WWW.CERT.RO

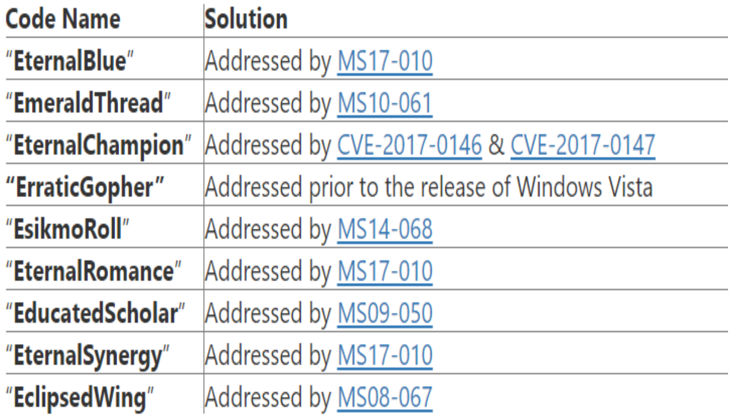
CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA
ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

Cătălin Pătrașcu
Coordinator of the Incident Handling Team @ CERT-RO
catalin.patrascu@cert.ro

Alexandru Stoian
Cyber security specialist @ CERT-RO
alexandru.stoian@cert.ro

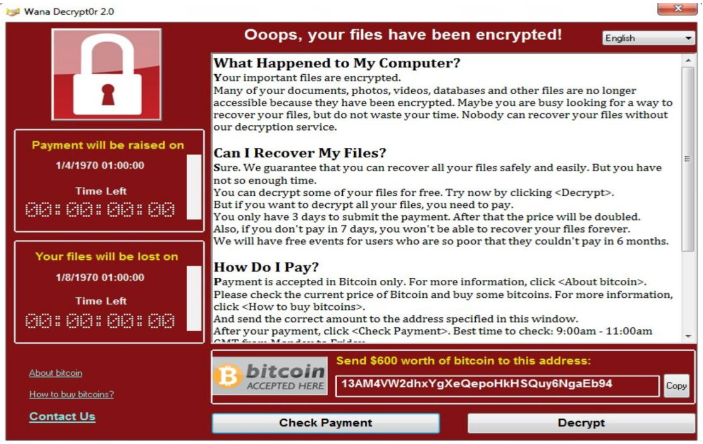
QUO VADIS, INTERNET?

What was all about in 2017



Code Name	Solution
"EternalBlue"	Addressed by MS17-010
"EmeraldThread"	Addressed by MS10-061
"EternalChampion"	Addressed by CVE-2017-0146 & CVE-2017-0147
"ErraticGopher"	Addressed prior to the release of Windows Vista
"EsikmoRoll"	Addressed by MS14-068
"EternalRomance"	Addressed by MS17-010
"EducatedScholar"	Addressed by MS09-050
"EternalSynergy"	Addressed by MS17-010
"EclipsedWing"	Addressed by MS08-067

The Shadow Brokers



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

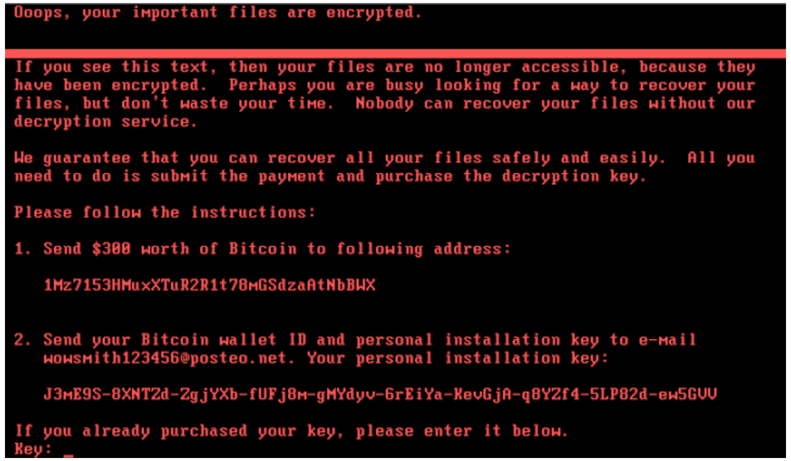
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

