CS 5472 - Advanced Topics in Computer Security

Topic 8: Ransomware (1)

Spring 2019 Semester
Instructor: Bo Chen
bchen@mtu.edu
https://cs.mtu.edu/~bchen
https://snp.cs.mtu.edu

Ransomware Attacks Keep Growing …

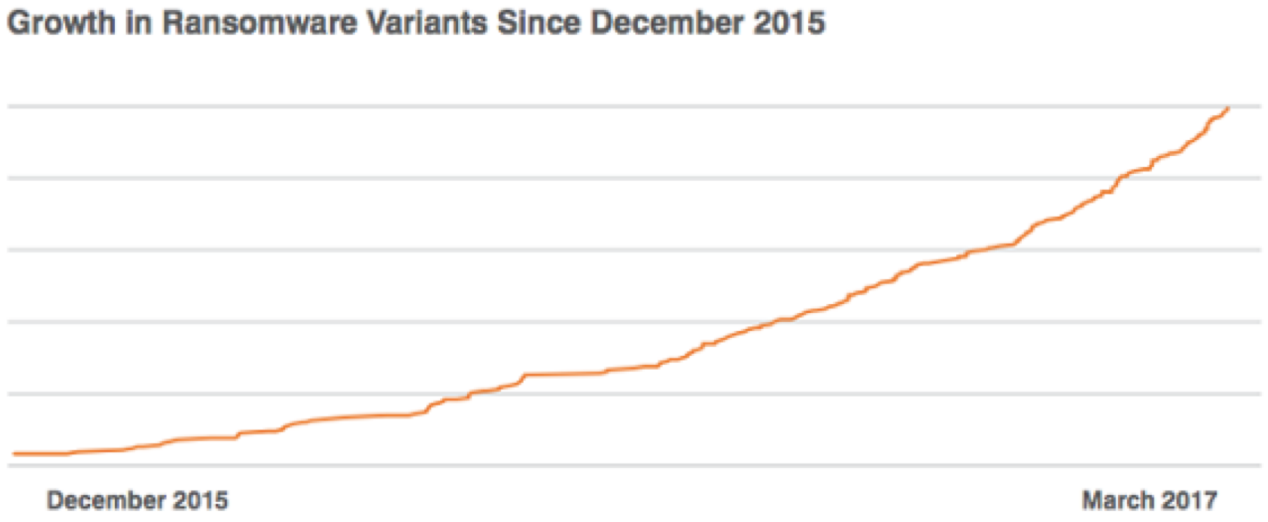


Figure 6: Indexed growth in total number of observed ransomware strains, December 2015-March 2017

Source: Proofpoint Q1 2017 Quarterly Threat Report

- A piece of special malware that infects a computer and restricts access to the computer and/or its files
- Ask for a ransom to be paid in order for the restriction to be removed

