KPMG

KPMG Cyber Threat Intelligence Platform

APT28 – Unveiling Russia's GRU Cyber Tactics

APT28, aka Blue Athena, Pawn Storm and various other aliases is a highly sophisticated hacking group affiliated with Russia's GRU military intelligence. Over the years, they have employed cyber espionage tactics such as spear-phishing and exploiting network vulnerabilities, targeting a wide range of sectors such as foreign affairs, energy, defense, transportation, and entities in government, military, and corporate sectors globally. Particularly active in Ukraine-related conflicts, they support Russia's foreign policy and military objectives.

Attack is initiated by crafting spear-phishing emails with disguised attachments or scripts, tailored to specific individuals within target organizations. They exploit vulnerabilities in Cisco network equipment for reconnaissance and deploying malware payloads for further infiltration and persistence. A critical vulnerability in Microsoft Outlook (CVE-2023-23397) is exploited to escalate privileges for unauthorized access over victim machines. WinRAR code execution vulnerabilities (CVE-2023-38831) are leveraged for NTLM relay attacks, enabling lateral movement within the network. Scripts hosted on Mockbin evaluate User-Agent values and country codes before potentially redirecting users to PHP scripts on free web hosting domains to malicious payloads. A PowerShell script facilitates the theft of Net-NTLMv2 hashes, leading to data exfiltration via WebDAV requests. Cactus VPN exit nodes are used for credential phishing campaigns, connecting to hacked email accounts via IMAP for data exfiltration, while compromised EdgeOS routers are employed for malicious emails employing CVE-2023-23397.

APT28's persistent and elusive nature over the past decade necessitates continuous innovation and adaptation in defensive strategies to effectively thwart their operations.

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

APT28 – Unveiling Russia’s GRU Cyber Tactics

Indicators of Compromise: IP Addresses	
166.0.24[.]2	89.96.196[.]150
42.98.5[.]225	5.199.162[.]132
62.4.36[.]126	144.76.16[.]109
69.51.2[.]106	149.50.208[.]22
73.80.9[.]137	194.14.208[.]15
24.11.70[.]85	194.14.217[.]63
45.83.90[.]11	14.198.168[.]140
61.14.68[.]33	74.208.228[.]186
95.85.72[.]160	87.249.139[.]239
80.246.28[.]58	183.178.180[.]158
85.195.206[.]7	202.175.177[.]238

Indicators of Compromise: Domains	
mocky[.]io	webhook[.]site
mockbin[.]org	

Indicators of Compromise: Hashes
358d9271b8e207e82dafe6ea67c1d198
24c9a871515d997106f5d59e343ae515
8cf9939cc180b5f63bb8cbd712085dc2
532e57f5f140a8e7e6c6bc27e552ae9b
2b9d21311c803ca26fa9741b37882c11
ce31e6a7bde3f2321d5a4b686ae16dc3
75d5bb70923f6873c395176df7f168bf
4b67eb93fb9abe16fb69929a90e9a24d
4beba318cfa8fbee08691815a8576d0f
75e1a44c80e64acce0322b8cdd641001
756ff05f86d3028c24b4769380c863b5
2599262f3fc50d7d4320acbb14ce40bc
c55d2eae6e2cd47be075e5e85a55056e
6128d9bf34978d2dc7c0a2d463d1bcdd
825a12e2377dd694bbb667f862d60c43