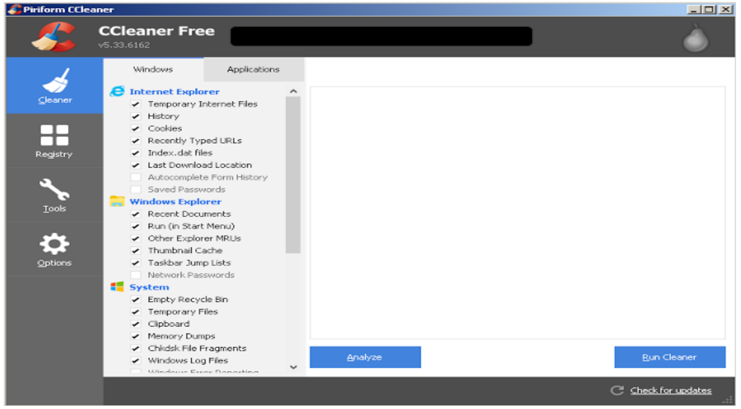
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

WannaCry



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   J3mE9S-8XNTZd-ZgjYXb-fUFj8m-gMYdyv-6rEiYa-KevGjA-q8YZf4-5LP82d-ew5GVV

If you already purchased your key, please enter it below.
Key: _
```

NotPetya



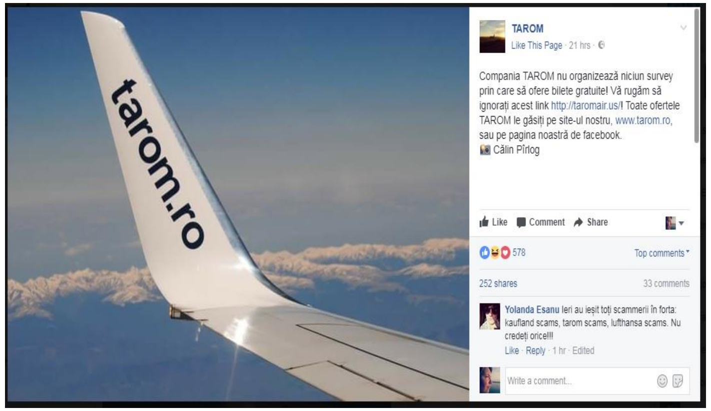
[redacted]

Internet Explorer
- ☑ Temporary Internet Files
- ☑ History
- ☑ Cookies
- ☑ Recently Typed URLs
- ☑ Index.dat files
- ☑ Last Download Location
- □ Autocomplete Form History
- □ Saved Passwords

Windows Explorer
- ☑ Recent Documents
- ☑ Run (in Start Menu)
- ☑ Other Explorer MRUs
- ☑ Thumbnail Cache
- ☑ Taskbar Jump Lists
- □ Network Passwords

System
- ☑ Empty Recycle Bin
- ☑ Temporary Files
- ☑ Clipboard
- ☑ Memory Dumps
