KPMG Cyber Threat Intelligence Platform

Unit 29155 - GRU's Shadows in Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Unit 29155, linked to the Russian GRU, has been conducting cyber warfare since 2020, focusing on espionage and sabotage. They deployed WhisperGate malware against Ukraine on 13 January 2022 and compromised critical infrastructure in Western nations. The FBI, NSA, and CISA link them to attempted coups and assassinations in Europe, aiming to destabilize NATO by exploiting digital vulnerabilities. Their targets include government services, financial institutions, transportation systems, energy, and healthcare sectors in NATO, the EU, and select countries in Central America and Asia.

Reconnaissance is conducted by using tools (Acunetix, Nmap, Amass) to scan for open ports and services, gather subdomain information, enumerate AD, and identify vulnerabilities in target networks. Utilizes CVE exploit scripts from GitHub repositories and use them against victim infrastructure. Initial access is obtained by exploiting vulnerabilities in internet-facing systems such as CVE-2021-33044 on Dahua IP cameras, to bypass authentication. Conducts lateral movement by scanning IoT devices with Shodan, exploiting default credentials on vulnerable IP cameras, performing RCE, and dumping plaintext configuration settings and credentials to access other network devices. Executed reverse shells (Netcat, Meterpeter), modified PHP scripts for persistence, exploited SMB vulnerabilities with EternalBlue, and achieved persistence through ProxyChains routed via SOCKS5. Employed VPNs and VPS infrastructure for anonymity, using reverse TCP connections via Meterpeter and ProxyChains for secure routing. DNS tunneling tools (Iodine) and proxies are used for encrypted communication. Rclone is used to compress and exfiltrate data to cloud storage.

Unit 29155's open-source approach poses a formidable challenge for various security agencies to track them down, highlighting the urgent need for cyber resilience and awareness.

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.

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

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

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

Chandra Prakash
Partner
T: +91 99000 20190
E: chandraprakash@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

Unit 29155 - GRU's Shadows in Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: IP Addresses

79.124.8[.]66	179.43.176[.]60
154.21.20[.]82	179.43.187[.]47
194.26.29[.]84	112.51.253[.]153
194.26.29[.]95	90.131.156[.]107
194.26.29[.]98	112.132.218[.]45
45.141.87[.]11	179.43.133[.]202
5.226.139[.]66	179.43.175[.]108
81.17.24[.]130	179.43.189[.]218
194.26.29[.]251	185.245.84[.]227
179.43.142[.]42	185.245.85[.]251
179.43.162[.]55	46.101.242[.]222
179.43.175[.]38	62.173.140[.]223

Indicators of Compromise: Domains

3237[.]site	interlinks[.]top
smm2021[.]net	

Indicators of Compromise: Hashes

032f5642d4fb2fdd74e6f20a13c57746
03af632aa6f87bf9dd4364ee3b612cbb
08dfebc04eb61c9a6d87b6524c1c0f2e
09a2d85e809d36bff82bd5ab773980a3
0a2affa6d895baab087b84e93145da35
0adc2530cf348c0a3d53a680291a3d67
0dc5ac12f7690db15c99eaabc11b129c

Follow us on:
kpmg.com/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Unit 29155 - GRU's Shadows in Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
0e03103e8110785156105946e48ea9e0
0e6374042b33d78329149a6189a7cb46
1220b580cef1bf22351e271773945d20
143594597130e301499e5940a5fb798a
1934e2ebc64d41e37ef53ea0c075e974
19cb20c4e7dbfe15c1aa284752d0fecb
1c85c0d044ac837e8939564afac1eb32
1cac5c0cb8801e8730447023270d8d56
1e22d64f263e8ea4b2d37dcd9b7c3012
2128361d8aaae1225d50c9add32006a1
246d9f9831b125ea7e6ef21bc4c8a0ca
246f31c86bbbe7f65c0126cf4a1a947a
251f3a4757d9e4de0499cc30c0bc00a9
28d571ddb5c04d065dfe1be9604663ba
2b2509c6ee46d6327f2f1c9a75122d15
2b39eab325906b0a3ab7e584c3d67349
2b5f159f022109a8de1bc5dd9e3138a0
2ca6bcf16ee4293a771a1cf7b7b9ee49
2e035360971a817b854d7d5a2b008717
32db8abce1618e60441f5c7cf4be0d22
332b7f6662e28e3577bd1b269904b940
343b140977b3f9b227e7e5f82b0fadb5
16525cb2fd86dce842107eb1ba6174b23f188537
892be61f0cf68425e42efda9aa31f0e14bc963b5
82d29b52e35e7938e7ee610c04ea9daaf5e08e90
d2d96f0d819abd771617e806994effc180c7438c

