KPMG Cyber Threat Intelligence Platform

Quasar APT – Leveraging DLL Sideloading

Quasar RAT(aka CinaRAT, Yggdrasil) was originally surfaced as "xRAT" in 2014 and was rebranded as "Quasar" in 2015. This open-source remote access trojan has gained notoriety for its advanced capabilities. Developed in C#, Quasar RAT comes equipped with features like capturing screenshots, recording webcam videos, altering proxy settings, modifying registry entries, monitoring user activities, keylogging, and stealing passwords. It has been extensively used by various threat actor groups targeting government and private entities in Southeast Asia, the Middle East, the US, India, Afghanistan, and Ukraine.

With initial access vector being unclear, it is likely distributed through phishing emails with an attached ISO image file containing two renamed legitimate windows files 'eBill-997358806.exe','monitor.ini' and a malicious DLL file 'MsCtfMonitor.dll'. Upon executing 'eBill-997358806.exe', it employs DLL side-loading to load a disguised 'MsCtfMonitor.dll' file, with concealed code, containing an additional executable named "FileDownloader.exe" which is injected into Regasm.exe, Windows Assembly Registration Tool, to initiate the subsequent stage. In the next stage, 'calc.exe' executes, employing DLL side-loading to load 'Secure32.dll', allowing "QuasarRAT" payload to infiltrate into memory, bypassing security measures. This payload utilizes 'process hollowing' within a legitimate system process to evade detection and establishes persistence through scheduled tasks and by modifying windows registry keys. It creates a socket connection with a remote server to transmit system information, victim's IP, country code etc. and configures a reverse proxy for remote access to the endpoint.

Quasar RAT poses a significant threat, utilizing DLL sideloading techniques for silent system infiltration and control. To counter this menace, it is crucial to implement robust security measures.

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

Quasar APT – Leveraging DLL Sideloading

Indicators of Compromise: IP Addresses
193.233.188[.]5

Indicators of Compromise: Domains	
dnuocc[.]com	nadehzdakr.duckdns[.]org
makaa.work[.]gd	newnewnewx.duckdns[.]org
zilhd.giize[.]com	filter-ranked.at.ply[.]gg
go-bean.at.ply[.]gg	some-cheapest.at.ply[.]gg
tractorandinas[.]com	input-helps.gl.at.ply[.]gg
router.negro[.]systems	gamerani188-34655.portmap[.]io

Indicators of Compromise: Hashes
b0db6ada5b81e42aadb82032cbc5fd60
532af2db4c10352b2199724d528f535f
c1362ae0ed61ed13730b5bc423a6b771
b4bcf7088d6876a5e95b62cee9746139
6e0597bbae126c82d19e1ceaea50b75c
03b88fd80414edeabaaa6bb55d1d09fc
b894ab525964231c3c16feb0f2cbcffa
6b9112b4ee34e52e53104dbd538e04d3
7ffbc50f20e72676a31d318bc8f50483
483e02ec373ac4ce5676af185225d035
313ae2a853e0f47ef81040dc58247c88
7f9ec838f1906b3ac75a52babd2f77d6
2c98cc1306c8e50112e907afa22cfc06
fd4557a540e35948c0ff20f5b717d9bd
c0dc33123fcfe80ba419c1a7fb8e26d3
af0091faafe64b5d1ecdaf654c6b6282
1ce3d7e716ee9635bb0bea1623793e85
247d68ff4007bea6865af4783f7b15ab
b45ff49959f07f2465b83ca044d7c345
A1840646c8050d92c4f5140549711694
081b7bc6d5161210dc65068d36a6b87b

