Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

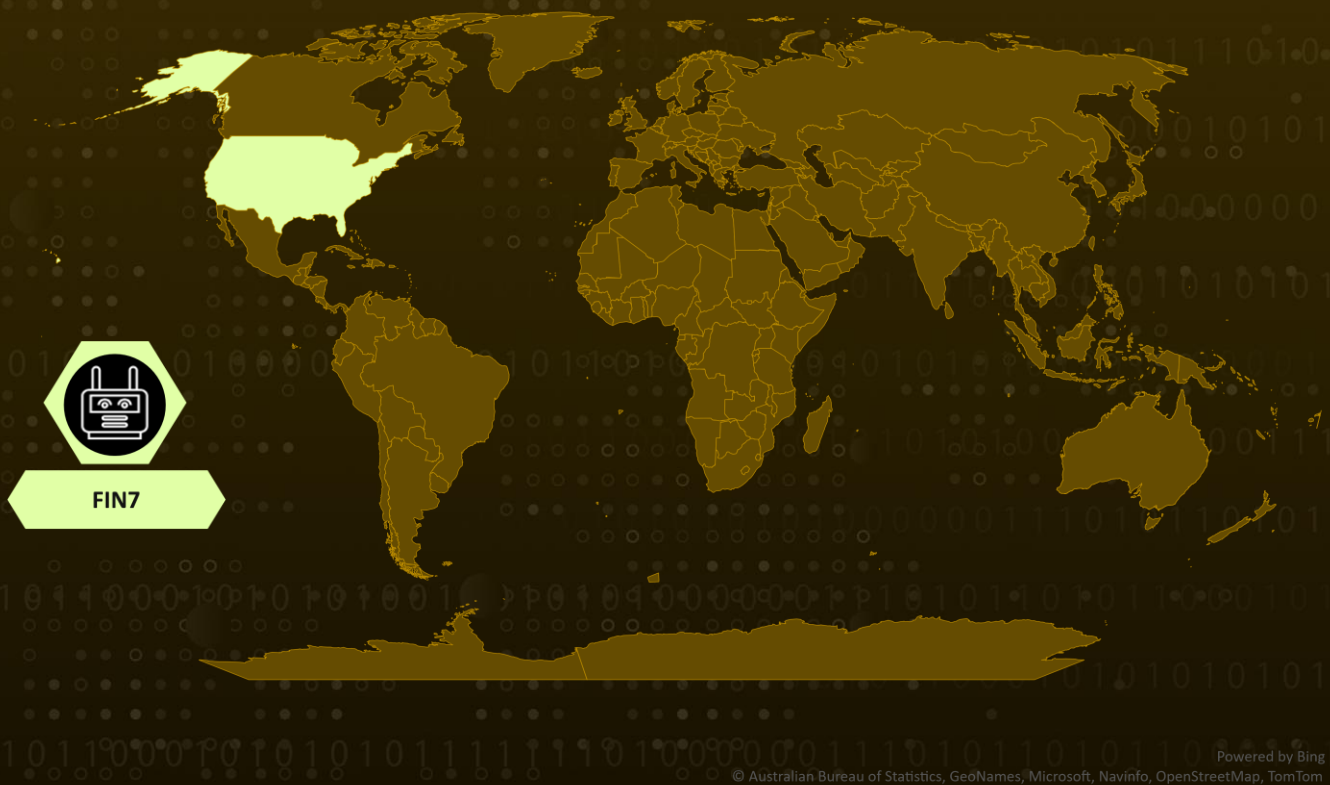
FIN7 Takes Aim at the U.S. Auto Industry

Date of Publication	Admiralty Code	TA Number
April 19, 2024	A1	TA2024156

Summary

Threat Actor: FIN7 (aka Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, ITG14, TAG-CR1)
Malware: Carbanak Backdoor (aka Anunak)
Attack Region: USA
Targeted Industry: Automotive
Attack: FIN7 has been orchestrating a spear-phishing campaign targeting the U.S. automotive sector. Their method involved enticing victims with a complimentary IP scanning tool, which was a conduit for installing the notorious Carbanak backdoor.

