Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

FIN7 Group Leverages Sponsored Ads to Disseminate Malicious Payloads

Date of Publication	Admiralty Code	TA Number
May 13, 2024	A1	TA2024184

Summary

Discovered: April 2024
Malware: NetSupport RAT, DiceLoader
Actor: FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)
Attack: The financially motivated threat actor, FIN7, has been observed utilizing malicious websites to impersonate reputable brands. This tactic serves as a vehicle for delivering malicious payloads such as NetSupport RAT and DiceLoader, which represent subsequent stages in the infection chain.

Attack Regions

Attack Details

#1 FIN7, a Russian-based threat group operational since 2013, has been observed impersonating reputable brands such as AnyDesk, WinSCP, BlackRock, Asana, Concur, The Wall Street Journal, Workable, and Google Meet through fraudulent websites. Users who click on sponsored Google Ads are directed to these malicious websites, where they are prompted to download a fake browser extension. Notably, the group used certificates with names like "SOFTWARE SP Z O O" and "SOFTWARE BYTES LTD" to sign MSIX files.

#2 In one instance, a NetSupport RAT infection was detected. A malicious PowerShell script embedded within the MSIX file collects system data, identifies antivirus products, and generates a unique identifier. This script then communicates with a Command and Control (C2) server to download and execute further payloads, including the NetSupport RAT. Upon decoding the downloaded script, additional instructions are executed to retrieve and execute payloads, ultimately leading to the deployment of the NetSupport RAT executable.

#3 In another instance while following the similar infection chain, the threat actor utilized commands like "whoami /upn" to display the user principal name (UPN) of the logged-in user. They employed a lambda function to decode the Python payload and created a scheduled job to execute it. The decrypted output contained an encrypted DiceLoader payload and instructions for allocating memory with execute permissions. Process injection was accomplished by creating and launching a new thread to execute the payload using the decrypted output. C2 IPs and ports for DiceLoader were stored in the .data area and XORed using a hardcoded key.

#4 The instances of FIN7 distributing NetSupport RAT and DiceLoader through fake web advertisements and reputable brand names underscore the persistent threat posed by these actors. Additionally, the usage of certificates to sign malicious binaries highlights the need for heightened security measures and vigilance to combat such cyber threats.

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.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0011 Command and Control	T1566 Phishing	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1059.006 Python	T1204 User Execution	T1204.001 Malicious Link
T1547 Boot or Logon Autostart Execution	T1033 System Owner/User Discovery	T1176 Browser Extensions	T1199 Trusted Relationship
T1056 Input Capture	T1036 Masquerading	T1053 Scheduled Task/Job	T1140 Deobfuscate/Decode Files or Information

T1055 Process Injection	T1588 Obtain Capabilities	T1588.003 Code Signing Certificates	T1518 Software Discovery
T1518.001 Security Software Discovery	T1592 Gather Victim Host Information	T1082 System Information Discovery	T1219 Remote Access Software
T1104 Multi-Stage Channels	T1132 Data Encoding	T1132.001 Standard Encoding	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	cdn41[.]space, cdn46[.]space, cdn45[.]space, cdn35[.]space, cdn30[.]space, cdn34[.]space, cdn32[.]space, cdn43[.]space, cdn37[.]space, cdn42[.]space, cdn27[.]space, cdn25[.]space, cdn36[.]space, cdn33[.]space, cdn40[.]click, cdn31[.]space, cdn38[.]space, eprst431[.]boo, cdn1124[.]net, cdn1701[.]com
IPv4:Port	193[.]124[.]24[.]51:443, 38[.]135[.]52[.]151:273
IPv4	5[.]8[.]63[.]140, 185[.]174[.]102[.]62, 109[.]107[.]170[.]126, 193[.]233[.]206[.]23
URL	wall-street-journal[.]link, sapconcur[.]pro, concur[.]pm,

TYPE	VALUE
URL	advancedipscannerapp[.]com, workable.uk[.]com, wsj[.]wf, wsj[.]re, wsj[.]pm, wsj[.]wales, asana[.]tel, advanced-ip-scanner[.]link, concur[.]re, concur[.]skin, asana[.]wf, blackrock[.]wf, blackrock[.]re, lexisnexis[.]day, quicken-install[.]com, vkontakte[.]in, autodesk[.]pm, 7-zip[.]cfd, meet-go[.]click, winscp-install[.]com, webex-install[.]com, investing[.]wf, pgadmin[.]link, asana[.]pm, aimp[.]day, workday[.]pm, www[.]any-connectcisco[.]com
MD5	b6f12d39edbfe3b33952be4329064b35, e7b1fb0ef5dd20f4522945b902803f10, 0740803404a58d9c1c1f4bd9edaf4186, 782621d1062a8fc7d626ceb68af314e5, bb0a503a83b1f9833c3d3d08784b78a8

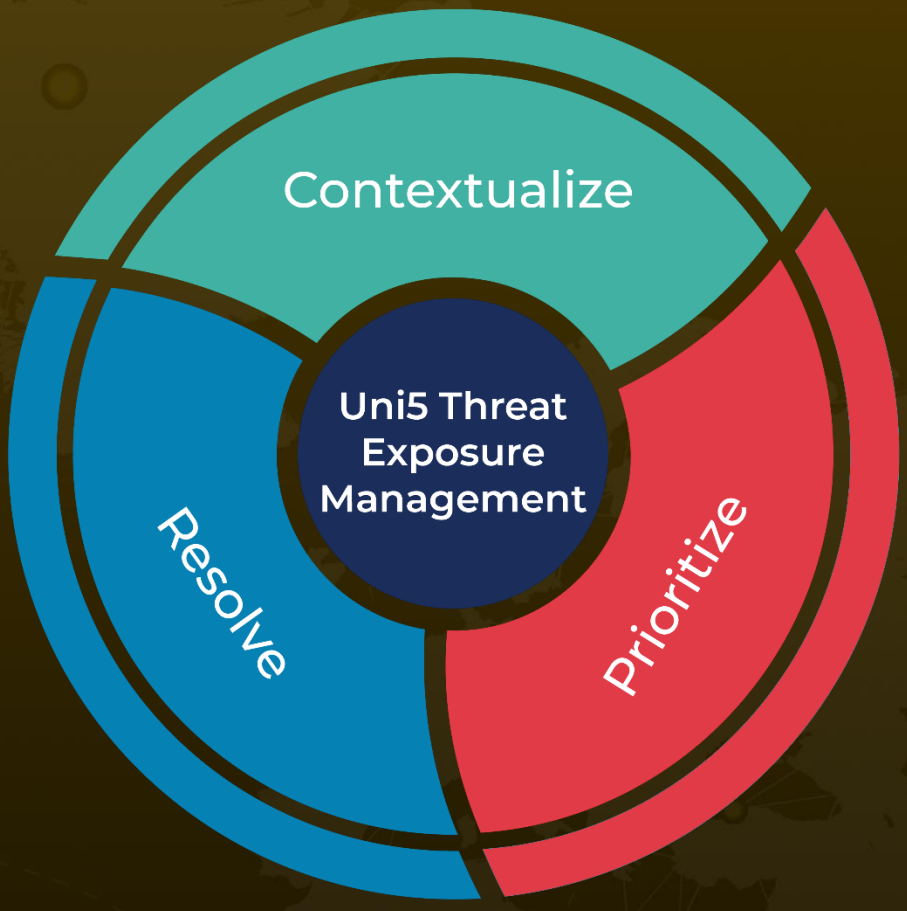
References

https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads

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 13, 2024 • 9:30 PM

More at www.hivepro.com