- ☑ Chkdsk File Fragments
- ☑ Windows Log Files

CCleaner

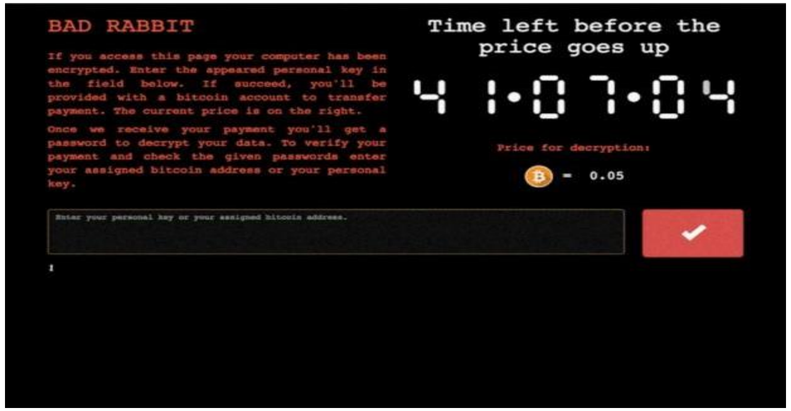


TAROM
Like This Page · 21 hrs

Compania TAROM nu organizează niciun survey prin care să ofere bilete gratuite! Vă rugăm să ignorați acest link http://taromair.us/! Toate ofertele TAROM le găsiți pe site-ul nostru, www.tarom.ro, sau pe pagina noastră de facebook.
Călin Pîrlog

Yolanda Esanu Ieri au ieșit toți scammerii în forta: kaufland scams, tarom scams, lufthansa scams. Nu credeți orice!!!
Like · Reply · 1 hr · Edited

Free vouchers for everything



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

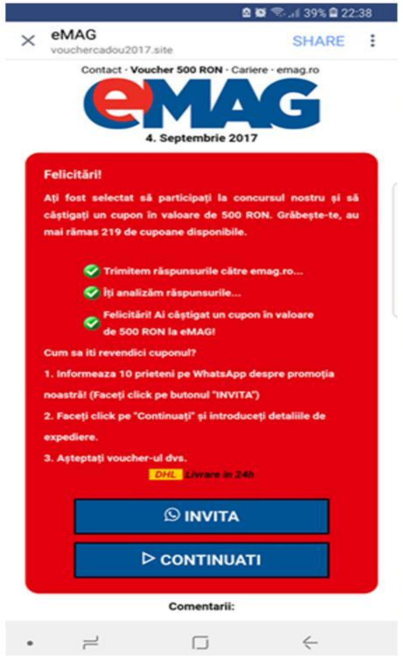
Time left before the price goes up
41:07:04

Price for decryption:
B = 0.05

Enter your personal key or your assigned bitcoin address.

BadRabbit

