KPMG Cyber Threat Intelligence Platform

ExCobalt Cyber Gang - Russian Entities Hit by GoRed Backdoor

Excobalt Gang is a cyber espionage focused threat actor whose activities trace back to at least 2019. Its recent campaign involves the deployment of a new, comprehensive, Golang-based backdoor known as "GoRed,". It exploits known Linux vulnerabilities and modifies standard utilities to evade detection. It targets multiple sectors within Russia, such as metallurgy, telecommunications, mining, government, IT, and software development.

Initial access is gained through compromised credentials or by a supply chain attack in the target company's software. They establish persistence by creating a service with a cronjob using the "service" command and setting environment variables starting with "BB". They use a packed version of Spark RAT with cmd.exe for command execution. Scripts are used to install Kitsune and Python scripts to establish C2 communication. They conceal their activities with modified Linux utilities and use tools like ProcDump, Metasploit, SMBexec, and Mimikatz for lateral movement and privilege escalation. The "gecko" command is run via icmp, dns, quic or wss protocol to intialise GoRed in beacon mode. GoRed connects to its C2 via RPC and registers the beacon, operating in the background or with a delay. GoRed uses "birdwatch" command to monitor the file system, starts a heartbeat for C2 communication, and enters heartbeat mode after command initialization. In the final stage, GoRed listens for initialized commands and executes system and built-in commands, including background tasks. Uses a custom codec for RPC communication with its C2 in beacon mode, serializing data with CBOR and encrypting it with AES-256-GCM to ensure secure transmission.

ExCobalt's evolution and enhancement of tools like GoRed emphasize its sophisticated and adaptable attack methods, highlighting the need for organizations to strengthen their cybersecurity defenses.

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

KPMG

KPMG Cyber Threat Intelligence Platform

ExCobalt Cyber Gang - Russian Entities Hit by GoRed Backdoor

Indicators of Compromise: IP Addresses	
45.146.7[.]26	45.87.247[.]239
45.146.7[.]16	45.147.200[.]165
193.37.71[.]75	188.127.225[.]231
75.119.130[.]76	135.125.107[.]221
94.131.113[.]95	

Indicators of Compromise: Domains	
rosm[.]pro	lib[.]rest

Indicators of Compromise: Hashes
6ea3feb1888ce02e3d0d2857b5ef71c4
64db61efc8acf370b91110b6f93d4dce
63f6de3c86de55172b147b947f29c808
d3cd9d9bad6450e8fd4fd2e972639c69
cad5cb82baccd1f28e381e5c924f204a
6f6e7fe49a8d5696f389e202d3b8c7e2
b5dc9a67f76fa18784b51fd3c5b9607c
caf68b393d56548074b9434564cb0625
b747c05888caf380edf6b2baab142272
0385b0f83dbfc99c243ff066e3fe3cb2
7dc1e49f1664af70d85d31af70f29071
fc3b7f47958f6c1c6a93a2f2f970734c
fad11b841d84bbe33248719341b298d3
c02bee46d6a7a46f54e6abe003fec897
ad5c0363e7e28c69007f891fbc3dd030
b3a07b9f99f8d36bda871b63d55afb01
c1f3f6efb9ef18268eb3b841065e6554
e210c26d26a1395d9bc1de21fe1b2975
376531d8a3a19016aa64d80dec23d980
fcc1ad58da960c5780a66fcc24c6c2fa
489fbca25049e5fab9dca10541e33214
a5fa43f822b6dd88298371232d49c597

