

IN YOUR PC & IN YOUR POCKET

DESKTOP AND MOBILE RANSOMWARE THREAT LANDSCAPE

Andrea Continella, Federico Maggi(*)
Politecnico di Milano

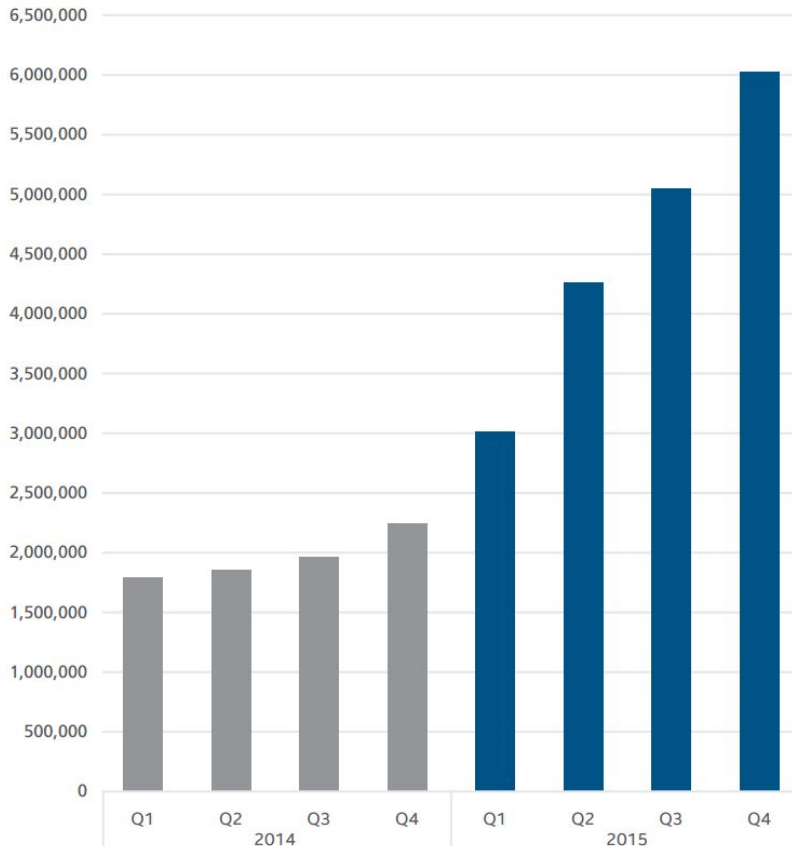
7/21/2016

(*) this work has been done while @ Politecnico di Milano. I recently joined Trend Micro.



2016 the "year of extortion"

Total Ransomware



Source: McAfee Labs, 2016.

CRYPTOWALL RANSOMWARE COST USERS \$325 MILLION IN 2015

by [NewsEditor](#) on November 2nd, 2015 in [Industry and Security News](#).



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION



June 23, 2015

Alert Number
I-062315-PSA

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

Ransomware Hackers Blackmail U.S. Police Departments

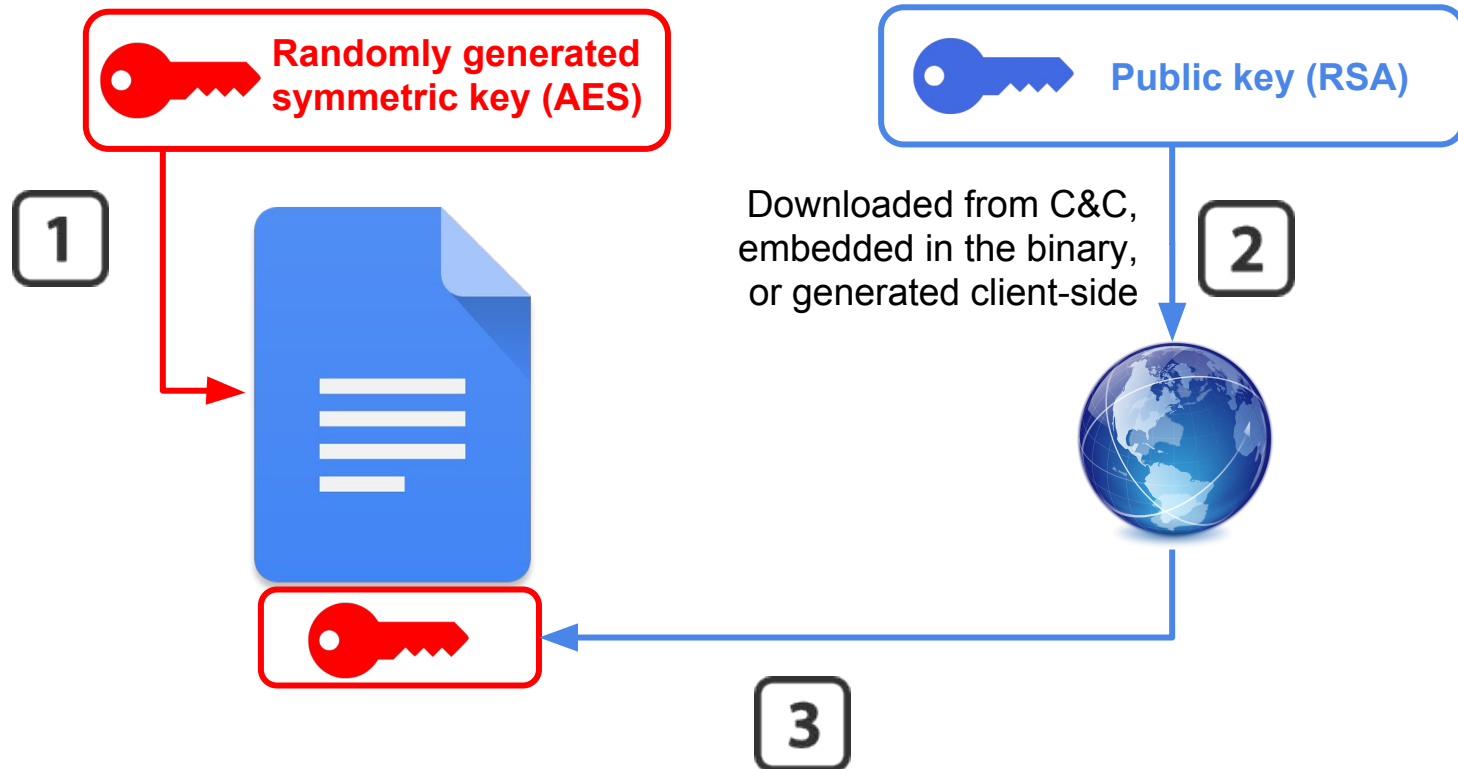
Chris Francescani
Tuesday, 26 Apr 2016 | 10:30 AM ET

