IN YOUR PC & IN YOUR POCKET
DESKTOP AND MOBILE RANSOMWARE THREAT LANDSCAPE

Andrea Continella, Federico Maggi(*)
Politecnico di Milano

7/21/2016

(*) this work has been done while @ Politecnico di Milano. I recently joined Trend Micro.
2016 the "year of extortion"

Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating
Encryption Mechanism

1. Randomly generated symmetric key (AES)

2. Public key (RSA)
   - Downloaded from C&C, embedded in the binary, or generated client-side

3. File
TeslaCrypt

- Continuous updates and increased sophistication
  - AES-256. Key stored in the victim machine (v.1, 2015)
  - AES-256 + EC. Weak EC key, recoverable by factorization (v.2, 2015)
  - AES-256 + ECDH + SHA (v.3 & v.4, 2016)
- Delete Shadow copies
  - `vssadmin.exe delete shadows /all /quiet`
- Target gamers!

All your important files are encrypted.
TeslaCrypt

Project closed
master key for decrypt
440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
wait for other people make universal decrypt software
we are sorry!

Master decryption key released for #TeslaCrypt
#ransomware via @threatpost kas.pr/1imU
Locky

- AES-128 + RSA-2048
- Contact the C&C server to get the Public Key
- Delete Shadow Copies
- Encrypt data on unmapped network shares
  - enumerate network SMB shares

We present a special software - Locky Decrypter - which allows to decrypt and return control to all your encrypted files.

How to buy Locky decrypter?

1. You can make a payment with BitCoins, there are many methods to get them.

2. You should register BitCoin wallet (simplest online wallet) OR some other methods of

3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler and
RAA & PowerWare

- **RAA JavaScript**
  - encrypt files using code from CryptoJS (AES-256)
  - Windows, by default, executes JS files through Windows Script Host or wscript.exe.
  - Delete Shadow copies

- **PowerWare / PoshCoder**
  - Powershell script
  - AES + RSA 4096
  - Target mainly via Microsoft Word
#ransomware sample asking to reinstall because it failed to encrypt files. lol

Your personal files are encrypted!

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced on this PC, and this computer is the only copy of the encrypted data.

The only copy of the private key is located on a secret USB stick.

Once this has been done, you will have no way to retrieve your encrypted files.

In order to decrypt your files, visit the following URL:

https://34r6hq26q2h4jkwzr2t.bak

Show encrypted files
Check Payment
Enter Decrypt Key

Unable to find locale data files. Please reinstall.
How to Deal With Ransomware?

- Good ol' AVs?
  - Unfortunately it's still a reactive approach
  - Signatures must be kept up to date

- Why don’t we monitor Crypto API calls?
  - Malware implement own crypto functions or use libraries
    - BART doesn't even use crypto (ZIP + password)!

- We envision an OS able to deal with ransomware
  - Better: the OS should be proactive, not just detect
  - Look at the file system’s activity!

What's Grilling? FS Activity Monitor

- Develop a Windows Kernel module to monitor and log the file system activity
  - Windows Minifilter Driver
  - Log IRPs (I/O Request Packets)
- Run ransomware samples and collect data about the activity of the file system during their execution
- Distribute the module to 10 clean machines
  - Collect data about the activity of the file system during “normal” clean executions
    - 2 months worth of data
    - ~1.5 billion IRPs
    - 1,963 distinct applications
Filter Manager APIs

```c
CONST FLT_OPERATION_REGISTRATION Callbacks[] = {
    { IRP_MJ_CREATE,
        0,
        PreCreateOperationCallback,
        PostCreateOperationCallback },

    { IRP_MJ_CLOSE,
        0,
        PreCloseOperationCallback,
        PostCloseOperationCallback },

    { IRP_MJ_READ,
        0,
        PreReadOperationCallback,
        PostReadOperationCallback },

    { IRP_MJ_WRITE,
        0,
        PreWriteOperationCallback,
        PostWriteOperationCallback }
};

FltRegisterFilter( DriverObject,
    &FilterRegistration,
    &Filter );
```
Our Analysis Environment

Windows 7 VM

Ransomware

User mode
Kernel mode

I/O Manager

FS Sniffer

File System

Virtualized Hardware

VirtualBox

Cuckoo Sandbox

1 https://github.com/cuckoosandbox/cuckoo
Analysis Environment Preparation

- **Anti-anti-sandbox**
  - Install common utilities (e.g., Adobe Reader, Office, browsers, media players)
  - No VBox guest addition
  - Real Differentiated System Description Table (DSDT)
  - Clone DMI (Desktop Management Interface)
  - Change default VM values (e.g., MAC, Graphics card name..)
  - Emulate basic user activity (e.g., moving the mouse, launching applications).

https://github.com/AlicanAkyol/sems
https://github.com/a0rtega/pafish
Analysis Environment Preparation

- Trigger ransomware activity
  - Include typical user data such as saved credentials, browser history.
  - **Realistic** decoy files (e.g., images, documents)
  - We used **real** files reflecting file-type and directory tree distribution of the aforementioned 10 clean machines.

