KPMG Cyber Threat Intelligence Platform

FIN8 – Continues to Evolve its Toolkit

FIN8 (aka ATK113, G0061, Syssphinx) is a financially motivated cybercrime group known for launching spear-phishing campaigns and has been operating since 2016. It specializes in Point-of-Sale (POS) attack, but in the past few years, the group has been observed launching ransomware attacks for maximizing profits. The group resurfaced with an updated version of BADHATCH in March 2021 and has been observed deploying Blackcat (aka ALPHV) ransomware via revamped Sardonic backdoor in December 2022. The group has been known to target a variety of industries, like chemicals, retail, hospitality and entertainment.

Initial access is achieved through spear-phishing emails with malicious documents or social engineering techniques. The malware then conducts network reconnaissance to identify trusted domains, users, and domain controllers. To establish persistence, it employs living-off-the-land tactics, abusing binaries like PowerShell and WMI to execute its malicious code. Post execution, the malware performs a series of tasks, including checking the process architecture, decoding and loading the .NET Loader binary, initiating the injector, decrypting the backdoor, and self-deleting. The injector operates as shellcode, injecting a backdoor into a newly generated WmiPrvSE.exe process, preferably in session 0, using a token acquired from the lsass.exe process. The backdoor uses PE DLL plugins, dedicated process execution for Shellcode formats, and explicit 64-bit argument passing to evade detection and enhance its activities. It communicates with its C&C server using RC4 encryption and variable-sized messages.

FIN8 constantly enhances its capabilities and malware delivery infrastructure, refining tactics to evade detection. Expanding from point-of-sale attacks to ransomware showcases their commitment to maximizing profits from targeted organizations.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

FIN8 – Continues to Evolve its Toolkit

Indicators of Compromise: IP Addresses	
37.10.71[.]215	104.168.132[.]128
170.130.55[.]120	192.52.167[.]199

Indicators of Compromise: Domains	
api-cdn[.]net	kapintarama[.]net
git-api[.]com	druhanostex[.]net
us-west[.]com	nduropasture[.]net
api-cdnw5[.]net	manrodoerkes[.]org
asilofsen[.]net	troxymuntisex[.]org
subarnakan[.]org	moreflorecast[.]org
ashkidiore[.]org	104-168-237-21.sslip[.]io
preploadert[.]net	

Indicators of Compromise: Hashes
10e75f522c3a52532d124e507d1d6561
bd265f2d3e827e2ffa22417a6334d5fa
2dad0e66463869b2565449e4c9e84417
52aa13beb502a784626b674c76169c08
7285d3b9ad2fee1969a22408f7efc324
43af915af6a0d60cc5875f69c7fa058b
655c3c304a2fe76d178f7878d6748439
087f82581b65e3d4af6f74c8400be00e
09ddc1ded40480e973243377971a2dcb
b3c30a575695e713e8307b7c0b429557
9774b2e5e34269bc3adc01d73bdfa76a
f12f70c4756826105d693af27bb10627
e73c4185f9712671c683f28fbddd1cca
bf7fcef0f51a7fe6d00752b8cdf25762
5b638fde02fb7bf18ff68e9d99bd8de0
39145f3e1ac2d74d19cb4137ee3db000
c9a1453b9a08c0667af1deada4323c83
01cadd7ccd80b4873183f340ef9a9878

