Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Novel remote access trojan CodeRAT uncovered

Date of Publication	Admiralty Code	TA Number
September 6, 2022	A1	TA2022193

Summary

CodeRAT is a remote access trojan (RAT). The malicious operation, which appears to have originated in Iran, employed a Word document with a Microsoft Dynamic Data Exchange (DDE) exploit to target Farsi-speaking software developers.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1566** Phishing	**TA0002** Execution	**T1106** Native API
T1059 Command and Scripting Interpreter	**TA0005** Defense Evasion	**T1070** Indicator Removal on Host	**TA0007** Discovery
T1057 Process Discovery	**T1083** File and Directory Discovery	**TA0009** Collection	**T1113** Screen Capture
TA0011 Command and Control	**T1090** Proxy	**T1105** Ingress Tool Transfer	

Technical Details

#1

CodeRAT allows attackers to monitor the victim's activity and has broad monitoring capabilities that support approximately 50 commands. These capabilities are aimed toward webmail, databases, Microsoft Office documents, social media platforms, and Windows.

#2

To produce the commands, the attacker uses a UI tool that generates and obfuscates them and then sends them to the malware using one of three methods:

- Telegram bot API with proxy (no direct requests)
- Manual mode (includes USB option)
- Locally stored commands on the 'myPictures' folder

#3

CodeRAT includes an anti-filter capability that creates a second request routing channel that can assist in bypassing the blockages. The malware can persist in reboots without modifying the Windows registry.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	25d6fccc82ec3c3c6786dcaa5d9f6920b769457502eef0759b235cd71c552b17 2a4e5e6f403ce913cb073d5c5d1fd999d8ae79deb04915b9777525e05e21a2b2 cd53fba6ddd4ae4ef7a5747c6003236c85791477854cc1b7ce00e0f8ee7677d9 F22041b2ea1fd6d8e7f6f1db7469dec61b000d067ab4be2c5b0654edfecbddb6
URLs	hxxps[:]//raw.githubusercontent[.]com/alberfrancis/camo/main/432gsbse5, hxxps[:]//api.telegram[.]org/bot5379338428:AAFkD8lIvAK1pvUDQYusiFHUOxo 7JlaziQ/getchat?chat_id=968019073, hxxps[:]//api.telegram[.]org/bot1335021029:AAHbdgFSOPJ5KtcF1YMdtsN2jc7 Yqu6Tou8/getchat?chat_id=968019073

References

https://www.safebreach.com/resources/blog/remote-access-trojan-coderat/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous 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

September 6, 2022 • 3:48 AM

More at www.hivepro.com