

RANSOMWARE: SHOULD I NOTIFY LAW ENFORCEMENT?

Common Definitions



Ransom: "A consideration paid or demanded for the release of someone or something from captivity."

Extortion: "Obtaining money or property by threat or force."

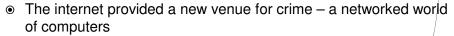
,

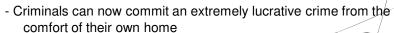
Everything Old is New Again

- Criminals engaged in these illegal activities long before the internet existed
 - Middle Ages knight warfare



- Pirates
- Salzburg-Bavaria 30 Years War
- Kidnapping









2

Cyber Definitions



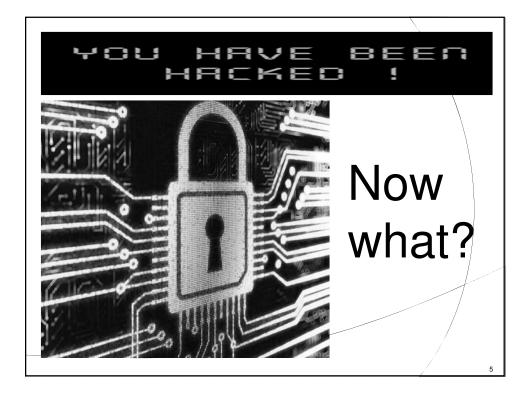
Ransomware: "A type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid."

www.trendmicro.com/vinfo/us/security/definition/Ransomware



Crypto-Ransomware: "More modern ransomware families which encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key." Id.

- Also referred to as Crypto-Extortion.



Imagine...



- ❖ No access to email
- ❖ No access to EHR
- Medical test results cannot be accessed or shared
- Have to resort to paper records
- Medical personnel have to talk in person
- Transfer of high-risk patients to other medical facilities
- ♦ \$3.6 million BitCoin ransom demanded

This is exactly what happened to Hollywood Presbyterian Medical Center in Los Angeles



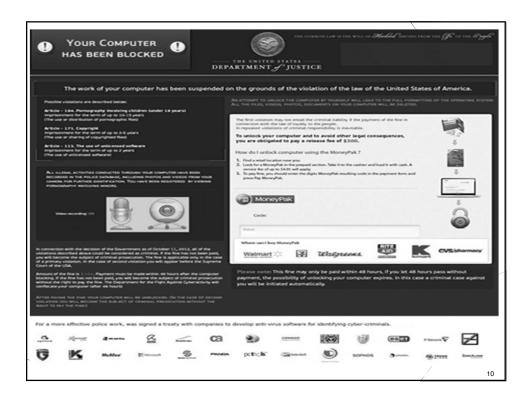
Loss per day on CT Scans alone: \$100,000

Ransom paid to decrypt files: \$ 17,000

The threat







The Risk



A recent U.S. Government interagency report indicates that, on average, there have been 4,000 daily ransomware attacks since early 2016.

This represents a 300% increase over the 1,000 daily ransomware attacks reported in 2015.

Source: How to Protect Your Networks from Ransomwate, US-Gevernment Interagency Technical Guidance Document filer/data_new01/Horizon/UserData/warrenr/My%20Documents/Healthcare/Ransomware/technical-document-ransomware-prevention-andresponse.odf

. .

The Cost

MONETARY

2015 - FBI's Internet Crime Complaint Center (IC3) received 2400 ransomware reports

Losses = \$24 million

Average Ransom demand: \$10,000

First Quarter 2016

Ransom Cost: \$209 million

FBI's forecast for 2016 losses = \$1 billion



OTHER COSTS

- > Downtime/loss of productivity
- > IT services review systems and data, remove malware, clean data
- > Addressing the breach of confidential information
- > Damage to reputation

Which law enforcement agency do you contact?



□ Local



□ State













□ International

Considerations



- ✓ Jurisdictional issues
- ✓ Computer crimes and forensics training
- ✓ Staffing
- ✓ Special Units
- ✓ Resources

15

State



- State laws vary
- Pennsylvania enacted Hacking and Computer Crimes legislation in February of 2003
- Felony Offenses
- PA State Police established a Computer Crimes Unit
- In 2002, PSP created Regional Computer Crime Task Forces

Federal



Hobbs Act, 18 U.S.C. 1951

interference with commerce by extortion

18 U.S.C. 875

interstate communication of threat to injure property of another

These laws were not seen as specifically covering computers

Commencing in 1996, Congress began to enact specific legislation to combat computer crime

17

Current Federal Laws

- Computer Fraud and Abuse Act (CFAA) 18 U.S.C. 1030
 - -Federal computers
 - -Bank computers
 - -Computers used in or affecting interstate and foreign commerce
 - -only "slight impact" on interstate commerce needed
 - -computer that accesses the internet
 - -victim and perp can be in same state
- Computers are the victims not a venue





- Identity Theft Enforcement and Restitution Act of 2008
- Economic Espionage Act 18 U.S.C. 1832 theft of trade secrets
- Money Laundering 18 U.S.C. 1956 and 1957
- Wire Fraud 18 U.S.C. 1343 yielded most computer crime convictions
- 18 U.S.C. 876 mailing threatening communications
- 18 U.S.C. 877 mailing threatening communications from foreign country
- 18 U.S.C. 880 receipt of the proceeds of extortion



