HC3 Intelligence Briefing
Zeppelin Ransomware

OVERALL CLASSIFICATION IS
TLP:WHITE

January 23, 2020
Agenda

- Ransomware in Healthcare
- Ransomware Types
- Zeppelin Overview
- Zeppelin Capabilities
- Deployment Strategy
- Country Specific Targeting
- Vegalocker Evolution
- Mitigations
- Indicators of Compromise
- References

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Ransomware in Healthcare

- A research firm documented 117 ransomware incidents targeting healthcare providers in the United States.
- Number of patient records impacted: 4,474,000
  - 57% included patient notification
  - The perception is that healthcare providers are more likely to pay ransoms than other industries, leading hackers to actively pursue healthcare.
    - Research of the 117 incidents suggests otherwise:
      - 61% did not pay
      - 15% confirmed payment
      - 24% unknown outcome
- A challenge with ransomware analysis is that many organizations either do not report incidents or limit the amount of information regarding the incident.

### Notable 2019 Ransomware attacks on Healthcare

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec</td>
<td>Hawaiian cancer specialty had to temporarily suspend cancer radiation services at two treatment centers</td>
</tr>
<tr>
<td>Nov</td>
<td>Nebraska healthcare organization; email, EHR, and other computer services had to be restored.</td>
</tr>
<tr>
<td>Nov</td>
<td>Milwaukee/Wisconsin based IT provider hit with ransomware, preventing 110 nursing homes from accessing patient records.</td>
</tr>
<tr>
<td>Oct</td>
<td>Three Tuscaloosa, Ala.-based Health System hospitals temporarily closed to new patients due to a targeted ransomware attack.</td>
</tr>
<tr>
<td>Dec</td>
<td>California based clinic closed after losing all access to its patients’ medical records</td>
</tr>
<tr>
<td>Apr</td>
<td>Michigan based practice closed down after ransomware attack deleted all their system files and records</td>
</tr>
<tr>
<td>Sep</td>
<td>Wyoming-based hospital suspended new inpatient admissions and canceled some surgeries.</td>
</tr>
<tr>
<td>Jun</td>
<td>Utah-based healthcare agency alerted 320,000 patients that their health information may have been exposed in a ransomware attack.</td>
</tr>
<tr>
<td>May</td>
<td>Louisiana physicians’ network alerted more than 116,000 patients of a ransomware attack that may have compromised their personal information.</td>
</tr>
<tr>
<td>May</td>
<td>Ransomware attack on Indiana Medical Surgical Eyecare Associates’ network server and EHR system may have compromised 106,000 patient records.</td>
</tr>
<tr>
<td>Jun</td>
<td>Two NY medical groups temporarily lost access to their computer and EHR systems following cyberattacks on the organizations.</td>
</tr>
</tbody>
</table>
Ransomware is commonly divided into 2 categories:

**Locker ransomware (Computer Locker)**
- Designed to deny access to computing resources, usually in the form of locking the computer or devices user interface
- Hacker will restore access once a fee has been paid
- User will typically be left with limited capabilities, allowing the user to interact with only the ransomware and pay the ransom
- Often uses social-engineering techniques to pressure victim
- Usually able to be removed cleanly by users

**Crypto Ransomware (Data Locker)**
- Designed to find and encrypt valuable data stored on the computer
- Often targets specific data sources with value (Ex: personal collections, work related information, financial data)
- More technical in nature, can stay hidden while encrypting data.
- The affecting computer will usually continue working since critical systems files are not targeted.

