Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

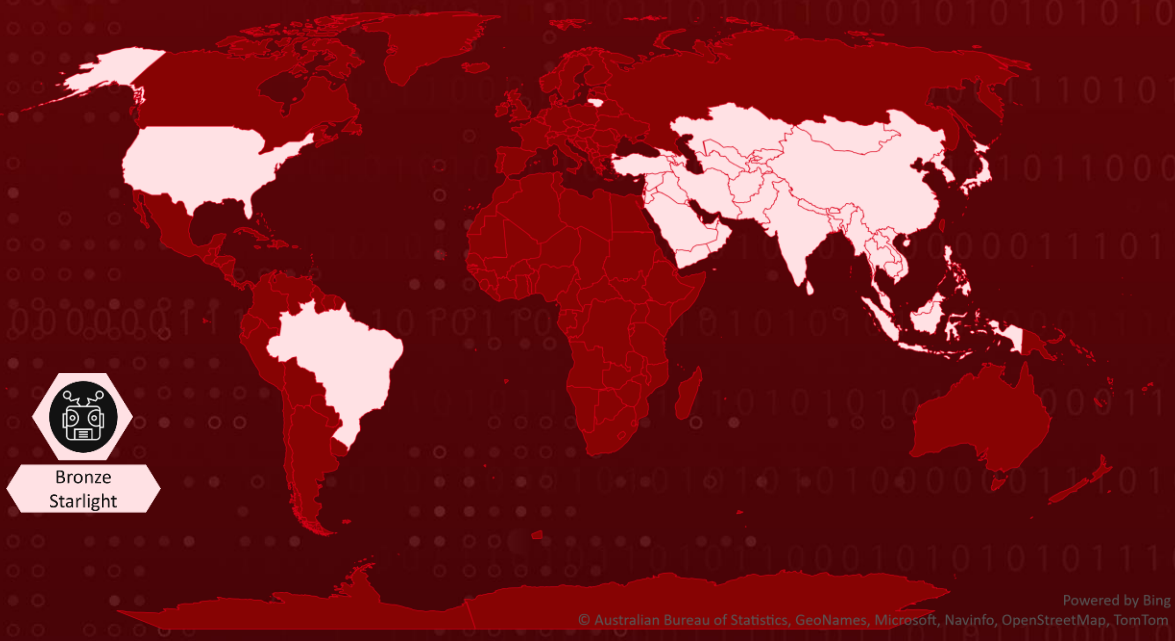
Bronze Starlight uses loader malware to deploy ransomware

Date of Publication	Admiralty code	TA Number
June 30, 2022	A2	TA2022136

Summary

Bronze Starlight, a Chinese APT, is deploying ransomware LockFile, AtomSilo, Rook, Night Sky, and Pandora via the HUI loader malware to carry out double extortion.

Actor Map



Potential MITRE ATT&CK TTPs

TA0002 Execution	**T1203** Exploitation for Client Execution	**TA0010** Exfiltration	**T1041** Exfiltration Over C2 Channel
TA0003 Persistence	**T1574** Hijack Execution Flow	**T1574.001** Hijack Execution Flow: DLL Search Order Hijacking	**T1140** Deobfuscate/Decode Files or Information
TA0005 Defense Evasion	**T1059** Command and Scripting Interpreter	**T1505** Server Software Component	**T1486** Data Encrypted for Impact
TA0040 Impact	**T1190** Exploit Public-Facing Application		

Technical Details

Bronze Starlight, a new threat actor, exploiting vulnerabilities in network perimeter devices. The actor uses the HUI loader to load Cobalt Strike Remote Access Trojans(RAT) beacons to achieve C2 communication and deploy ransomware services such as LockFile, AtomSilo, Rook, Night Sky, and Pandora. The APT group threatens the victims by using the double extortion method.

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONS	TARGET INDUSTRIES
Bronze Starlight	China	Information theft and espionage	Brazil, India, United States, Lithuania, Japan, Kazakhstan, Asia	Manufacturing, Financial services, Legal, Engineering, Media, Defense, Aerospace

Indicator of Compromise (IOC)

TYPE	VALUE
IPV4	45.32.101[.]191, 45.61.139[.]38, 172.105.229[.]30
Domain Name	update.ajaxrenew[.]com, update.microupdate[.]xyz, api.microsoftlab[.]xyz, update.microsoftlab[.]top, api.wensente[.]xyz, peek.openssl-digicert[.]xyz
MD5	b16bb2f910f21e2d4f6e2aa1a1ea0d8b, 809fcab1225981e87060033d72edaeaf, a4a6abf4ed4c9447683fba729a17197b, 4c3c7053ec145ad3976b2a84038c5feb, 0c4a84b66832a08dccc42b478d9d5e1b, bde2a3c8e034d30ce13e684f324c6702

TYPE	VALUE
MD5	f259765905cd16ff40132f35c85a862a, 69ef2d7f9ed29840b60a7fd32030cbd1, 577a47811b3c57a663bcbf2aab99c9e3, b0175b09e58d34689a7403abed2ae2f5, f3355c8f43dada5a62aab60089c03d1e
SHA1	a75e9b702a892cc3e531e158ab2e4206b939f379, 64f5044709efc77230484cec8a0d784947056022, ead02cb3f6b811427f2635a18398392bc2ebca3a, 3246867705e8aad60491fe195bcc83af79470b22, 160320b920a5ef22ac17b48146152ffbef60461f, a413f4bcb7406710b76fabdaba95bb4690b24406, d9efd4c4e1fb4e3d4a171c4ca0985839ad1cdee9, b24e254f6fdd67318547915495f56f8f2a0ac4fe, dbc48357bfbe41f5bfdd3045066486e76a23ad2d, 46a9b419d73a518effbc19c3316d8a20cff9ce4a, 5df448af3f7935c3f4a2904b16af9ea00d13cb0c
SHA256	8502852561fcb867d9cbf45ac24c5985fa195432 B542dbf8753d5f3d7175b120, 62fea3942e884855283faf3fb68f41be747c5baa 922d140509237c2d7bacdd17, b0fb6c7eecbf711b2c503d7f8f3cf949404e2dd2 56b621c8cf1f3a2bdfb54301, 15b52c468cfd4dee4599ec22b1c04b977416fbe5 220ab30a097f403903d28a3a, 5b56c5d86347e164c6e571c86dbf5b1535eae6b9 79fede6ed66b01e79ea33b7b, f04f444d9f17d4534d37d3369bf0b20415186862 986e62a25f59fd0c2c87562f, 7fe5674c9a3af8413d0ec71072a1c27d39edc14e 4d110bfeb79d1148d55ce0b6, 91f8805e64f434099d0137d0b7ebf3db3ccbf5d7 6cd071d1604e3e12a348f2d9, 70225015489cae369d311b62724ef0caf658ffdf 62e5edbafd8267a8842e7696, 5b5cd007fb96eef68d3d123eba82a4e4dfce50cd F3b05fe82bfa097870c09903, c7a515276883a03981accfac182341940eb36071 e2a59e8fb6cb22f81aa145ae

References

https://www.secureworks.com/research/bronze-starlight-ransomware-operations-use-hui-loader

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 30, 2022 • 12:30 AM

More at www.hivepro.com