Attack Regions



Attack Details

#1 FIN7 has been implicated in a spear-phishing campaign targeting the U.S. automotive sector, utilizing the infamous Carbanak (also known as Anunak) backdoor. Their strategy involved luring targets with the promise of a free IP scanning tool, which acted as the means to install the Carbanak backdoor.

#2 The initial foothold was established via living off-the-land binaries, scripts, and libraries. FIN7 (aka Carbon Spider), is a significant cybercrime syndicate primarily motivated by financial gain. It has gained notoriety for its extensive history of infiltrating various industries to deploy malware capable of stealing data from point-of-sale (PoS) systems since 2013.

#3 Recently, their tactics have shifted from broad-scale attacks to precise strikes against major entities, a strategy commonly referred to as big game hunting. In this case, individuals with elevated access privileges were specifically targeted through spear-phishing emails containing links to an IP scanning tool, disguised as a legitimate website but a malicious URL.

#4 Upon visiting the fake site, they were redirected to a Dropbox account controlled by the attackers, resulting in the unintentional download of a malicious executable onto their systems. This executable initiates a multi-stage process that ultimately executes Carbanak, while also facilitating the deployment of additional payloads like POWERTRASH and establishing persistence by installing OpenSSH for remote access.

Recommendations

Enforce Multi-Factor Authentication (MFA): Strengthen account security by implementing MFA on all user accounts to mitigate unauthorized access, even in the event of password compromise.

Enhance Email Filtering and Authentication: Deploy advanced email filtering solutions to intercept and block phishing emails before they reach users' inboxes. Utilize SPF, DKIM, and DMARC to authenticate email senders and identify spoofed emails.

Privileged Access Management (PAM): Implement PAM solutions to enforce least privilege access policies, restricting access to sensitive systems and data to authorized personnel only.

Increase Social Engineering Awareness: Expand training to include identifying social engineering tactics across various communication platforms, such as social media, phone calls, texts, and video calls.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0008** Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1027** Obfuscated Files or Information	**T1021.004** SSH	**T1033** System Owner/User Discovery
T1041 Exfiltration Over C2 Channel	**T1053.005** Scheduled Task	**T1057** Process Discovery	**T1059.001** PowerShell
T1069.002 Domain Groups	**T1082** System Information Discovery	**T1087.002** Domain Account	**T1090** Proxy
T1124 System Time Discovery	**T1204.002** Malicious File	**T1222.001** Windows File and Directory Permissions Modification	**T1543.003** Windows Service
T1562.004 Disable or Modify System Firewall	**T1564.001** Hidden Files and Directories	**T1566.002** Spearphishing Link	**T1566** Phishing
T1571 Non-Standard Port	**T1583.001** Domains	**T1608.005** Link Target	**T1569.002** Service Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	87aa5f3f514af2b9ef28db9f092f3249, Bb23dde1e3ecef7d93a39e77e32ef96c
SHA256	bc4ef49e904d63415ee1c810c90019e12a590ff3b6293f4b69af65713a8da9fa, d4960f3c7cc891ff2bafd0a080451e42e0a23ba4db54ae2d7d355497a3b3d81a, 7e927e1db12c404683c9c8b232e8cecb7334eed618992e965388b0b63508509f, cdc0186ff3fcb67986f4f1f54e3a2991dd73f8bde20acf3a739e0fff7c6d94a7, c8d8d666b509afaa0ef349cc3de9a6eec6dde98cc8a0e50228f8793275fae401, 5ce7b63ef05d9f5cb8e309e6b195e3acb69cc72b899f4ae07c48b85bedfb286e, ff4c287c60ede1990442115bddd68201d25a735458f76786a938a0aa881d14ef, d63060e61c98074c58926a6239185e8128fd0fbc2a45ccf60f3c831bb18ffc93
Domains	advanced-ip-sccanner[.]com, myipscanner[.]com, theipscanner[.]com, ipscanneronline[.]com, ipscannershop[.]com, myscannappo[.]com, myscannappo[.]info, myscannappo[.]online
IPv4	181[.]215[.]69[.]24, 166[.]1[.]160[.]118, 185[.]39[.]204[.]179, 109[.]107[.]171[.]62, 38[.]180[.]1[.]17, 109[.]107[.]170[.]47, 162[.]248[.]224[.]79, 166[.]1[.]190[.]171, 166[.]1[.]190[.]186, 172[.]82[.]87[.]69, 185[.]161[.]210[.]18, 185[.]72[.]8[.]6, 185[.]72[.]8[.]70, 193[.]233[.]206[.]146, 207[.]174[.]31[.]205,