NBC NEWS



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

Encryption Mechanism

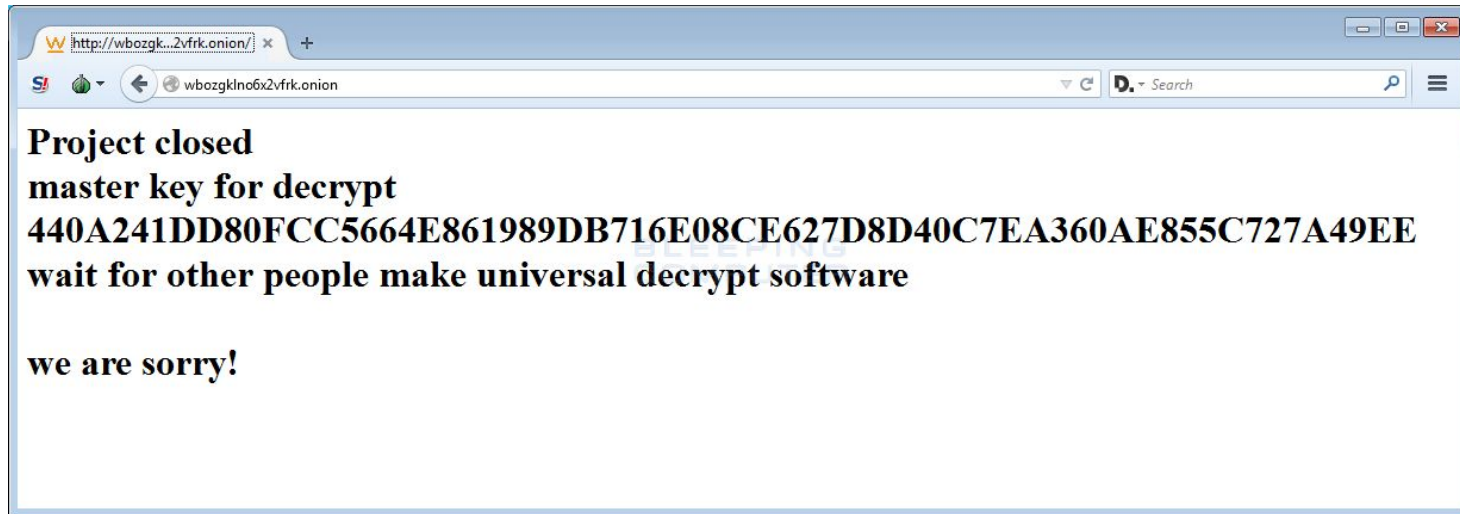


TeslaCrypt

- 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!



TeslaCrypt



Following

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?

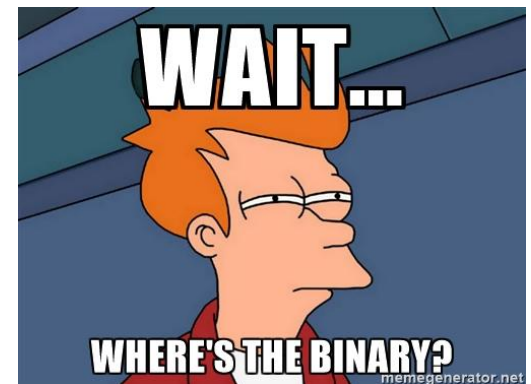
1. You can make a payment with BitCoins, there are many methods to get them.

 bitcoin

2. You should register BitCoin wallet ([simplest online wallet](#) OR [some other methods](#))
3. Purchasing Bitcoins - Although it's not yet easy to buy bitcoins, it's getting simpler e

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





Andrea Continella

@_conand

#ransomware sample asking to reinstall because it failed to encrypt files. lol

The screenshot shows a ransomware window titled "CryptoLocker-v3" with a red background. On the left, a shield icon is displayed above the text: "Your private key will be destroyed on: 2/6/2016". The main text reads: "Your personal files are encrypted!". Below this, it states: "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." It then says: "Encryption was pro... for this computer. T... The only copy of the... is located on a sec... after a time period... Once this has bee... In order to decry... https://34r6hq2... Use your bitcoin address to enter the site: 1FspFcGikHGgx4EjstTrKyRkf2QpGggJ39". A button labeled "Click to copy Bitcoin address to clipboard" is present. Below that, it says: "if https://34r6hq26q2h4jkzj.tor2web.org is not opening, please follow the steps: You must install this browser www.torproject.org/projects/torbrowser.html.en After installation, run the browser and enter address 34r6hq26q2h4jkzj.onion Follow the instruction on the web-site. We remind you that the sooner you do, the more chances are left to recover the files. Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server." At the bottom, there are three buttons: "Show encrypted files", "Check Payment", and "Enter Decrypt Key". An error dialog box titled "Missing File Error" is overlaid on the main window, containing the message: "Unable to find locale data files. Please reinstall." with an "OK" button.

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!**

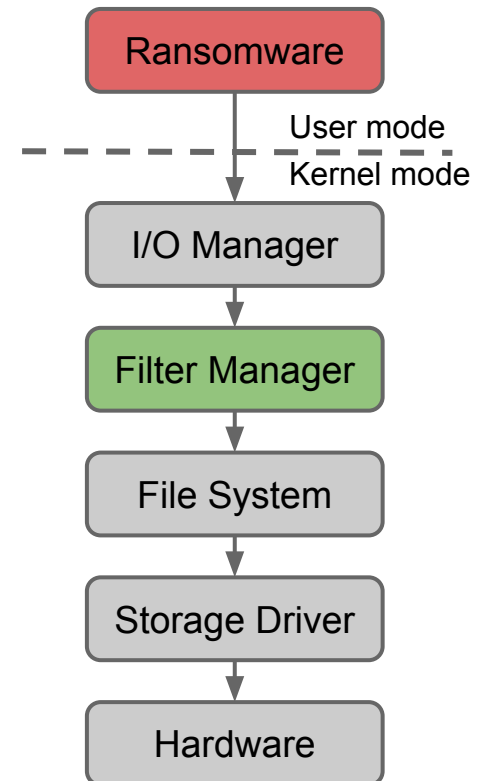
[1] A.Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*, DIMVA 2015

[2] A. Kharaz, S. Arshad, W. Robertson, E. Kirda, *UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware*, USENIX Sec 2016

[3] N.Scaife, H. Carter, P. Traynor, K. Butler, *CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data*, ICDCS 2016

