Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

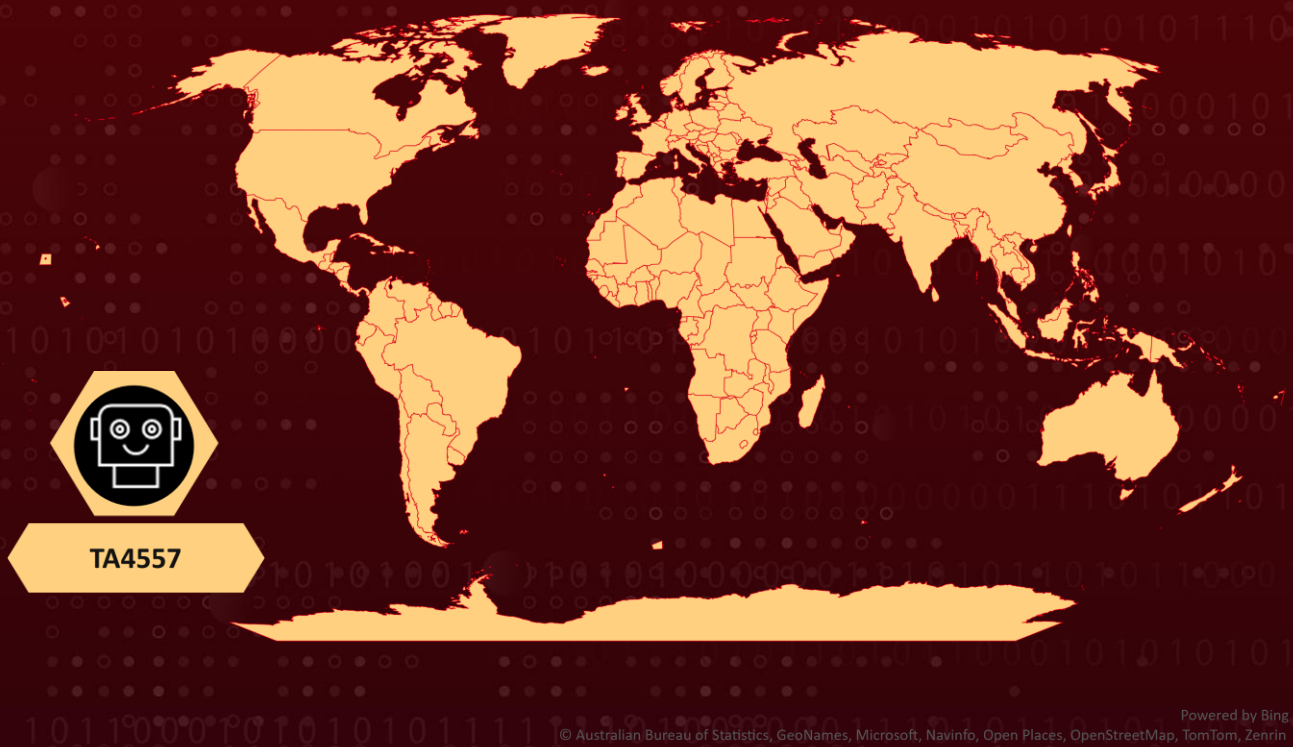
TA4557 Targets Recruiters by Delivering Malware Disguised as Job Applicant

Date of Publication	Admiralty Code	TA Number
December 14, 2023	A1	TA2023504

Summary

First appeared: October 2023
Targeted Industry: Recruiters
Actor: TA4557
Malware: More_Eggs
Attack: Threat actor TA4557 has been focusing on recruiters by posing as job applicants to distribute malware. While this approach is not unprecedented, there have been notable shifts in both technique and attack vectors compared to their previous methods. The attackers have demonstrated an enhanced ability to deliver their malware, particularly through the utilization of direct emails to recruiters, resulting in more effective malware delivery compared to their past attacks.

Attack Regions



Attack Details

#1 TA4557 has adopted a novel tactic, focusing on targeting recruiters through direct emails that lead to the transmission of malware, a strategy observed at least since October 2023. The initial emails are crafted in a polite manner, expressing interest in an available position. The attack chain unfold if the targeted recipient responds to the initial communication.

#2 TA4557 stands out as a proficient and financially motivated threat actor, distinguished by their distribution of the More_Eggs backdoor, endpoint profiling, and deployment of additional payloads. What sets TA4557 apart from other high-priority threat actors is their distinctive use of tools, targeted campaigns, employment of job candidate-themed lures, implementation of sophisticated evasion techniques, unique attack chains, and the management of actor-controlled infrastructure.