Ransomware Propagation

Cast Study: WannaCry


https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/

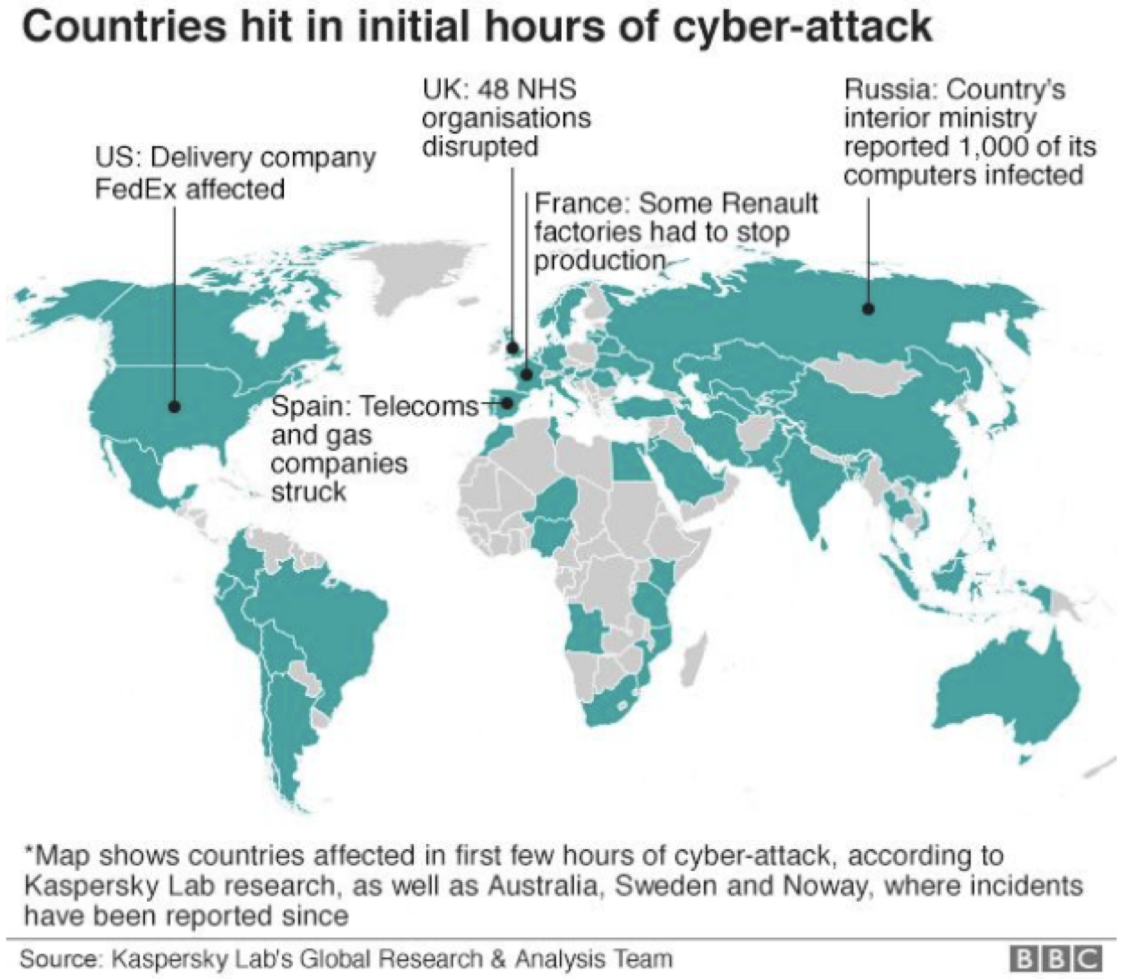
DATA CENTER SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH

Security

74 countries hit by NSA-powered WannaCrypt ransomware backdoor: Emergency fixes emitted by Microsoft for WinXP+

