Ransomware
Destructive Attack

Jay Spreitzer, Vice President, Cyber Threat Management
Wells Fargo Bank
Has over 18 years information security experience. Over the last 10 years as a senior member of a cyber intelligence team at Wells Fargo. Prior to joining Wells Fargo Jay retired from the US Army, after 23 years of service working in various technology and information security roles. He holds a Masters in Information Assurance and Security as well as multiple computer security certifications.
What is ransomware?

Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction.

Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying.
What is ransomware?

Ransomware wreaking havoc in American and Canadian hospitals
Tech & Science March 23, 2016

Spike in ransomware spam prompts warnings
Technology, March 10, 2015

Ransomware alert issued by US and Canada following recent attacks
April 4, 2016,

Big paydays force hospitals to prepare for ransomware attacks
Tech, April 23, 2016
The first known ransomwares and its evolution

- Contained a warning message in the letter regarding licensing fee and penalty.
- Users were supposed to send a license fee to a PO box in Panama for "PC Cyborg Corporation."
The first known ransomwares and its evolution

- **Gpcoder was ransomware discovered in 2005**
  - 2005 encoded 15 different file types
  - 2012 encoded 41 different file types
  - 2015 encoded 228 different file types

- **Encryption 1024-bit to 4096-bit**

- It creates the file ATTENTION!!!.txt in every folder in which it encoded a file. The textfile contains the following:

  Hello, your files are encrypted with RSA-4096 algorithm http://[REMOVED]).
  
  You will need at least few years to decrypt these files without our software.
  
  All your private information for last 3 months were collected and sent to us.
  
  To decrypt your files you need to buy our software. The price is $300.
  
  To buy our software please contact us at: [MAIL ADDRESS] and provide us your personal code [PERSONAL CODE].
  
  After successful purchase we will send your decrypting tool, and your private information will be deleted from our system.
  
  If you will not contact us until 07/15/2007 your private information will be shared and you will lost all your data.

Glamorous team
Fake Anti-Virus and Scareware
1. Arrives at users computer.

2. Ransomware - Locks the screen or Crypto-ransomware finds and encrypts certain files.

3. Displays the ransom note on screen.

How file encryption works

How the ransom is paid
Malware Family Variants Timeline

1989:
- AIDS Diskette

2005:
- Gpcoder

2012:
- Reveton

2013:
- Urasy
- Kovter
- Nymaim
- Cryptowall
- Browlock

2014:
- Slocker
- CTB-Locker/Citron
- Synolocker
- Onion
- TorrentLocker
- Zerolocker
- Coinvault
- Linkup
- VirLock

2015:
- TeslaCrypt
- BandarChor
- Cryptvault
- Tox
- Troldesh
- Encryptor RaaS
- CryptoApp
- LockDroid
- LowLevel404
- CryInfinite
- Radamant
- Unix.Ransomcrypt

2016:
- Locky
- Umbrecrypt
- Hydracrypt
- Vipasana
- Hi Buddy
- Job Cryptor
- PayCrypt

- ValutCrypt
- XRTN
- Cryptolocker2015
- Simplocker
- Pacman
- Pclock
- Threat Finder
- Hidden Tear
- ORX-Locker
- Dumb
- Mabouia OSX POC
- Power Worm
- DMA-Locker
- Gornasom
- Chimera-Locker1

- KeRanger
- 73v3n
- CryptoJacker
- Nanolocker
- Lechiffre
- Magic
- Ginx
ATTENTION!

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Codes, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 5, Section 8, Clause 8, also known as the Copyright of the Criminal Code of the United States of America.

Article 5, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (CNN Porno/DeTouch and etc). Thus violating Article 323 of the Criminal Code of the United States of America. Article 323 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Federal charges have been initiated from your PC, without your knowledge or consent, your PC may be seized by authorities, thus you are violating the law On Negligent Use of a Personal Computer. Article 323 of the Criminal Code provides for a fine of up to $100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of the United States of America on May 28, 2011, this law infringement of 323 is not repeated – first time – may be considered as conditional in case you pay the fine to the State.

Fine may only be paid within 72 hours after the infringement. As soon as 72 hours elapse, the possibility to pay the fine expires, and a criminal case is initiated against you automatically within the next 72 hours.

To unlock the computer, you must pay the fine through MoneyPak of 100s.

How do I unlock computer using the MoneyPak?

1. Find a retail location near you.
2. Line up a MoneyPak in the keypad section. Take it to the cashier and load it with cash. A service fee of up to $4.95 will apply.
3. To pay fine, you should enter the digits MoneyPak resulting code in the payment form and press Pay MoneyPak. When you pay the fine, your PC will get unlocked in 1 to 48 hours after the money is put into the State’s account.

In case of an error occurs, you’ll have to send the code by email food@fbi.gov (Do not forget to specify IP address.)

Reveton “Police” Ransomware
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 $200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through fine@fbi.gov

To pay the fine, you should enter the digits resulting code, which is located on the back of your credit card in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

If an error occurs, send the codes to address fine@fbi.gov.
The marked shift from scareware to crypto-ransomware

CryptoLocker Ransomware  
(2013)  

You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

3. Enter your personal decryption code there:

If you already purchased your key, please enter it below.

Key:

Petya Ransomware  
(2016)
File encryption and deletion ransomware

Jigsaw Ransomware
(2016)
Ransomware-as-a-Service (RaaS)
  - Tox and Encryptor RaaS
Targeting – Targeted vs Spammed
JavaScript Ransomware
Delayed Execution
Decrypers
Spike in Media Attention
Hospitals/targeting
New Variant ~1-2 weeks
Targeting enterprises using vulnerably third party applications like JBoss
New Threat actors with better/newer skills and specializations
Current State: 2016 – Present & Impact

- **Locky**
  - Utilized malicious Word macros
  - Dridex distribution

- **Petya**
  - Overwrites master boot record (MBR)

- **KeRanger**
  - Second known OS X ransomware variant

- **SamSam/Samas/Maktub**
  - Attackers used server side vulnerabilities (Jboss) to deliver the ransomware
  - Targeted attacks
  - Not a worm, but shares characteristics...

- **JIGSAW**
  - File Deletion
Mitigation/Preventions

- Enable the ‘Show file extensions’ option in the Windows settings on your computer.
- Ensure patches are applied for all vulnerabilities
- Ensure anti-virus/endpoint protection up-to-date
- Ensure end-users are educated to follow security best practices
  - Avoid suspicious email curiosity
  - Do not enable Macros on Office documents
- Ensure regular backups are made to protect data
- Exercise privilege restriction, limit admin access, network segmentation, DMZ hardening, etc.
- Limited open shares
- No more ransomware: [https://www.nomoreransom.org/](https://www.nomoreransom.org/)
Where could ransomware go from here?

- “Cryptoworms”
- Cloud-specific
- (Even more) Targeted attacks
- (Better) Mobile variants
- Internet of Things (IoT)
- Greater evasion and detection avoidance capabilities
Sources and additional reading

- http://blog.talosintel.com/2016/04/ransomware.html#toc
- https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure
- https://www.comparitech.com/blog/information-security/the-history-of-ransomware/
- http://blog.talosintel.com/2016/03/samsam-ransomware.html
- http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0WU1GB
Open discussion and questions