Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

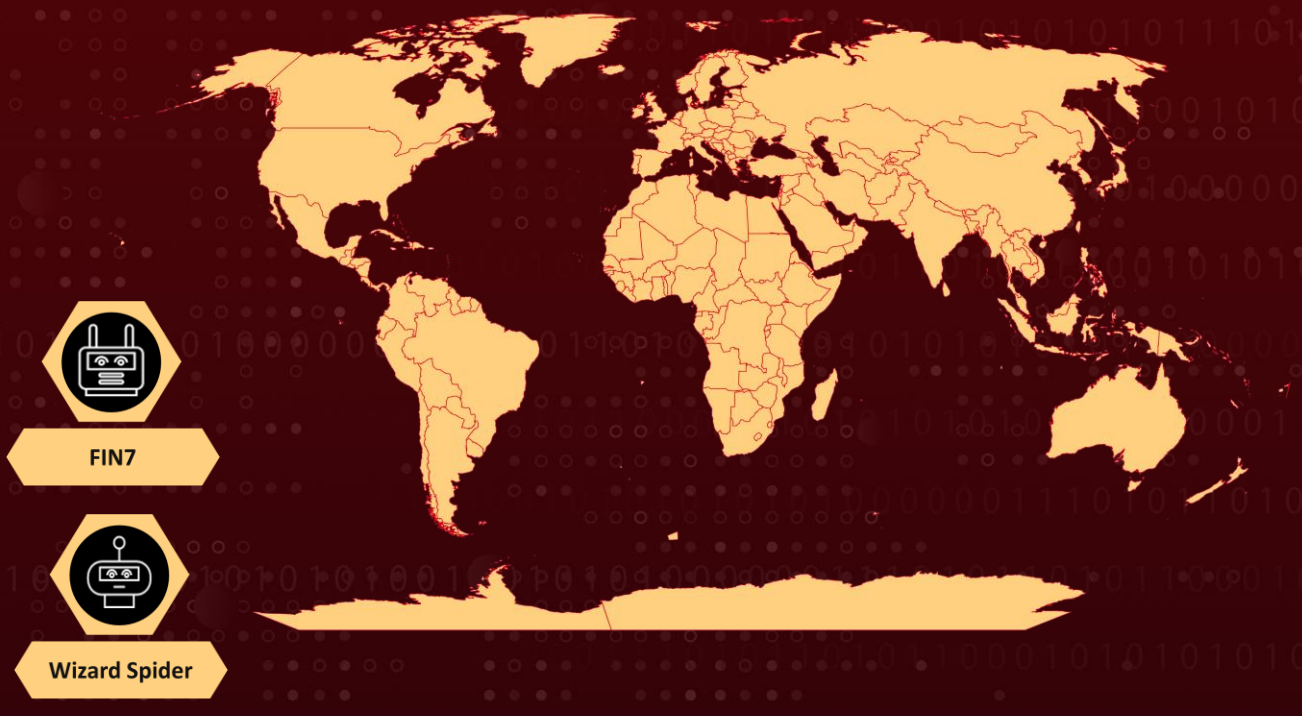
FIN7 & Wizard Spider team up to disseminate Domino malware

Date of Publication	Admiralty Code	TA Number
April 18, 2023	A3	TA2023192

Summary

Attack began: February 2023
Malware: Dave Loader, Domino Backdoor, NewWorldOrder Loader, Carbanak Backdoor, Project Nemesis infostealer
Threat Actors: FIN7(aka ITG14, Gold Niagara, Calcium, Navigator, ATK 32, APT-C-11, TAG-CR1) and Wizard Spider(aka ITG23, Grim Spider, TEMP.MixMaster, Gold Blackburn, Gold Ulrick)
Attack Region: Worldwide
Attack: Wizard Spider group have teamed up with the FIN7 threat actors to distribute a new malware family named 'Domino' in attacks to deploy either the Project Nemesis information stealer or more capable backdoors such as Cobalt Strike.

Attack Regions



Attack Details

#1 Former members of Wizard Spider (ITG23 aka, the Trickbot/Conti syndicate) are likely behind recent campaigns utilizing Dave Loader to execute the Domino Backdoor. They likely collaborated with present or former developers of FIN7 (aka ITG14) to obtain or employ the new malware family.

#2 Dave Loader is one of several loaders developed by members of the Wizard Spider group. Furthermore, Dave Loader has been utilized this year to load IcedID and Emotet, which serve as initial access vectors for ransomware attacks originating from factions associated with Wizard Spider.

#3 Samples of Dave Loader, which were recently discovered, are now seen to be loading a new malware known as the Domino. The Domino Backdoor obtains fundamental system information, which it then transmits to the C2, and receives an AES-encrypted payload in return.

#4 The Domino malware family consists of two parts: the backdoor called "Domino Backdoor" that drops a "Domino Loader," which in turn inserts an info-stealing malware DLL into the memory of another process. The Domino Backdoor and Loader have similarities in code with the Lizar Malware (also known as Tirion and DiceLoader), which is linked to the threat group FIN7.

#5 The Domino Loader includes an encrypted payload in its resources, which it decrypts using AES. The decrypted payload is a .NET infostealer identified as "Nemesis Project," which is one of Domino's final payloads. The Domino Backdoor is configured to connect with a different C2 address for systems joined to a domain, suggesting that a more advanced backdoor, such as Cobalt Strike, will be installed on high-value targets.

#6 Additionally, the NewWorldOrder loader, typically used in FIN7's Carbanak attacks, was recently employed to distribute the Domino malware. The use of malware associated with multiple groups in a single campaign offers insights into their methods and collaborations.