Free vouchers for everything and for everybody



4. Septembrie 2017

Felicitări!

Ați fost selectat să participați la concursul nostru și să câștigați un cupon în valoare de 500 RON. Grăbește-te, au mai rămas 219 de cupoane disponibile.

✓ Trimitem răspunsurile către emag.ro...

✓ Îți analizăm răspunsurile...

✓ Felicitări! Ai câștigat un cupon în valoare de 500 RON la eMAG!

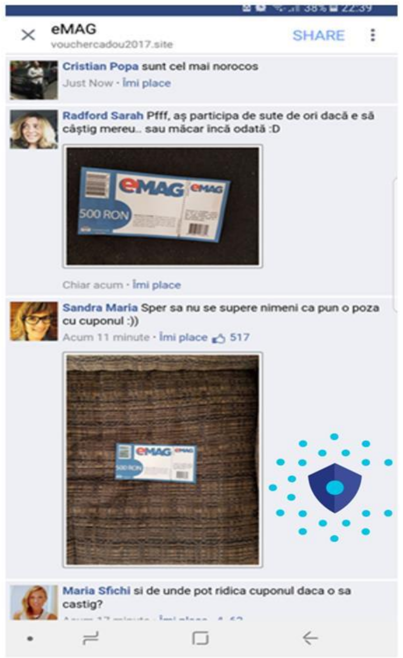
Cum sa iti revendici cuponul?

1. Informeaza 10 prieteni pe WhatsApp despre promoția noastră! (Faceți click pe butonul "INVITA")

2. Faceți click pe "Continuați" și introduceți detaliile de expediere.

3. Așteptați voucher-ul dvs.

DHL Livrare in 24h

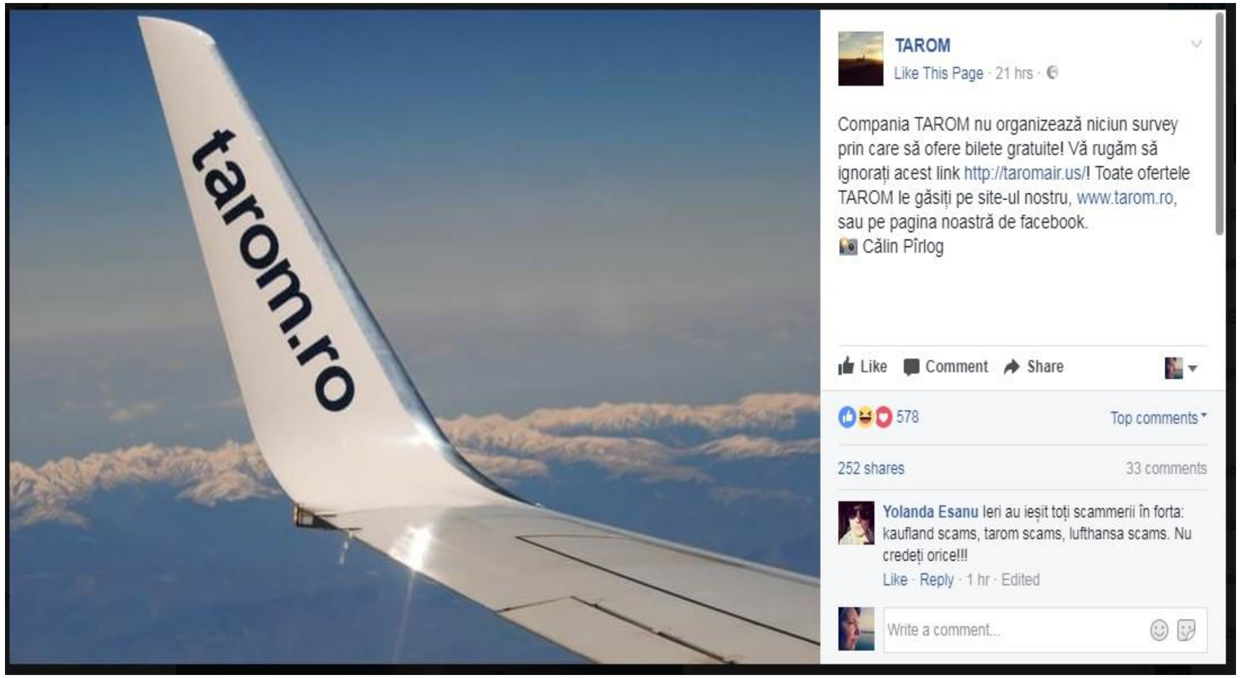


Cristian Popa sunt cel mai norocos
Just Now · Îmi place

Radford Sarah Pfff, aș participa de sute de ori dacă e să câștig mereu.. sau măcar încă odată :D
