FOX IT

Ransomware detection

with Bro

Mike Stokkel

13 Sept 2016

Introduction

- Who am I?
  - Mike Stokkel
  - Security Analyst @ Fox-IT
  - Internship at Fox-IT
  - Bachelor July 2016

Agenda

- What am I going to talk about?
  - Fox-IT
  - Ransomware
  - Bro Policy
  - Results
  - Demo

FOX IT

Fox-IT

Company

- Located: Delft, The Netherlands
- IT security
  - Managed Security Services
  - Auditing
  - Cryptographic solutions

Security Operation Center

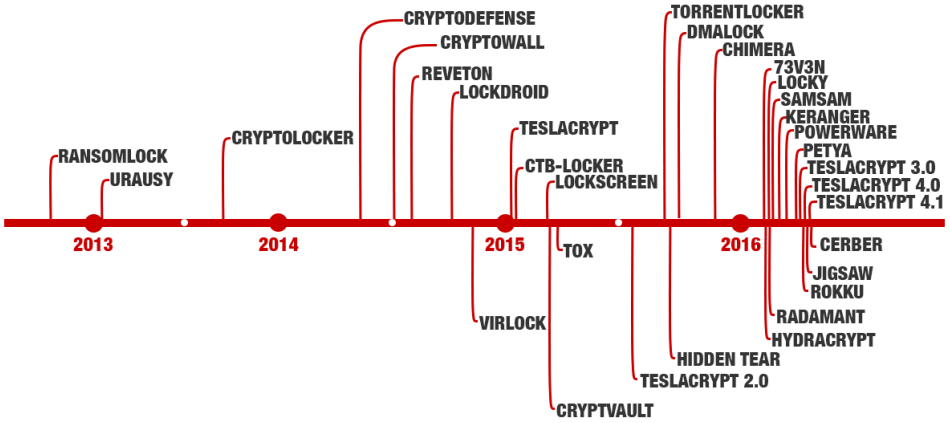
- Snort-based detection
- Bro

FOX IT

Ransomware

Explanation

- Malware
  - Encryption
  - Payment
  - Decryption
- Rising concern

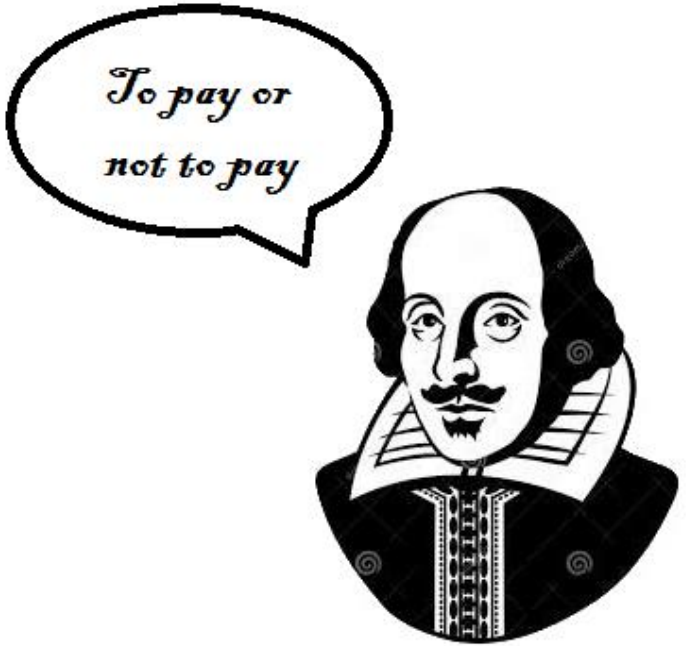


Encryption

- Process
  - Master key (public and private key)
  - Generating a key for the victim
  - Encrypting the victim’s key

Impact

- Personal Computer
  - Local files
- Company
  - Network Share
- To pay or not to pay?



Spreading Methods

- Exploit Kits
  - Browser vulnerabilities
- E-mail
  - Malicious document
  - Macros

Exploit Kit

- Version check
- IP check
- Download ransomware payload
- Run payload

Malicious document

- Macro
- VBS script
- Download & execute payload

Remote desktop programs

- TeamViewer hack
- RDP brute force

Detection Methods

- IDS
  - Snort rules
- Problem

FOX IT

Bro Policy

Approach

- Ransomware behavior
  - SMB
- Possible solutions
  - File extension listing
  - Threshold SMB commands
  - Command-and-Control communication

Entropy

- Randomness of data

- 0 – 8 bits per character

What about ….

- Compressed files
- Images
- PDF

- Mime/Media type

Functions

- SMB parser
  - Events
    - File over new connection
    - Chunk event
- SumStat
  - Threshold
- Notice.log

File over new connection

- Check for SMB traffic
- Check for certain filenames
- Check for Mime type
- Check for SMB action
- Check if SMB action equals Write
- Add File analyzer

Chunk event

- Check if the offset equals 0
- Calculate entropy of data collected from SMB write command
- Use SumStat to add +1 for the threshold
- Write to log file
- Write a Notice.log

FOX IT

Results

YOUR COMPUTER HAS BEEN LOCKED!

Your data has been encrypted by your webbrowser. Due to improving the security measures for the user, your webbrowser made sure that your browser data is being stored in a encrypted cache.

The following violations were detected:
Your IP address was used to visit websites, to improve the speed of your webbrowing a
cache was created. If an unencrypted cache is being used, third party programs may have the ability to use this information for bad intentions or slowing webbrowsing.

To unlock the data you are obliged to pay a fine of $0.

You have ~ hours to pay the fine, otherwise we'll keep encrypting your caches.

You must pay the fine through caching@google.com or caching@firefox.com
To pay the fine, you need purchase bitcoins and deposit 0 bitcoin to:

1e2n3c4r5y6p7t8e9d0c9a8c7h6e!

Live Testing

- Two new kinds of Ransomware
  - Google Chrome & Mozilla Firefox
    - Encrypted cache

- Encryption tools
  - TrueCrypt
  - VeraCrypt

- Documents
  - Printing
  - Creating

FOX IT

Demo

Samples

- Locky/Zepto
- Cryptowall
- CTBLocker
- Jigsaw (and all families)
- Mobef
- Shade
- Maktub
- Cerber/Alpha
- Teslacrypt
- Rokku
- Crysis
- Cerber
- Bandarchor

Demo

FOX IT

Thank you for having me!