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

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

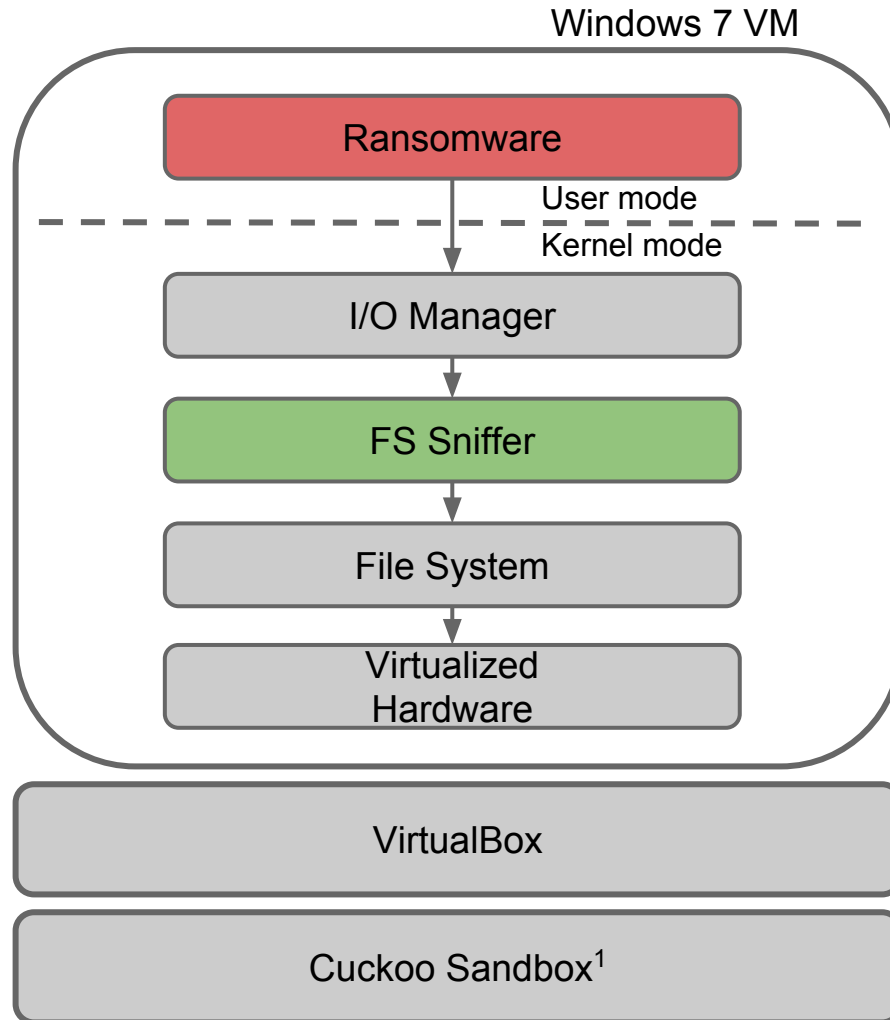
    { IRP_MJ_CLOSE,
      0,
      PreCloseOperationCallback,
      PostCloseOperationCallback },

    { IRP_MJ_READ,
      0,
      PreReadOperationCallback,
      PostReadOperationCallback },

    { IRP_MJ_WRITE,
      0,
      PreWriteOperationCallback,
      PostWriteOperationCallback },
}
```