Chiar acum · Îmi place

Sandra Maria Sper sa nu se supere nimeni ca pun o poza cu cuponul :))
Acum 11 minute · Îmi place 517

Maria Sfichi si de unde pot ridica cuponul daca o sa castig?



TAROM
Like This Page · 21 hrs ·

Compania TAROM nu organizează niciun survey prin care să ofere bilete gratuite! Vă rugăm să ignorați acest link http://taromair.us/! Toate ofertele TAROM le găsiți pe site-ul nostru, www.tarom.ro, sau pe pagina noastră de facebook.
Călin Pîrlog

578 · Top comments

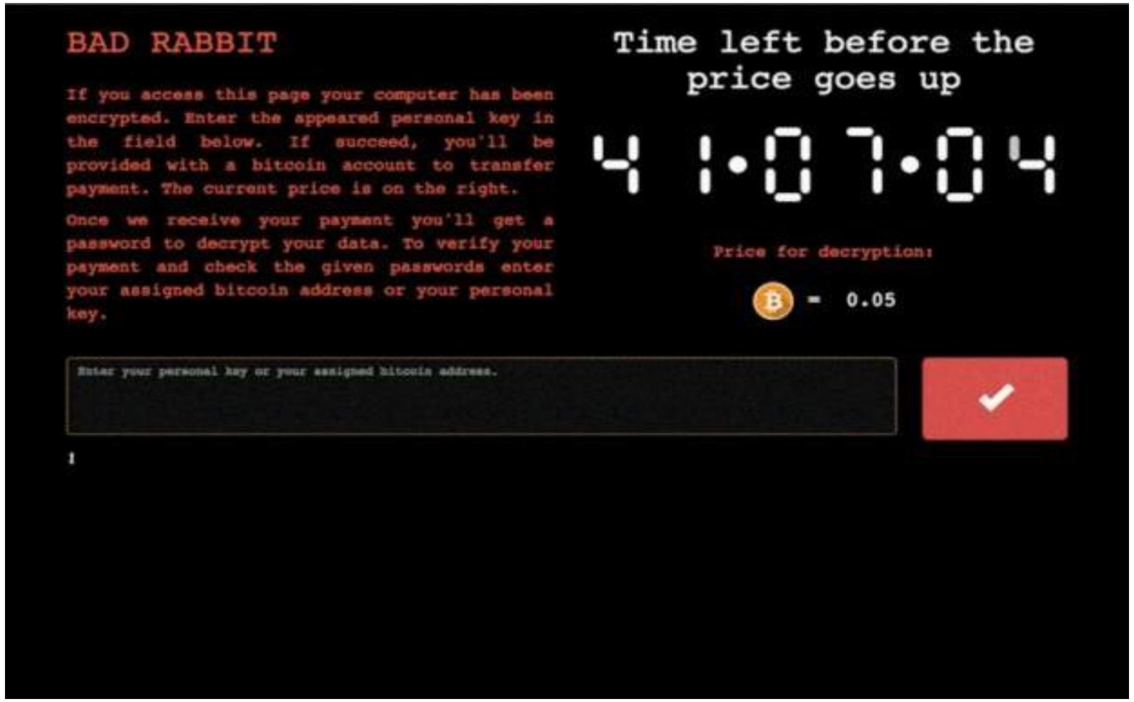
252 shares · 33 comments

Yolanda Esanu Ieri au ieșit toți scammerii în forta: kaufland scams, tarom scams, lufthansa scams. Nu credeți orice!!!
Like · Reply · 1 hr · Edited

Yep! That’s very effective
Last big campaign? … Yesterday

