KPMG Cyber Threat Intelligence Platform

SugarGh0st Malware – Twin Infection Chains Revealed

SugarGh0st, a remote access trojan, speculated to be operated by Chinese threat actors, surfaced in August 2023 as a new customized variant of the "Gh0st RAT." It has improved features for remote administration and evading detection, such as keylogging, webcam access, remote binary execution, and malware dissemination. Utilizing malicious Windows Shortcut and JavaScript files, it has targeted entities like Uzbekistan's Ministry of Foreign Affairs, as well as users in South Korea.

Initial access is achieved via phishing emails malicious RAR files. The malicious RAR archive contains a Windows Shortcut embedded with a JavaScript that deploys two infection chains. The first infection chain uses Windows Shortcut double extensions triggering a JS script execution which drops decoys, encrypted SugarGh0st payload, DLL loader, and batch script. Batch script sideloads the DLL using a copy of rundll32, decrypts and reflectively runs SugarGh0st. In second Infection, the JavaScript dropper in %TEMP% is executed utilizing the "cscript" binary. The dropper leverages a legitimate DLL called "DynamicWrapperX" to run embedded shellcode, which in-turn injects the SugarGh0st payload into the running process. Once successfully injected, SugarGh0st attempts C2 connection every 10 seconds and starts with an 8-byte heartbeat "0x000011A40100", followed by sending buffer data. Establishes persistence by modifying the Registry run keys to execute itself at system startup. SugarGh0st packs a long list of features to enumerate and terminate processes, capture screenshots, perform file operations, and even clear event logs to cover its tracks and evade detection.

SugarGh0st's dual infection chains, coupled with customized features, exemplify its advanced threat landscape, urging heightened cybersecurity 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

SugarGh0st Malware – Twin Infection Chains Revealed

Indicators of Compromise: IP Adresses	
103.108.67[.]191	103.148.245[.]235

Indicators of Compromise: Domains
drive-google-com[.]tk

Indicators of Compromise: Hashes
27ce72f35709ec9898c57f1c4ea7324e
e0cd08754753bd540bcdf62fa1733bff
782b8a96d3f80dd562b538af12233cc3
e11f6b3f3298ebbb86885559266feb7b
996580c90c5efe2a727d22a77b7e69eb
8dea867b72374fad43cc301d9af5a24b
cfe4a2fc19b77dea154c106918dcc1a3
77afbb6a6b85eecaad65d15e066476ec
4dac23960a5dc7377d684773a82c26ba
f4b1528911b6cce7abba58d87c3c2c10
09de5d9b53439c38676e83cf41b5fa8b
66cd6769abfa5439865a6c69c5181d06
7fb78e726f98ab58780373cce18babd5
177c38a8d0781d4ed1331be551d0c297
982ced1fdbe25c720da4c792430e85af
ecf6bffdc0358525bc2ab7dd7eed6b9e
2757b9108308be6ce8ea00fbf629224cbafb2a5c
27c089afffd705a6aa2c405c253273f6fa64e8b5
55078ff881ca0e3e1e07a271671fb8f8f8d71f87
4f622f871ad7d0d3b359d2554b4a9bb853459f16
C6c65bf93081e4af6dcf24cb6be6cbd533eaa415
15f433e7c5618551b3488bdd347042277ca22f44
3a4eb198f5a671ef38a646485f7390e1d5c3edaa
d087874940617cab3254f09389806d03a1336e31
5f883ab9efbee14a8c7645e32137c81689957067
4b99b8d7de07fcf96cc667575bc83dae2449418a

KPMG

KPMG Cyber Threat Intelligence Platform

SugarGh0st Malware – Twin Infection Chains Revealed

Indicators of Compromise: Hashes
309dd685b6734011b4979f369dd7556785f7eedc
36b4607e0ef65e0675c5b1ff138e2d588bb30033
fcca38ea685e551818b58889bd8adecac12bb28d
9e5515e5aa0881fc48a18712beba7e07aa46cedc
f46168c357438d37ea26fbb9cec8a659568356f9
4fb249a7fbffeb32a730e2b491b1c5c42a131d73
8584094f79fce97321ee82ca5da41b6830ecc6a0921bcaddb8dd337827cd7d1a
3436135bb3839521e7712882f0f6548aff78db66a1064408c49f820a0b85d980
c758eed6660786097b63ac6748236b5b6084783703ea7ee2111e8f0bcaa3652e
6dff111b6adc9e33bed20eae99bec779f1c29dd55895a71125cfbe3c90950eb2
7c87451261dfce64fda987eb395694b5330fd958466c46c931440cd9dc227505
ddac61f918ed87b49ef15d05873e7f52b919758aef713145f6a7d538c714fa2e
f3ea4611c72d57eabf381d5639c3c8d1840cb005ed811f3038410fb2e04978c1
38c815729f34aef6af531edf3f0c3f09635686dbe7e5db5cb97eca5b2b5b7712
2e543adb701afd40affcb4c51bd8246398b0210bee641ca9aeffcca893c9e4a5
66982ebd5ebb75633723c7057a1e948ac3aafe3ff808397eb0c55c853c82f9e6
21f19d87d2169c82efd76ddb1baa024a1e59b93f82d28f276de853fc3ef8b20e
ee5982a71268c84a5c062095ce135780b8c2ffb1f266c2799173fb0f7bfdd33e
410d7dc973d188cd0d962a59f48deb1cfc73adf37857765e90194f6e878d4488
bd0a1efe07fcb4af4bec1b2881a0711f0be34044680ad8cff958a68a70d4a914
ff0f28f96bbb6c80fc3823fe71d5e07e1a05b06986e82a2fbe324d68ba5ab2ea
9d9a0af09fc9065bacabf1a193cad4386b5e8e5101639e07efa82992b723f3b0
9783c0eee31ce6c5f795ecf387025af5d55208ff2713c470af2042721ab38606
5ad182c913f0b5cb6a34126137c335110d4c9472f5c745cb7a438d108b03b27c
adb4eb33213fa81c8b6cc013a6f4a43fa8b70eb8027433cf4339b532cb6e84cf
7cacdc84a0d690564c8471a4f58ab192ef7d9091ab0809933f616010bbf6846a
362fde3362e307af3787b9bf0b5c71f87b659a3217e054c4d0acea8b9e6d74b0