```
FltRegisterFilter ( DriverObject,
                   &FilterRegistration,
                   &Filter );
```

Our Analysis Environment



¹ <https://github.com/cuckoosandbox/cuckoo>

Analysis Environment Preparation

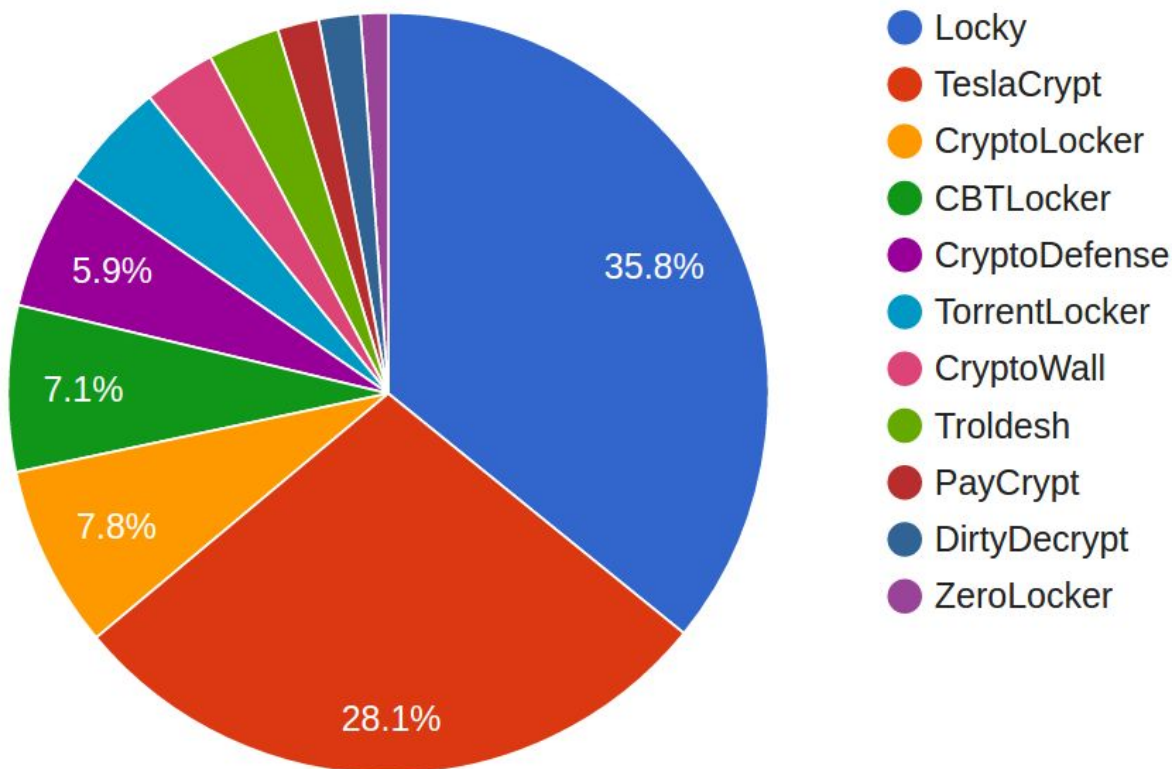
- Anti-anti-sandbox
 - Install common utilities (e.g., Adobe Reader, Office, browsers, media players)
 - No VBox guest addition
 - Real Differentiated System Description Table (DSDT)
 - Clone DMI (Desktop Management Interface)
 - Change default VM values (e.g., MAC, Graphics card name..)
 - Emulate basic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

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

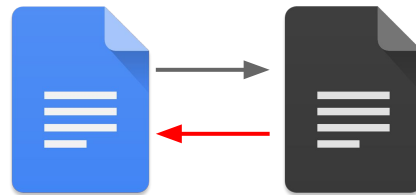
- 642 manually verified samples from VirusTotal



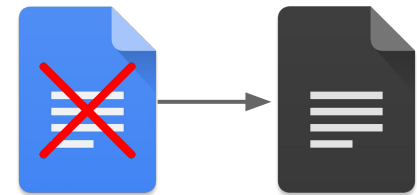
FS Access Patterns



Overwrite the content of the original file in place

