Ransomware
Speaker

- Kin (Sam) Wong, CEHv9
- Worked in Public and Private Sectors
- Ethical Hacking w/ AI
Learn

- Ransomware
  - Who
  - What
  - Where
  - When
  - Why
  - How
Ransomware (NOUN)

- “A type of malicious software designed to block access to a computer system until a sum of money is paid.”

  -  https://en.oxforddictionaries.com/definition/ransomware
Ransomware - When

1989 - AIDS

2005 - Fake Antivirus Shutdown

1996 - Ransomware Theory Developed

2005 - GPcode - Symmetric

2006 - Redplus (China)

2009 - Bitcoin Invented

2013 - CryptoLocker - Asymmetric

2017 - WannaCry
Ransomware - Who

VICTIMS
- Home
- Business
- Medical
- .Gov

 HACKER
- Hacker Wannabe


Ransomware - What

Lock System

Pay-Per-view (Public Key)

Exploit System (Max $$)

Reconnaissance

Command and Control

Weaponization

Design Malware

Send to Victims

Installation

Exploitation

Delivery

Exploitation
Ransomware Algorithm

- **Symmetric Key**
  - One-time pad (Encrypt Data)

- **Asymmetric Keys**
  - Public Key (Encrypt One-time pads)
  - Private Key (Decrypt Public Key List)
Ransomware Source Code

GitHub - mauri870/ransomware: A POC Windows crypto-ransomware...
https://github.com/mauri870/ransomware
A POC Windows crypto-ransomware (Academic). Contribute to ransomware development by creating an account on GitHub.

theZoo/malwares/Binaries/Ransomware.WannaCry at master · ytsf ...
https://github.com/ytsf/theZoo/tree/master/malwares/.../Ransomware.WannaCry
theZoo - A repository of LIVE malwares for your own joy and pleasure.

GitHub - goliate/hidden-tear: ransomware open-sources
https://github.com/goliate/hidden-tear
It's a ransomware-like file crypter sample which can be modified for specific purposes. ... hidden tear may be used only for Educational Purposes. ... You could go to jail on obstruction of justice charges just for running hidden tear, even though you are innocent.
Ransomware - Where

Exploit

Phishing E-MAIL

Download
Phishing Email

Google Drive

I just uploaded this document for you using Google Docs.

VIEW HERE
Thank you.

Notice: This e-mail message and any attachment to this email message contain confidential and proprietary information that may be legally privileged. If you are not the intended recipient, you must not review, retransmit, convert to hard copy, copy, and use or disseminate this e-mail or any attachments to it. If you have received this email in error, please immediately notify us by return e-mail or by telephone at

PLZ Sign in?

Got U, $%&#!
Exploit

• Exploit
  – Hack the Web Browser (Entry Point)
    • Buffer/Heap Overflow
    • Web Application Injection

• Privilege Escalation
  – Weak File Privilege
  – Entered → Run Exploit → Get Root → Domain Admin
Advanced Exploit

• **Jackpot**
  - Obtains **Domain Admin** privilege then infects all enterprise computers.
  - **Saudi Arabia State Oil Company (Cover-Up)**
    - Malfunction Oil Grids = Oil Price ($>80)
    - Record Deleted = Free Oil (Millions $$$)
Step 1

https://support.microsoft.com says:

** YOUR COMPUTER HAS BEEN BLOCKED **

Error # 268D3-XCD0037

Please call us immediately at: 1-844-313-7003

Do not ignore this critical alert.

If you close this page, your computer access will be disabled to prevent further damage to our network.

Your computer has alerted us that it has been infected with a virus and spyware. YOUR COMPUTER HAS BEEN LOCKED!!...

Virus Alert!

> Zeus Virus has been detected into your computer
> Trojan.FakeAV-Download
> Spyware.Banker.Id

You must contact us immediately so that our engineers can walk you through the removal process over the phone. Please call us within the next 5 minutes to prevent your computer from being disabled.

Toll Free: 1-844-313-7003

---

Step 2

![System Doctor 2014]

**Threats found when scanning.**

- Viruses found: 14 Threats

**To keep your computer safe, repair is required.**

- Repair all
- Continue

---

Step 3

![Payment for private key]

**Payment for private key**

- Choose a current payment method:
  - Bitcoin (most cheap option)

Bitcoin is a cryptocurrency where the creation and transfer of bitcoins is based on an open-source cryptographic protocol that is independent of any central authority.

Bitcoin can be transferred through e-computer or smartphone without an intermediate financial institution.

You have to send below-specified amount to Bitcoin address:

**Enter the transaction ID and press «Pay»**

Click back to continue.

---
Ransomware - Why
Ransomware - How

- Bitcoin(Entry)  → Shapshift.IO(Money Laundering)*7X(TOR)  → Bitcoin(Exit)
- Bitcoin(Ransom)  → Ethereum(Silkroad)  → Litecoin(Blackdeath)  → Monero(Childporn)  → Bitcoin(Clean Money???)  → Cash (Exit)
- Math
  - Fee (5%)
  - 7*5% = 35% commission

LESS IS MORE??
FACE ↔ FACE
Easy Ransomware Prevention

• **Antivirus (Best Practice?)**
  - Drive-by Download
  - Embedded In Pirate Software

• **Patch Management/Exploit Mitigation**
  - Web Browser Exploit
  - System Exploit (Priv.Esc.)

• **Training**
  - Phishing Email / Weak Password
Bypass AV

“Our AV does not cover all assembly types”
- AV Sales Guy

• Compiler (Maybe)
  - VS .NET(C#), VSCC and GCC(C and C++)

• Interpreter (Maybe)
  - Powershell, Ruby, Python, Perl, Java, NodeJS

• More Tricks
  - 7-ZIP(SFX) + UPX (Packer)
How to Configure Applocker in Windows Server 2012 R2
https://youtu.be/Z2-Sjw9UYdU
Backup

Recovery

OFFSITE

CLOUD

INTERNAL
Bye Bye

- **Questions/Comments**
- **Contact**
  - Email: Kin.Wong@jjay.cuny.edu
  - Text: 646.461.0067