KPMG

KPMG Cyber Threat Intelligence Platform

Unit 29155 - GRU's Shadows in Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
5fbd9bd73040d7a2cac0fc21d2fe29ebe57fb597
c3181fd7cb463893fc73974acc0016605d90ef6c
90fa56e79765d27d35706d028d32dc5be7efb623
fb83899dc633c59a8473a3048c9aacce7e1bf8d8
b2d863fc444b99c479859ad7f012b840f896172e
91f7690be7d36bde753719398761084828 9e0f56
88c76d31b046227d82f94db87697b25e482eb398
cbfda4cee8151534198623d13ff101f47b211b35
80abdc5c36eb4a2745783e6590a13d92497c8513
27c176bbd3e254d5e46ccb865d29c8c166ba4a9f
2e113050a81bbd0774db7e86fad4abd44e5b6ec2
5d60c8507ac9b840a13ffdf19e3315a3e14de66a
db370ee79d9b4bd44e07f425d7b06beffc8bdded
4f06d376648def0bb8a325e70046a5030d2cb1d1
50566fdea2f4b8a3466427f9c6798dabe2587823
b5e3e65cd6b09b17d4819a1379dde7db3e33813b
189166d382c73c242ba45889d57980548d4ba37e
7070b7e9d537c96a2218b3907b05af2d7378661c
f6acdc16c695c3c219116aea3d585efedcafdab5
a67205dc84ec29eb71bb259b19c1a1783865c0fc
731dab83ef1d02203db64fbefbe59f3791db1e21
d33f12dbcdd427c527a8285fd9ab0c848051288b
16525cb2fd86dce842107eb1ba6174b23f188537
9a4a1581cc3971579574f837e110f3bd6d529dab
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b

KPMG

KPMG Cyber Threat Intelligence Platform

Unit 29155 - GRU's Shadows in Cyber Espionage

TLP : Clear

KPMG. Make the Difference.

Indicators of Compromise: Hashes
fd4a5398e55beacb2315687a75af5aa15b776b5d36b9800a1792ede3955616c2
34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907
aa212493331277dd28a8b9b2f535c7b719ff9c6d4ccad121fd0a59dcb78697d9
d3a80ce2fded8144d347ee0b42c18ff6ad8cb386c3a2fc884ef2348afe7633c9
35feefe6bd2b982cb1a5d4c1d094e8665c51752d0a6f7e3cae546d770c280f3a
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
bc2e7451995e188f50581efb2b564dfbc5b593f57f7b52072eeba235a0861670
fae14137605c6a173eaca1e89ad92961e6cb2b66b924087f2f109c0ab38a0d71
db5a204a34969f60fe4a653f51d64eee024dbf018edea334e8b3df780eda846f
7f8d4a36d05b60f0dd986a3bbde1be34b10a2d80297d1ae28d3fdaaa914fb8bf
4ff07f308da5b18f4a71ef09eea3f3c968683c93e8aa55d3f03975207e3b19ce
a5833236a73c66add109c8b53adda6f998bf92d63955fa06787d66d670d7889e
163932f1d39d2ae140bcf89aee6d514f65902ce8b4d46c7061c1cc94eb2a25b2
0dd61a16c625c49ffefaf4ce24cabf9a074028a06640d9bbb804f735ff56dfa3
3de02a782987b4463e02dda90df57a06fb0022eb8840a17c4c812631705ebf7c
3c02aeeb57d3c64feae109f50a89774111a443142859891bae4fb2f469fa0466
923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6
b72e8c0e4291e85ad683d6dcba449f18eacd31e8e5395c7064dcb05077db4a06
c27a3b0ffaba2258d66d595c5478f12ee8a107cd590132a4a72d8bfdaf486fc1
887936dc1db271c6970ca78f25c4eb62d3816761b675db2cf4a46645c98a5fd9
a05f2999844495bffb3405b1db2d1927e5237e61d71edb599a5fa64e3e575856
489ab4819830d231c3fc3572c5386cad9d18773a8121373ea8174de981cc9166
9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
eab7c6ef336c0fe2e0d15e2ccfe851f7ee172bdc14cee2d25e1c245e9034279d
aa79afbf82b06cda268664b7c83900d8f7a33e0f0071facba0b3d8f7a68ce56a
b9e64b58d7746cb1d3bed20405ef34d097af08c809d8dad10b9296b0bebb2b0b