- Network configuration: Host-only + iptables
  - Allow samples to communicate with their C&C servers
  - Deny any potentially harmful traffic (e.g., spam)
Our Dataset

- 642 manually verified samples from VirusTotal
FS Access Patterns

- **Overwrite** the content of the original file in place
- Copy the original file
  - Encrypt the new copy
  - **Overwrite** the original one
- Copy the original file
  - Encrypt the new copy
  - **Delete** the original one
Some versions of CBTLocker exploit **one single** file as a write-and-encrypt-buffer.

The malware moves the target original file in **the same** temporary file, encrypts it, and then overwrites the original one.

More on this, by the end of the year :-)
IN YOUR PC & IN YOUR POCKET
RECENT DEVELOPMENTS

<table>
<thead>
<tr>
<th>Country</th>
<th>% of users attacked with ransomware out of all users encountering malware</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>10.4%</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>7.8%</td>
</tr>
<tr>
<td>Ukraine</td>
<td>6.7%</td>
</tr>
<tr>
<td>Germany</td>
<td>4.5%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>2.6%</td>
</tr>
<tr>
<td>Russian Federation</td>
<td>2.5%</td>
</tr>
<tr>
<td>Belarus</td>
<td>1.7%</td>
</tr>
<tr>
<td>S. Arabia</td>
<td>1.6%</td>
</tr>
<tr>
<td>Switzerland</td>
<td>1.5%</td>
</tr>
<tr>
<td>Brazil</td>
<td>0.16%</td>
</tr>
</tbody>
</table>

The "Android behind bars" clipart is stolen from Malware don't need Coffee - data from Kaspersky
Ransomware Evolution (cont'd)

- Cryptovirology theorized
- GPCode
- CryptoLocker
- DirtyDecrypt
- Filecoder
- Cryptodetermine
- CBTLocke
- TorrentLocker
- CoinVault
- CryptoDefense
- TeslaCrypt
- C4.0 Linux Encoder
- Locky
- TeslaCrypt 4.0
- Jigsaw
- Radamant
- Hydracrypt
- Fusob (Jan '15-Apr '16)
- Small (Mid '14-Apr '16)
- New Simplocker (Jan '15)
- New PornDroid (May '15)
- Lockerpin (Dec '15)
- Simplocker (May '14)
- Koler (May '14)
- TkLocker (Jun '14)
- Pletora (Jun '14)
- Svpeng/Scarepackage (Jun-Oct '14)
DETECTING ANDROID RANSOMWARE

- Analysis techniques that we have already implemented and released
- We PoC'd them for Android
  - given the recent increase of families
- Some can be ported to other platforms
- One of them definitely very generic
FROM MANUAL ANALYSIS

- we reverse engineered a few samples for each family

COMMON CHARACTERISTICS

THREATENING TEXT

DEVICE LOCKING

DATA ENCRYPTION

ADMIN API ABUSE
Svpeng (2014)

---

THE FBI
FEDERAL BUREAU OF INVESTIGATION
WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN PORNOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION "THE LEGAL BASIS OF VIOLATIONS". ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS $500.00

ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED.

---

Lockerpin (2015)
ATTENTION! YOUR DEVICE HAS BEEN LOCKED REASONS INDICATED BELOW.

Remaining time to pay a fine

71:59:56

Otherwise the case file will be transferred to the court.

All actions are illegal, are fixed. History query stored in the database of the U.S. Department of Homeland Security

Offender Information

Pay to unlock device with iTunes Gift Card. Your case will be closed immediately after the transaction processing!

Type your iTunes gift card code

Pay a fine

Pay a fine to unlock device.

Fusob (2016)
Small (2016)

Обслуживание Вашего устройства временно приостановлено, Вы нарушили закон, а именно просмотр и распространение порнографии посредством сети Интернет (ст. 242 УК РФ) это грозит вам лишением свободы на срок от двух до пяти лет!

Для возобновления доступа к устройству и закрытия вашего уголовного дела, Вам необходимо оплатить штраф в размере 700 рублей в течение 12 часов. Следуйте инструкции для оплаты:

1. Найдите терминал сотовой связи для оплаты VISA QIWI WALLET.
2. Введите номер телефона + 79637143258
3. В поле комментарий введите код - id133019
4. Оплатите 700 рублей
5. После поступления оплаты Ваше 

---

Штраф составляет $300

You can settle the fine with MoneyPak express Packet vouchers.

