Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Industrial Spy trades stolen data on dark web Marketplace

Date of Publication	Admiralty Code	TA Number
August 9, 2022	A1	TA2022167

Summary

Since March 2022, Industrial Spy ransomware, a new menace in the threat environment, has been stealing and selling data on the dark web marketplace and conducting double extortion attacks, combining data theft and file encryption for around 30+ organizations.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	**T1070** Indicator Removal on Host	**T1036** Masquerading	**T1027** Obfuscated Files or Information
TA0040 Impact	**T1496** Resource Hijacking	**T1490** Inhibit System Recovery	**T1486** Data Encrypted for Impact
TA0002 Execution	**T1072** Software Deployment Tools	**TA0007** Discovery	**T1083** Files and Directory Discovery
TA0009 Collection	**T1005** Data from Local System		

Technical Details

#1

Industrial Spy has two executables. The first binary samples are spread via cracks, adware, and in-the-wild loaders and stealers and have no disruptive action. In contrast, the second executable encrypts files on the targeted machine.

#2

When the ransomware is executed, it parses command-line inputs before deleting Windows shadow copies, making file recovery extremely difficult. This ransomware encrypts data using a combination of 3DES and RSA standards.

#3

Unlike other ransomware families, Industrial Spy does not change the file extension after encryption. A "readme.html" file is dropped together with a ransom note threatening to expose the extorted sensitive data on the dark web marketplace

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	8a5c7fff7a7a52dca5b48afc77810142b003b9dae1c0d6b522984319d44d135a, dfd6fa5eea999907c49f6be122fd9a078412eeb84f1696418903f2b369bec4e0, 5ed4ffbd9a1a1acd44f4859c39a49639babe515434ca34bec603598b50211bab, 62051ec55c990d2ff21f36a90115986e4ac0eada18306f39687e209f49f2c6ec, 911153af684ef3460bdf568d18a4356b84efdb638e3e581609eb5cd5223f0010, 85ea71c910ebb00ba8cae266bf18400a15b08bd341e37e12083ab9a79ff6c943, C96b098cab47c0a33d0b6d8f14b24e7c9ba897b0c59a2ac1f3dc608ca7a2ed7e

References

https://www.zscaler.com/blogs/security-research/technical-analysis-industrial-spy-ransomware

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

August 9, 2022 . 5:11 AM

More at www.hivepro.com