BadRabbit

- Infection via watering-hole
- 48+ web domains in RO used as watering-hole (one single IP)
- Hoster’s opinion: probably due to weak passwords or vulnerable CMS’s for each of them (pure coincidence to be on the same IP)
- Under investigation on the hoster side (we’ll keep you posted)



BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

41:07:04

Price for decryption:

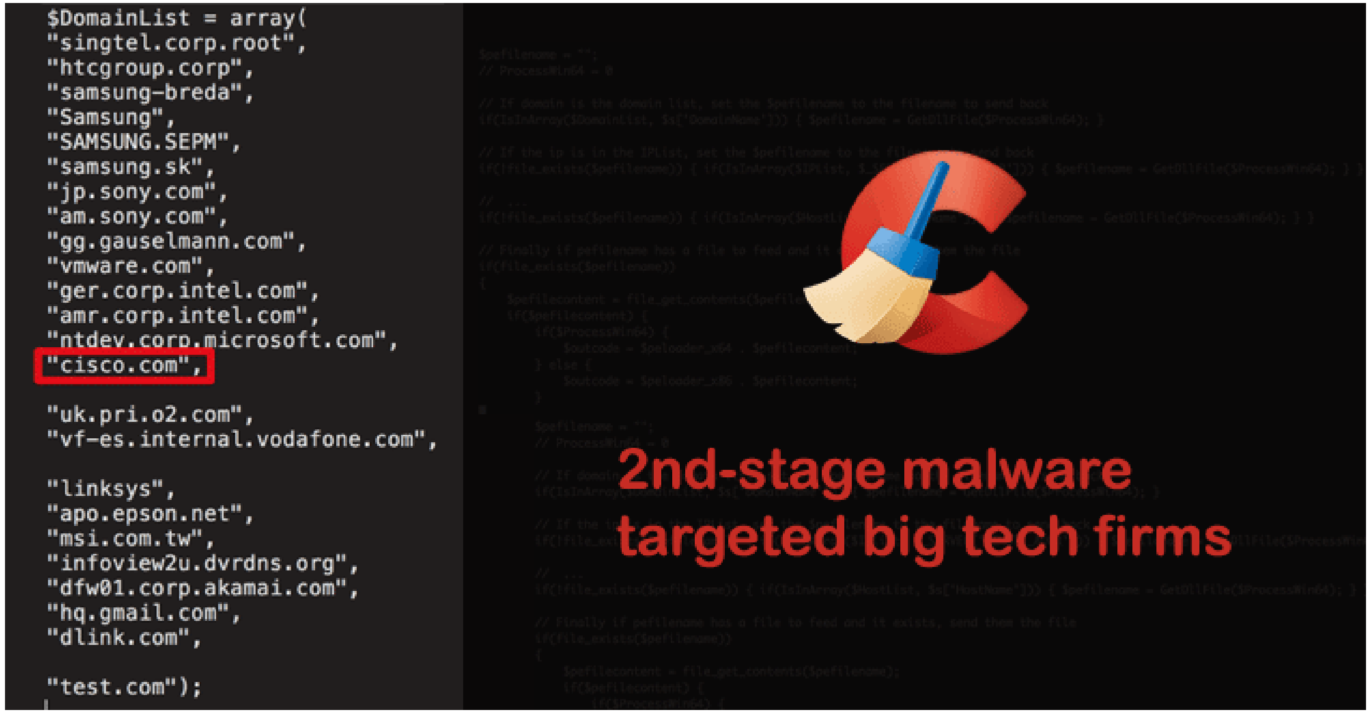
B - 0.05

Enter your personal key or your assigned bitcoin address.

✓

CCleaner

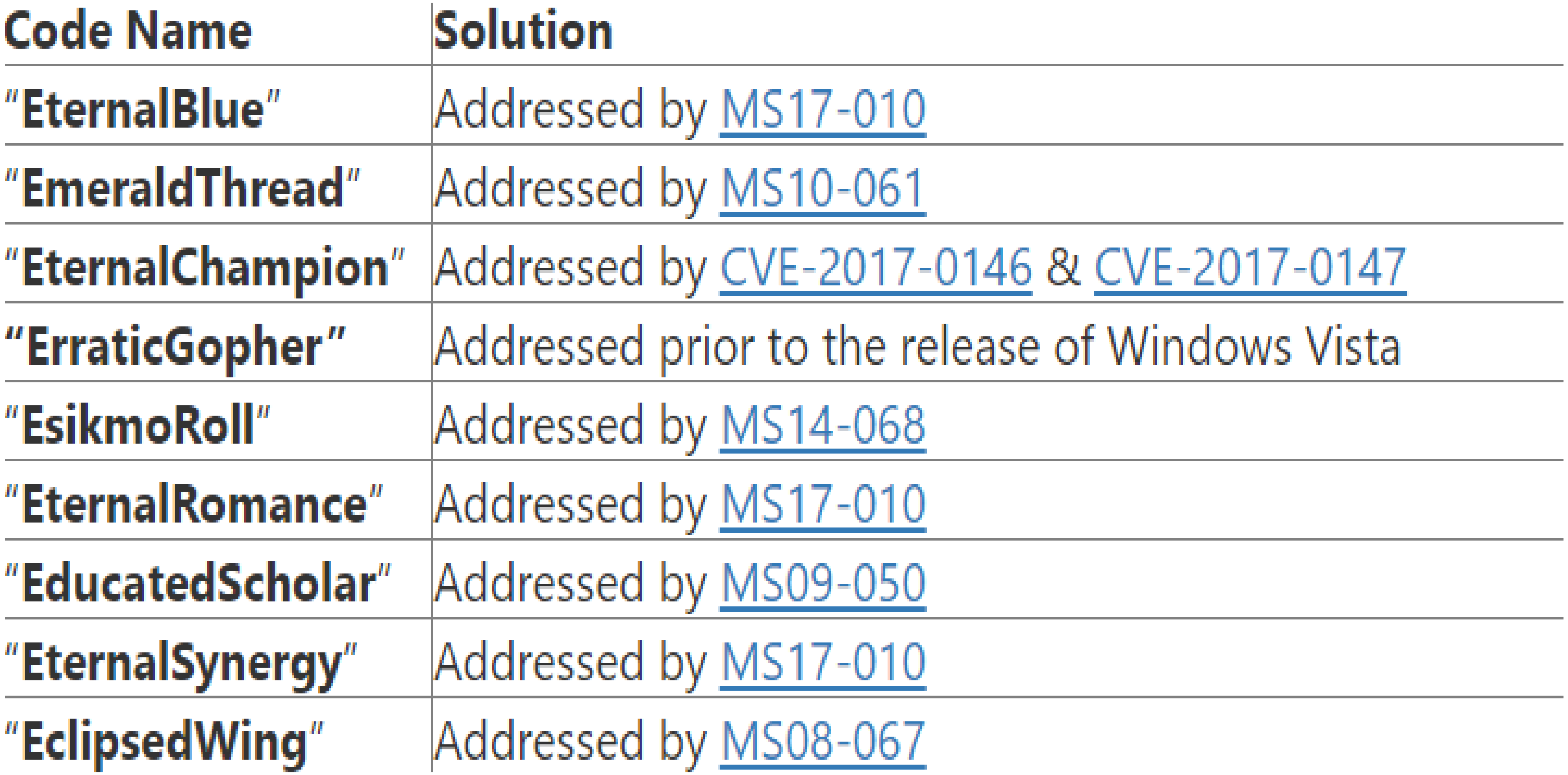
- Some specific versions contained malware (v5.33 and Cloud v1.07.3191)
- But signed with valid certificates from Piriform
- Distribution period: Aug. 15 – Sept. 12
- “Luckily” it was targeted
- “Luckily” I had a different version … an older one



