Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

Chile government's Windows and Linux servers hit by RedAlert ransomware

Date of Publication	Admiralty Code	TA Number
September 2, 2022	A2	TA2022191

Summary

The Chilean Ministry of Interior asserted that RedAlert ransomware aka N13V attack had disrupted the operations and online services of a government agency in the country. In classic double-extortion manner, the malware targeted the agency's Microsoft and VMware ESXi servers.

Potential MITRE ATT&CK TTPs

TA0006 Credential Access	**T1552** Unsecured Credentials	**T1552.001** Credentials In Files	**TA0005** Defense Evasion
T1112 Modify Registry	**TA0007** Discovery	**T1012** Query Registry	**T1057** Process Discovery
T1082 System Information Discovery	**T1120** Peripheral Device Discovery	**TA0003** Persistence	**T1547** Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder			

Technical Details

#1 The malware initially collects credentials from web browsers, lists removable devices for encryption, and avoid scrutiny by antivirus software by employing execution delay.

#2 Then intruders terminate all active virtual machines and encrypted their documents via NTRUEncrypt public key encryption algorithm and appending the ".crypt" extension to the encrypted filenames. The malware's behaviour suggests that it is RedAlert ransomware.

#3 Before deploying the final payload, intruders leave a ransom note named 'readme_for_unlock.txt' which provides a communication channel to negotiate the ransom payment that would inhibit the files from being leaked and unlock the encrypted data.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	39b74b2fb057e8c78a2ba6639cf3d58ae91685e6ac13b57b70d2afb158cf742d ac73234d1005ed33e94653ec35843ddc042130743eb6521bfd3c32578e926004 c42834ac1c8efc19c44024f1e4960c5a9aaab05dc9fceb0d1596ffe0c244f5f2
URL	https://api.telegram[.]org/bot1840149904:AAF9D1mm8ZITxzSWfLFbRBfwFML1TyPoOMk/sendMessage?chat_id=1796245478

Recent Breaches

https://www.coarc.org/

https://keystonelegal.co.uk/

https://vahanen.com/

http://www.syredis.fr/

References

https://csirt.gob.cl/alertas/2cmv22-00338-01/

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

September 2, 2022 • 4:11 AM

More at www.hivepro.com