TYPE	VALUE
IPv4	207[.]174[.]31[.]206, 209[.]209[.]113[.]91, 217[.]196[.]101[.]116, 38[.]180[.]14[.]240, 38[.]180[.]40[.]23, 46[.]246[.]98[.]196, 5[.]181[.]159[.]11, 62[.]233[.]57[.]98, 104[.]166[.]127[.]197, 104[.]166[.]127[.]200, 155[.]254[.]192[.]66, 166[.]1[.]190[.]48, 185[.]72[.]8[.]147, 193[.]233[.]22[.]136, 193[.]233[.]22[.]28, 193[.]233[.]22[.]36, 193[.]233[.]22[.]43, 193[.]233[.]23[.]177, 207[.]174[.]31[.]253, 23[.]133[.]88[.]52, 38[.]180[.]1[.]103, 38[.]180[.]20[.]94, 5[.]61[.]39[.]157, 5[.]8[.]63[.]105, 5[.]8[.]63[.]108, 5[.]8[.]63[.]139, 5[.]8[.]63[.]245, 62[.]233[.]57[.]195, 91[.]149[.]254[.]85

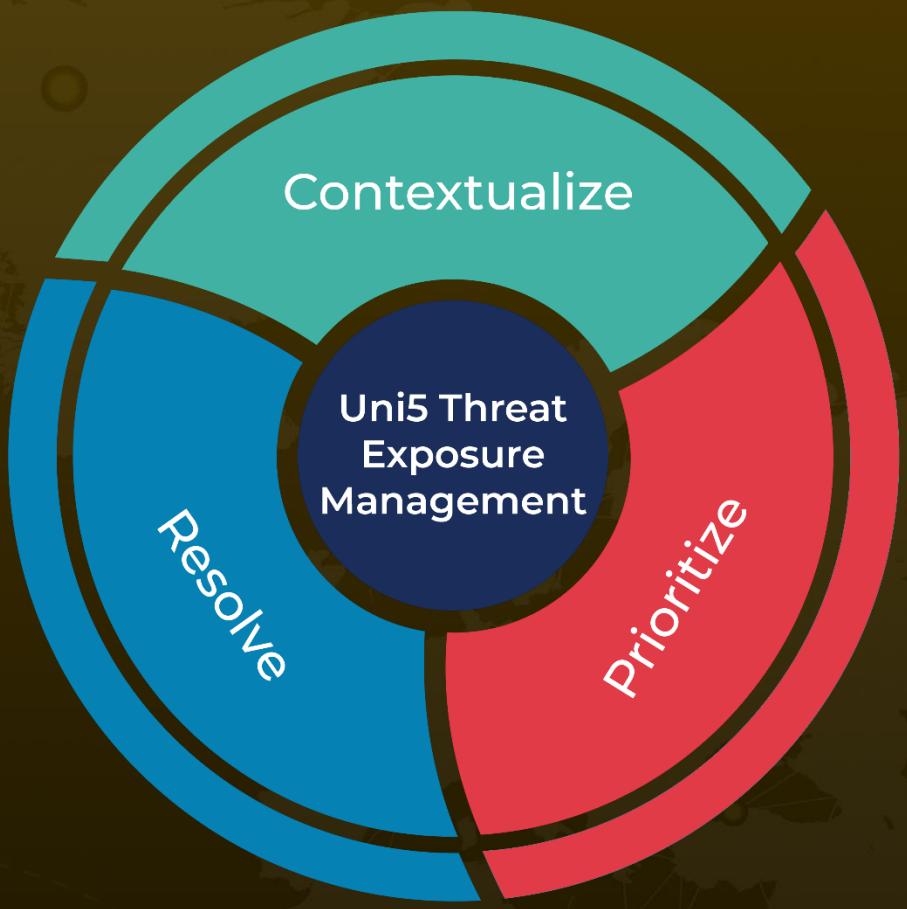
References

https://blogs.blackberry.com/en/2024/04/fin7-targets-the-united-states-automotive-industry

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

April 19, 2024 • 4:50 AM

More at www.hivepro.com