#3 TA4557 employ two primary methods to target recruiters: sending job applications with malicious URLs or attachments through job portals and directly reaching out to recruiters via email, posing as job applicants. In both scenarios, victims are enticed to visit a specified domain or URL, where a filtering check is conducted to redirect them to a download page housing a ZIP archive file. This LNK shortcut file executes a Living-off-the-Land attack, facilitating the download of additional payloads onto the victims' systems.

#4 The scriptlet employs advanced techniques, including evasion tactics, to execute DLLs covertly. It tries to launch a regsvr32 process through WMI or the ActiveX Object Run function, decrypts and positions the DLL, and retrieves the RC4 key using a loop to unlock the More Eggs backdoor. The DLL also utilizes the NtQueryInformationProcess method to detect active debugging. Upon successful execution, it opens the More Eggs backdoor, initiates the MSXSL process via WMI, and then deletes itself to remain concealed.

#5 TA4577 employs tactics focused on building trust to deliver malicious content, effectively enhancing trust among recipients. However, the challenge lies in TA4557's strategy of constantly changing sender emails, fake resume domains, and infrastructure, making it difficult for defenders and automated security tools to detect and counter the threat. Organizations utilizing third-party job posting websites should maintain vigilance and prioritize educating employees, especially those involved in recruiting and hiring, to enhance awareness and protect against this specific threat.

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.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

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.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	T1566 Phishing	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link
T1218 System Binary Proxy Execution	T1047 Windows Management Instrumentation	T1204 User Execution	T1204.001 Malicious Link
T1204.002 Malicious File	T1547 Boot or Logon Autostart Execution	T1497 Virtualization/Sandbox Evasion	T1070 Indicator Removal
T1070.004 File Deletion	T1622 Debugger Evasion	T1220 XSL Script Processing	T1082 System Information Discovery
T1105 Ingress Tool Transfer			

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	wlynch\[.]com, annetterawlings\[.]com
SHA267	9d9b38dffe43b038ce41f0c48def56e92dba3a693e3b572dbd13d5fbc9abc1e4, 6ea619f5c33c6852d6ed11c52b52589b16ed222046d7f847ea09812c4d51916d, 010b72def59f45662150e08bb80227fe8df07681dcf1a8d6de8b068ee11e0076

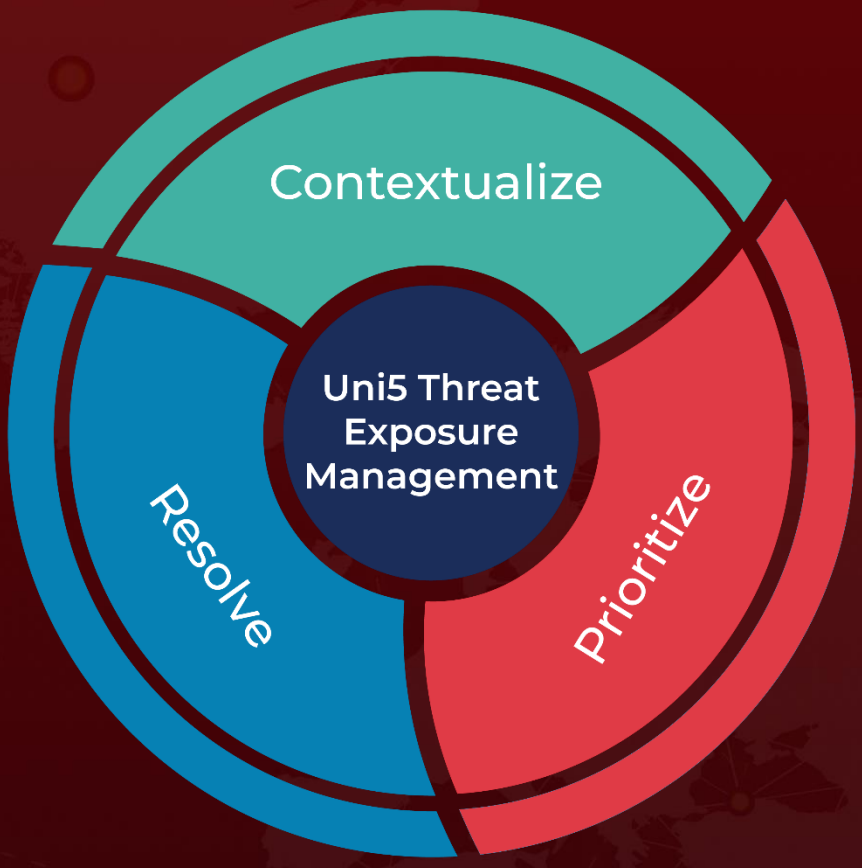
References

https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta4557-targets-recruiters-directly-email

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

December 14, 2023 . 4:10 AM

More at www.hivepro.com