Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Revamped version of Redeemer Ransomware has been uncovered on Dark Web Forums.

Date of Publication	Admiralty Code	TA Number
July 26, 2022	A1	TA2022156

Summary

A new version of the free Redeemer ransomware has been discovered on hacker forums, providing inexperienced threat actors with an easy entry into the field of encryption-backed extortion campaigns. The new 2.0 release was developed entirely in C/C++ and is compatible with Windows Vista, 7, 8, 10, and 11. Aside from cross-compatibility, Redeemer features strong obfuscation capabilities, and the builder claims medium-AV detection.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**T1204** User Execution	**TA0007** Discovery	**T1012** Query Registry
T1082 System Information Discovery	**T1083** File and Directory Discovery	**TA0005** Defense Evasion	**T1027** Obfuscated Files or Information
T1070 Indicator Removal on Host	**TA0040** Impact	**T1486** Data Encrypted for Impact	**T1489** Service Stop
T1490 Inhibit System Recovery	**TA0003** Persistence	**T1547** Boot or Logon Autostart Execution	

Technical Details

#1 When the malware is executed on the victim's device, it creates a mutex called "RedeemerMutex" to ensure that only one instance of malware is running on the victim's system. It then creates a folder, copies itself into the Windows directory with legitimate file names such as svchost.exe, calc.exe, and so on, and executes itself as a new process via the ShellExecuteW() API method.

#2 The process that is executed deletes shadow copies and backups, clears the event log, and terminates processes. The ransomware will enumerate the victim's files and directories and begin the encryption process, leaving a ransom note in the Winlogon registry key with key values "LegalNoticeCaption" and "LegalNoticeText."

#3 According to the contract signed by the malevolent ransomware user, the developer has specified that 20% of the ransom from the victims will be going to them.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	4368f30798a1caa0a7b30735111e143068678a0547dfd38c050926619869c73a Bf8f74a05e4a10ab893c73bc95ed16c3b5c6ffe6e257c098b33c04c3a893acb9 86bd9cdfdb425266c477544a5cf951fdc56733d46f1a7b44f8188168b5e2fb15 1178e2b691fd266ccd29867acf134c855241b18b730b766da0ae69c53d4b9776
SHA1	9aa9290d337d68136030fc8182f7d499951a207e b8a0d70e602684067b2dc5565a5f6a786fb298fa 1a22bc573674186f234dd541b9fccaf938195b33 e6f98d1666896c84279db4fb6af5c5e6d815bb75
MD5	56a13812819c8426941c9bd8b63d3a9f 4b01f0d2de0b557cd13e42a36b78894f cd513de769a9c385b218306e7affc131 cd4b9ae02fdddfdb555ee45591deca4f

References

https://blog.cyble.com/2022/07/20/redeemer-ransomware-back-action/

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 26, 2022 • 4:08 AM

More at www.hivepro.com