Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

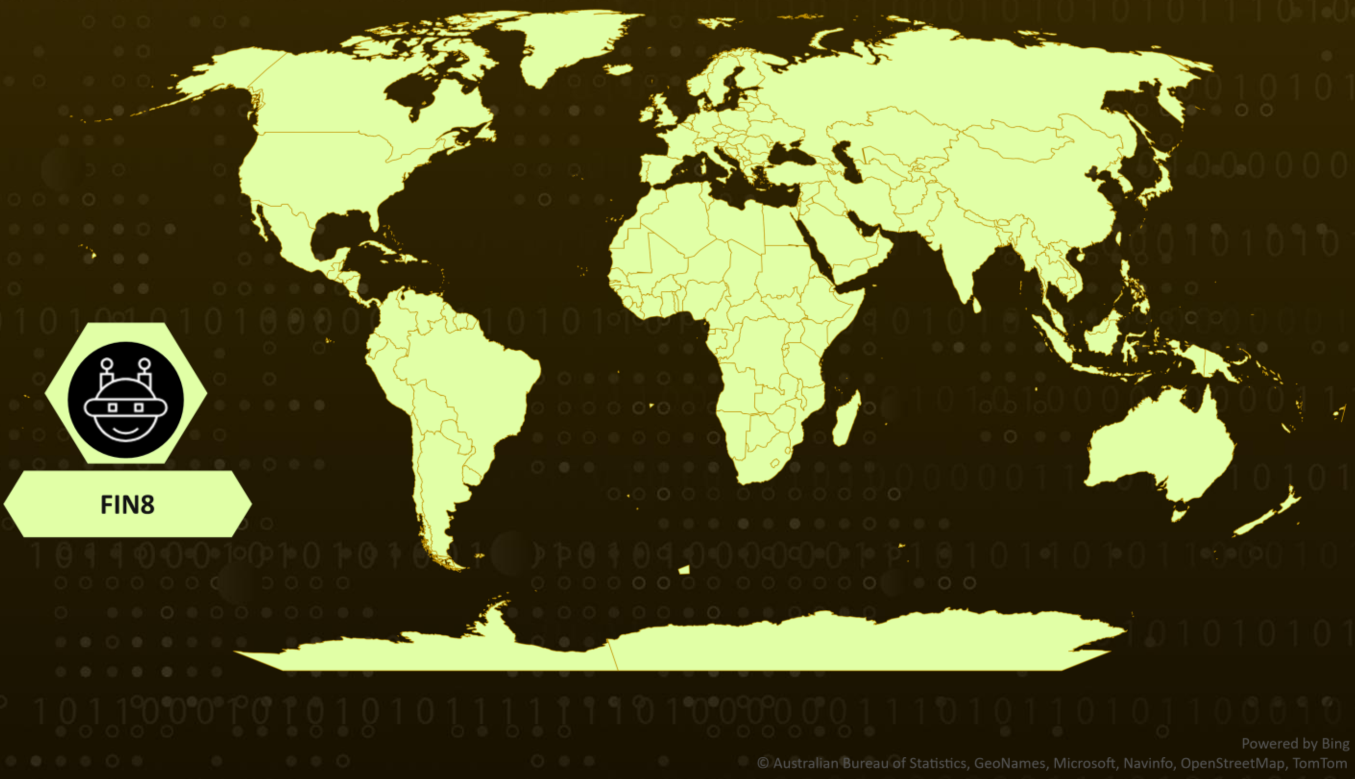
FIN8 Strikes with Noberus Ransomware via Altered Sardonic Backdoor

Date of Publication	Admiralty Code	TA Number
July 19, 2023	A1	TA2023304

Summary

Attack Began: December 2022
Malware: Sardonic backdoor and Noberus ransomware (aka BlackCat, ALPHV)
Actor: FIN8 (aka Syssphinx, ATK 113)
Targeted Industries: Hospitality, Retail, Entertainment, Insurance, Technology, Chemicals, and Finance Sectors.
Attack Region: Worldwide
Attack: The financially motivated threat actor FIN8 has been detected employing a revised variant of the backdoor known as Sardonic to deliver the Noberus ransomware.