```
$DomainList = array(
"singtel.corp.root",
"htcgroup.corp",
"samsung-breda",
"Samsung",
"SAMSUNG.SEPM",
"samsung.sk",
"jp.sony.com",
"am.sony.com",
"gg.gauselmann.com",
"vmware.com",
"ger.corp.intel.com",
"amr.corp.intel.com",
"ntdev.corp.microsoft.com",
"cisco.com",

"uk.pri.o2.com",
"vf-es.internal.vodafone.com",

"linksys",
"apo.epson.net",
"msi.com.tw",
"infoview2u.dvrdns.org",
"dfw01.corp.akamai.com",
"hq.gmail.com",
"dlink.com",

"test.com");
```

2nd-stage malware targeted big tech firms

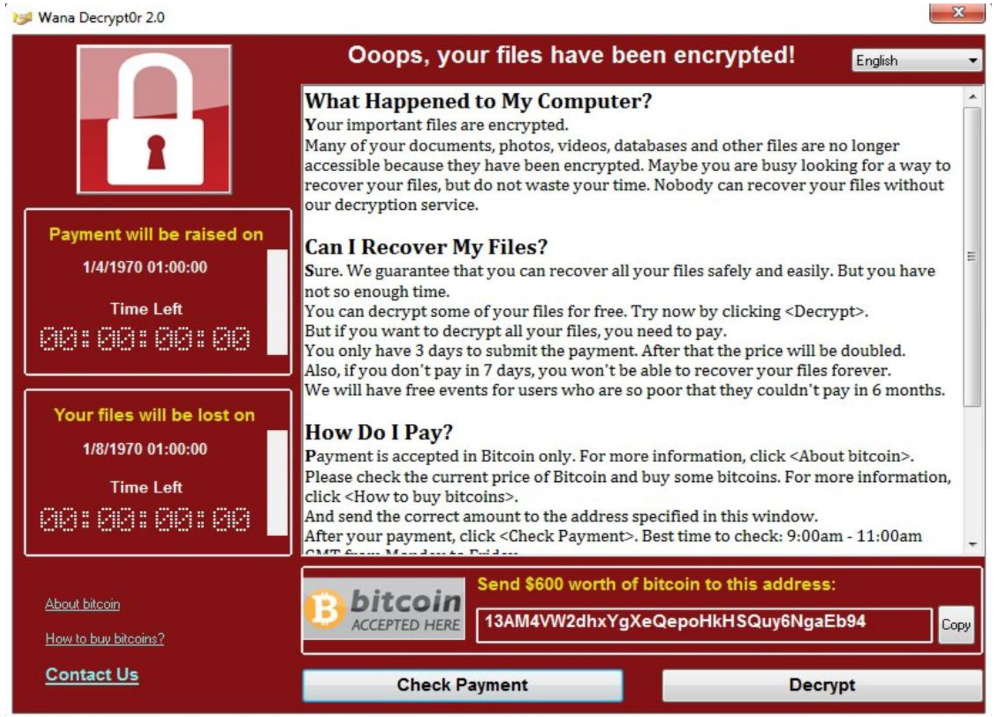
The Shadow Brokers
Fifth leak: "Lost in Translation‟ - April 14, 2017



Code Name	Solution
“EternalBlue”	Addressed by MS17-010
“EmeraldThread”	Addressed by MS10-061
“EternalChampion”	Addressed by CVE-2017-0146 & CVE-2017-0147
“ErraticGopher”	Addressed prior to the release of Windows Vista
“EsikmoRoll”	Addressed by MS14-068
“EternalRomance”	Addressed by MS17-010
“EducatedScholar”	Addressed by MS09-050
“EternalSynergy”	Addressed by MS17-010
“EclipsedWing”	Addressed by MS08-067

WannaCry

- First important outbreak of the year (thanks to TSB)
- One month after Microsft patched the SMB exploited vulnerability (MS17-010)
- 500+ affected IPs identified in RO (10 from public institutions)
- 5 incident reports at CERT-RO
- “Luckily” it had a kill-switch



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

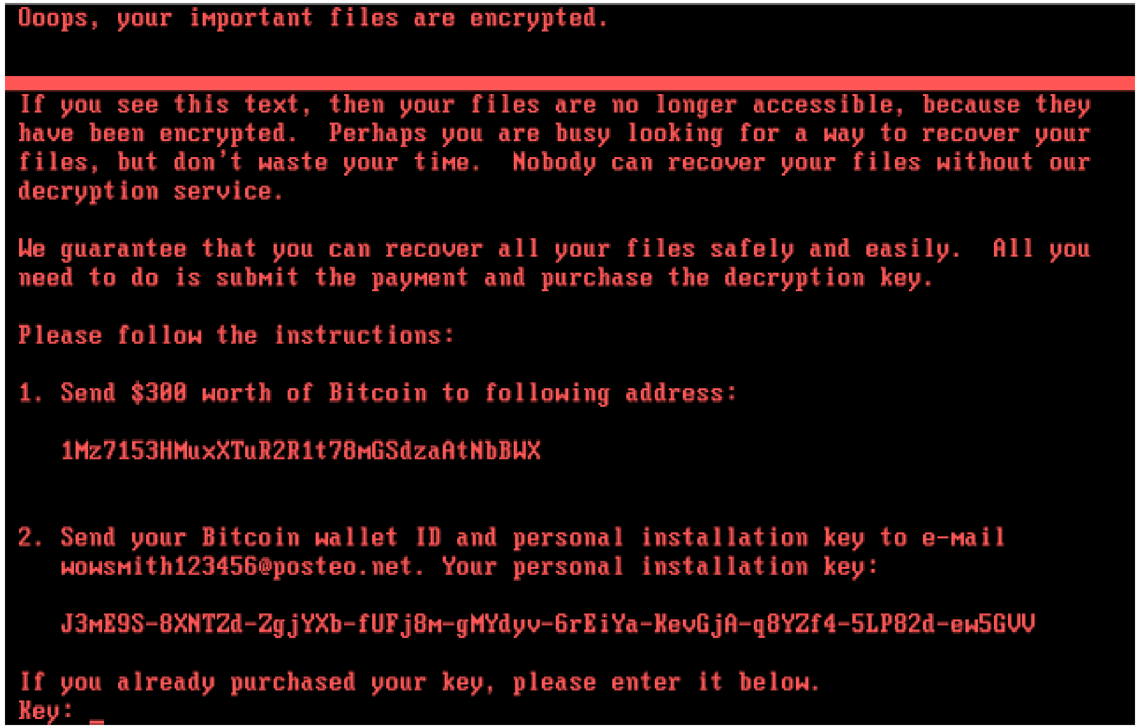
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

NotPetya

- Infection vector: software supply-chain (M.E.Doc)
- More wipeware than ransomware
- Not a single notification to CERT-RO
- We do know about victims in RO (from Facebook)
- Other ransomware campaigns hided under NotPetya wave (Karo)



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   J3mE9S-8XNT2d-ZgjYXb-fUFj8m-gMYdyv-6rEiYa-KevGjA-q8YZf4-5LP82d-ew5GVV

If you already purchased your key, please enter it below.
Key: _
```

