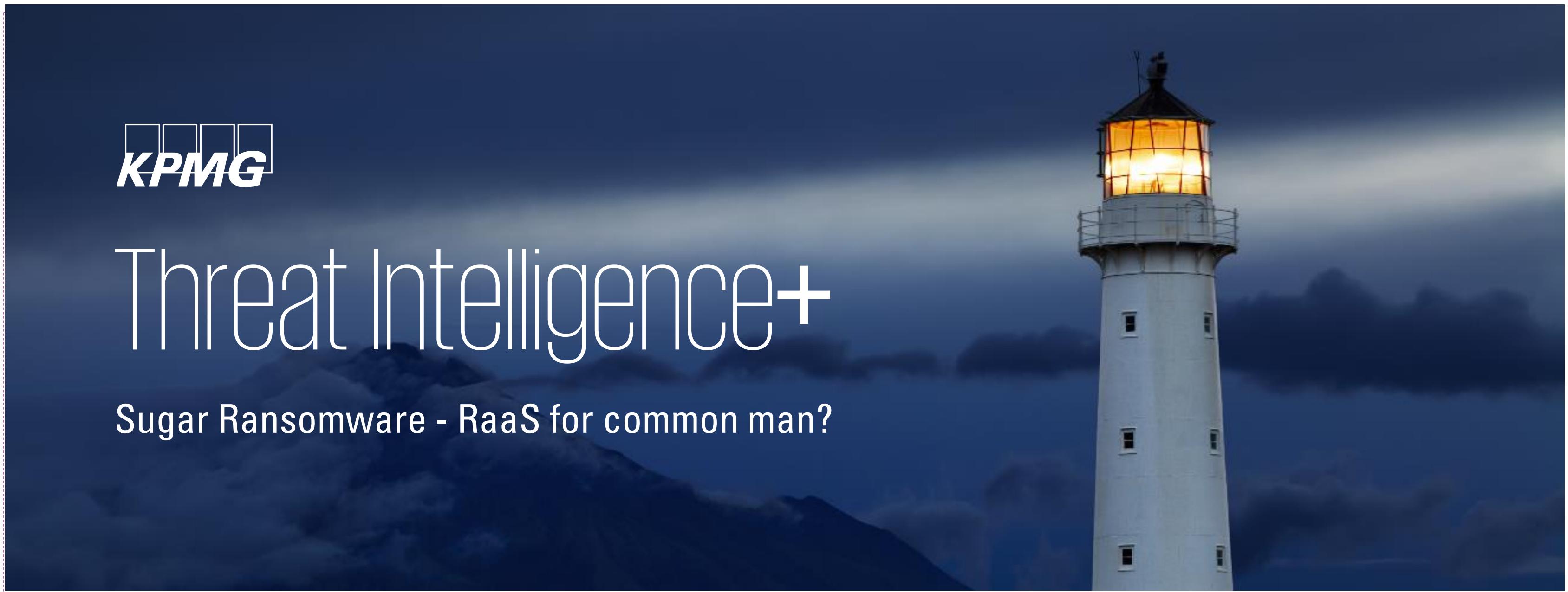

KPMG

Threat Intelligence+

Sugar Ransomware - RaaS for common man?

Sugar Ransomware aka Encoded01, since its origin in November 2021, the group has targeted individual devices and small businesses rather than enterprise networks. Unlike prevalent ransomware campaigns, that intend to make headlines and extort large ransoms, Sugar is observed to operate in the dark and relies on low ransoms, as low as $4. Sugar ransomware has reportedly compromised multiple personal devices across various countries like the US, Canada, Israel and Lithuania.