Zeppelin is considered a Crypto Ransomware

Source: Symantec
Zeppelin Overview

• **Zeppelin** – new ransomware observed targeting U.S and European Healthcare and IT companies
  • Derived from the VegaLocker Ransomware family
  • Distributed through remote desktop servers publicly exposed to the internet
  • Many elements of Zeppelin are similar to ransomware campaigns like sodinokibi
    • Known to steal victim data before the encryption process
    • Targeted Managed Service Providers (MSP) in order to further infect customers via management software
  • Considered a Ransomware-as-a-Service or Attack-as-a-Service package.
    • Allows users to selectively craft ransomware payloads for customized campaigns.
    • Offers high degree of evasion against anti-malware tools and services.
  • Checks to see if the user is in a Commonwealth of Independent States (CIS) country, namely (specifically Russia, Ukraine, Belorussia, and Kazakhstan).
    • Will stop processes if the user is found to be in a CIS country.

Source: Zdnet, Beckers Hospital Review
Zeppelin Capabilities

Configuration Options

**Startup** – Ensure ransomware persistence on the target computer

**IP Logger** – Track locations and IP addresses of victims

**Delete Backups** – Deletes backup copies and disables file recovery in order to prevent users from getting their files back without paying the ransom

**Task-Killer** – End specific tasks

**Auto-Unlock** - Automatically unlocks files that are locked during the encryption

**Melt** – Used to self-destruct files through notepad.exe

**UAC prompt** – Attempts to run the ransomware as an administrator, giving it elevated privileges and letting it do more damage

Obfuscation capabilities

Zeppelin is able to evade detection by using several layers of obfuscation to avoid detection by antimalware tools. This includes using pseudo-random keys, different-sized code, encrypted string, and delays in execution to outrun sandboxes, among other methods.

Estimates suggest that around a third of antivirus programs (30%) are unable to detect Zeppelin.

Source: Reactionary Times

Zeppelin Ransomware Builder

- Payloads can customized as an .exe, .dll, or a .ps1 script payloads so that they can be used in different types of attacks.

- Also allows the affiliate to create custom ransom notes that fit the theme of their attack.

Example: if targeting a particular company, builder can specify the company name in the note to provide more impact.
Zeppelin is distributed by using:

- Email, spam, and malicious attachments, deceptive downloads, botnets, exploits, malicious ads, web injects, fake updates, repackaged and infected installers.
- Some of the Zeppelin attacks were launched through managed security services providers (MSSPs).
  - The attacks bear similarities to Sodinokibi campaigns (although not in scale)
- Zeppelin was also observed collecting and stealing victim data before encrypting the files
  - Also a trait that mirrors Sodinokibi attacks (although not in scale)
- RDP vulnerabilities have been found to be exploited by Zeppelin for distribution
  - Researchers have specifically observed Zeppelin ransomware being delivered through ConnectWise (formerly ScreenConnect)
    - Connectwise is a central web application remote desktop control tool that is designed to allow IT admins to manage remote computers and remotely execute commands on a user’s computer.
Country Specific Targeting

- Zeppelin does not target computers from Russia, Belorussia, Kazakhstan, and Ukraine.
  - It is speculated that the criminals do not want to draw the attention of local law enforcement.
- The Zeppelin strain has been designed to target western and European countries.
  - Different tactic than it’s Vegalocker predecessors
- Victims of the Zeppelin ransomware campaign have mostly been IT and healthcare companies in Europe and North America.

Attribution

- The whitelisting of CIS nation countries would suggest that a different group is behind zeppelin’s rise then that of vegalocker.
- Given that underground hackers would offer Vega ransomware-as-a-service, researchers believe that Zeppelin was either developed from bought or stolen assets or that it has found its way into the hands of other users.

Source: Threat Vector; Geekflare
VegaLocker Evolution

- Zeppelin is derived from the VegaLocker ransomware family
  - Includes VegaLocker, Jumper (Jamper), and Buran
  - Notably quick evolution timeline in 2019
  - Malware authors often evolve malware code to improve it’s effectiveness and more business functional.
- A notable predecessor is Buran ransomware
  - First Ransomware-as-a-Service instance in the VegaLocker family
  - Advertised on well-known Russian forum.
  - Included user region detection capability.
  - Delivered through exploit kits (RIG EK).