As soon as the money arrives to the Treasure account, your device will be unblocked and all information will be decrypted in course of 24 hours.
THREATENING TEXT

- must be clear, understandable and convincing

- coercion techniques
  - refer to law codes
  - various accusations
    - copyright violation
    - illegal content found
    - prohibited sites visited

- detailed payment instructions
- src: strings + network + scraping
TEXT ANALYSIS: PREPARATION

1. Language detection
   - frequency-based analysis (e.g., English, French)

2. Segmentation
   - "This device has been locked for safety reasons"
   - "All actions performed are fixed"

3. Stop-words removal
   - "This device has been locked for safety reasons"
   - "All actions performed are fixed"

4. Stemming
   - "This device has been locked for safety reasons"
   - "All actions performed are fixed"

5. Stem vector
   - presence/absence of each word in a binary vector
TRAINING

T
PRE-LABELED TRAINING

$T$

$T_{\text{money}}$

$T_{\text{law}}$

$T_{\text{accusation}}$
SCORING

$\text{text: } x = \{c_1, c_2, ..., c_n\}$

$\text{score: } m(x) = \max\{\cos\text{-sim}(c, t)\}$

decision thresholds: minimum to detect known ransomware
DECISION (examples)

if (best score in "money")
    could be ransomware

if (best score in "accusation" or "law")
    could be scareware

Note: adding new categories and building new decision criteria in the future would require only text samples.
LOCKING TECHNIQUES

- **Immortal activity:**
  - fill screen with an activity
  - inhibit navigation with home/back keys
    - cover/hide the software-defined keys
      - intercept `onKeyDown/onKeyUp` and do nothing

- **Immortal dialog:**
  - create a dialog that cannot be closed using the `setCancelable(false)` API

Request **device administration privileges** and use the `lockNow` API to lock the device
EXAMPLE of LOCKING DETECTION

on "back" or "home" key pressed

return true -> event handled -> screen locked

Detection based on custom Smali emulation.
ENCRIPTION USAGE DETECTION

TYPICAL SEQUENCE

a. **loop/read** from the filesystem (e.g., external SD card)
b. call some **encryption** API function
c. **write** to the filesystem (and optionally **delete** original)
ENCRIPTION USAGE DETECTION

FlowDroid + modified InfoFlow (taint analysis)

- to handle tainted flows through files
  - Output of `read()` is input `javax.crypto.Cipher`
- to handle conditional tainted flows
  - `javax.crypto.Cipher.init(1, *)`: 1 = encrypt mode

Note: adding new flows is a configuration option.
ADMIN API ABUSE

● Parse the admin policy metadata

```xml
<device-admin xmlns:android="http://schemas.android.com/apk/res/android">
  <uses-policies>
    <limit-password />
    <watch-login />
    <reset-password />
    <force-lock />
    <wipe-data />
    <expire-password />
    <encrypted-storage />
    <disable-camera />
  </uses-policies>
</device-admin>
```

● Navigate the CFG to find where/if are used
  ○ Resolve "reflective" calls along the way if not found
OPEN RELEASE OF HelDroid THIS WINTER

● REST API ~> http://ransom.mobi
● Analysis run daily ~> http://ransom.mobi/scans
● Special thanks to: Nicola Della Rocca
  ○ for building the next generation of HelDroid and keeping ransom.mobi active!

HELDROID: Dissecting and Detecting Mobile Ransomware

Nicolò Andronio, Stefano Zanero, and Federico Maggi

DEIB, Politecnico di Milano, Milano, Italy
nicolo.andronio@mail.polimi.it,
{stefano.zanero,federico.maggi}@polimi.it

Abstract. In ransomware attacks, the actual target is the human, as opposed to the classic attacks that abuse the infected devices (e.g., botnet...
WAIT! THERE'S MORE ON THE GRILL!

- Mere detection is insufficient
  - Stopping a suspicious process may be too late

- We're working on something revolutionary
  - We hope we'll make the World less "ransomwary"

- But unfortunately we can't disclose it yet
  - We have a work under submission :-(
FOR THE IMPATIENTS

● Files protected: **always 100%**
  ○ Even in case of missed detection
● Detection rate: **97.80%**
● False positive rate: **0.035%**
THANK YOU FOR ATTENDING

IN YOUR PC & IN YOUR POCKET
DESKTOP AND MOBILE RANSOMWARE THREAT LANDSCAPE

andrea.continella@polimi.it
@_conand

federico@maggi.cc
@phretor