DATA AND NETWORK SECURITY

Case Study V: Ransomware

Overview

- Classification: Malware/Attack
- Acquired via
  - ‘Trojan’
  - phishing attacks
  - Drive-by downloads
- Numerous tactics
  - Encrypt files
  - Lock system/application
  - Exfiltrate Data - Threaten to release
- Demands payment (bitcoin) to
  - Unlock system
  - receive decryption key
  - Destroy exfiltrated data without release

Variants of Ransomware

- Encrypting Ransomware
  - Encrypts important files
  - Encrypts master boot record or file table
- Non-encrypting Ransomware
  - Locks out or partially locks out system access
  - Various means:
    - Display pornographic images and block screen from accepting mouse clicks
    - Dialog box asking to re-activate Windows due to ‘fraud’

Variants of Ransomware

- Leakware
  - Exfiltrates sensitive data then threatens release unless ransom is paid
- Mobile Ransomware
  - Usually Android based
    - Via an APK file
    - Android allows application installs from 3rd party sites

Infection Techniques

- Trojan ← Most common
  - Emails with malicious payload attachments
  - Trick user into executing attachment [Cool game!]
- OS facilities
  - RDP (Remote Desktop Protocol) brute-force attack [weak passwords]
- Subverted Ads
  - Fake advertisements divert user to roque web server that downloads malware payload

Recent Attacks

- **TeslaCrypt** – [2016] – Mainly targeted Gamer's files
- **SimpleLocker** – [2015/2016] – Targeted Android devices
- **WannaCry** – [mid 2017] – First ransomware to use leaked NSA hacking tools
- **SamSam** – [2015-forward] – Attackers 'pre-selected' targets (City of Atlanta, Colorado DOT, Healthcare orgs)
- **CryptoLocker** – [2013] – Brought in age of ransomware
- **Ryuk** – [2018, 2019] – Targeted attack. Most recently, city of New Orleans

Ransomware – Early attempts

- AIDS Trojan [1989]
  - Distributed on 5 ¼ inch floppies
  - Survey program to estimate likeliness of contracting AIDS
  - Ransomware displayed message demanding $189
  - Author was caught stopping the distribution
- GPCode [2004]
  - Targeted Windows
  - Encrypted files – Users could purchase a ‘decryption’ program to unlock files
  - GPCode used ‘custom’ encryption that was easily broken
- Archievus [2006]
  - Encrypted files in My Documents using RSA [660 bit key]
  - Used same key for all infections so, once found and published, demands were useless

Ransomware – 2006-2013

- Trojan.Ransom.A – [2006]
  - Locking Trojan placed in Windows startup
  - Ransom note displayed covering entire screen
  - Demanded $10.99 payment via Western Union – CIDN on receipt was entered to remove ransom note
- Reveton – [2012]
  - Pretends to be a message from FBI: Machine locked down due to copyright violations, distribution of pornographic content, etc.
  - Demanded Fine be paid to release machine
- CryptoLocker – [2013]
  - Spread through compromised websites & malicious email attachments
  - AES-256 encryption
  - First to use Bitcoin for ransom
  - Used Zeus botnet for Command and Control + Distribution of decryption keys
  - Ended when Zeus botnet was dismantled in 2014

Ransomware – 2014

- CryptoWall
  - Utilized 2048 bit RSA encryption
  - Left decryption key in plain text on victim PC
  - Hard to kill – Copied into registry keys and startup folder
- CTB-Locker
  - Deleted Windows ‘Shadow’ copies used to restore files/data
- Sypeng
  - First ransomware against mobile devices
  - Targeted Android
  - Fake messages about Adobe Flash update needed
  - Locked phone or tablet. Demanded $200 in MoneyPaks

Ransomware – 2015

- Encoder – (1st Linux)
  - 1st Ransomware targeting Linux
  - Targeted web hosting platforms (Magento, cPanel)
  - Locked web directories and encrypted contents
- Chimera
  - Encrypted files and threatened to release them online
- Raas – Ransomware as a Service
  - Ransomware ‘kits’ developed facilitating distribution of ransomware
  - Cost to distribute initially $3000.
  - 2016 – New kits, competition increased lowering price

Ransomware – 2016

- KeRanger
  - First to target Macs
  - Transmitted via fake Transmission BitTorrent Client
- Ransom32
  - 1st Javascript ransomware
  - Could infect multiple platforms
- Jigsaw
  - Threatened to delete 1 file per hour until ransom paid
  - Threatened to delete 1000 files if machine was rebooted
  - $150 ransom

Ransomware – 2016 (cont)

- SamSam
  - 2048 bit RSA encryption
  - Demanded .8 bitcoin per PC or 4.5 bitcoin for entire site decryption
  - Increasing infections between 2015 and 2018
  - Hit:
    - Healthcare (Hospital in Indiana which paid ransom)
    - Colorado
    - City of Atlanta
- Petya
  - Propagation – Used cloud file sharing service (dropbox)
  - Locked machinery by encrypting the Master Boot Record
- TeslaCrypt
  - Hit gamers
  - Demanded $500 in bitcoin to decrypt critical files

Ransomware – 2017-Present

- WannaCry – [May 2017]
  - Based on ‘EternalBlue’ malware developed by US NSA
  - EternalBlue was stolen and leaked by The Shadow Brokers
  - Attacked MS Windows OS
  - Hit: Telefonica, British National Health Service, FedEx, Deutsche Bahn, Honda and Renault
- Ryuk – [Nov 2018]
  - Code derived from/related to Hermes
  - Group in N. Korea is thought to have developed this
  - Responsible for New Orleans ‘state of emergency’ on Fri, 13-Dec-2019
    - Recoverable
    - 20 City Systems
    - 400 Servers
    - 7000 Terrabytes of data

Ransomware - Trends

- Recent decline in number of attacks
- Amount of ransom collected has not dropped
- Newer attacks appear very targeted
  - Large organizations
  - Ability to pay

Sources

- https://www.kaspersky.com/resource-center/threats/ransomware-examples
- https://www.csoonline.com/article/3212260/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
- https://en.wikipedia.org/wiki/Ransomware
- https://coingeek.com/ransomware-attack-forces-new-orleans-to-declare-state-of-emergency/
- https://www.smartcitiesworld.net/news/news/new-orleans-cyber-attack-triggered-by-phishing-email-4884
- https://www.tcdi.com/ransomware-timeline/
- https://www.govtech.com/security/Ransomware-in-New-Orleans-Attack-Is-Likely-Organized-Crime.html