KPMG Cyber Threat Intelligence Platform

Bronze Starlight - Ransomware for Intelligence theft

A Chinese state-sponsored group dubbed Bronze Starlight, active since 2021 has been observed to deploy ransomware as camouflage for systematic, government-sponsored espionage. The threat actor deploys different ransomware tools such as LockFile, AtomSilo, Rook, Night Sky, and Pandora for a short period of time to gain intellectual property of interest for China. This group has been seen targeting a pharmaceutical company in US and Brazil, electronic component designers and manufacturers in Lithuania and Japan, a law firm, a media company in the US, aerospace, and the defense division of an Indian conglomerate.

The threat actor targets their victim by exploiting known vulnerabilities in the network peripheral devices. After getting access to the network, Windows legitimate programs are used for loading the malware by using DLL search order hijacking. It uses a custom DLL Loader i.e., HUI Loader, to decrypt the payload in the compromised host such as Cobalt Strike Beacon for Command and Control. Further, they deploy the ransomware and exfiltrate the data in a double extortion scheme. In addition to the data exfiltration, the malware disables the windows event tracing, antimalware scan interface, and hooking windows API calls to destroy the forensic evidence of their activities.

In a Nutshell, the operational structure and the methodology adopted is distinct from other ransomware groups as each ransomware family is deployed sequentially and is emphasized in a pattern for a short period of time. Since this group targets the victims by scanning internet-facing servers that are vulnerable, hence the prominent mitigation step for network defenders is to patch their servers on regular basis in order to fortify the risk.

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

Bronze Starlight - Ransomware for Intelligence theft

Indicators of Compromise: IP Addresses	
45.61.139[.]36	45.32.101[.]191
45.61.139[.]38	137.220.55[.]245
162.33.178[.]57	172.105.229[.]30
45.76.152[.]167	139.180.191[.]212
45.76.158[.]153	

Indicators of Compromise: Domains	
api.wensente[.]xyz	api.sophosantivirus[.]ga
api.microsoftlab[.]xyz	update.microupdate[.]xyz
update.ajaxrenew[.]com	update.microsoftlab[.]top
sub.sophosantivirus[.]ga	peek.openssl-digicert[.]xyz

Indicators of Compromise: Hashes
a4a6abf4ed4c9447683fba729a17197b
5e5d8beedb707dcfa9fad40d179e6694
cea87f04a39343fcc7105afbf6a02a6e
fd0331a50faf263299b3514f971b2cf5
71dbc4228719163f003b7711c5bb2bf2
7241e7e0800e72889d9c4f6d6e348ab6
f3355c8f43dada5a62aab60089c03d1e
0c4a84b66832a08dccc42b478d9d5e1b
d41d8cd98f00b204e9800998ecf8427e
29fe31cec867a1a57006f5cc53d30857
492ea09d908fe2c21eb468d92369b76c
4c3c7053ec145ad3976b2a84038c5feb
577a47811b3c57a663bcbf2aab99c9e3
69ef2d7f9ed29840b60a7fd32030cbd1
a06f5d11b5e0ac3114198bbcc2b006f1
14d66e2111d7f2cdae45600dcdf412dc
19dc19f99dc0ce9ddf3c19bc29ce127b
5c76fc84d73ba13ec15cf0bdc3f9a580
de1f8581cbb7332d13aaf3a0bb1b6146
b0175b09e58d34689a7403abed2ae2f5

KPMG

KPMG Cyber Threat Intelligence Platform

Bronze Starlight - Ransomware for Intelligence theft

Indicators of Compromise: Hashes
b16bb2f910f21e2d4f6e2aa1a1ea0d8b
725e4d6a5526cf44c72ec82706c45321
64ae15ec96720372393bbc7792b24f56
bde2a3c8e034d30ce13e684f324c6702
a28611027186f8f12f407901c201e48e
6dbdd4799c763243bd36c98a0d3c3eb8
239cb3c61d001775a307d5cbd0a9be09
4889c5aa7ba2f7d394698033a991a74f
f259765905cd16ff40132f35c85a862a
809fcab1225981e87060033d72edaeaf
52e1fed4c521294c5de95bba958909c1
04a8307259478245cbae49940b6d655a
1c49f3b47e301d6117f326f6868d3817
30e6a67e2ee2ab84150eb86b9ca7254b
ead02cb3f6b811427f2635a18398392bc2ebca3a
160320b920a5ef22ac17b48146152ffbef60461f
3246867705e8aad60491fe195bcc83af79470b22
46a9b419d73a518effbc19c3316d8a20cff9ce4a
5df448af3f7935c3f4a2904b16af9ea00d13cb0c
64f5044709efc77230484cec8a0d784947056022
a413f4bcb7406710b76fabdaba95bb4690b24406
a75e9b702a892cc3e531e158ab2e4206b939f379
b24e254f6fdd67318547915495f56f8f2a0ac4fe
d9efd4c4e1fb4e3d4a171c4ca0985839ad1cdee9
dbc48357bfbe41f5bfdd3045066486e76a23ad2d
1d01528de63c9581be0ea5ebc18dff7f6a2272d4
0f5259812be378bbd764cef94697019075990b4d
b0fb6c7eecbf711b2c503d7f8f3cf949404e2dd256b621c8cf1f3a2bdfb54301
15b52c468cfd4dee4599ec22b1c04b977416fbe5220ab30a097f403903d28a3a
5b56c5d86347e164c6e571c86dbf5b1535eae6b979fede6ed66b01e79ea33b7b
5b5cd007fb96eef68d3d123eba82a4e4dfce50cdf3b05fe82bfa097870c09903
62fea3942e884855283faf3fb68f41be747c5baa922d140509237c2d7bacdd17
70225015489cae369d311b62724ef0caf658ffdf62e5edbafd8267a8842e7696
7fe5674c9a3af8413d0ec71072a1c27d39edc14e4d110bfeb79d1148d55ce0b6

KPMG

KPMG Cyber Threat Intelligence Platform

Bronze Starlight - Ransomware for Intelligence theft

Indicators of Compromise: Hashes
8502852561fcb867d9cbf45ac24c5985fa195432b542dbf8753d5f3d7175b120
91f8805e64f434099d0137d0b7ebf3db3ccbf5d76cd071d1604e3e12a348f2d9
c7a515276883a03981accfac182341940eb36071e2a59e8fb6cb22f81aa145ae
f04f444d9f17d4534d37d3369bf0b20415186862986e62a25f59fd0c2c87562f
d9f7bb98ad01c4775ec71ec66f5546de131735e6dba8122474cc6eb62320e47b
bf315c9c064b887ee3276e1342d43637d8c0e067260946db45942f39b970d7ce
1fca1cd04992e0fcaa714d9dfa97323d81d7e3d43a024ec37d1c7a2767a17577
8c1a72991fb04dc3a8cf89605fb85150ef0e742472a0c58b8fa942a1f04877b0
8e088a27f99414f9913b16d824454d3b521acf741f4eabf61c315059061aa801
a077a55608ced7cea2bd92e2ce7e43bf51076304990ec7bb40c2b384ce2e5283
bcbd18374cd23bafd46d8dcd4007ffb239b0fe6c101a9e6c9087459f8bc057b9
ff5757086c464d624f4a6674d65409fb6fa84ad5ac089583ebc994ba949458d7
ba1f9c68fccc42d231cc0de9142039853b3437501dc9ec6f111a3cac177dd1a9
6ecad2171819ca386ffe61ff9eb31e99471fa4f315762c7da658165d7e09a55d