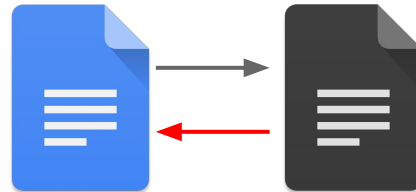


Copy the original file
Encrypt the new copy
Overwrite the original one



Copy the original file
Encrypt the new copy
Delete the original one

FS Access Patterns



Copy the original file
Encrypt the new copy
Overwrite 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 :-)

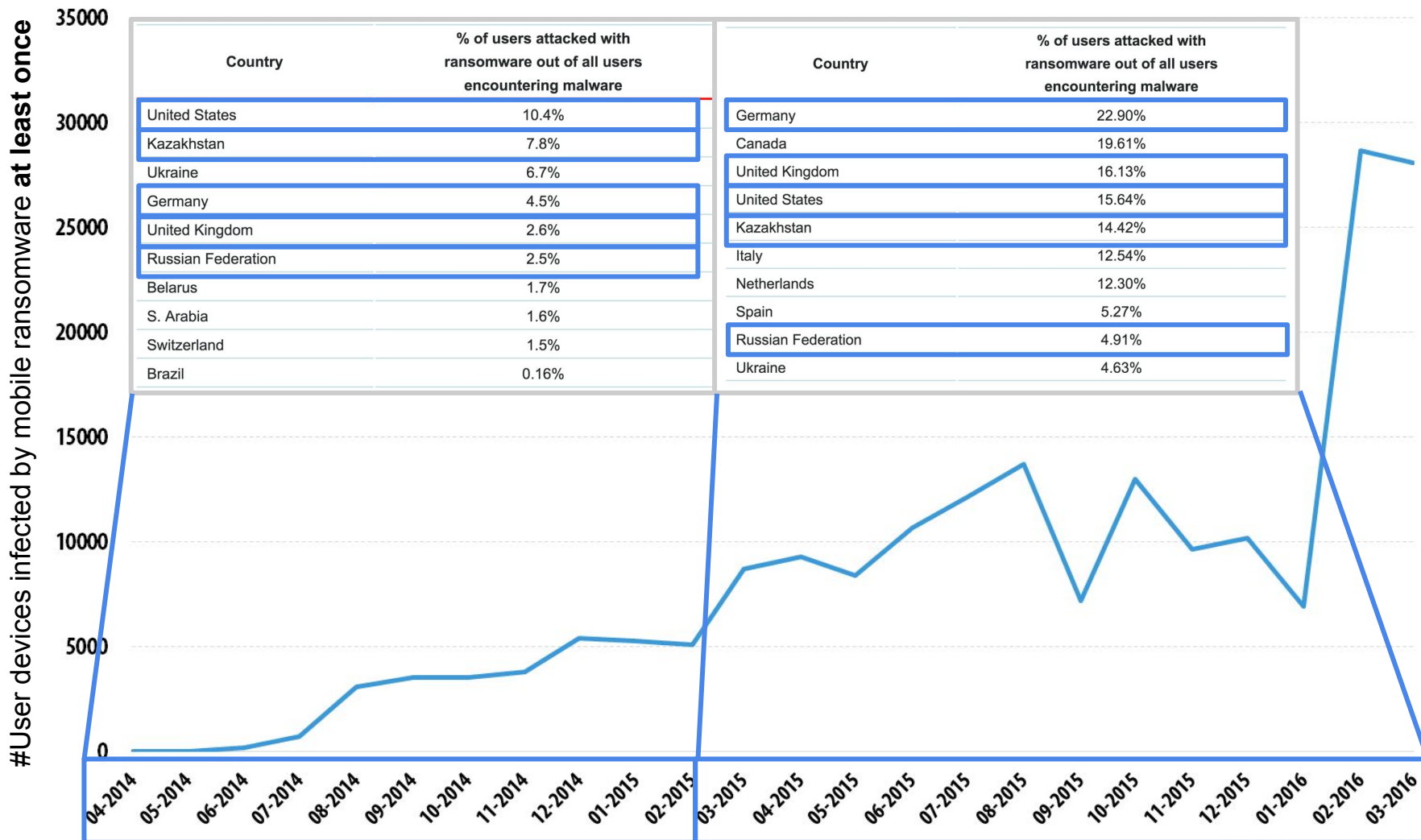
**IN YOUR
PC**

&

**IN YOUR
POCKET**



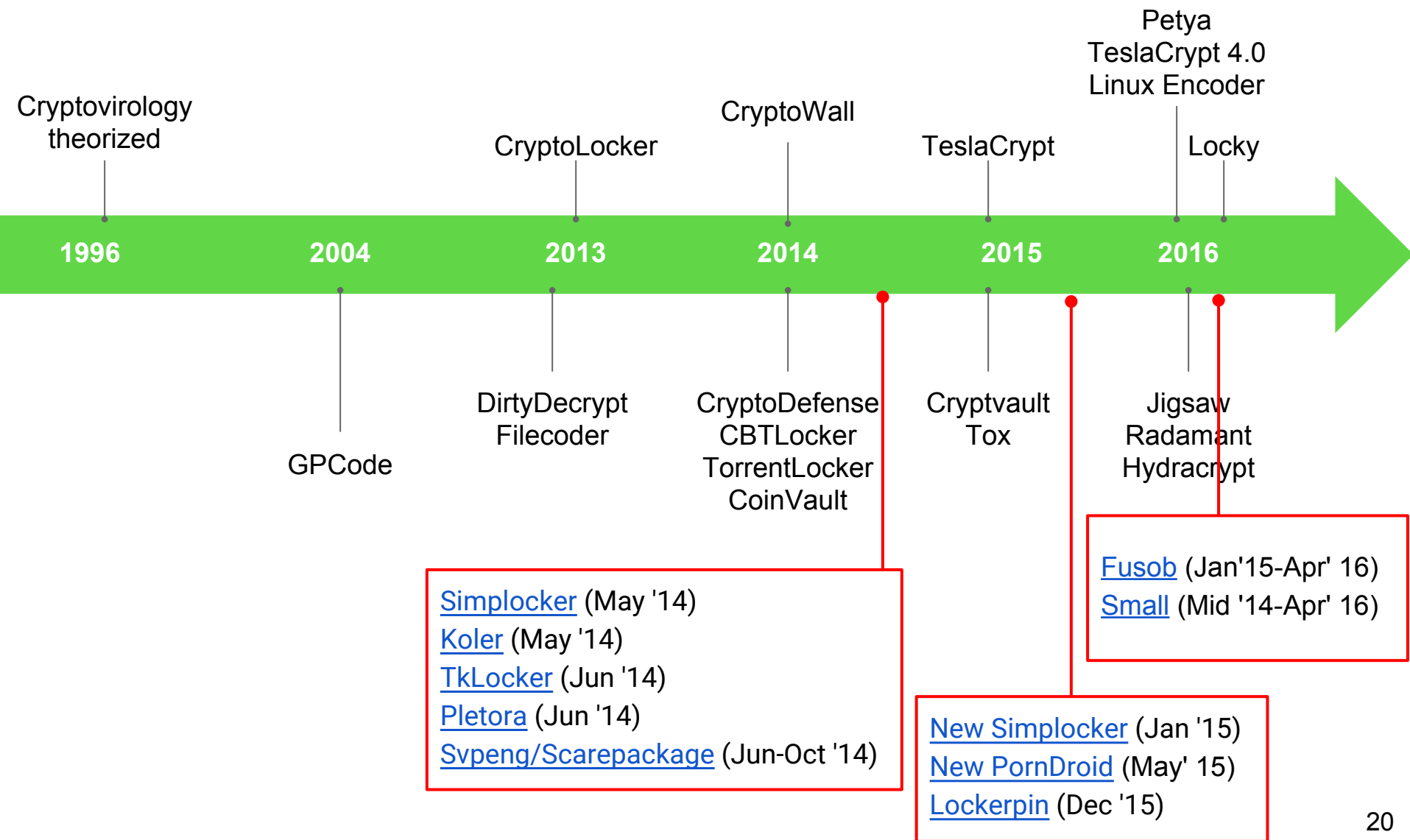
RECENT DEVELOPMENTS



© 2016 AO Kaspersky Lab. All Rights Reserved.

The "Android behind bars" clipart is stolen from [Malware don't need Coffee](#) - data from [Kaspersky](#)

Ransomware Evolution (cont'd)



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



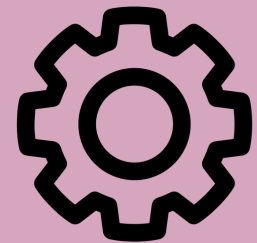
THREATENING
TEXT



DEVICE
LOCKING



DATA
ENCRYPTION



ADMIN API
ABUSE

Svpeng (2014)



DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FBI HEADQUARTERS
