Mphasis
The Next Applied

Advisory: Zeppelin Ransomware

Severity: High

Date: 12th Aug 2022

Background

Zeppelin is the latest member of the VegaLocker ransomware family, which also contains strains like Jumper, Storm, or Buran. Zeppelin is an example of well-organized threat actors, as those behind Zeppelin have been incredibly strategic in carefully targeting these ransomware attacks. First spotted in November 2019, Zeppelin has been targeting primarily large companies in Europe and the United States.

Description

Zeppelin ransomware is a derivative of the Delphi-based Vega malware family and functions as a Ransomware as a Service (RaaS). From 2019 through at least June 2022, actors have used this malware to target a wide range of businesses and critical infrastructure organizations, including defense contractors, educational institutions, manufacturers, technology companies, and especially organizations in the healthcare and medical industries. Zeppelin actors have been known to request ransom payments in Bitcoin, with initial amounts ranging from several thousand dollars to over a million dollars.

Methodology

The VegaLocker family appears to be an example of an increasingly common Ransomware-as-a-service (RaaS), in which cybercriminals create ransomware, and either sell it to others or rent it and take a portion of any bounty collected when it is used in a successful attack. Unlike the broader reach of VegaLocker family attacks geared toward Russian speakers, the threat actors behind Zeppelin are running a precision campaign, targeting high-profile technology and healthcare companies in western countries. A more recent attack may also indicate that real estate firms are their latest target.

Other VegaLocker strains used methods like malvertising, in which malware laden advertisements are placed directly on webpages or through advertising networks, infecting anyone who clicks on them. Zeppelin, on the other hand, is believed to be relying heavily on water-holing attacks, in which websites that are likely to be visited by targeted victims are embedded with malware.

Once Zeppelin has entered the infrastructure, it installs itself in a temporary folder named .zeppelin, and spread, it begins to encrypt files. Though what is encrypted can be configured by the threat actor, by default, it encrypts

Windows operating system directories, web browser applications, system boot files, and user files in order to preserve system function. Once encryption is complete, a note appears in Notepad informing the victims that they have been attacked, and that ransom must be paid for the return of their data. The contents have varied from a generic one titled, !!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT, to those more personalized to the organization. There is often an offer of free decryption of a single file offered as proof that decryption is possibly used as a lure to encourage payment.

Mitigation Plans

The FBI and CISA recommend network defenders apply the following mitigations to limit potential adversarial use of common system and network discovery techniques and to reduce the risk of compromise by Zeppelin ransomware:

- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- Require all accounts with password logins (e.g., service accounts, admin accounts, and domain admin accounts) to comply with National Institute for Standards and Technology (NIST) standards for developing and managing password policies.
- Require multifactor authentication for all services to the extent possible, particularly for webmail, virtual private networks, and accounts that access critical systems.
- Keep all operating systems, software, and firmware up to date.
- Segment networks to prevent the spread of ransomware. Network segmentation can help prevent the spread of ransomware by controlling traffic flows between—and access to—various subnetworks and by restricting adversary lateral movement.
- Identify, detect, and investigate abnormal activity and potential traversal of the indicated ransomware with a networking monitoring tool.
- Install, regularly update, and enable real-time detection for antivirus software on all hosts.
- Disable command-line and scripting activities and permissions.

Indicators of Compromise (IOC)

