How to Respond to a Ransomware Attack

HIPAA Summit (Mar. 5, 2019)

Nicholas Heesters
Health Information Privacy and Security Specialist
Office for Civil Rights, HHS

John Boles
Principal,
PricewaterhouseCoopers Advisory Services, LLC

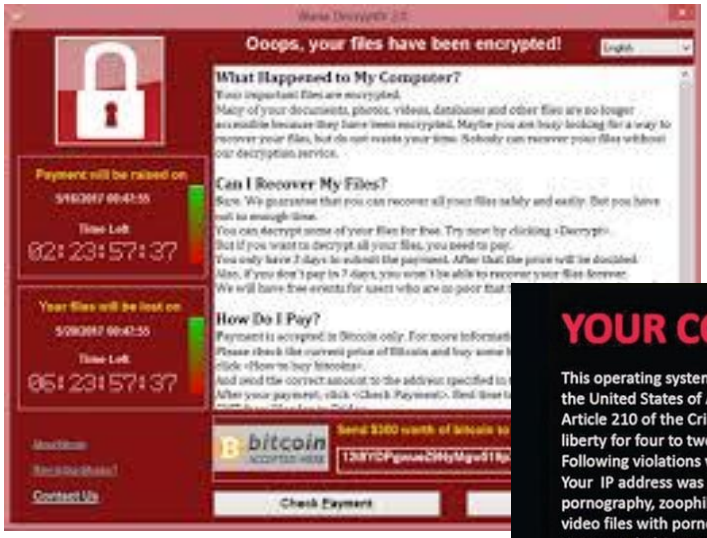
Adam Greene
Partner
Davis Wright Tremaine LLP

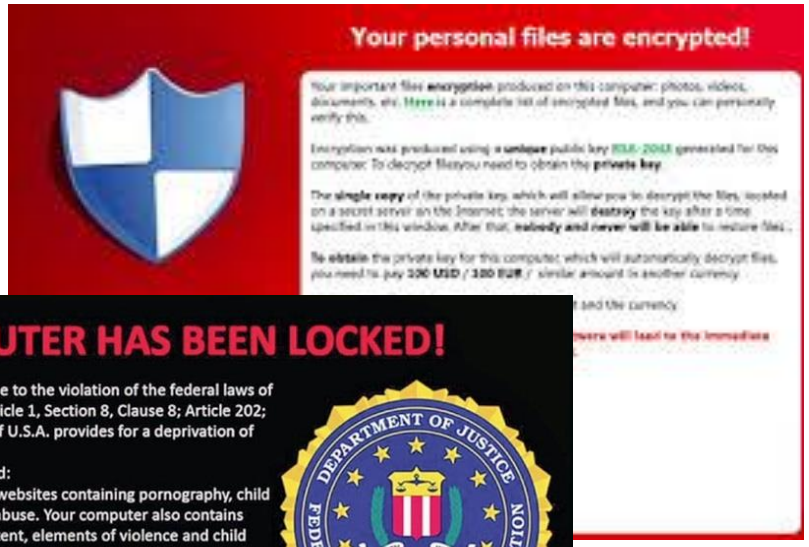
Agenda

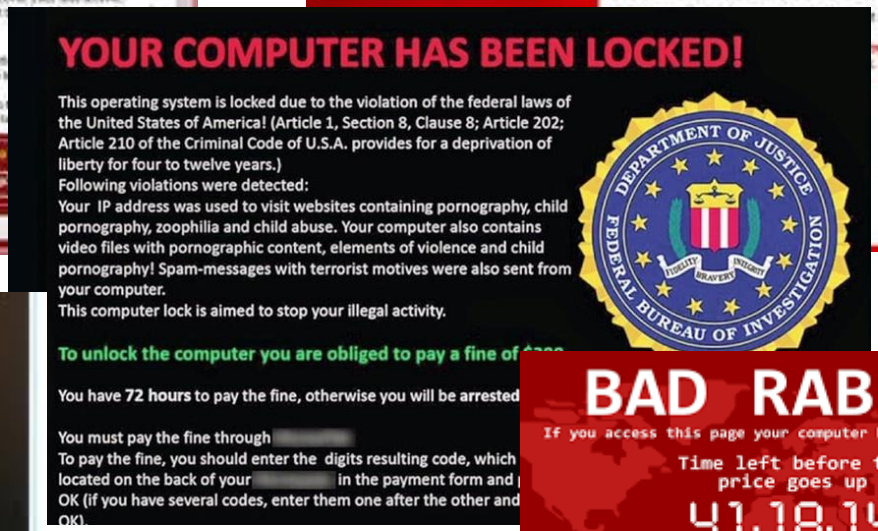
- Introductions
- Responding to a Ransomware Attack – the Technical Side
- OCR Guidance on Ransomware
- An Outside Counsel's Perspective
- Q&A