All you need to know – from ports to samples

By Iain Thomson in San Francisco 13 May 2017 at 00:16 413 SHARE ▼



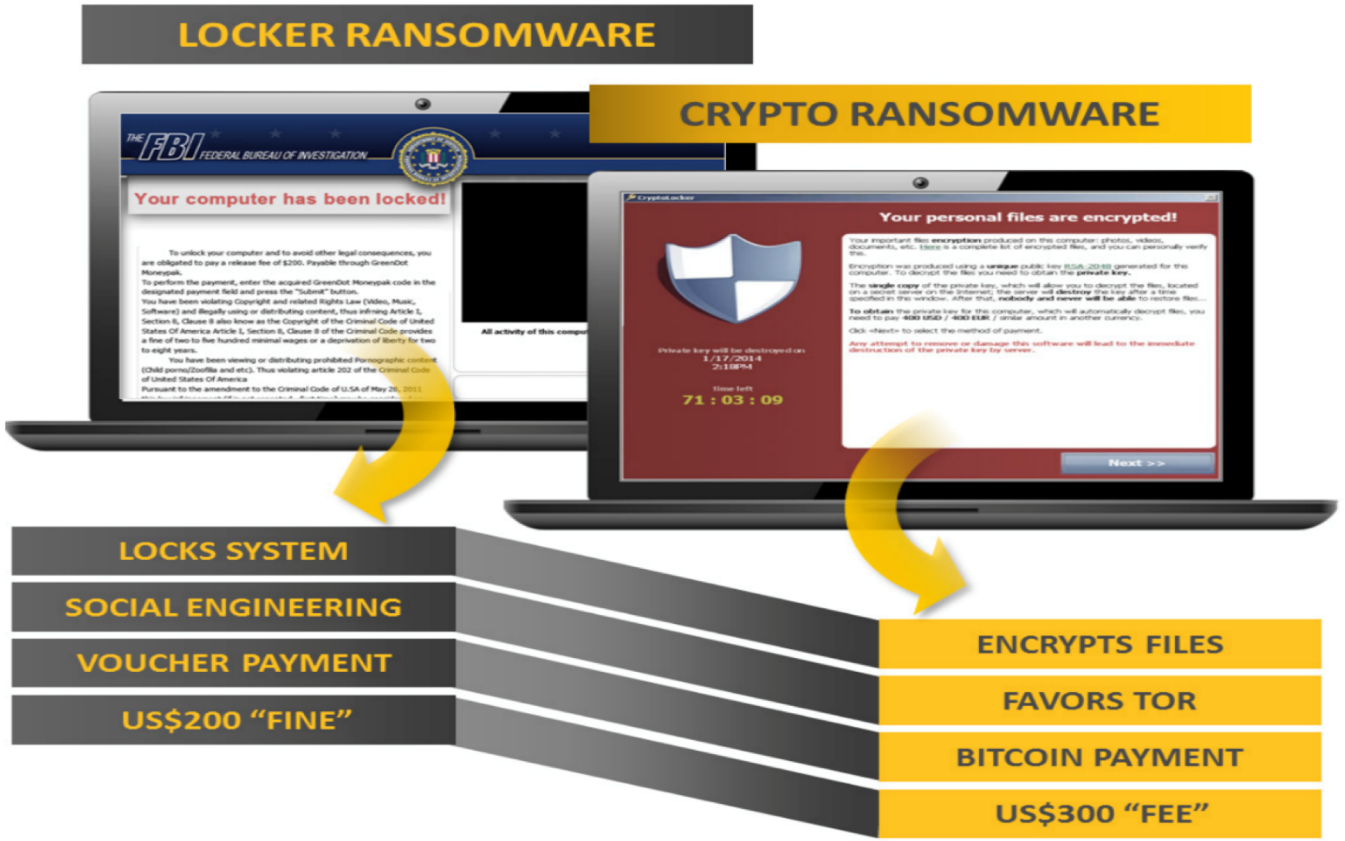
Propagated through EternalBlue, an exploit developed by the US National Security Agency (NSA) for older Windows systems

- Vulnerabilities in Windows Server Message Block (SMB) protocol
- NSA discovered the vulnerability, but used it to create an exploit for its own offensive work, rather than report it to Microsoft

Within a day the code was reported to have infected more than 230,000 computers in over 150 countries

Types of Ransomware

- Locker ransomware
- Crypto ransomware



Locker Ransomware

- Lock the victim system

- Easy to be combat, since only the system is locked, but data remain intact

How to Combat Locker Ransomware?

- Observation: only the system is locked by the ransomware, but the data are stored intact

- Unplug the storage medium(e.g., hard drives, SSD drives, SD cards), plug the storage medium to a new computing device, and copy out the data

- Plug the storage device back to the device which has been locked, and re-install/initialize the system, then copy the data back

Crypto Ransomware

- The victim data are encrypted, and cannot be recovered if not able to obtain the key for decryption

- How does it work
  - Symmetric encryption: the encryption and decryption are using the same key
    - Good for ransomware: fast encryption
    - Bad for ransomware: the encryption key in plaintext needs to be distributed during encryption process, and can be easily leaked
  - Asymmetric encryption: use public key to encrypt, but private key to decrypt
    - Good for ransomware: only need to distribute the public key during encryption process
    - Bad for ransomware: the asymmetric encryption is expensive, and can be easily detected
  - Others

How to Combat Crypto Ransomware

- Detection: detect the ransomware once it starts to work
  - Detection needs to be fast enough so that ransomware can be blocked before it encrypts more victim data
  - Rationale: ransomware has some sort of working patterns

- Recovery: if all the data encrypted by ransomware can guarantee to be recovered, ransomware would not be a problem
  - Obtaining the key: pay the ransom; extract the key in the victim system
  - Backup
    - Off-device backup: e.g., iCloud
    - In-device backup: e.g., utilizing the out-of-place update property of flash memory, such that old data can be temporarily preserved

- Detection + recovery

A Little More on Ransomware Detection

- Crypto ransomware may be detected since it behaves differently from normal software and other types of malware
- Crypto ransomware usually encrypts a large amount of data in a short time, and over-writes the old data
  - A large number of read access
  - Expensive computation is required for a large amount of encryptions
  - A large number of writes/over-writes in a short time

The most challenging issue is how to detect the crypto ransomware fastly, since the detection is time-sensitive

Paper Presentation

- UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

- Presented by Jamie Berger