Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Recruitment Under Siege: The Rise of the More_eggs Malware

Date of Publication	Admiralty Code	TA Number
October 3, 2024	A2	TA2024377

Summary

Attack Discovered: August 2024
Targeted Industry: Recruitment
Targeted Countries: Worldwide
Malware: More_eggs
Actor: FIN6 (aka Skeleton Spider, Gold Franklin, White Giant, ITG08, ATK 88, TAG-CR2, TAAL, Camouflage Tempest)
Attack: A recent spear-phishing campaign has been observed targeting recruiters with a JavaScript backdoor known as More_eggs, disguising itself as fake job applications. This malicious campaign highlights a continued focus on infiltrating the recruitment sector, leveraging the lure of potential hires to deliver malware. More_eggs is part of the Golden Chickens malware-as-a-service (MaaS) toolkit, a widely used platform by financially motivated threat actors.

Attack Regions

Attack Details

#1 A recent spear-phishing campaign has been detected targeting recruiters, deploying a malicious JavaScript backdoor known as More_eggs disguised as fake job applications. This campaign underscores the growing sophistication of attacks on the recruitment sector, where attackers exploit the inherent trust that recruiters place in potential candidates. By posing as job applicants, threat actors aim to deliver malware and gain unauthorized access to sensitive information. The More_eggs backdoor is part of the Golden Chickens MaaS toolkit, which has been widely utilized by financially motivated threat groups, including FIN6 and the Cobalt Group . These groups have a history of targeting financial institutions and retail organizations, making the current campaign particularly alarming.

#2 The attack typically begins when a recruiter is deceived into downloading a ZIP file that appears to contain a resume from a prospective candidate. This ZIP file includes an obfuscated LNK file, which, when executed, initiates a series of malicious actions. The LNK file executes commands that lead to the installation of the More_eggs backdoor by employing legitimate Windows processes like regsvr32.exe to circumvent detection mechanisms. Once the malware is installed, it establishes persistence by creating registry entries, ensuring that it runs each time the system is started. The backdoor then carries out reconnaissance activities, querying the system for information about network adapters, running processes, and startup configurations. This intelligence allows the attacker to assess the level of access and identify further exploitation opportunities within the compromised environment.

#3 The More_eggs backdoor serves as a potent tool for attackers, enabling them to exfiltrate sensitive data, deploy additional malicious payloads, and move laterally within networks. By facilitating unauthorized access to systems, the malware enhances the attackers' operational capabilities, making it easier for them to carry out their objectives. Moreover, the backdoor communicates with its C2 server through the IServerXMLHTTPRequest2 interface, allowing for remote execution of commands and additional module downloads.

#4 The use of More_eggs highlights how financially motivated threat actors continue to refine their tactics by utilizing MaaS platforms, which complicate attribution efforts. Multiple groups can leverage the same malware, making it challenging to identify the specific actors behind an attack. However, the TTPs observed in this campaign share similarities with those employed by FIN6. The use of sophisticated social engineering techniques, such as malicious files disguised as resumes and legitimate-looking websites, emphasizes the need for heightened security awareness among recruitment teams and organizations.

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.

Network Segmentation: Implement network segmentation to isolate critical infrastructure components from other systems. This can limit lateral movement for attackers and contain potential breaches.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link
T1204 User Execution	T1204.001 Malicious Link	T1037 Boot or Logon Initialization Scripts	T1037.001 Logon Script (Windows)
T1218 System Binary Proxy Execution	T1218.010 Regsvr32	T1016 System Network Configuration Discovery	T1497 Virtualization/Sandbox Evasion
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1059 Command and Scripting Interpreter	T1059.007 JavaScript