Sugar Ransomware is traded as a Ransomware-as-a-Service, and is written in Delphi, providing attackers with high level of customizations. Although the details of the initial attack vector is largely unknown, operators mainly focus on attacks through Remote Desktop Protocol (RDP). Once inside the target device the ransomware attempts to geolocate the victim machine via the IP address. It accomplishes the same by connecting to publicly available services. Sugar then attempts to connect to the Command & Control (C2) server prior to launching the attack, which allows the attacker to configure execution parameters. The ransomware provides attackers with 3 encryption algorithms with varying speeds, namely SCOP, RC6 & Salsa20, however parameters like the C2 IP and Onion URL are fixed. Once attack is launched, Sugar starts encrypting all the files except critical folders like boot, DRIVERS, Perflogs, etc. and appends '.encoded01' to the existing extension, all while sending information about the device to the C2 every few minutes.

Once encryption is done, a ransom note, very similar to that of REvil's, with link to their TOR site is dropped. The TOR site itself is a look-alike of CLOP with details of payment, trial decryptor and chat service to negotiate. While Sugar ransomware still remains in its early phase, it is expected to expand its scope of attack through its affiliates which could lead to more serious threats.

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.

What is KPMG Threat Intelligence+?

The KPMG Threat Intelligence+ approach is an industry defining, research-based capability for enhanced visibility into cyber threats. Our machine ingestible feeds are the result of automated, sensor-based intelligence metrics with dedicated, expert analysis of each threat to provide you the right context on a timely basis in industry standard formats such as STIX/ TAXII/ MISP. These feeds are additionally co-related with out industry partners and independent researchers to ensure you have the most accurate and contextual data. The intelligence is then curated from Strategic, Tactical and Operational perspective to give you 360 degree 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.

Range of services
Strategic Threat Intelligence Report
Machine Ingestible Threat Intelligence feeds
Threat Intelligence driven pre-emptive Threat Hunting Exercise
Cyber Incident Response Services

Contact us

KPMG Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security, KPMG India
+91 98100 81050
atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG India
+91 98455 45202
raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG India
+91 98455 65222
santhony@kpmg.com

Chandra Prakash
Partner, KPMG India
+91 99000 20190
chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner, KPMG India
+91 98181 99432
mtembhurkar@kpmg.com

Rishabh Dangwal
Associate Director, Cyber Security
+91 78277 54752
rishabhd@kpmg.com

KPMG

Threat Intelligence+

Sugar Ransomware - RaaS for common man?

Indicators of Compromise

IP Addresses	
45.138.172[.]69	179.43.160[.]195
91.193.183[.]58	82.146.53[.]237

Domains	
1702[.]info	2010colombia[.]com
1902a[.]top	hwfcdqnvovij[.]com
anlc[.]info	cdnmegafiles[.]com
sexbd[.]net	sugarpanel[.]space
dc143c[.]com	0mhmcz7hvpuir[.]top
rsusa[.]info	fvkpjxytxojs[.]info
seriehd[.]org	1upsecurity[.]com
alra7ma[.]net	bottomcdnfiles[.]com
gidwabj[.]com	kunden-verifi[.]info
bmores[.]info	porzadkimistrz[.]com
mehrps[.]info	majorenterprise[.]info
samonqw[.]top	10428valleyspring[.]com
camwirless[.]top	gludlandsquintjem[.]com
privseek[.]com	24pcupgradesafe4younow[.]top
tradertop[.]top	liveupdatesystem4evernew[.]top
inboxdeals[.]top	rbtyitjfboucqxcfukujxlrhnbp[.]top
nigelcowan[.]com	gksyegybkqtrtcjcckcvizgwbntgrtpblsxhz[.]top
uk-cinema[.]info	xfnqbtukoukbuvkukgybmesczrwaruznipjlq[.]top

