Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Social Engineering Campaign Abuses RMM Tools, Linked to Black Basta

Date of Publication	Admiralty Code	TA Number
May 15, 2024	A1	TA2024188

Summary

Discovered: April 2024
Attack Region: Worldwide
Malware: Cobalt Strike Beacon
Attack: An ongoing social engineering campaign has been uncovered, targeting enterprises with spam emails. The threat actor entices affected users to download remote monitoring and management software such as AnyDesk or utilize Microsoft's built-in Quick Assist feature to establish a remote connection. The primary objective of this campaign is to gain initial access to their environments for subsequent exploitation.

Attack Regions

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

Attack Details

#1 A novel social engineering campaign has emerged since late April 2024, aiming to infiltrate users' computers and networks through a multi-stage process. It begins with spam emails, cleverly disguised as newsletter sign-up confirmations from reputable organizations, to initiate contact with targets.

#2 The attackers then pose as IT support personnel, reaching out to users and offering assistance with email issues. Their goal is to persuade users to grant remote access to their computers, often by convincing them to download and run software like AnyDesk or Quick Assist.

#3 Upon gaining access to a user's computer, they deploy batch scripts disguised as updates. These scripts connect to a command and control (C2) server, download legitimate tools like OpenSSH, and establish persistence by creating registry entries.

#4 The threat actors use batch scripts to execute SSH commands in a loop, establishing a reverse shell connection to the C2 server using downloaded RSA keys. They also harvest user credentials under the guise of an "update" and exfiltrate them to their server using SCP commands.

#5 Furthermore, remote monitoring tools like ScreenConnect and NetSupport RAT are deployed, along with Cobalt Strike beacons disguised as legitimate DLLs. These beacons are injected into other network assets, allowing the attackers to maintain access and potentially deploy ransomware in the future.

#6 The campaign shares similarities in indicators of compromise (IOCs) with those linked to known ransomware groups such as Black Basta. This raises concerns about future ransomware attacks and underscores the importance of proactive security measures to prevent such incidents.

Recommendations

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. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

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.

Monitor RMM Connections: Implement a comprehensive domain blocking strategy to restrict access to websites associated with unapproved RMM solutions. By preventing users from accessing these domains, we can minimize the potential for unauthorized software installations and mitigate security threats.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0010 Exfiltration
TA0011 Command and Control	TA0040 Impact	T1566 Phishing	T1566.004 Spearphishing Voice
T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1059.001 PowerShell	T1547 Boot or Logon Autostart Execution

T1547.001 Registry Run Keys / Startup Folder	**T1222** File and Directory Permissions Modification	**T1222.001** Windows File and Directory Permissions Modification	**T1140** Deobfuscate/Decode Files or Information
T1056 Input Capture	**T1056.001** Keylogging	**T1033** System Owner/User Discovery	**T1570** Lateral Tool Transfer
T1572 Protocol Tunneling	**T1498** Network Denial of Service	**T1041** Exfiltration Over C2 Channel	**T1036** Masquerading

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	195[.]123[.]233[.]55, 38[.]180[.]142[.]249, 5[.]161[.]245[.]155, 20[.]115[.]96[.]90, 91[.]90[.]195[.]52, 195[.]123[.]233[.]42, 15[.]235[.]218[.]150, 77[.]246[.]101[.]135
Domain	upd7[.]com, upd7a[.]com, greekpool[.]com, rewilivak13[.]com, limitedtoday[.]com, thetrailbig[.]net
SHA256	C18E7709866F8B1A271A54407973152BE1036AD3B57423101D7C3DA98664D108, 59F1C5FE47C1733B84360A72E419A07315FBAE895DD23C1E32F1392E67313859, 2EC12F4EE375087C921BE72F3BD87E6E12A2394E8E747998676754C9E3E9798E, 35456F84BC88854F16E316290104D71A1F350E84B479EEBD6FBB2F77D36BCA8A, 6F31CF7A11189C683D8455180B4EE6A60781D2E3F3AADF3ECC86F578D480CFA9, A47718693DC12F061692212A354AFBA8CA61590D8C25511C50CFECF73534C750, 76F959205D0A0C40F3200E174DB6BB030A1FDE39B0A190B6188D9C10A0CA07C8

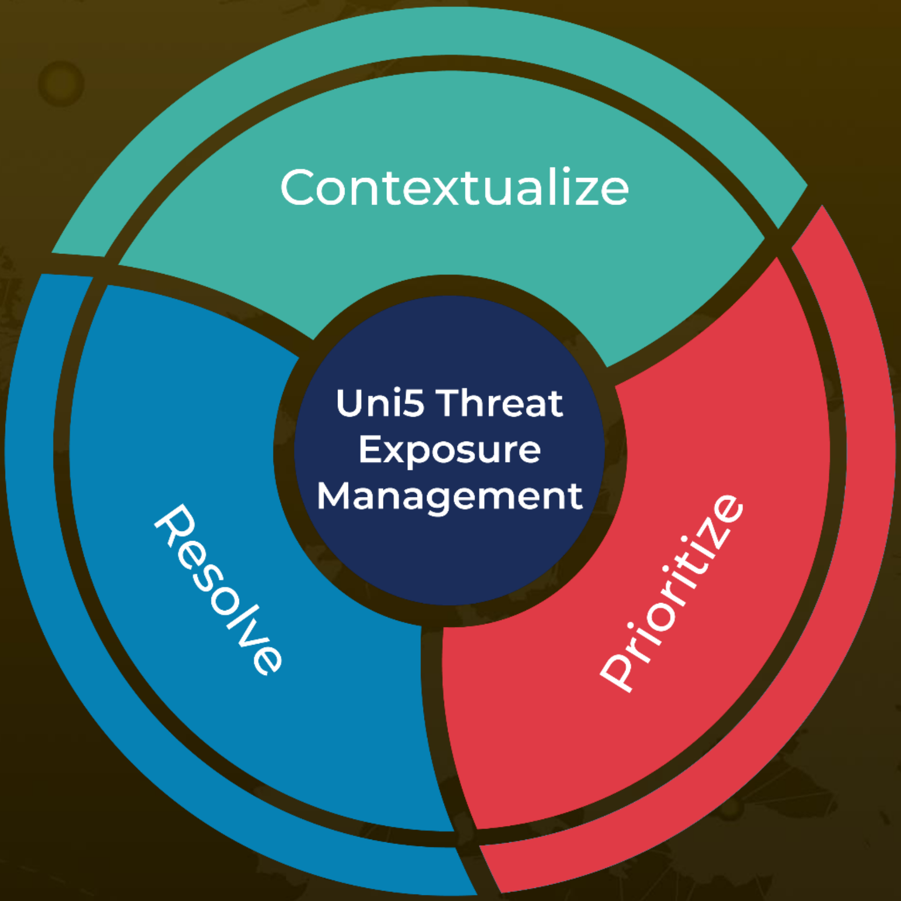
References

https://www.rapid7.com/blog/post/2024/05/10/ongoing-social-engineering-campaign-linked-to-black-basta-ransomware-operators/

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

May 15, 2024 • 7:30 AM

More at www.hivepro.com