Attack Regions


FIN8
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 A financially motivated cybercrime syndicate, identified as FIN8 (aka Syssphinx), has been observed deploying Noberus ransomware (aka BlackCat or ALPHV) payloads on compromised networks using an enhanced version of the Sardonic malware. This sophisticated threat actor has been actively operating since January 2016, initially targeting point-of-sale (PoS) systems with malware like PUNCHTRACK and BADHATCH.

#2 The FIN8 group is renowned for employing "living-off-the-land" techniques, leveraging built-in tools and interfaces such as PowerShell and WMI, while exploiting legitimate services to conceal their malicious activities. Social engineering and spear-phishing are the group's favored methods for initiating their attacks.

#3 In the December 2022 breach, the assailants utilized PsExec to execute the command "quser," allowing them to access and display session details before deploying the backdoor. Furthermore, FIN8 made a transition from BadHatch to a more sophisticated C++-based backdoor named Sardonic, which enables the collection of information, execution of commands, and deployment of malicious DLL plugins.

#4 Syssphinx exhibits an unwavering dedication to the continuous progression and refinement of its capabilities and malware delivery infrastructure, ceaselessly optimizing its tools and tactics to elude detection. Among the additional attributes of the backdoor, it possesses the capability to deliberately drop arbitrary files and covertly exfiltrate file contents from the compromised system to infrastructure under the control of the threat actors.

Recommendations

Strengthen network defense measures against PsExec usage and implement behavior-based detection to thwart FIN8's session details reconnaissance.

Enhance endpoint security with advanced threat detection to counter the evolving capabilities of Syssphinx's C++-based backdoor and prevent arbitrary file drops and data exfiltration.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0007 Discovery
TA0011 Command and Control	T1055 Process Injection	T1070 Indicator Removal	T1070.004 File Deletion
T1497 Virtualization/Sandbox Evasion	T1010 Application Window Discovery	T1057 Process Discovery	T1082 System Information Discovery
T1083 File and Directory Discovery	T1518 Software Discovery	T1518.001 Security Software Discovery	T1573 Encrypted Channel
T1598 Phishing for Information	T1598.002 Spearphishing Attachment	T1059.001 PowerShell	T1047 Windows Management Instrumentation

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509, 307c3e23a4ba65749e49932c03d5d3eb58d133bc6623c436756e48de68b9cc45, 48e3add1881d60e0f6a036cfdb24426266f23f624a4cd57b8ea945e9ca98e6fd, 4db89c39db14f4d9f76d06c50fef2d9282e83c03e8c948a863b58dedc43edd31, 356adc348e9a28fc760e75029839da5d374d11db5e41a74147a263290ae77501, e7175ae2e0f0279fe3c4d5fc33e77b2bea51e0a7ad29f458b609afca0ab62b0b, e4e3a4f1c87ff79f99f42b5bbe9727481d43d68582799309785c95d1d0de789a, 2cd2e79e18849b882ba40a1f3f432a24e3c146bb52137c7543806f22c617d62c, 78109d8e0fbe32ae7ec7c8d1c16e21bec0a0da3d58d98b6b266fbc53bb5bc00e,