KPMG

KPMG Cyber Threat Intelligence Platform

FIN8 – Continues to Evolve its Toolkit

Indicators of Compromise: Hashes
15ba461bbe05838f295cea910dee25df
4e693689526ee28290ddd9cdd242a3c5f0383b8d
ea50aa7c4d8b3097a2e7d8a4c575b08cfabbbdd8
12c3b36ee26b031e6c7b80b7e34b48489bfd108d
e8d3e810d1752237b2121cde19719c282acecd75
ef071f69df4a7ed21526804830d60a67c604228f
a384c188376b2dc98e855609bb8392f66e3295ac
ea2033e3c6190a2a025c288cdf429894dc86721b
ec35eeb8afaf0d7521ac098c20acfbb1680fd3d8
42963c342a761abcbff74df9efc27007b40e329c
949d36ea8e47cb9530b1bbd3af29cf7b1a01b612
adc27dc8a9e33cc2c7684bf47d5cc98d0bdc7958
79e5ac6f2a517ab7fa0e2bd0103ea0c14958e8e9
75fc0ce25767c0366b9c330de99f077620bb7c37
5d97e581853be9a8ca94a3b09d9f75f4ce99ef56
6c21e2aef9f3441786920acc6aa7bfddb240b2a6
f229183304a5a1308b844a06b2b618cdd5518111
4b4dfeb0b340ebec14f0d2d6c7f314aca9038f45
dfb235d59d9f35d43895395dd1b168ab258c861f
68051b0726e19b16867d3bc46434c6a3d1840e82
1d3e573d432ef094fba33f615aa0564feffa99853af77e10367f54dc6df95509
307c3e23a4ba65749e49932c03d5d3eb58d133bc6623c436756e48de68b9cc45
48e3add1881d60e0f6a036cfdb24426266f23f624a4cd57b8ea945e9ca98e6fd
4db89c39db14f4d9f76d06c50fef2d9282e83c03e8c948a863b58dedc43edd31
356adc348e9a28fc760e75029839da5d374d11db5e41a74147a263290ae77501
e7175ae2e0f0279fe3c4d5fc33e77b2bea51e0a7ad29f458b609afca0ab62b0b
e4e3a4f1c87ff79f99f42b5bbe9727481d43d68582799309785c95d1d0de789a
2cd2e79e18849b882ba40a1f3f432a24e3c146bb52137c7543806f22c617d62c
78109d8e0fbe32ae7ec7c8d1c16e21bec0a0da3d58d98b6b266fbc53bb5bc00e
ede6ca7c3c3aedeb70e8504e1df70988263aab60ac664d03995bce645dff0935
5b8b732d0bb708aa51ac7f8a4ff5ca5ea99a84112b8b22d13674da7a8ca18c28
4e73e9a546e334f0aee8da7d191c56d25e6360ba7a79dc02fe93efbd41ff7aa4
05236172591d843b15987de2243ff1bfb41c7b959d7c917949a7533ed60aafd9
edfd3ae4def3ddffb37bad3424eb73c17e156ba5f63fd1d651df2f5b8e34a6c7

KPMG

KPMG Cyber Threat Intelligence Platform

FIN8 – Continues to Evolve its Toolkit

Indicators of Compromise: Hashes
0e11a050369010683a7ed6a51f5ec320cd885128804713bb9df0e056e29dc3b0
0980aa80e52cc18e7b3909a0173a9efb60f9d406993d26fe3af35870ef1604d0
64f8ac7b3b28d763f0a8f6cdb4ce1e5e3892b0338c9240f27057dd9e087e3111
2d39a58887026b99176eb16c1bba4f6971c985ac9acbd9e2747dd0620548aaf3
8cfb05cde6af3cf4e0cb025faa597c2641a4ab372268823a29baef37c6c45946
72fd2f51f36ba6c842fdc801464a49dce28bd851589c7401f64bbc4f1a468b1a
6cba6d8a1a73572a1a49372c9b7adfa471a3a1302dc71c4547685bcbb1eda432
03e8b29ad5055f1dda1b0e9353dc2c1421974eb3d0a115d0bb35c7d76f50de20
4ee21b5fd8597e494ae9510f440a1d5bbcdb01bc653226e938df4610ee691f3a
a9dcdf037d39e88bc71ae844971e63aa78379d50ce47e8aaad0e4b1baf6c7040
Da89d50220da32060ef38546d1160162637ff72e3c3fa2268febca9331eb5adc
8637b972d5db5c4cb152b0a42f4866c9b574e68023b7620911af8e3d472d4701
5634140992891d2382fa103031b96023b75470ecd1bf0cf88006a45e63ef41bc
Ee188b38b4ab978e71a84fe20b9609d888832f2f543a5ec6aa112d61450986d1
6f0f702fc0f0a5420a1dbaf1aa88b13b557bebc2631a4157b8e026d80f7651b2
32863daa615afbb3e90e3dad35ad47199050333a2aaed57e5065131344206fe1
E058280f4b15c1be6488049e0bdba555f1baf42e139b7251d6b2c230e28e0aef
Aa07611ce06d7482c1d2d2f26c8721d6833718abd72360b81598bc2935811dcb
Cb28e7980ba2f1c718cd96401b9290719e7748ab9987abcf9ad9e376f6f60b37
Dbb3a665f9460343eb7625f8625815179e63aaa83f91b9283a296142ec4b2bbb
C328b3714df8400f4d4c071edb1f6d3b82d42488ebf8d9437c300bec9108755b
981ecfc67d7192f0e82f3f8042d7c26c78396a3a62e5e34c717db31aee566eca
428cf5d05d9c3d4f7601ff785a175c1d86a90fe060a1f33976b363e8f9530a88
355d200eebf9d9102d5f2ba0c8a576948aef43640ae8f0eedf101e0e881be0b0
09ae2b4fce92a0afe9eb27ac113548a2f881e49cb55a9245e957b5d75c727fdd
73871d1f5fa5683e984e26f22c6242d25c2ac7ee84ff8418fdf0f27c2e7d146b
d1d0b81bcc6309fbfaba324feabc2952e310b24a4c7d479f64860372b5d9dd66
827448cf3c7ddc67dca6618f4c8b1197ee2abe3526e27052d09948da2bc500ea