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 SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

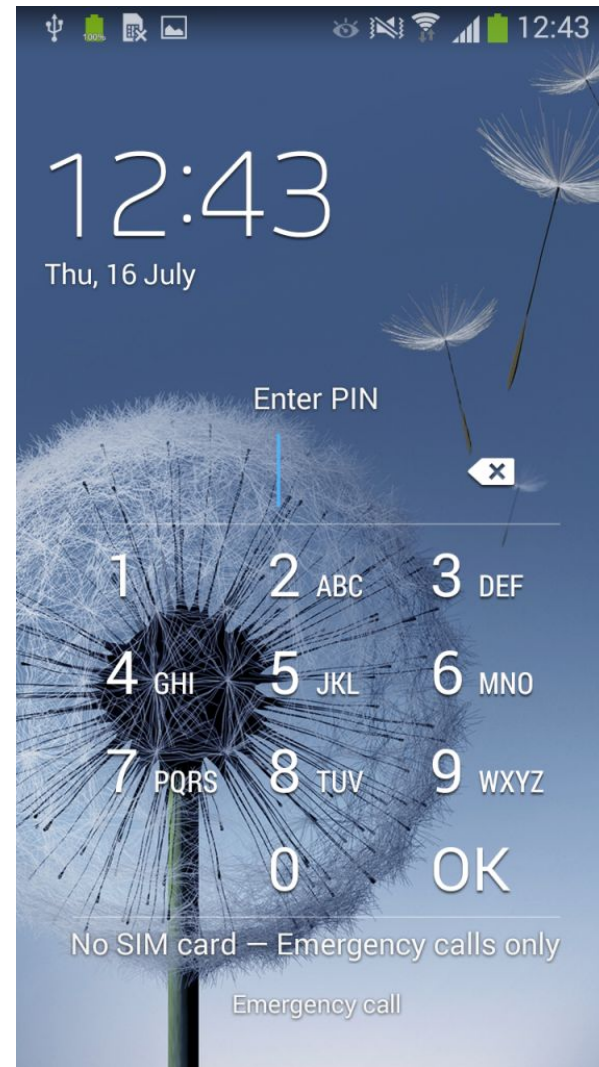
FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION "THE LEGAL BASIS OF VIOLATIONS". ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU

WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED. THE SIZE OF THE PENALTY IS **\$500.00**

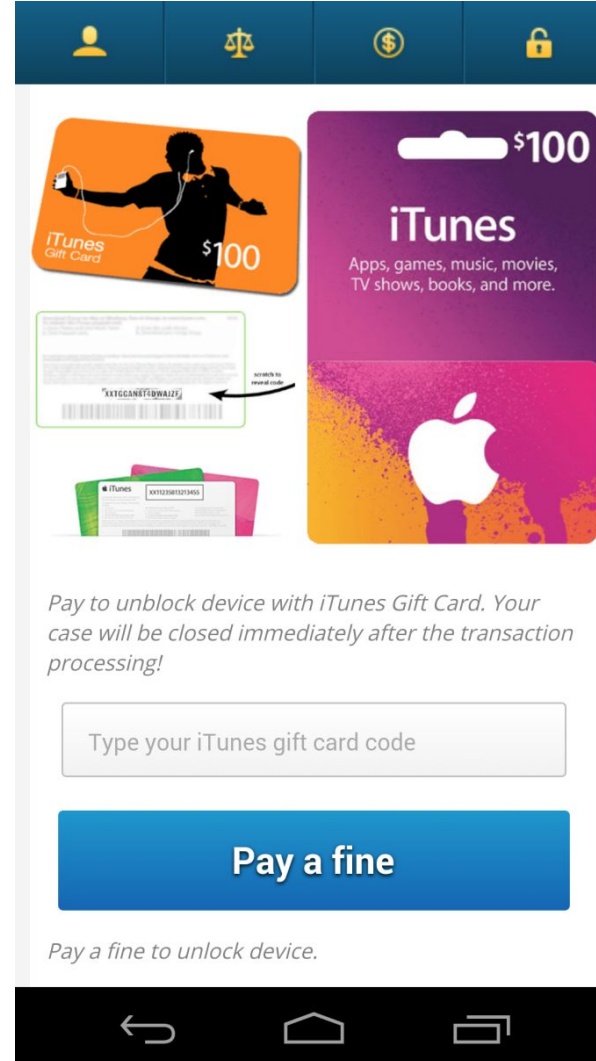
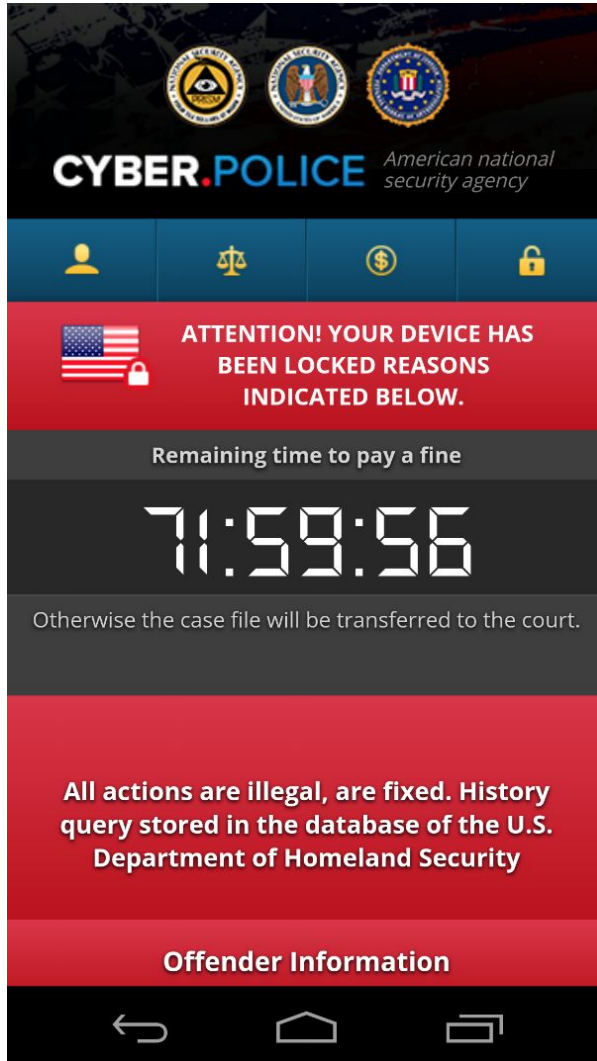
ATTENTION! DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED



Lockerpin (2015)



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 течении 12 часов. Следуйте инструкции для оплаты:

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



a matter of whether you have paid the fine to the Treasury (to the affect of initiatives aimed at protection of cyberspace).