FBI





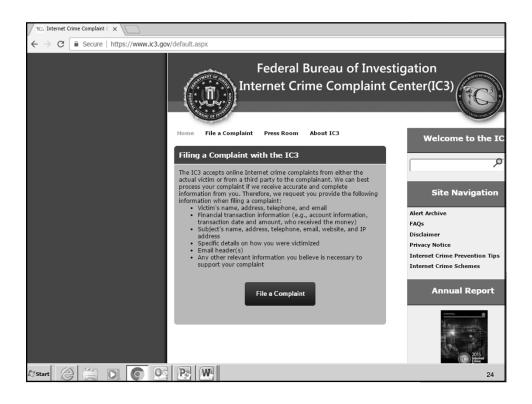
- FBI is the lead federal agency for investigating criminal cyberattacks
 - Cyber Division at HQ
 - Cyber Squads at HQ and 56 field offices
 - Cyber Action Teams –mobilize on moment's notice
 - 93 Computer Crimes Task Forces
 - Partnerships with other Federal agencies

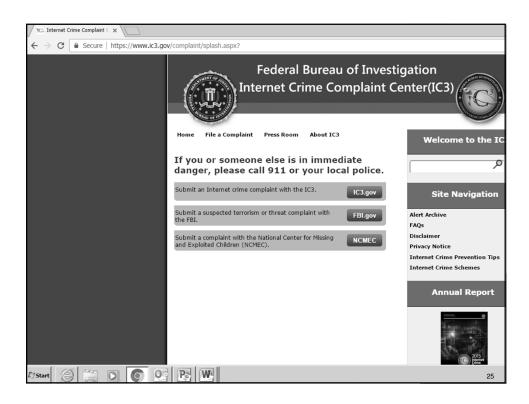
21

- Leads the National Cyber Investigative Joint Task Force (NCIJTF)
 - domestic coordination established 2008
- National Cyber Forensics and Training Alliance (NCFTA)
- Partners with private sector through InfraGard and Information Sharing and Analysis Centers (ISACs)

16 crucial infrastructure sectors Includes healthcare and public health







Q: What details will I be asked to include in my complaint?

- · Victim's name, address, telephone, email
- Financial transaction information
- Suspect's name, address, telephone, email, website, IP address
- Date and details on how you were victimized
- Initial entry vector or vulnerability if known
- · How detected
- · Specific assets impacted
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint





- Analysts review each report
- Refer to appropriate law enforcement agency for investigation and prosecution
- IC3 database shared through Law Enforcement Enterprise Portal (LEEP) – compare and compile
- Report cannot be withdrawn once submitted

27

Secret Service



- Electronic Crimes Task Force
 - national network to prevent, detect and investigate cybercrimes (39 task forces)
- Electronic Crimes Special Agent Program
- Computer Emergency Response Team
- Collaboration with international law enforcement agencies
- National Computer Forensics Institute training for state and local LEO

https://www.secretservice.gov/investigation/#field

- Official position: FBI does not support paying ransom
 - Not guaranteed that data will be released
 - Emboldens the cybercriminals



- Encourages others to engage in cyberextortion
- Helps to fund other illegal activities

https://www.fbi.gov/investigate/cyber

- But, in 2015 a Special Agent speaking at the 2015 Cyber Security Summit said: "pay up"
 - Why? "The ransomware is that good."

http://www.businessinsider.com/fbi-recommends-paying-ransom-for-infected-computer-2015-10

00

International

- Budapest Convention on Cybercrime November 2001
 - -first international treaty on computer crimes
 - -foundation for global law enforcement of cyberspace
- Main objective: Pursue common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation
 - -24/7 access and response -exchange of information -mutual assistance
- Russia has not signed or ratified cites violations of international law and sovereignty claims
- US ratified 2006

Future



- The growth of the IoT has exponentially increased the range and number of devices which can be attacked
- Medical devices
 - -pacemakers
 - -defibrillators
 - -insulin pumps



21

Why Report to Law Enforcement?

- Access to tools and contacts not available to private citizens
- Location of the stolen data
- Apprehension of the perpetrator
- Creation of a more safe and secure cyberspace
- Compilation of data and trends
- Improvement in future responses
- Prevention of future losses



So, where does that leave us? Be vigilant

- Prevention
- > up-to-date antivirus and firewalls
- > enable pop-up blockers
- > always backup data
- > be skeptical
- > read FBI and industry alerts
- > educate employees
- > risk analysis
- Business continuity plan



00

Reporting helps law enforcement make cyberspace safer for everyone

References

 $\frac{https://www.dhs.gov/sites/default/files/publications/USSS\%20Electronic\%20Crimes\%20Task}{\%20Force.pdf}$

 $\underline{http://www.riskmanagementmonitor.com/tag/ransomware/}$

http://www.securityweek.com/ransomware-four-ways-assess-growing-threat-business-risk

https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

https://www.justice.gov/criminal-ccips/file/872771/download

http://www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware

 $\underline{https://arstechnica.com/security/2015/06/fbi-says-crypto-ransomware-has-raked-in-18-\underline{million-for-cybercriminals/}}$

 $\underline{\text{http://tech.firstpost.com/news-analysis/symantec-classifies-ransomware-as-the-most-dangerous-cyber-threat-336688.html}$

https://www.trendmicro.com/vinfo/us/security/definition/Ransomware

 $\underline{\text{https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561}}$

 $\underline{\text{https://www.fbi.gov/file-repository/law-enforcement-cyber-incident-reporting.pdf/view}}$

https://www.justice.gov/usao/priority-areas/cyber-crime