Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

North Korean state-sponsored actors employ Maui Ransomware to target the health care industry

Date of Publication	Admiralty Code	TA Number
July 19, 2022	A2	TA2022150

Summary

North Korean state-sponsored intruders are targeting the health care and public health care sectors utilising Maui Ransomware. This ransomware does not rely on external infrastructure to create encryption keys, instead relying exclusively on manual execution by malicious actors via command-line interface.

Potential MITRE ATT&CK TTPs

TA0040 Impact	**T1486** Data Encrypted for Impact	**TA0002** Execution	**T1059.008** Command and Scripting Interpreter: Network Device CLI

Technical Details

#1

The Maui Ransomware is being used by North Korean state-sponsored malicious actors to encrypt servers that provide services such as electronic health records, diagnostics, imaging, and intranet services. Several reported incidents resulted in long-term service disruptions, and the primary access to these security breaches is unidentified.

#2

To encrypt the assets from compromised devices, Maui ransomware integrates the Advanced Encryption Standard (AES), RSA, and XOR encryption. The files are encrypted using AES 128-bit encryption and have custom headers that include information like the original path of the file and encrypted copies of the AES key.

#3

RSA encryption is used to encrypt the AES key. The Maui Ransomware loads the RSA public key-maui.key and private key-maui.evd to the same directory. The RSA public key is then encoded using XOR encryption, with the key generated from hard drive information. Finally, the malware generates the maui.log file, which contains the output of Maui execution. Actors would then probably exfiltrate maui.log and decrypt it with corresponding decryption tools.

Indicator of Compromise (IOC)

TYPE	VALUE
Filename	maui.exe maui.log maui.key maui.evd aui.exe
MD5	4118d9adce7350c3eedeb056a3335346 9b0e7c460a80f740d455a7521f0eada1 fda3a19afa85912f6dc8452675245d6b 2d02f5499d35a8dffb4c8bc0b7fec5c2 c50b839f2fc3ce5a385b9ae1c05def3a a452a5f693036320b580d28ee55ae2a3 a6e1efd70a077be032f052bb75544358 802e7d6e80d7a60e17f9ffbd62fcbbeb
SHA256	5b7ecf7e9d0715f1122baf4ce745c5fcd769dee4 8150616753fec4d6da16e99e 45d8ac1ac692d6bb0fe776620371fca02b60cac8 db23c4cc7ab5df262da42b78 56925a1f7d853d814f80e98a1c4890b0a6a84c8 3a8eded34c585c98b2df6ab19 830207029d83fd46a4a89cd623103ba2321b866 428aa04360376e6a390063570 458d258005f39d72ce47c111a7d17e8c52fe5fc7 dd98575771640d9009385456 99b0056b7cc2e305d4ccb0ac0a8a270d3fceb21e f6fc2eb13521a930cea8bd9f 3b9fe1713f638f85f20ea56fd09d20a96cd6d288 732b04b073248b56cdaef878 87bdb1de1dd6b0b75879d8b8aef80b562ec4fad 365d7abbc629bcfc1d386afa6

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-187a

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

July 19, 2022 • 5:13 AM

More at www.hivepro.com