KPMG Cyber Threat Intelligence Platform

APT28 - Exploit Driven Access Facilitating Persistent Espionage

TLP : Clear

KPMG. Make the Difference.

APT28 (aka Fancy Bear, Sofacy, and UAC-001) is a Russia-aligned cyber-espionage group linked to GRU Unit 26165. Active since the mid-2000s, the group has employed a wide range of custom malware families, including GooseEgg and Jaguar Tooth, as well as more recent tools such as BeardShell and the NotDoor Outlook VBA backdoor. APT28 consistently targets government, defense, energy, logistics, academic, and NGO sectors, particularly those associated with European, North American, and pro-Ukraine interests.

APT28 gains access via spearphishing emails delivering weaponized Microsoft Office documents exploiting 'CVE-2026-21509'. These files retrieve a LNK file and a first-stage loader (SimpleLoader) that decrypts its hidden payloads and deploys tools like the NotDoor Outlook VBA backdoor or loads concealed shellcode from an image to inject the BeardShell implant into memory via the 'explorer.exe' process. Persistence is achieved through COM hijacking and the temporary creation of a scheduled task, that trigger the malware. To evade detection, it uses encrypted payloads, dynamic API loading, anti-analysis tricks, mutex checks, steganography inside PNG files, and fileless in-memory execution, making forensic detection extremely difficult. The malware communicates with its C2 servers over encrypted HTTPS using legitimate cloud storage platforms, allowing BeardShell/EhStoreShell traffic to blend in with normal cloud activity. NotDoor is used to access email accounts and collect sensitive local files related to military, diplomatic, or transportation operations. After exfiltration, stolen data is transmitted through encrypted C2 channels (Covenant Grunt) over trusted cloud infrastructure, enabling long-term stealthy espionage and sustained access.

APT28's modular infection chain shows the group's continued agility while underscoring the need for rapid patching, tighter Office and OLE controls, and strong defense-in-depth.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Patch your Windows environment with the latest version asper the OEM and secure it with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

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

KPMG in India Cyber Response Hotline: 1800 2020 502

KPMG in India contacts:

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

Sony Anthony
Partner
T: +91 98455 65222
E: santhony@kpmg.com

Manish Tembhurkar
Partner
T: +91 98181 99432
E: mtembhurkar@kpmg.com

Rishabh Dangwal
Director
T: +91 99994 30277
E: rishabhd@kpmg.com

kpmg.com/in

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

APT28 - Exploit Driven Access Facilitating Persistent Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses	
146.0.41[.]204	146.0.41[.]233
146.0.41[.]205	146.0.41[.]234
146.0.41[.]206	72.62.185[.]31
146.0.41[.]207	159.253.120[.]2
146.0.41[.]208	23.227.202[.]14
146.0.41[.]231	193.187.148[.]169
146.0.41[.]232	

Indicators of Compromise: Domains	
longsauce[.]com	wellnesscaremed[.]com
freefoodaid[.]com	wellnessmedcare[.]org

Indicators of Compromise: Hashes
859c4b85ed85e6cc4eadb1a037a61e16
2f7b4dca1c79e525aef8da537294a6c4
4727582023cd8071a6f388ea3ba2feaa
b6a86f44d0a3fa5a5ac979d691189f2d
e4a5c4b205e1b80dc20d9a2fb4126d06
7c396677848776f9824ebe408bbba943
d47261e52335b516a777da368208ee91
4423b8f3456e54eb48dfbde0b4c7984b
744bbe8d7c3d0421fa0deb582481f5ba
ee0b44346db028a621d1dec99f429823
95e59536455a089ced64f5af2539a449
154ff6774294e0e6a46581c8452a77de

