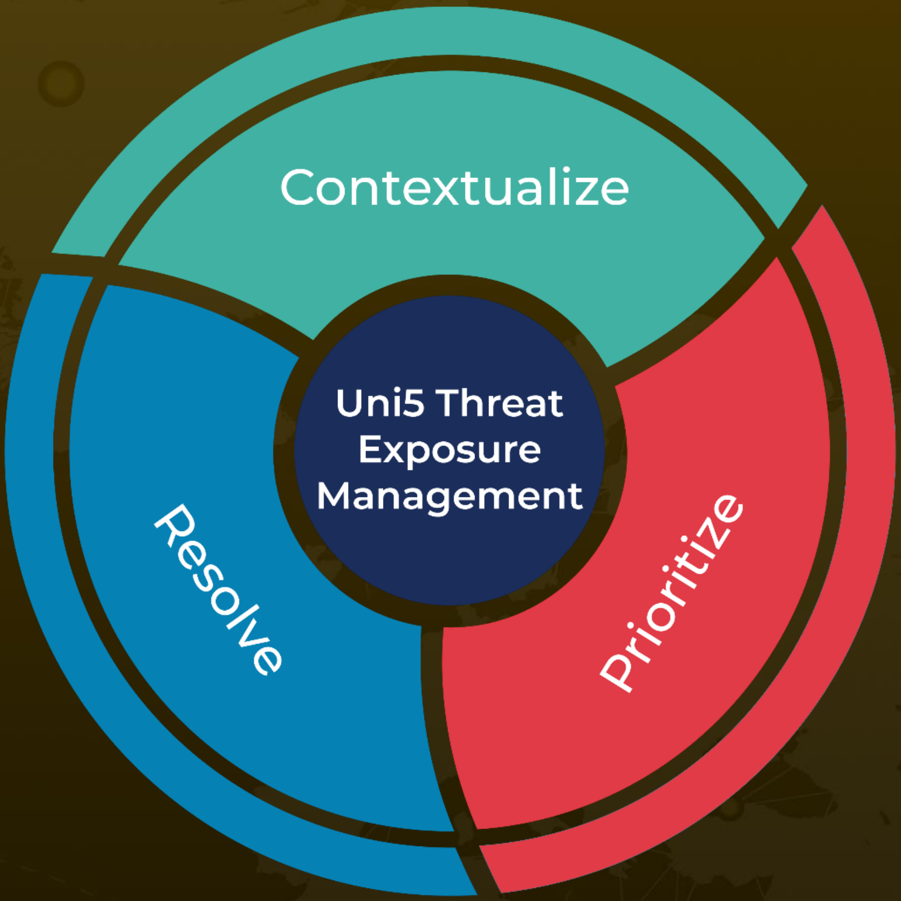
https://www.uptycs.com/blog/remcos-rat-uac-0500-pipe-method

https://attack.mitre.org/software/S0332/

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 5, 2024 • 4:00 AM

More at www.hivepro.com