Hive Pro

Threat Level

Red

THREAT ADVISORY

ATTACK REPORT

Zeppelin ransomware target organization in Europe and USA

Date of Publication	Admiralty Code	TA Number
August 12, 2022	A1	TA2022171

Summary

Zeppelin, the newest member of the Delphi-based Vega ransomware family, has been quite clever in meticulously tailoring these ransomware operations. Zeppelin, first identified in 2019 as ransomware-as-a-service (RaaS) , has been predominantly targeting international corporations in Europe and the United States.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**T1133** External Remote Services	**T1190** Exploit Public-Facing Application	**T1566** Phishing
TA0002 Execution	**T1204** User Execution	**T1204.001** Malicious Link	**T1204.002** Malicious File
TA0003 Persistence	**T1543** Create or Modify System Process	**T1543.003** Windows Service	**TA0040** Impact
T1486 Data Encrypted for Impact			

Technical Details

#1 Zeppelin threat actors obtain access to victim networks through RDP exploitation, SonicWall firewall exploits, and phishing tactics. Zeppelin is deployed as a.dll or.exe file or bundled in a PowerShell loader

#2 Before encryption, adversaries exfiltrate sensitive corporate files to sell or disclose if the victim does not pay the ransom in Bitcoins.

#3 Zeppelin infiltrates the infrastructure and implants itself as a .zeppelin temporary folder. As a file extension, a randomized nine-digit hexadecimal number is assigned to each encrypted file.

#4 Finally, a file containing a ransom note is placed on compromised Devices, most often on the desktop. There have been instances of Malicious actors executing the malware numerous times within a target's network, leading in the generation of various IDs or file extensions. As a result, the victim requires several unique decryption keys.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA1	4fee2cb5c98abbe556e9c7ccfebe9df4f8cde53f, Eaeff8d315cca71e997063a2baec5cc73fad9453, 1cb5e8132302b420af9b1e5f333c507d8b2a2441,db398e38ee6221df7e4aa49d8f96799cca4d87e1,4b91a91a98a2f0128c80f8ceeef0f5d293adf0cd,9892cc90e6712d3548e45f34f14f362bccedf0be,ffd228b0d7afe7cab4e9734f7093e7ba01c5a06e,0f47c279fea1423c7a0e7bc967d9ff3fae7a0de8,f561f9e3c949fe87f12dbfa166ffb2eb85712419,a243ce234fc8294e2e2e526418b4eaadc2d6c84f

TYPE	VALUE
SHA-256	001938ed01bfde6b100927ff8199c65d1bff30381b80b846f2e3fe5a0d2df21d a42185d506e08160cb96c81801fbe173fb071f4a2f284830580541e057f4423b aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe a2a9385cbbcfacc2d541f5bd92c38b0376b15002901b2fd1cc62859e161a8037 54d567812eca7fc5f2ff566e7fb8a93618b6d2357ce71776238e0b94d55172b1 fb59f163a2372d09cd0fc75341d3972fdd3087d2d507961303656b1d791b17c6 1e3c5a0aa079f8dfcc49cdca82891ab78d016a919d9810120b79c5deb332f388 347f14497df4df73bc414f4e852c5490b12db991a4b3811712bac7476a3f1bc9 7d8c4c742689c097ac861fcbf7734709fd7dcab1f7ef2ceffb4b0b7dec109f55 37c320983ae4c1fd0897736a53e5b0481edb1d1d91b366f047aa024b0fc0a86e
MD5	981526650af8d6f8f20177a26abb513ac25d45e9bbfea29cb6d9ee0d9bf2864d 183b6b0c90c1e0276a2015752344a4cf9349e1cc3de7c7f6893a21bd6c3c4a6bc8f75487d0d496a3746e6c81a5ecc6dc 477eedb422041385e59a4fff72cb97c15841ef35aaff08bb03d25e5afe3856a2 d6c4b253ab1d169cf312fec12cc9a28ffba7180ad49d6a7f3c60c890e2784704 bc6c991941d9afbd522fa0a2a248a97a

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-223a

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 12, 2022 • 1:37 AM

More at www.hivepro.com