SHA256	
ed1548744db512a5502474116828f75737aec8bb11133d5e4ad44be16aa3666b	001938ed01bfde6b100927ff8199c65d1bff30381b80b846f2e3fe5a0d2df21d
cf9b6dda84cbf2dbfc6edd7a740f50bddc128842565c590d8126e5d93c024ff2	a42185d506e08160cb96c81801fbe173fb071f4a2f284830580541e057f4423b
21807d9fcaa91a0945e80d92778760e7856268883d36139a1ad29ab91f9d983d	aa7e2d63fc991990958dfb795a0aed254149f185f403231eaebe35147f4b5ebe
0d22d3d637930e7c26a0f16513ec438243a8a01ea9c9d856acbcda61fcb7b499	a2a9385cbbcfacc2d541f5bd92c38b0376b15002901b2fd1cc62859e161a8037
6fbfc8319ed7996761b613c18c8cb6b92a1eaed1555dae6c6b8e2594ac5fa2b9	54d567812eca7fc5f2ff566e7fb8a93618b6d2357ce71776238e0b94d55172b1
e8596675fef4ad8378e4220c22f4358fdb4a20531b59d7df5382c421867520a9	fb59f163a2372d09cd0fc75341d3972fdd3087d2d507961303656b1d791b17c6
353e59e96cbf6ea6c16d06da5579d3815aaaeeefacabd7b35ba31f7b17207c5b	1e3c5a0aa079f8dfcc49cdca82891ab78d016a919d9810120b79c5deb332f388
85f9bf4d07bc2ac1891e367f077dd513d6ca07705bffd1b648d32a7b2dc396f5	347f14497df4df73bc414f4e852c5490b12db991a4b3811712bac7476a3f1bc9
614cb70659ef5bb2f641f09785adc4ab5873e0564a5303252d3c141a899253b2	7d8c4c742689c097ac861fcbf7734709fd7dcab1f7ef2ceffb4b0b7dec109f55
fb3e0f1e6f53ffe680d66d2143f06eb6363897d374dc5dc63eb2f28188b8ad83	37c320983ae4c1fd0897736a53e5b0481edb1d1d91b366f047aa024b0fc0a86e
594df9c402abfdc3c838d871c3395ac047f256b2ac2fd6ff66b371252978348d	894b03ed203cfa712a28ec472efec0ca9a55d6058115970fe7d1697a3ddb0072
2dffe3ba5c70af51ddf0ff5a322eba0746f3bf3ae0751beb3dc0059ed3faaf3d	307877881957a297e41d75c84e9a965f1cd07ac9d026314dcaff55c4da23d03e
45fba1ef399f41227ae4d14228253237b5eb464f56cab92c91a6a964dc790622	bafd3434f3ba5bb9685e239762281d4c7504de7e0cfd9d6394e4a85b4882ff5d
774ef04333c3fb2a6a4407654e28c2900c62bd202ad6e5909336eb9bc180d279	faa79c796c27b11c4f007023e50509662eac4bca99a71b26a9122c260abfb3c6
677035259ba8342f1a624fd09168c42017bdca9ebc0b39bf6c37852899331460	e48cf17caffc40815efb907e522475722f059990afc19ac516592231a783e878
26ec12b63c0e4e60d839aea592c4b5dcff853589b53626e1dbf8c656f4ee6c64	4a4be110d587421ad50d2b1a38b108fa05f314631066a2e96a1c85cc05814080
37efe10b04090995e2f3d9f932c3653b27a65fc76811fa583934a725d41a6b08	9ef90ec912543cc24e18e73299296f14cb2c931a5d633d4c097efa372ae59846
a5847867730e7849117c31cdae8bb0a25004635d49f366fbfaebce034d865d7d	dd89d939c941a53d6188232288a3bd73ba9baf0b4ca6bf6ccca697d9ee42533f
e61edbddf9aed8a52e9be1165a0440f1b6e9943ae634148df0d0517a0cf2db13	79d6e498e7789aaccd8caa610e8c15836267c6a668c322111708cf80bc38286c
746f0c02c832b079aec221c04d2a4eb790287f6d10d39b95595a7df4086f457f	b22b3625bcce7b010c0ee621434878c5f8d7691c2a101ae248dd221a70668ac0
b191a004b6d8a706aba82a2d1052bcb7bed0c286a0a6e4e0c4723f073af52e7c	961fbc7641f04f9fed8391c387f01d64435dda6af1164be58c4cb808b08cc910
614cb70659ef5bb2f641f09785adc4ab5873e0564a5303252d3c141a899253b2	d618c1ccd24d29e911cd3e899a4df2625155297e80f4c5c1354bc2e79f70768c
85f9bf4d07bc2ac1891e367f077dd513d6ca07705bffd1b648d32a7b2dc396f5	8170612574f914eec9e66902767b834432a75b1d6ae510f77546af2a291a48a2
353e59e96cbf6ea6c16d06da5579d3815aaaeeefacabd7b35ba31f7b17207c5b	5326f52bd9a7a52759fe2fde3407dc28e8c2caa33abf1c09c47b192a1c004c12
e8596675fef4ad8378e4220c22f4358fdb4a20531b59d7df5382c421867520a9	6bafc7e2c7edc2167db187f50106e57b49d4a0e1b9269f1d8a40f824f2ccb42b
6fbfc8319ed7996761b613c18c8cb6b92a1eaed1555dae6c6b8e2594ac5fa2b9	f7af51f1b2b98b482885b702508bd65d310108a506e6d8cef3986e69f972c67d
0d22d3d637930e7c26a0f16513ec438243a8a01ea9c9d856acbcda61fcb7b499	bc214c74bdf6f6781f0de994750ba3c50c0e10d9db3483183bd47f5cef154509

Reference Links

https://www.coresecurity.com/core-labs/articles/what-zeppelin-ransomware-steps-prepare-respond-and-prevent-infection

What is Zeppelin Ransomware? Steps to Prepare, Respond, and Prevent Infection (coresecurity.com)