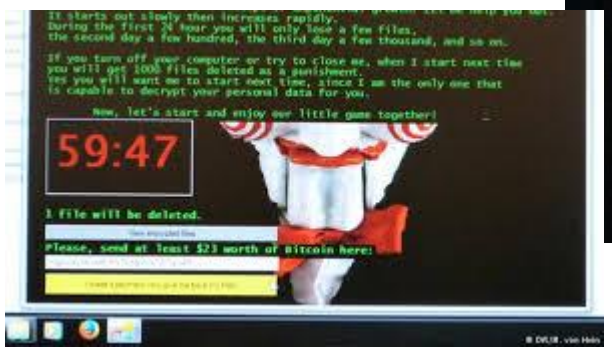
Responding to a Ransomware Attack – the Technical Side

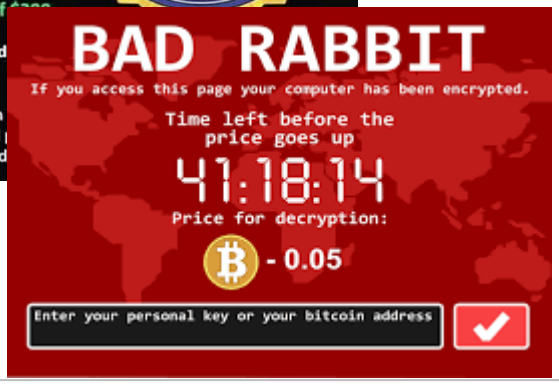
Ransomware


Oops, your files have been encrypted!
What Happened to My Computer?
Can I Recover My Files?
How Do I Pay?
Payment will be raised on
Time Left
02:23:57:37
Your files will be lost on
05:23:57:37
bitcoin
Check Payment
Contact Us

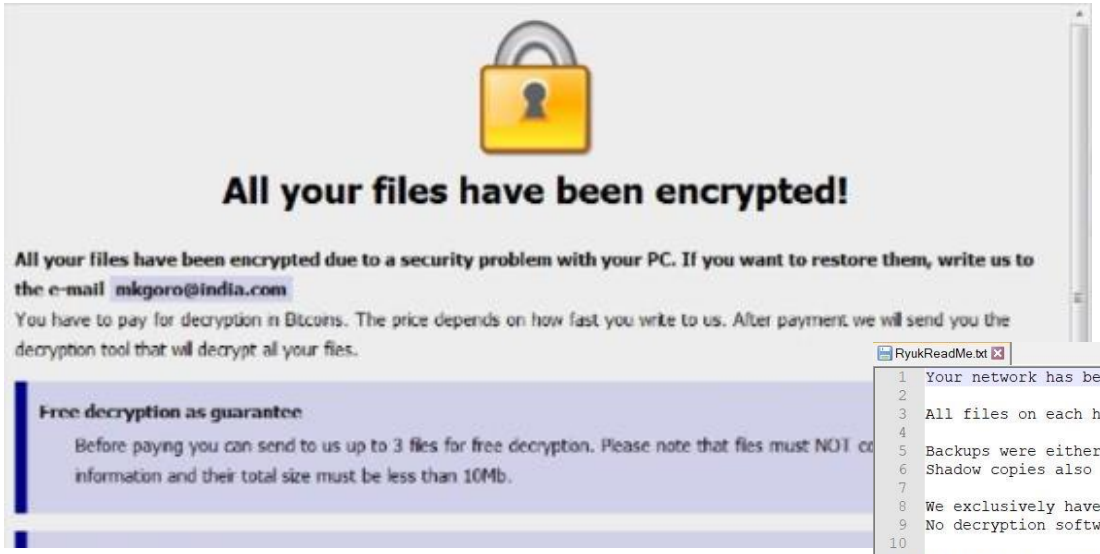

Your personal files are encrypted!


YOUR COMPUTER HAS BEEN LOCKED!
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.
To unlock the computer you are obliged to pay a fine of
You have 72 hours to pay the fine, otherwise you will be arrested
You must pay the fine through
To pay the fine, you should enter the digits resulting code, which
located on the back of your in the payment form and
OK (if you have several codes, enter them one after the other and
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


59:47
1 file will be deleted.
Please, send at least $23 worth of Bitcoin here:


BAD RABBIT
If you access this page your computer has been encrypted.
Time left before the price goes up
41:18:14
Price for decryption:
- 0.05
Enter your personal key or your bitcoin address

The Attack



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail mkgoro@india.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send to us up to 3 files for free decryption. Please note that files must NOT co
information and their total size must be less than 10Mb.