KPMG

KPMG Cyber Threat Intelligence Platform

ExCobalt Cyber Gang - Russian Entities Hit by GoRed Backdoor

Indicators of Compromise: Hashes
d08bef69aee69d91b8cd0315175f665c
89ae36448f1922870f1a09c29f17c775
46eb5fa7c75cc29d89f3e48be26bbd46
848faa5839487c4331cb2a1146811f23
0cda2ee10f5b8e9a241ef3e7e352752d
2cad1092a2828a33df2156a3a97d7cf1
a2ff5b0bc0782560090574c992ccf995
d3064fe5d8a402b26099fcdbaeaedef1
fbb3f02b37b10bde868fed9d7b750fd8
9b6122f1b4f6513c22b50ef05e881f38
bc421b337fc639749528f2e756239269
76cc921e5b26a0720db213479bff1ea2
c5540ec2ec79a21f07b0d793cc36b024a0db64cc
a81373d92d798418109552fb91d4c407d4c37a89
5a504869350a4bdbcda22b09dbe7b05a7551a860
a190448a0c01a6e58610de27d022ccba0e755f79
81861a853216f78219dd8cb0b4717d5d63260e7d
1d784e6c7d12fb7730895f21e4bfd3cde4b3900f
de243b57b087f5d1cde50db1949aa3744f1f6b5e
680cb0a25e4a5148f5a1f7d3b75fad4fd345cdb0
ef50067027e27bea188023fa6a8ce9054c7d4ce9
4f6164321d10c7a54a54398ccc7b11c1e7390e38
1981f9a1d885c0ccb2d1f5910765a52d1989bc37
8030f2430234426ab3bdc8cdd995be7c4805d7d2
fd7532d2a42dd3ba26a1a3453698b8bc481f4675
58d03630792f287184177660d9fd846fbde5416c
3dd9bd38a8f8166b1af25cb523a9a6f25b1791df
7e3d46ce5aa7345d8b84e6145323366122bd21f4
ca9a2e18119ac348962e2112c6681268e1df73d1
4ba1ae554f2cfeeccf250ba5a258a4ffb8651c66
0f621d371782f8e610c630f942a8951878e90bfe
928e4e776e82645fe14a53e2ad62b5cb75b98b53
91eeab83ddcd82a77804f2e5572d849dc846b225
1aa5b4deae98f707b0a529d97fd8e7f2372c549e

KPMG

KPMG Cyber Threat Intelligence Platform

ExCobalt Cyber Gang - Russian Entities Hit by GoRed Backdoor

Indicators of Compromise: Hashes
ada92c3a38e227aa8d42b4886e036caddba2cf84
3b1329e81739b1ea6acbb4ec4dff11f02ff42570
36ef757aa3eedc3ec22bb56d60931c88cc62770e
f67dbe68fc11139b719fec11784247c5f6e7ea93
6ffe11b31443bd9cef4928aa3f29b11d0e47ccec
27dd8d144d0ac3af9f4ad3df8a060d86166ae7a5
97a3ead87af829f77dacfa23ab2786b21b427332
f07e31056001ccc26be75772c9a2f3972cd8d96a
7c27d25dbc01958724fd55f0fadf966e892d181e
6559a9eda3b8164e0c8926b4b71780f7744c4cb7
d75faee2f8ec90a69354a2c033f20e18e5ed0589
f640f70d1b65b0bfc8bcbf5261f3cdc85cfe7a21
6ff2821bef28476341b75b67d9c9f2d66d4b6cfe
5e79fffbbafddeb2d85c8fe835b07eeda08cc319
9de84bd7118dee80f5b309ddbc46dc31283cbb0e
352a62abc61c93fdb08f6f4201326f147cb819ca
a16120cca64e0c9a73f02975691e4675bb4c44a4
1af6946263f4f548ffcf510c9f68378a4d7e0895
ad6653a7ee1bcb9590f5da12cf46d856135bbb71
1fc930a59587fd9faf7536add47d92de0cecea53
1d4c0b3c74ddacf7459743cc60dd2a819c0c7e27
7e0a4c53bf3dfcb08993231539986a220a6803fd
2683dcce7fc3886f8305030b128103bd82cea528
67b7a8fad28dcc40c0889e5c4e40aef9348441c64bba74bd6db885d88ce6d246
f43c99ef85166774ed47cad96c70b8273aa82c313e55bb08d9c74e2b3f59b000
f91c9fd27bf0e3a7e82998721946ee70735ec46ee672ca80e3062aa2d5195447
be246cdf932aa5b1c2ada0d74c8d1eca4028538b28fb61d7a8d930b4266fd55c
ec36fcd64432843292d16f601a758ba4091ada906c5c4c4e540e326676911141
41d35016c78f86eee8972808c7de8c200ff24625639adff5b9d0ab8773fff6b4
aca34d7c3832879f6f7ebe8f7c59160896909574c94d1d12d7c71b6f7918bc50
8d055f3ad4d01f601df24a7c20ded981005adef7e6d26750415d1f95a471c2e3
17e57c5e71b99a386b18728eac4a27e83415756071c9e85859940da41e94976b
32d76f2fe1188a131cb3219356639e83c60d47a703e40b8801a364d98e37128f
f3bb44d52e43477ce43c91eb8d9830e356fc105b96377edd6b190fcccda61e2f