Hashes	
3f4ef30207e9aad34d1db7d0662e4f36	68f265ea120eb28d1d5caea84183bbfe
4436364d2fe3c1a879e5a667cb316b51	69a02d2253e3a15ac0f7c1b59d9de7ae
B593c02d556d6ba6d8648f39269bd385	74d2bc6526dcc38f61fa9a15adf0e698
Ceb48bff47efab43e33d8d02e278fd4f	889054df21e8be51c4184ab4a9d2f3e3
E0bbf5fb08acfc3e28fa447eee6e786b	8fc4a53cedf99bb2cd9829f52fd441e9
0260832cee87619332599f7d5c43bdd9	d41d8cd98f00b204e9800998ecf8427e
08a47eef094b17b5a0a69c5c4436683c	e343c6fcbd3120812992378663c6503e
0b60d9a762284e837297521d96ed37fb	f67f72cb76d5bfc3461277b72e83f2a3
17c7b47b68f75df9eec21698decad5b4	3f4ef30207e9aad34d1db7d0662e4f36
1cc5b508da9567f032ed78375bb45959	4436364d2fe3c1a879e5a667cb316b51

KPMG

Threat Intelligence+

Sugar Ransomware - RaaS for common man?

Indicators of Compromise

Hashes	
2777e8741fa2fd754d20489295b62c12	b593c02d556d6ba6d8648f39269bd385
3aa78724e792fb766c52edf9c8148a6d	ceb48bff47efab43e33d8d02e278fd4f
598529f5a52d25329ebdef602fcb39a0	e0bbf5fb08acfc3e28fa447eee6e786b
15a7fb45f703d5315320eef132f3151873055161	a4854ce87081095ab1f1b26ff16817e446d786af
320eefd378256d6e495cbd2e59b7f205d5101e7f	c31a0e58ae70f571bf8140db8a1ab20a7f566ab5
98137dd04e4f350ee6d2f5da613f365b223a4f49	e835de2930bf2708a3a57a99fe775c48f851fa8f
06812b8d48f1bb00b49bd2366031a471598e093ff117e7403b5bdc87dbc189fa	
06cce1044e58ebfa48fe2399857e82519d47773f112a81c053455d0dd6955de4	
09ad72ac1eedef1ee80aa857e300161bc701a2d06105403fb7f3992cbf37c8b9	
0f05b893b67c4fc8680f2040b4069eba81e144253a7f6e20507eaa4d2576461d	
1761e180a8ca1bba2ca0ba449faf376d1fcb377cb055fe04af9de6470e1ada9b	
1be90c72735d56e2f9ee9583d6bece1b9e6a78ecc475f08d6f133863b56256ea	
231eb63b7ac037adeafced3d01b81285961ad2824473d4f5e3b33ff976a08866	
2521dca8f13dac18ff87e3f5d0137c16237a3e424bc59ded348ff747de0da5fc	
2e740053dd9e7362c5c77f32538c536507390a82228bdde787a428eccd319f52	
3ba56ddf64d47823cccc06974d70ed281e2e3faee542949c9e0fc4ab153a99cb	
4a7d59f010f47f975b912798cf1f30f748170518554047f8ebdbb52b26ab9987	
4d2d9e6f414fdd4b1a0cf46e0cee5c86b1220b15888e7b8370fc378ca6d034b7	
4e1014acb0ced914da9d173dcf9896de39ad3817fdd33243d041e394e6f0c0f4	
55f27751ff974ed4cf1d735b6b8970687cf2245e087c266bc470022fad84d18e	
5c4401aac499d8a57a73954b2d1580ddd6aaeb389e1bfdc87e97cc55a08da1b4	
5fbd2cc6d4c46f3f055cc8cb6581bab2fe86c0fecc978b707e0dcc329f7002ff	
6adaae97acc7bf8000ee33ddfcc3cddf2e788dce4c490b151f80cb5ac324e9c3	
6e55abff396da18decfe8e56f7e3948ef14421e9b7d8e71562e3085a72d22da7	
7bedaf779cec9dc26d5978c8a2e83ba66d609d77d083ec3bbed7ad9f95406d6e	
7c59de68c2d0d126bc1be96d5c305886b99485be2efe8b290a0d21282791c3c3	
7c62f1b57017599f3fdcfa369e40b3646fe219e9015a2878b66f286b9ce78aab	
7dae105b96c5c8e3a3bcbdd99f0a42252c54f88c397d2d9dc633f57bc853c06c	
7f9b80a914e41e6b1cd1daf0458a199f847ec64bdfdb24749244f36bd7ac17d1	
83b0f2e5f95d06f5566503b089b8f2a24e18f6d4b0155e108212274d9ebabf1e	
85c68a55c365047af57f1aa89b0eedb36aeec1826af4fe3658dfa2e943ae0941	
86c88f48f4bf43df3217759a60717731583441fdc68d3be11000d09534777116	
5816a77bf4f8485bfdab1803d948885f76e0c926fed9da5ac02d94e62af8b145	
879631b3c7bce996f0c17b918b1c9f2fd54c331dd389d7162da6d03be570587b	
8964a18b1aae408d35c17481d503fd461fbff89aaaa08d89347e227203000d6b	

