KPMG Cyber Threat Intelligence Platform

Evilnum – Evolved As Cyber Demon?

The Sophisticated APT Group Evilnum is believed to be active since 2018, marking its return in the cyber space with a recent attack in an immigration organization. Majorly Targeting Fintech organizations, the notorious group has been primarily seen directing the attacks towards UK and European Fintech organizations with few of its targets in Canada and Australia as well. The group is known to be using VBA code stomping technique alongside a well-crafted spear phishing attacks to achieve their ulterior motive.

Previously The attacker was known to send out mails with a zip attachment disguised as personal documents which used to contain the threat vector Windows Shortcut files inside it. However, in its recent attack, evolution in TTPs has been observed as MS- word document's template injection was leveraged. Post the delivery of malicious document user is asked to enable the editing option which results in deployment of heavily obfuscated malicious JavaScript used for decryption and payload injection at the endpoints. Further, the persistence is achieved via a scheduled task to execute the dropped loader binary, post which the backdoor chooses the C&C domain, selects a path string for sending the beacon network request and takes screenshots further sending it to C2 server resulting in encrypted format of data exfiltration.

The infamous APT group has come off even stronger with its evolved Tactics, techniques, and procedures in it recent attacks thus creating chaos in the financial sector provided fintech in their new prey. This makes it inevitable for organizations to adhere to best security practices and carry out end to end gap analysis assessment on periodic basis to detect the presence of such threat actors in their ecosystem.

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

Evilnum – Evolved As Cyber Demon?

Indicators of Compromise: IP Addresses	
51.195.57[.]232	185.236.231[.]74

Indicators of Compromise: Domains	
covdd[.]org	azuredcloud[.]com
khnga[.]com	bgamifieder[.]com
8as1s2[.]com	csmmmsp099q[.]com
938jss[.]com	infcloudnet[.]com
udporm[.]com	bookingitnow[.]org
bunflun[.]com	kalpoipolpmi[.]net
msdllopt[.]com	traveladvnow[.]com
yomangaw[.]com	aka7newmalp23[.]com
appdllsvc[.]com	estoniaforall[.]com
book-advp[.]com	inetp-service[.]com
mscloudin[.]com	moreofestonia[.]com
netrcmapi[.]com	moretraveladv[.]com
netwebsoc[.]com	muasaashishaj[.]com
travinfor[.]com	nortonalytics[.]com
tripadvit[.]com	pcamanalytics[.]com
webinfors[.]com	refinance-ltd[.]com
windnetap[.]com	travelbooknow[.]org
advertbart[.]com	mailservice-ns[.]com
cspapop110[.]com	bingapianalytics[.]com
deltacldll[.]com	bookaustriavisit[.]com
meetomoves[.]com	pallomnareraebrazo[.]com
roblexmeet[.]com	visitaustriaislands[.]com

Indicators of Compromise: Hashes
4406d7271b00328218723b0a89fb953b
51425c9bbb9ff872db45b2c1c3ca0854
63090a9d67ce9534126cfa70716d735f
ea71fcc615025214b2893610cfab19e9
0b4f0ead0482582f7a98362dbf18c219

KPMG

KPMG Cyber Threat Intelligence Platform

Evilnum – Evolved As Cyber Demon?