RyukReadMe.txt

```
1  Your network has been penetrated.
2
3  All files on each host in the network have been encrypted with a strong algorithm.
4
5  Backups were either encrypted or deleted or backup disks were formatted.
6  Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
7
8  We exclusively have decryption software for your situation
9  No decryption software is available in the public.
10
11 DO NOT RESET OR SHUTDOWN - files may be damaged.
12 DO NOT RENAME OR MOVE the encrypted and readme files.
13 DO NOT DELETE readme files.
14 This may lead to the impossibility of recovery of the certain files.
15
16 To get info (decrypt your files) contact us at
17 WayneEvenson@protonmail.com
18 or
19 WayneEvenson@tutanota.com
20
21 BTC wallet:
22 14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk
23
24 Ryuk
25
26 No system is safe
```

Ransomware Response Lifecycle

Pre-Attack

Back Up

Back up data regularly and segregate them from the network

Logs

Enable logs and review them for suspicious activity. Set retention for 30 days for investigations

Know Your Business

Isolate and protect the most sensitive data

Train Your Team

Have an IRP in place and practice it. Recognize suspicious activity and report it

Immediate

Stop the Bleeding

Take machines offline/terminate the connection – BUT leave them powered on, if possible

Preserve Evidence

Capture memory/image, preserve firewall and other logs

Initiate Your IR Plan

In-house IT teams can be quickly overwhelmed, depending on the incident. Consider outside forensics and outside counsel who specialize in Incident Response

Recovery and Remediation

Recover from Back Ups

Best case scenario

Rebuild and Reload

Can be a long process

Prepare for the Next Incident

Always learn from the incident to reduce the risk of another one

To Pay or Not To Pay

Pros

- **May be only option**
- **Quick recovery of critical data**
- **Minimize business interruption**

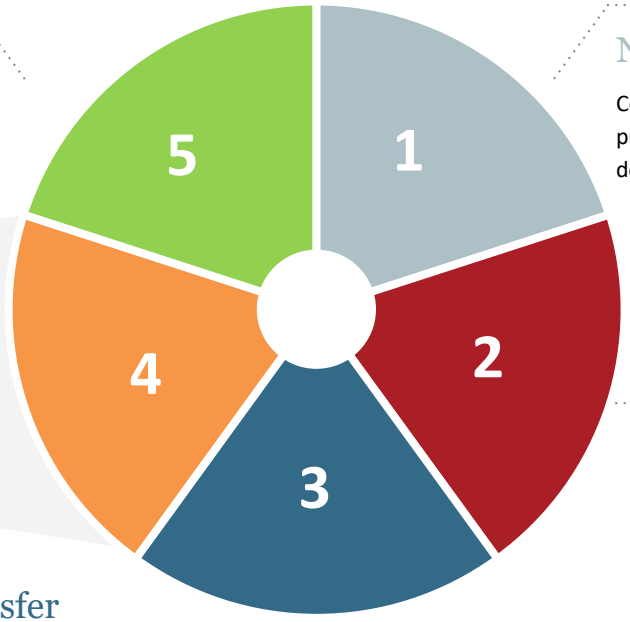
Cons

- **Incentivizes future attacks**
- **Rewards the attacker**

Risks

- **Attacker may not provide key**
- **Attacker may partially decrypt or raise the ransom**
- **Key may contain additional malicious payload**

Payment Process



Negotiation/Contact

Contact attacker from an off-network address via a protected/segregated machine. Clarify the initial demand in BTC and negotiate from there.

Proof of Life

Ensure attacker has ability to decrypt – require 2-3 files be decrypted prior to any payment. Verify it's your data and where it's valid/current.

Payment Transfer

Obtain BTC from a reliable source. Larger sums can take 48 hours to obtain and release.

Key Validation

Review the decryption key in a safe environment (sandbox) to ensure it does not contain a hidden malicious payload.

Restore

Run decryption script per attacker's instructions.

OCR Guidance on Ransomware

Breach Reporting Analysis

- Contain the impact and propagation of the ransomware
- Eradicate the ransomware and mitigate vulnerabilities that permitted the ransomware attack and propagation
- Recover from the ransomware attack by restoring data lost during the attack and return to “business as usual” operations
- Conduct post-incident activities

An Outside Counsel's Perspective

Breach Reporting Analysis

- Is there a use or disclosure that is impermissible under HIPAA and state law?
  - If malware did not exfiltrate data, is there really a "use" or "disclosure"?
- Was the PHI secured?
  - If you lose access to encrypted data, does that fall under safe harbor?

Breach Reporting Analysis

- Do any of the three statutory exceptions to breach apply?
  - In ransomware incident, is there a good faith belief that unauthorized person could not retain the PHI?

Breach Reporting Analysis

- Is there a low probability of compromise?
  - Is compromise limited to confidentiality, or does it include loss of integrity or availability?
    - On the one hand, focus of breach law is violation of Privacy Rule, not Security Rule. Privacy Rule is focused on confidentiality.
    - But OCR guidance is to consider integrity and availability.
  - If availability is relevant, how much of a delay constitutes a “compromise”?

Preparing for Investigations and Litigation

- Expect to receive an HHS Office for Civil Rights data request if reported to OCR.
  - Is Security Rule risk analysis and risk management current?
  - Are all relevant HIPAA policies and procedures in place and approved?
    - Do you have prior versions.
  - Were sanctions imposed and documented where appropriate?
  - Are changes to policies and procedures or additional training needed?

Preparing for Investigations and Litigation

- OCR preparation (cont'd)
  - Finalize security incident report and create non-privileged version.
  - Begin drafting narrative while events are fresh in your mind for future inclusion in data request response.
  - Begin gathering relevant documents in one place.

Questions?