KPMG

KPMG Cyber Threat Intelligence Platform

Quasar APT – Leveraging DLL Sideloading

Indicators of Compromise: Hashes
9ffbd9c5f170871b8dd14373a030d2e4
58179e91bf9385c939c159f8b8faad17
37c498392689608c709fc4532fea6fdfa6d35b3e
f235afdde92069aa7f05a61b85220dc6bfa0a29d
d53e3444c17acdafd8a814116af7c1991b82d8f1
e6943665229f4deef881fcc268f385929590b20b
3e03ba741a3e44c14b72590506e7c07907a2bd5c
6e6c399bda3c1f06ade71053fddd8fbefa15029c
ab8411ddb5f5cb936a82d5589a36c844f03d339b
7aaf61afb6301cb828157628ccbf226c0816a686
3e5297db371a7ba5102f3147a8e2450e34c60fcf
53291b84fe4de85a9f2288f1eb6cef3c6f340f27
d07ee9ed74e48814aeb21ed74e2a4d1f6c74ad1c
c964e5040d4679ab4c733694296a6eedc53e3611
d2d6789823038b1cdb90e79d1801471931a78adf
db85cbf6cef95fd4b60a6fd75b1496d0216567cd
b45f35712fb78d9442aea57a94b7a270309653d4
94c3e6acf992f2acfaea744e56e89c2818782001
2117ba6378d130124081f2a3ba4247629e7f8c67
a73026052353d1ed77298b44870b7b3939cdee2a
dbefb9e2735887c8865b30616b5c056ba9b0eb93
d98fa4a5ae818890b144f2b925557b9d23596428
98a6be29ac008a66830d32236016b03f810671ae
a06a58c884b9c2522d7802781fadd10bbb504205
f35b107c73296636ac1df090c1da43e4760da5f6
4958c30b3bf3288ff5ed3e8356a069b9c5ea72cca6076af60dfb9c34f8f07352
0479ca2ab203a75a4c9664063e6b4997feca51c132582f1baf21c88f5784a061
f7e5b3f3b44f6a7f1196a155733772d7a48dec93744b3a710a4db7f1b49e486b
592e49f2336d156a2dbf23b8834ae9f621d27c26c80cfaf6716a20d512e58ac1
1db48679a795088c0cc2df4d6bc94e26c841b931fd8d2ea464c43af875a3707b
e16fe53a057b8beb144a101759b65c691d27c21aa7897d3b809668c20c5e05be
c7c4dd7c8d55bed53f1bc094ee1806ca13313cb067d0ca0a2ceedb6591fe6cd5
c0936e1b7e1f1eda0f49349591830bcb6bd129a3bd9ddfda7066eef642aedaa4
c410842bde2d561c98811e95395b9a1a0e387a4193b8cfc843bcf6c7721740ff

KPMG

KPMG Cyber Threat Intelligence Platform

Quasar APT – Leveraging DLL Sideloading

Indicators of Compromise: Hashes
a4ea0152b51958133912af7a7785c1e70132c8770670a290a276327634b0d9a2
51e7d81e4d24c47f8720c79f32406220b32053ad3e8373aa9ca5111293ba078f
b750bf77d8c13296f14b7012ae3a3df809d3ac0dd64cd960279e58ecb9ad831a
25c3c6f992123a2c43ace3d0bbf013bd3830ed53547ba2210a173a248f0fb1be
3464547056165d4f48d89285e9fbcc33e0e6a155b9ca4b2dcf8d4c1b5d6d86fe
667afdfcb9c0002a93911c2d979afffdf31294a9a497524c6fffd0b7acc9d3d7
c39915de4a2a68a8763c7b2d4e68902376084785e18b708feeb6de60a906f0c4
a13cec0431c4a2484f5a7e6d4dca08dca33ad3be07cf315a3b5245c3f6b4c313
f24106e0124b2eb49b708226022bab6629d7a7e6d766100f62f9707aae2351b4
3d044e5b221bdddc0ad0fed711cbd5bc19bdc7523f465ba8798d4bf55748795c
845accde827ee9cfe54cbe7d44a1b6acc09c3187060d815e6d071caa77b7430b
798f97a6393165544491738a66a049d79328ad3140824645a2fe5f7b06930cec
6a9f695d6dae542894d0bea82b6352dd9cc705d651857d877707bc0ce64372e3
ae8bf4ffdd13e1f7e911c63ac425504cee8a34d987af6f4f1e2197247b31aea2