KPMG

KPMG Cyber Threat Intelligence Platform

ExCobalt Cyber Gang - Russian Entities Hit by GoRed Backdoor

Indicators of Compromise: Hashes
ab801eaa9ad11199e1382a124d6024f9551a5a33ca1b9e5cafc0098621abb91f
e2b2ebe1b82d1c122dc2750f318f2484fe5361fcd964bfdcdcae631cf32f8d37
4561a38ff34cc71cc73d54e2adfbd378f58d54596b012ff1841fdd7fc42063c3
f56b7fbc5dda7e46aff1b7753a1edb1f6fad5c8953dd3dbff30b3d8675b1dbd3
9bad8f88be8f143e37616556b9331af69a806281019b8a336ee6e14cd04b3c0e
5a3a44d5482bb9b632d0a9da47e5ae7d27cd397ca08d764bdf1ed636565ef5e7
8c545687a21481969ea4299e997cfc527a16503d042c2116801ee08f14ec6595
f6e8220dbf407300fbc78d823004de5d0c4d2816218b8e2b5f8993e97f1e6a32
017e03f9185e24c30de6b94bd6a36d48788d0b72134235e3f3dd1322dca426c9
9ec7495bb6d3a7d3bfd5d5ae9e704d0f42f3136166652a5576f15d0379126d75
7d2ae888fd06b811f6ba880c1fec3f37d49d50e0716de1b28f978240abe7795e
0ac2f15f3a36e67b8e03f69685193480edf3e3b10fc69ccbec76d3d5878c708c
f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1
c287956c4eb683e1ee62bc9ddb739d3d1c9c5dad7a73be3977bc53468665c7f7
37affeab7fb06a052413e9cc9272ea9cb2fd160fd204b506620d4303b06298c4
6262558adf132ae3c67d6f241c7abd62f987ce2881d459a66332234971e49e95
c738d594d09c651109c4422acbecad23a461bab6cd4eafc41546f036816533a0
c0cd580d83f4171b34b956d0c29dbc8fcafba8889594d85d471c14d7cf33be79
22ab2abda59edc1b6ba733fc140ab0c6b0c503b726a377a2e2ee6e6c95644aae
211a73ab3fb49957277a2efb50ad3140673b65df577961a58c3c9c90791e961e
1b96adc3c129e7e41f7c67f0d56dc05d6cdee31f69ff85f27e6a90270cfefdcf
bc159721bbe192f9c5cd24d3e9356a28f5b0c6b182de9fecf0b0ac28035f566a
1807c7a44da958f15e4dcb77cab78e92eeb96b3ace91d6923c2022d646d5593c
a5e61987676b7aed2c6d6d32c657f9351c2daa7c36365db20713dd42a03b1504
86bd9caab7526f2cd7e468d692ee2bac571465d25eb0619a10b0b46ae9a5b8e2
91136b3145a52b66a3f5edd7d8a8d06698666300f24861074df1308491f50ba5
895988088f25c89295f1a17f222a4553eafb2137b115f2ad4a0a25d273eb6521
a6dfef8616959969c06b65685e39929630f2819e6d5920498cdb1e89185ab7cd
20927a1fc3441668264673d77c81652818a630f3b2055545b0e0938c523827c3
10f1aa385108a88a15c281774f424e18070dcc256d0f778883efe6d7bcacacb6
a9b1a99729860c004fbef463958871956cbb3c8e365383042978c260012055bd
7e8bde3e34fbf9b99b7915e12de42f6b806153e44b6aaf68b172db50e18e3b9e
ac0906ff674c555e102f076100d0c12ea4a4aa7d74cc15f67c4038a84100f4cf
8fe0ba1cb68225ab9a2cb11c1419f52adb03898c5f11d2221ba9765843443d24