TYPE	VALUE
SHA256	ede6ca7c3c3aedeb70e8504e1df70988263aab60ac664d03995bce645dff0935, 5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a8ca18c28, 4e73e9a546e334f0aee8da7d191c56d25e6360ba7a79dc02fe93efbd41ff7aa4, 05236172591d843b15987de2243ff1bfb41c7b959d7c917949a7533ed60aafd9, edfd3ae4def3ddffb37bad3424eb73c17e156ba5f63fd1d651df2f5b8e34a6c7, 827448cf3c7ddc67dca6618f4c8b1197ee2abe3526e27052d09948da2bc500ea, 0e11a050369010683a7ed6a51f5ec320cd885128804713bb9df0e056e29dc3b0, 0980aa80e52cc18e7b3909a0173a9efb60f9d406993d26fe3af35870ef1604d0, 64f8ac7b3b28d763f0a8f6cdb4ce1e5e3892b0338c9240f27057dd9e087e3111, 2d39a58887026b99176eb16c1bba4f6971c985ac9acbd9e2747dd0620548aaf3, 8cfb05cde6af3cf4e0cb025faa597c2641a4ab372268823a29baef37c6c45946, 72fd2f51f36ba6c842fdc801464a49dce28bd851589c7401f64bbc4f1a468b1a, 6cba6d8a1a73572a1a49372c9b7adfa471a3a1302dc71c4547685bcbb1eda432
IPv4	37.10.71[.]215
Domains	api-cdn[.]net, git-api[.]com, api-cdnw5[.]net, 104-168-237-21.sslip[.]io

References

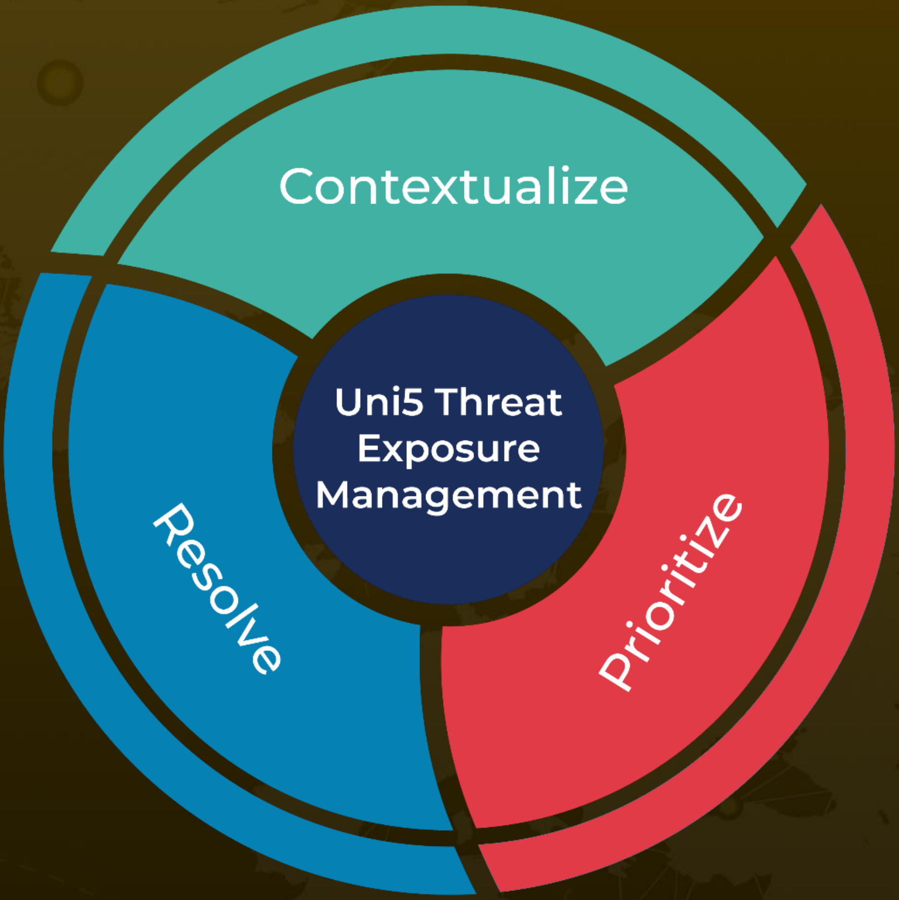
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/Syssphinx-FIN8-backdoor

https://attack.mitre.org/groups/G0061/

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

July 19, 2023 • 6:00 AM

More at www.hivepro.com