Source: Mcafee
Mitigations

Ransomware Best Practices:

Data protection

✓ Perform frequent backups
✓ Store backups separately
✓ Train personnel

Infection prevention

✓ Update and patch
✓ Exercise caution when clicking links
✓ Exercise caution with email attachments
✓ Verify email senders
✓ Use end point security and content filtering

Respond

✓ Isolate the infected system
✓ Turn off other computers and devices
✓ Secure your backups

Source: US-CERT

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

HHS 405d Health Industry Cybersecurity Practices

TLP:WHITE
Indicators of Compromise

**SHA-256**
04628e5ec57c983185091f02fb16dfdac0252b2d253ff4c4d8d79f3c79de2722
39d8331b963751bbd5556ff71b0269db018ba1f425939c3e865b79cc770bfe4
4894b1549a24e964403565c61f9ae5f8daf244c90b1ffbd5709ed1a8491d56bf
39d8331b963751bbd5556ff71b0269db018ba1f425939c3e865b79cc770bfe4
4894b1549a24e964403565c61f9ae5f8daf244c90b1ffbd5709ed1a8491d56bf
e22b5062cb5b02987ac32941ebd71872578e9be2b8c6f8679c3e0e1a84764dba7
1f94d1824783e8edac62942e13185ffd02ebd129970ca04e0dd5b245dd3002bc
d61bd67b0150ad77e6fb19100df890c48db680d089a96a28a630140b9868d86

**Associated file names:**

- **HMAC\Software\Zeppelin**

**Associated registry keys:**

- **Ransom note:**

```
!!! ALL YOUR FILES ARE ENCRYPTED !!!

All your files, documents, photos, databases and other important files are encrypted.
You are not able to decrypt it by yourself! The only method of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decrypter and it works you can send an email: admin@datastex.club and decrypt one file for free.
But this file should be of not valuable!

Do you really want to restore your files?
Write to email: admin@datastex.club
Reserved email: admin@datastex.xyz

Your personal ID: 236-158-2D2

Attention!
* Do not rename encrypted files.
* Do not try to decrypt your data using third party software, it may cause permanent data loss.
* Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.
```

**Email Addresses**
- bad_sysadmin@protonmail[.]com
- Vsbb@firemail[.]cc
- Vsbb@tutanota[.]com
- buratino@firemail[.]cc
- buratino2@tutanota[.]com
- ran-unlock@protonmail[.]com
- ranunlock@cock[.]nl
- buratin@torbox3uiot6wchz[.]onion

**Sources:** Trend Micro, Bleeping Computer

**URLs**
- hxxps://iplogger[.]org/1HVwe7[.]png
- hxxps://iplogger[.]org/1HCne7[.]jpeg
- hxxps://iplogger[.]org/1Hpee7[.]jpeg
- hxxps://iplogger[.]org/1syG87
- hxxps://iplogger[.]org/1H7Yt7[.]jpg
- hxxps://iplogger[.]org/1wF9i7[.]jpeg
References

• Early Analysis of Ransomware Attacks on the Healthcare Industry
  https://www.recordedfuture.com/healthcare-ransomware-attacks/

• Michigan Practice Forced to Close Following Ransomware Attack

• 15 notable ransomware attacks on healthcare providers in 2019

• The Evolution of Ransomware

• Zeppelin Malware: The Swiss Army Knife of Ransomware
  https://www.reactionarytimes.com/what-is-zeppelin-ransomware/

• Connectwise Control Abused Again to Deliver Zeppelin Ransomware

• Buran Ransomware; the Evolution of VegaLocker

• Security Tip (ST19-001) Protecting Against Ransomware
  https://www.us-cert.gov/ncas/tips/ST19-001

• Ransomware Recap: Snatch and Zeppelin Ransomware

• Zeppelin Ransomware Targets Healthcare and IT Companies

• Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
  https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx

Source: ICS.SANS, USCERT
Questions

Upcoming Briefs

• Ryuk Update
• A.I. Application in the Healthcare in Industry

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.