The penalty set must be paid in course of 24 hours as of the breach. On expiration of the term, 24 hours that follow will be used for automatic collection of data on yourself and your misconduct, and criminal case will be opened against you.

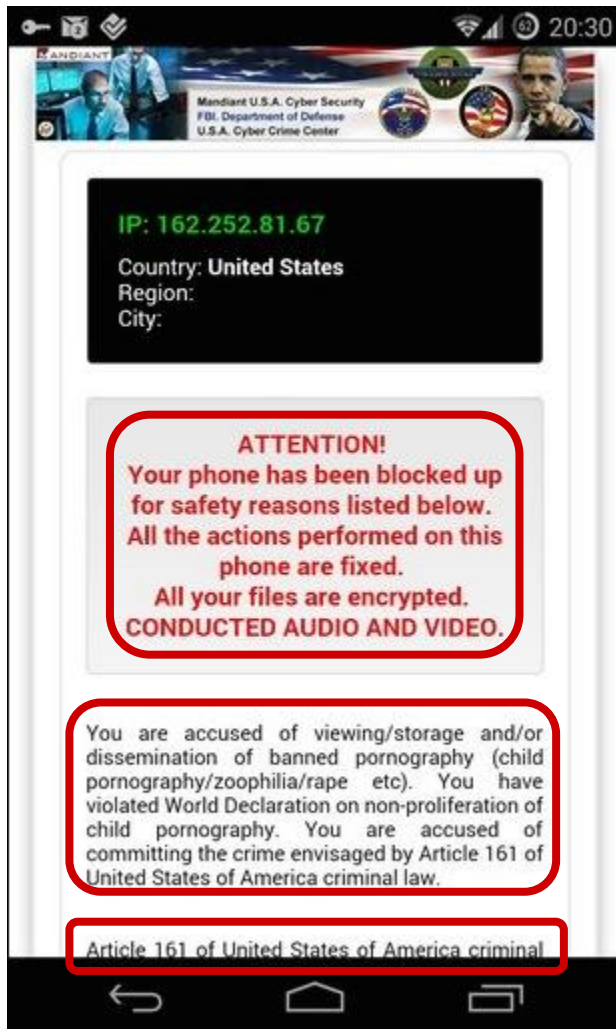



Amount of fine is \$300

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

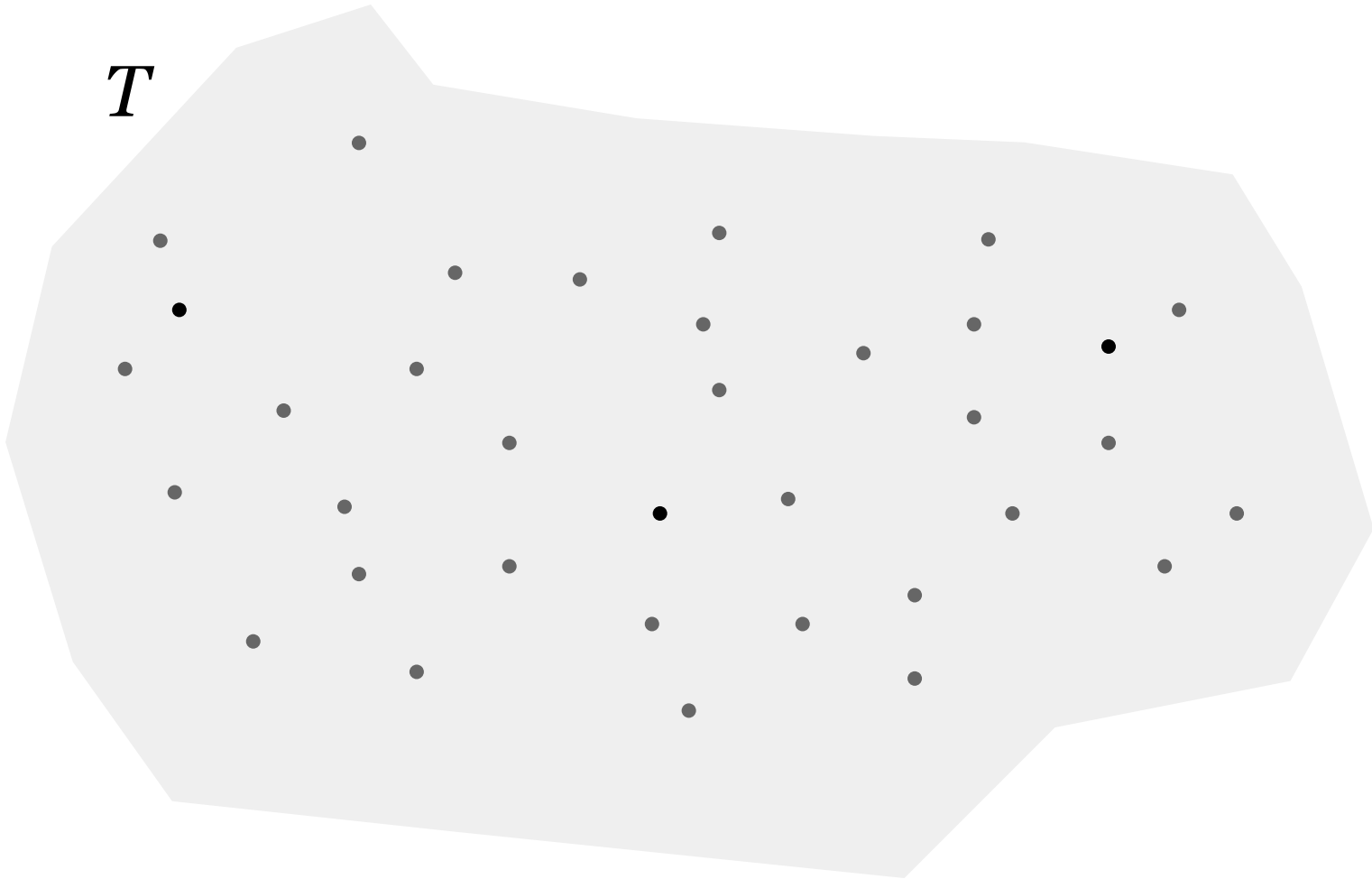
- presence/absence of each word in a binary vector

TRAINING

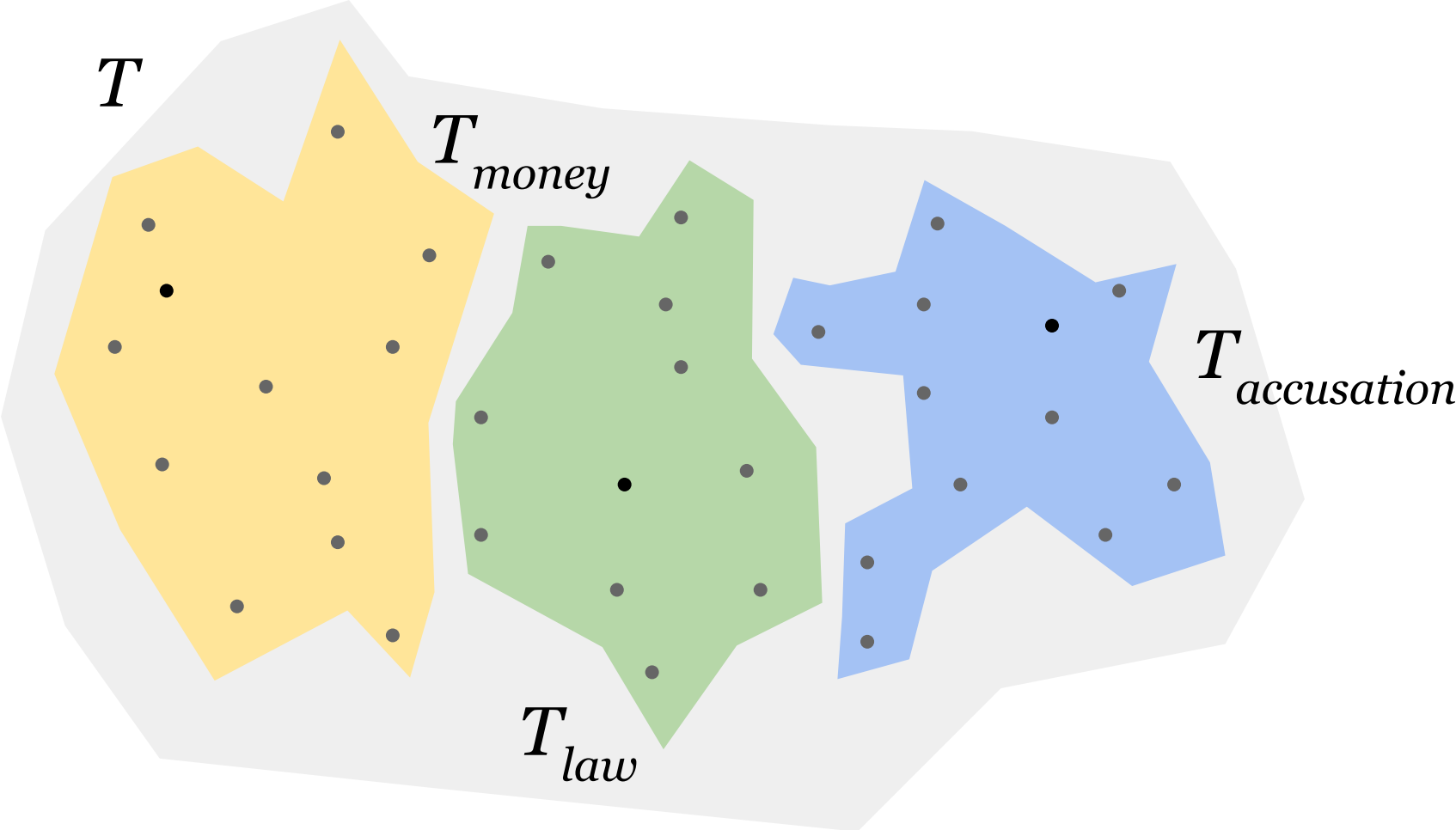


THREATENING
TEXT

T



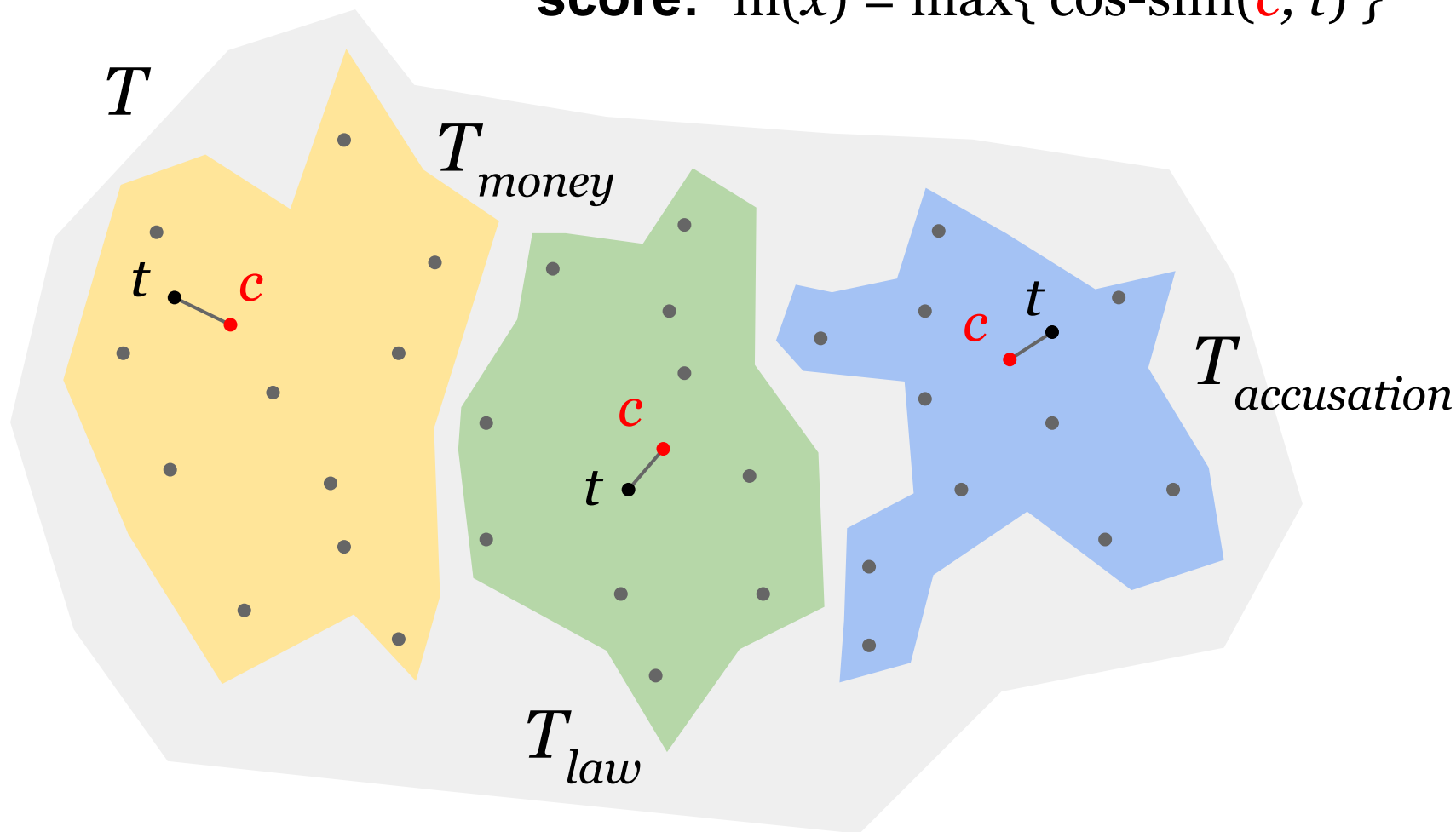
PRE-LABELED TRAINING



SCORING

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

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



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

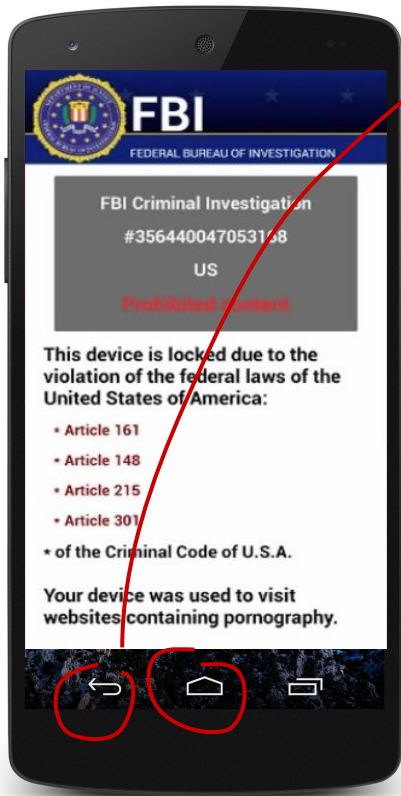
- **Immortal dialog:**

- 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