KPMG

Threat Intelligence+

Sugar Ransomware - RaaS for common man?

Indicators of Compromise

Hashes
922d67a120929b45c899461b63de71c3561833c79a98381b9da35cf2679c8f89
a0f16ca699ba17c039bad3b8330cf7fc26e03f81c140b205113267d74eb6a962
a12ac49c226d3dc5b6ce1d0191414976f953aa5e94665786a1c2ba4f0ca85028
a71fbe562bb24b1ef24a1d20276689f3ee4f45553d0e776cb80e25aaf5d3a217
ac522f2582615cada7cf96eafcc52ea1f6db0a34b3dc2b23bed27a629e83b917
afa053437390a31269e1c942a36c0acd651f8b55fca6b53974e8c359b68dea8f
b48ae64c87cf08fb2ae3a4296a14b45a094eba7a025b1146d5c9d05731cbf10c
ba6f35c2ca5b8d813ce65a3f23269409d99f56de6610cb4ebae54092d5f027dc
bc2bcf51e874b4d36714988173e57526f4a55d81c391cda28d0e935b4fb4a038
bf059e8dac659003de1bc44b406f0a226b1ea4c05559b46d4dc5f3ef2c136772
c7cd594e7bb19a6bafa01ca895fcf18960726bcc411ecaad1dd7a03fb7dec981
dde10bff829a62b46a2585f1f332a0fe65affdd3082480a191158b898ae07c4f
e32d3b39d74f9c9b731f2ae94ad569f2a64bb53c85091b8be6cd8198c227b9cd
e40db4911ae465cbb8e01e6dca819be0f882ba4bc01a0bb19760bf984ba2664e
e74c78d6a739279ca5e66cfb74cabe5a5a7bcb70819dca1fa947c38a550163f8
e7c69adea18537cc6499639c3c6aba895509684c6d261f9d9d0389a218c56125
eaec76909ad02fc0f87a5aeaff07113b8f300f0bb743f0f5b387827f749242f9
ed5649ec329fc5fe7387a8f616a839fb126f9bc13e4705fd7154b5a560bf6153
efb362cf40203f7bbac16e1b233548ce73067afc39793363cee7ca3c07b2b2d1
f19f635b5afbeb8419fa0376c431c8025d0be96ec613dad5935c4dc98d47b0a4
f848f2a226eebde9d18e0c867b41c8ae4dc5d7cea79332e5d4fbc31368fd0a18
f8ddfeb2a27162ece478199089a606b0d9a6b0e49904c0234d3f3c60b89eb836
fb40a3200981273a1ceef35e7f86ea31f3c764718a17a55269c4f90c081a31c3
fcf213a7801540e4981761652fadb8117610571a25e7f6f59c05cc9bcdbbcc97
1318aeaea4f2f4299c21699279ca4ea5c8fa7fc38354dd2b80d539f21836df5a
18cb9b218bd23e936128a37a90f2661f72c820581e4f4303326705b2103714a9
315045e506eb5e9f5fd24e4a55cda48d223ac3450037586ce6dab70afc8ddfc9
4a97bc8111631795cb730dfe7836d0afac3131ed8a91db81dde5062bb8021058
aa41e33d3f184cedaaaabb5e16c251e90a6c4ff721a599642dc5563a57550822

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.