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

APT28 - Exploit Driven Access Facilitating Persistent Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
58f517bdc9ba8de1b69829b0dcf86113
331e055e6a519d443233bd740dbfe8ee
418dc7365e78f79ef7dfcfbfe1bc8b0e
d8e880975ab01c745386663409a9d3aa
f05d0b13c633ad889334781cf4091d3e
f3b869a8d5ad243e35963ba6d7f89855
6408276cdfd12a1d5d3ed7256bfba639
045d1e0686f8b4b49b2d9cf48ac821f8
0df3fde016f3c0974d4aa01b06724a33
1550ae7df233bb9a9c9e78bf8b236072
337cecf067ecf0609b943b54fb246ed2
41c51784f6d601ffd0e09b7d59ff6025
c306e0a3ec528368f0b0332104148266
da1c3e92f69e6ca0e4f4823525905cb6969a44ad
c4799d17a4343bd353e0edb0a4de248b99295d4d
d788d85335e20bb1f173d4d0494629d36083dddc
8913090d7329c09b096625e9d57edf6c5d00978e
e52a9f004f4359ea0f8f9c6eb91731ed78e5c4d3
d577c4a264fee27084ddf717441eb89f714972a5
c8c84bf33c05fb3a69bc5e2d6377b73649b93dce
e55cacbbff9ad573cbaddf8a59bac187bf8c78f3
7bc3bafa39f61969a577f54bff28c0d1eff75d5c
cea7e9323d79054f92634f4032c26d30c1cedd7e
4592e6173a643699dc526778aa0a30330d16fe08
22da6a104149cad87d5ec5da4c3153bebf68c411
34f77c7e57f4f1798835b09c398765cc40414461

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

APT28 - Exploit Driven Access Facilitating Persistent Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
7bbb530eb77c6416f02813cd2764e49bd084465c
c1b272067491258ea4a2b1d2789d82d157aaf90a
0bb0d54033767f081cae775e3cf9ede7ae6bea75f35fbfb748ccba9325e28e5e
1ed863a32372160b3a25549aad25d48d5352d9b4f58d4339408c4eea69807f50
5a17cfaea0cc3a82242fdd11b53140c0b56256d769b07c33757d61e0a0a6ec02
969d2776df0674a1cca0f74c2fccbc43802b4f2b62ecccecc26ed538e9565eae
a876f648991711e44a8dcf888a271880c6c930e5138f284cd6ca6128eca56ba1
c91183175ce77360006f964841eb4048cf37cb82103f2573e262927be4c7607f
fd3f13db41cd5b442fa26ba8bc0e9703ed243b3516374e3ef89be71cbf07436b
52b6fb40e7efb09c2bebe8550178e7e30009600bdedd1acae085d753761b7598
8c1dc9732884c6078b23953b78314a8d0d8b8d9fe42e5f97a7cd09b8ace943a9
9f4672c1374034ac4556264f0d4bf96ee242c0b5a9edaa4715b5e61fe8d55cc8
b2ba51b4491da8604ff9410d6e004971e3cd9a321390d0258e294ac42010b546
2822c72a59b58c00fc088aa551cdeeb92ca10fd23e23745610ff207f53118db9
be859b4f4576ec09b69a2ef2d119939f7eb31de121aa01d38e1f0b2290f5a15e
7ccf7e8050c66eed69f35159042d8043032f8afe48ae1f51fce75ce2c51395f2
968756e62052f9af80934b599994addbab29f8dc2615c47cda512bae48771019
b7342b03d7642c894ebad639b9b53fd851d7958298f454283c18748051946585
baad1153e58c86aa1dc9346cdd06be53b5dd2a6cf76202536d6721c934008f8e
d213b5079462e737eb940ac46c59e386eb6ca7f8decc95a594b3d8f3b6940010
e792adf4dff54faca5b9f5b32c1a2df3a6a955e722f1be8df2451c03ed940e41
495cf3fd22d4fc2c6c86b689b68141ac7d0130b0bb5cbc834ef59275132ee5c2
b2e771cbfa0a74d0774db162d28c1eecd3a7cb384dfe97522e9baabd1c04d304
c4389cc34b672c4f885547f413bf38575e6ee2b23a0ddfdd306a69c1775db6fc
a944a09783023a2c6c62d3601cbd5392a03d808a6a51728e07a3270861c2a8ee
bb23545380fde9f48ad070f88fe0afd695da5fcae8c5274814858c5a681d8c4e

Follow us on:
kpmg.com/in/socialmedia