Indicators of Compromise: Hashes
61776b209b01d62565e148585fda1954
6d329140fb53a3078666e17c249ce112
79157a3117b8d64571f60fe62c19bf17
f0d3cff26b419aff4acfede637f6d3a2
f5f9ba063e3fee25e0a298c0e108e2d4
Db0866289dfded1174941880af94296f
028057e54a2e813787a14b7d33e6a2caa91485ed879ef1bbcb94df0e1cf91356
0a9c183f0b5a225228da5e8589fac8b3affe2e51c790a08148ef72481de610c4
0cdf27bb8c0c90fc1d60fb07bd30b7e97b16d15e3f58fb985350091ecad51ba6
15a076c7bb6a38425d96aa08b8a15e9a838c9697d57c835aaca92fd01607b07a
17fe047b9a3695d4fd8ad9d2f7f37486c0bc85db0f9770471442d31410ff26a1
1ac7715b1762788b5dc1f5f2fc35243a072fe77053df46101ce05413cca62666
1d01b143a56eba431387b9b973790d174deb48c2e3445d96b131a7d8e0a9d4ef
1f0d908c677fb3ec5b9422eb5f7d2a2b3ffa01659521afc07cc4dfaea27aa532
24ace8fd73b2a5a13f3e5b459f0764dd4b5bda2cea2b0e13bbf88a88afe0cdac
259cebed2cd89da395df2a3588fadde82cd6542bc9ff456890f7ee2087dc43c9
2665a09ec5b4ca913f9f3185df62495f13611831dba9073779a36df088db143b
32ce8d0dcbfcc2517480d0e08f8896ab4f6ea13ccb0eefe7205cd352c7b359c3
3329f5e3a67d13bd602dca5bbe8e2d0b5d3b5cb7cb308965fb2599a66668c207
3a6694567e9d722357b8e92153d9c878bbcab55a2f65cd0f9a2e6579fbeb935a
3eb84676249cb26dd3d1962cfca2a9fde442d0feaa1b0351f6331313f3ac1138
414a11e8eabb64add97a866502edcd7e54108bd247f4ae12fe07feeae4e549f6
4244f274a12f4672f2dda1190559d96c5a9631c9ee573b853c89e30701819b63
43eda4ff53eef4513716a5b773e6798653ee29544b44a9ae16aa7af160a996f2
46fbfc263959084d03bd72c5b6ee643711f79f7d76b391d4a81f95b2d111b44e
4959cdba7edee68b5116cc1b8ef5016978d3dff2016f027a4f76b080b7c3849a
4ecc2925cfb073323314611a3892d476a58ff2f6b510b434996686e2f0ac3af7
4ffa29dead7f6f7752f2f3b0a83f936f270826d2711a599233dc97e442dee85f
541b3011953a3ce1a3a4a22c8c4f58c6a01df786a7cc10858649f8f70ee0a2f3
5ba84191a873d823ccf336adfa219cc191a004e22b56b99c6d0e1642144129b8
5e04dd49b82320eca63b483e87453d2a68a9f4873f47d37e5080d537bc811d0e
5fb252474237a4ca96cc0433451c7d7a847732305d95ceeaeb10693ecef2eeee
7913cdf40cc17a28487a71ab0d7724b8bf3646a2a53e3905798ce23a657061b8
7add6700c6e1aa1ac8782fdd26a11283d513302c672e3d62f787572d8ad97a21

KPMG

KPMG Cyber Threat Intelligence Platform

Evilnum – Evolved As Cyber Demon?

Indicators of Compromise: Hashes
7b478cd8b854c9046f45f32616e1b0cbdc9436fa078ceddb13ce9891b24b30a5
7c06a03d712be8c0df410bea5d1c2004c6247bcde5a46ce51746f18de9621ac1
864dccbeda7d88cad91336b5ae9efd50972508d1d8044226e798d039a0bc1da2
8a49a7f6c95fade72ef86455794cdedfca9129aa0f5281e09929dfebfb3417c4
8e4a4c5e04ff7ebacb5fe8ff6b27129c13e91a1acc829dbb3001110c84dc8633
9cf7f8a93c409dd61d019ca92d8bc43cc9949e244c9080feba5bfc7aac673ac3
a6a70c85b8c40932678c413fde202a55fcfc9d9cae23822708be5f28f9d5b6d2
a826570f878def28b027f6e6b2fcd8be1727e82666f8b65175d917144f5d0569
b8ba2c0478649dc099d0a869755a7e205173a9b0d15fad920317a89d07eaa930
be544a1f9f642bb35a9bd0942ae16a7a6e58a323d298a408a00fa4c948e8ea17
c192684d296ea587e93457d060cbef900143cf1a11301e6c2e34e264e3e55ef6
c50ebe13972e6e378248d80d53478d8e01e754c5d87113d9b6f93bf3b84380b4
c66e6ee55e9799a8a32b7a2c836c26bb7ebea98d09c1535ad9ae59e9628835fb
d0899cb4b94e66cb8623e823887d87aa7561db0e9cf4028ae3f46a7b599692b9
d95853e6e16d90c00fd72aaeaca9885b953dae14d7d6aa7fedcc6150fb788667
dc8190279dcea4f9a36208ba48b14e6c8313ef061252027ef8110b2d0bd84640
72337c08d6b884b64fd9945c5a01557ccf40db93af866c00c48d36b6605f3a0
eb5e42c726c7b125564455d56a02b9d42672ca061575ff911672b9165e8e309d
f25cbc53d0cc14b715ee83e51946d5793e4e86e71e96f68e9b6c839b514e8cb8