T1082 System Information Discovery	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1105** Ingress Tool Transfer
T1027 Obfuscated Files or Information	**T1036** Masquerading	**T1047** Windows Management Instrumentation	**T1057** Process Discovery
T1053 Scheduled Task/Job			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5131dbacb92fce5a59ac92893fa059c16cf8293e9abc26f2a61f9edd, 624afe730923440468cae991383dd1f7be1dadf65fa4cb2b21e3e5a9, ccf8276b55398030b6b7269136c5ee26a5c422d68793dc9ec5adee79a057c7f4, f2196309bc97e22447f6e168a9afbbb4291edd1cca51bf3789939c3618a63ec0, 3beda3377b060a89b41553485e06e42b69d10610f21a4a443f75b39605397271, d207aebf701c7fb44fe06993f020ac3527680c7fa8492a0b5f6154ca, 17ac712a84af8e5c7906bff6e1662a5278d33fa36f1c13fcf788
URLs	hxxps[:]//1212055764.johncboins[.]com/some/036e91fc8cc899cc20f7e011fa6a0861/sbosf, hxxp[:]//36hbhv.johncboins[.]com/fjkabrhhg, hxxps[:]//webmail.raysilkman[.]com
Email Address	fayereed11@gmail[.]com
Registry	HKCU\Environment /t 1 /v userinitmprlogonscript /d cscripT -e:jsCript "%APPDATA%\ Microsoft\D30F38D93CA9185.txt"

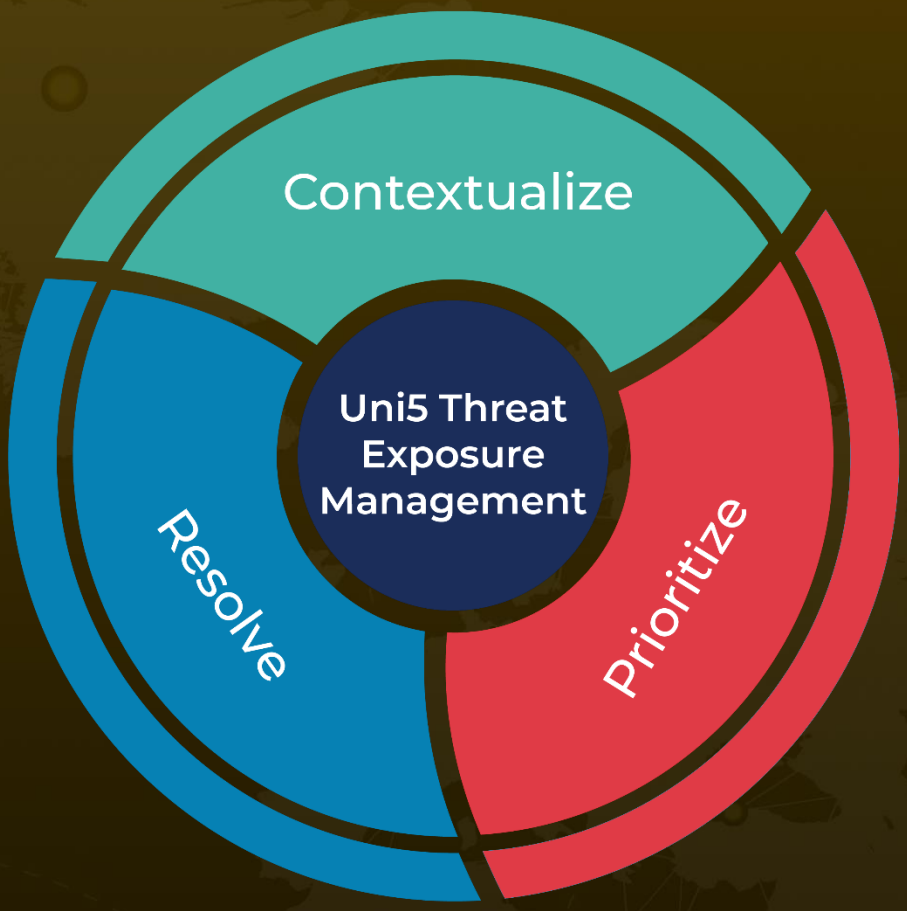
References

https://www.trendmicro.com/en_us/research/24/i/mdr-in-action--preventing-the-moreeggs-backdoor-from-hatching--.html

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

October 3, 2024 • 7:00 AM

More at www.hivepro.com