```
.method public onKeyDown(Landroid/view/KeyEvent;)Z
.locals 1

# p1 = integer with the key code associated to the pressed key.

const/4 v0, 0x4      # 4 = back button
if-ne p1, v0, :cond_0
iget-object v0, p0, Lcom/android/x5a807058/ZActivity;->q:Lcom/android/zics/ZModuleInterfac

if-nez v0, :cond_0
iget-object v0, p0, Lcom/android/x5a807058/ZActivity;->a:Lcom/android/x5a807058/ae;

# we track function calls as well
invoke-virtual {v0}, Lcom/android/x5a807058/ae;->c()Z
:cond_0

const/4 v0, 0x1      # True = event handled -> do not forward
return v0
.end method
```

on "back" or "home" key pressed

return true -> event handled -> screen locked

Detection based on custom Smali emulation.

ENCRYPTION USAGE DETECTION



DATA
ENCRYPTION

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)

EXAMPLE of ENCRYPTION FLOW



DATA
ENCRYPTION

```
invoke-static {},  
    Landroid/os/Environment;->getExternalStorageDirectory()Ljava/io/File;  
move-result-object v0  
invoke-virtual {v0}, Ljava/io/File;->toString()Ljava/lang/String;  
move-result-object v0  
new-instance v1, Ljava/io/File;  
invoke-direct {v1, v0}, Ljava/io/File;-><init>(Ljava/lang/String;)V
```

```
invoke-virtual {v2, v0, v4},  
    Lcom/free/xxx/player/a;->a(Ljava/lang/String;Ljava/lang/String;)V  
new-instance v4, Ljava/io/File;  
invoke-direct {v4, v0}, Ljava/io/File;-><init>(Ljava/lang/String;)V  
invoke-virtual {v4}, Ljava/io/File;->delete()Z
```

```
invoke-direct {v1, p2}, Ljava/io/FileOutputStream;-><init>(Ljava/lang/String;)V  
iget-object v2, p0, Lcom/free/xxx/player/a;->a:Ljavax/crypto/Cipher;  
const/4 v3, 0x1  
iget-object v4, p0,  
    Lcom/free/xxx/player/a;->b:Ljavax/crypto/spec/SecretKeySpec;  
iget-object v5, p0,  
    Lcom/free/xxx/player/a;->c:Ljava/security/spec/AlgorithmParameterSpec;
```

ENCRYPTION USAGE DETECTION

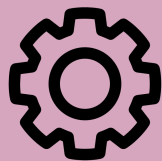


DATA
ENCRYPTION

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.

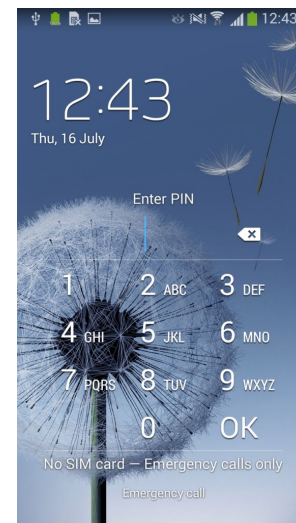


ADMIN API ABUSE

- Parse the admin policy metadata

```
<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>
```

Lockerpin (2015)



- Navigate the CFG to find where/if are used
 - Resolve "reflective" calls along the way if not found

OPEN RELEASE OF HeIDroid 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 HeIDroid and keeping ransom.mobi active!

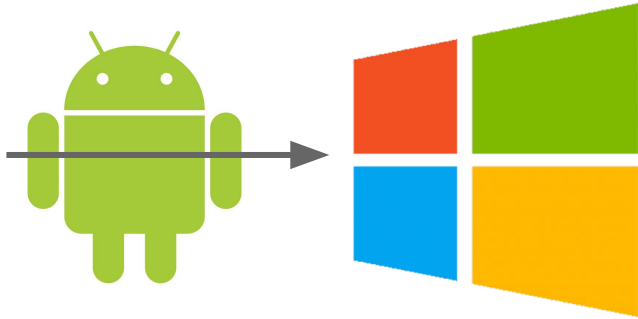
HELDROID: Dissecting and Detecting Mobile Ransomware

Nicoló 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

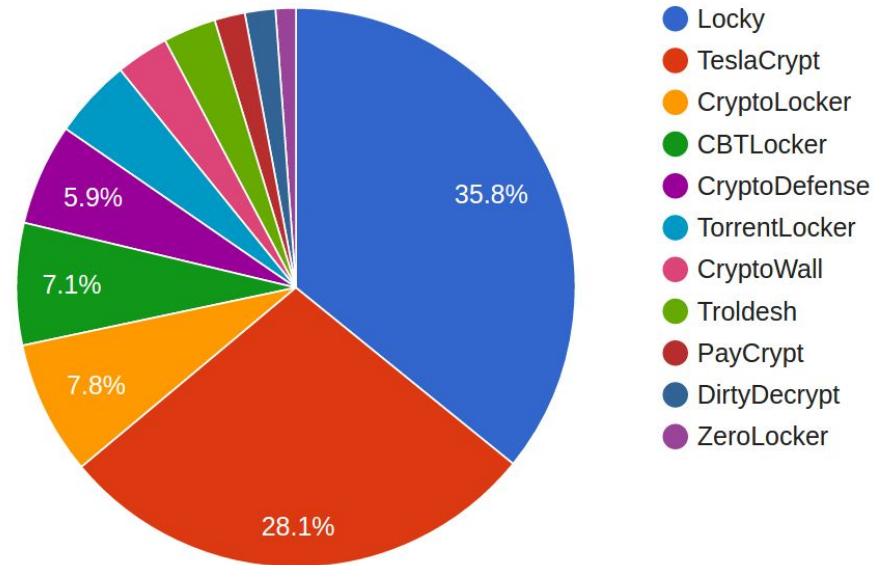
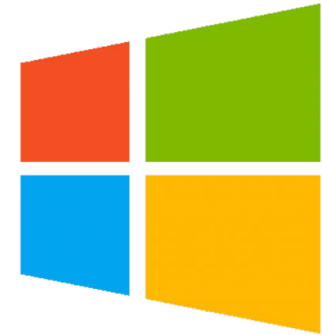
WAIT! THERE'S MORE ON THE GRILL!



- 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