Recommendations

To avoid falling victim to cyber-attacks, businesses must remain vigilant and take necessary precautions. While routine education and awareness training is important, it is crucial to also consider factors such as MFA fatigue and web browser hygiene. Additionally, it is important to always verify the authenticity of email attachments and avoid opening untrusted links. By implementing these measures, businesses can better protect themselves against potential threats.

To ensure the safety of important data, conduct regular offline backups and install reputable anti-virus and Internet security software on all connected devices. It is also advised to turn on automatic software updates whenever possible and practical. Moreover, consider implementing proactive security measures like blocking indicators of compromise (IoCs) to stay ahead of potential threats.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0007** Discovery
TA0009 Collection	**TA0011** Command and Control	**T1047** Windows Management Instrumentation	**T1059** Command and Scripting Interpreter
T1129 Shared Modules	**T1036** Masquerading	**T1497** Virtualization/Sandbox Evasion	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1027** Obfuscated Files or Information	**T1497.002** User Activity Based Checks	**T1564** Hide Artifacts
T1564.003 Hidden Window	**T1003** OS Credential Dumping	**T1056** Input Capture	**T1056.001** Keylogging
T1010 Application Window Discovery	**T1057** Process Discovery	**T1518** Software Discovery	**T1115** Clipboard Data
T1005 Data from Local System	**T1071** Application Layer Protocol	**T1573** Encrypted Channel	**T1518.001** Security Software Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	88.119.175[.]124 94.158.247[.]72 178.23.190[.]73 185.225.17[.]202 5.182.37[.]118 45.67.34[.]236
Domain	es-megadom[.]com
URLs	hxxp://170.130.55[.]250/x64.exe hxxps://upperdunk[.]com/mr64.exe
SHA256	de9b3c01991e357a349083f0db6af3e782f15e981e2bf0a16ba618252585923a b14ab379ff43c7382c1aa881b2be39275c1594954746ef58f6a9a3535e8dc1a8 dbdfc3ca5afa186c1a9a9c03129773f7bc17fb7988fe0ca40fc3c5bedb201978 ce99b4c0d75811ce70610d39b1007f99560e6dea887a451e08916a4f8cf33678 f1817665ea2831f775e23cbda27cbeb06d03e6c39bbfad920b50f40712dd37cb 51e0512a54640be8e3477363c8d72d893c6edd20399bddf71e95eec3ddfdb42e f4ebd59fb578a0184abf6870fc652210d63e078a35dace0a48c5f273e417c13d 92651f9418625e5281b84cccb817e94e6294b36c949b00fcd4046770b87f10e4 e5af0b9f4650dc0193c9884507e6202b04bb87ac5ed261be3f4ecfa3b6911af8

References

https://securityintelligence.com/posts/ex-conti-fin7-actors-collaborate-new-domino-backdoor/

https://attack.mitre.org/groups/G0046/

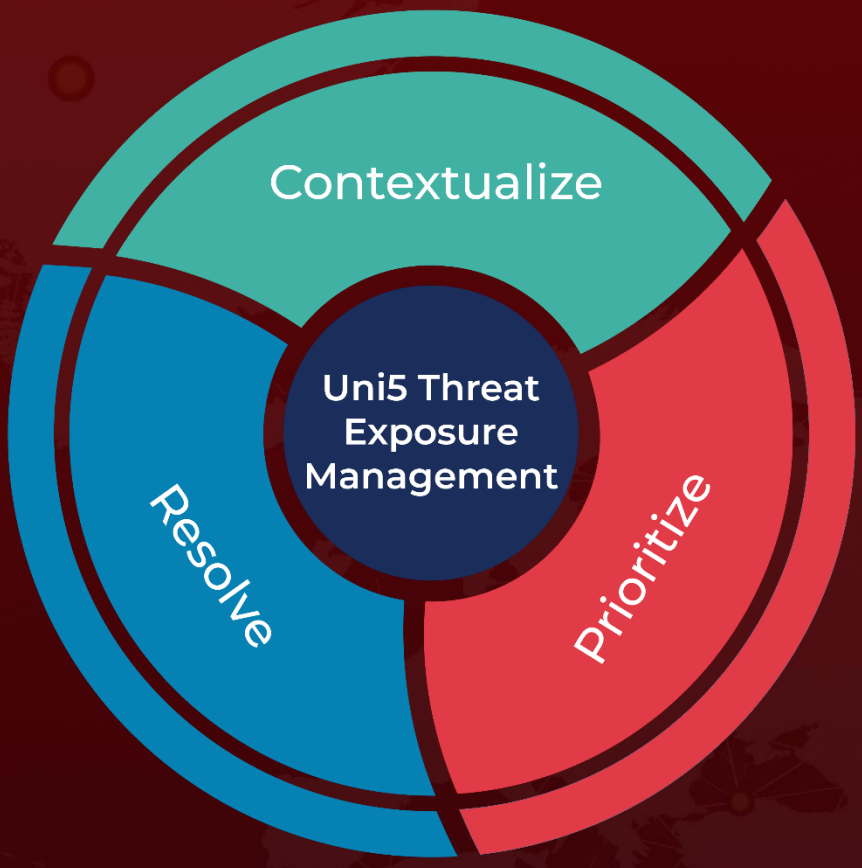
https://attack.mitre.org/groups/G0102/

https://www.darkreading.com/attacks-breaches/fin7-former-conti-gang-members-collaborate-domino-malware

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 18, 2023 • 6:18 AM

More at www.hivepro.com