Indicators of Compromise: Hashes
a758342ead4fd5a7c9543cedae3f0c76
988681231e47401983f67f64aa75fda7
050e2d68903681dbde4acd5ce83aea01
9724cecaa8ca38041ee9f2a42cc5a297
5f126b2279648d849e622e4be910b96c
acd9fc44001da67f1a3592850ec09cb7
8d1b91e8fb68e227f1933cfab99218a4
6fdd416a768d04a1af1f28ecaa29191b
5db75e816b4cef5cc457f0c9e3fc4100
825a12e2377dd694bb667f862d60c43
47f4b4d8f95a7e842691120c66309d5b
6827679a4fc3736516468afd6aa00f72ecb785d2
a651a388e910bcf6f0ebb4d4c75f2231e3e300a1
e4aabd90fed1704646a5467a6cb42ab8f80b3bd3
8d1d5a38b2f8ac0bb3ee511fe9052572599f3f9e
e9db80181b228d347e8a0c1f5fd3487c143bfd3f
da9370af012574f3e112db8d1f62ecb03d85fc58
03d8dadf3647a57b335b96ea4e8a60c70d114243
bf474f4278095 3a1b91a74344d05d961809404cb
4a901003de3b4f2ab2d045f1b08ac7c905261a28
2462b7ed405a8c5df8b2942b83110060ec2720c7
8b89ce35bc331f6bf76edf3b68a97ba8584b3fbe
5d3e73a071674e84d00c5f0b44d852fda6381d4a
bda8396b1eb70b42091747a8e86b3fa9bf9b0afd
7adf410aa45b05740c7c22b09b36e33bd24db3af
4018b68de4b2eda4a831852df158a7a756470aaf
b6e07fbe7f28c8691faa75151a5dd83ea4edb0c6
859152dfd48da8f38bce4839e2628518c676b41e
bf01902ffa7ecb530b410ea4e1b769a9c16f74a3
2a1461189052a014d345444557611af0c9d3fe34
1922698073911b18f60edd84ff8d13461fbd4c5a
52951f2d92e3d547bad86e33c1b0a8622ac391c614efa3c5d167d8a825937179
c8a86d0132b355ee8a22e48e81bb8aef71d3b418878df1bd9c46e53cfb3d2d61
4f3992b9dbd1c2a64588a5bc23f1b37a12a4355688d6e1a06408ea2449c59368

KPMG Cyber Threat Intelligence Platform

APT28 – Unveiling Russia's GRU Cyber Tactics

Indicators of Compromise: Hashes
45e44afeb8b890004fd1cb535978d0754ceaa7129082cb72386a80a5532700d1
22ed5c5cd9c6a351398f1e56efdfb16d52cd33cb4b206237487a03443d3de893
9a798e0b14004e01c5f336aeb471816c11a62af851b1a0f36284078b8cf09847
243bab79863327915c315c188c0589202f64b3500a3fee3e2c9f3d34e8e1f154
2f1c2afdf17831e744841029bb5d5a3ea9fda569958303be03e50fb3a764913f
f5b7a2d9872312e000acbe3dc8153707acecc5ba184f97ad6014327db16549c7
ed56740c66609d2bbd39dc60cf29ee47743344a9a6861bee7c08ccfb27376506
19e95b32b77d8dfd294c085793cd542d82eddac8e772818fea2826fa02a5cc54
00ff432de1e4698d68a5ebc2f09056f230836b4cc9e4da8565286abaaade3ae6
9f31754206df706ad45b9a8f12c780295da1c71d98cdb6b8d119ab8001c64bf8
494b6bc171912c22ecc3613c93cbb46880a659a1c0a487de1221e40eb01c5b86
19d0c55ac466e4188c4370e204808ca0bc02bba480ec641da8190cb8aee92bdc
593583b312bf48b7748f4372e6f4a560fd38e969399cf2a96798e2594a517bf4
d84c39579e61c406380f37da7c2a6758ed9a4c9a0e7697c073e2ddbb563360cd
1b598c7c35f00d2c940dfd3745bd9e5d036df781d391b8f3603a2969c666761b
0429bdc6a302b4288aea1b1e2f2a7545731c50d647672fa65b012b2a2caa386e
4238c061102400fa27356266c6f677d1d7320f66f955a7f389eb24f10a49b53d
4fa8caea8002cd2247c2d5fd15d4e76762a0f0cdb7a3c9de5b7f4d6b2ab34ec6
6bae493b244a94fd3b268ff0feb1cd1fbc7860ecf71b1053bf43eea88e578be9
c22868930c02f2d6962167198fde0d3cda78ac18af506b57f1ca25ca5c39c50d
6d44532b1157ddc2e1f41df178ea9cbc896c19f79e78b3014073af2d8d9504fe
fb2c0355b5c3adc9636551b3fd9a861f4b253a212507df0e346287110233dc23
24fd571600dcc00bf2bb8577c7e4fd67275f7d19d852b909395bebcbb1274e04
18f891a3737bb53cd1ab451e2140654a376a43b2d75f6695f3133d47a41952b6