How it really was?
WannaCry: Behind the scenes

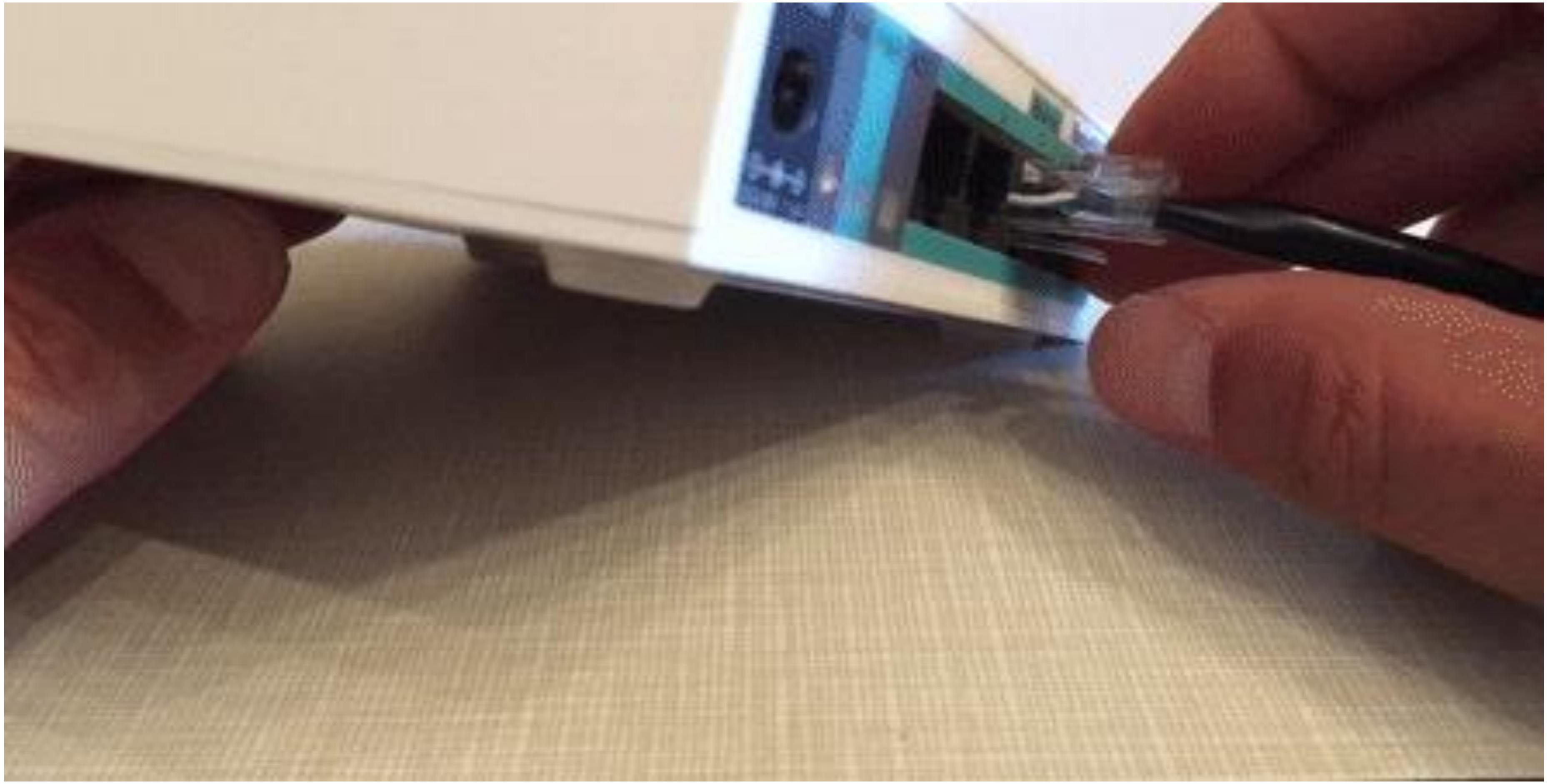
It’s Friday and WannaCry seems to be a big thing: we are deep into DENIAL stage

Everybody expects us to know it all already
So let’s write about it

Infection vector? It must be Spam

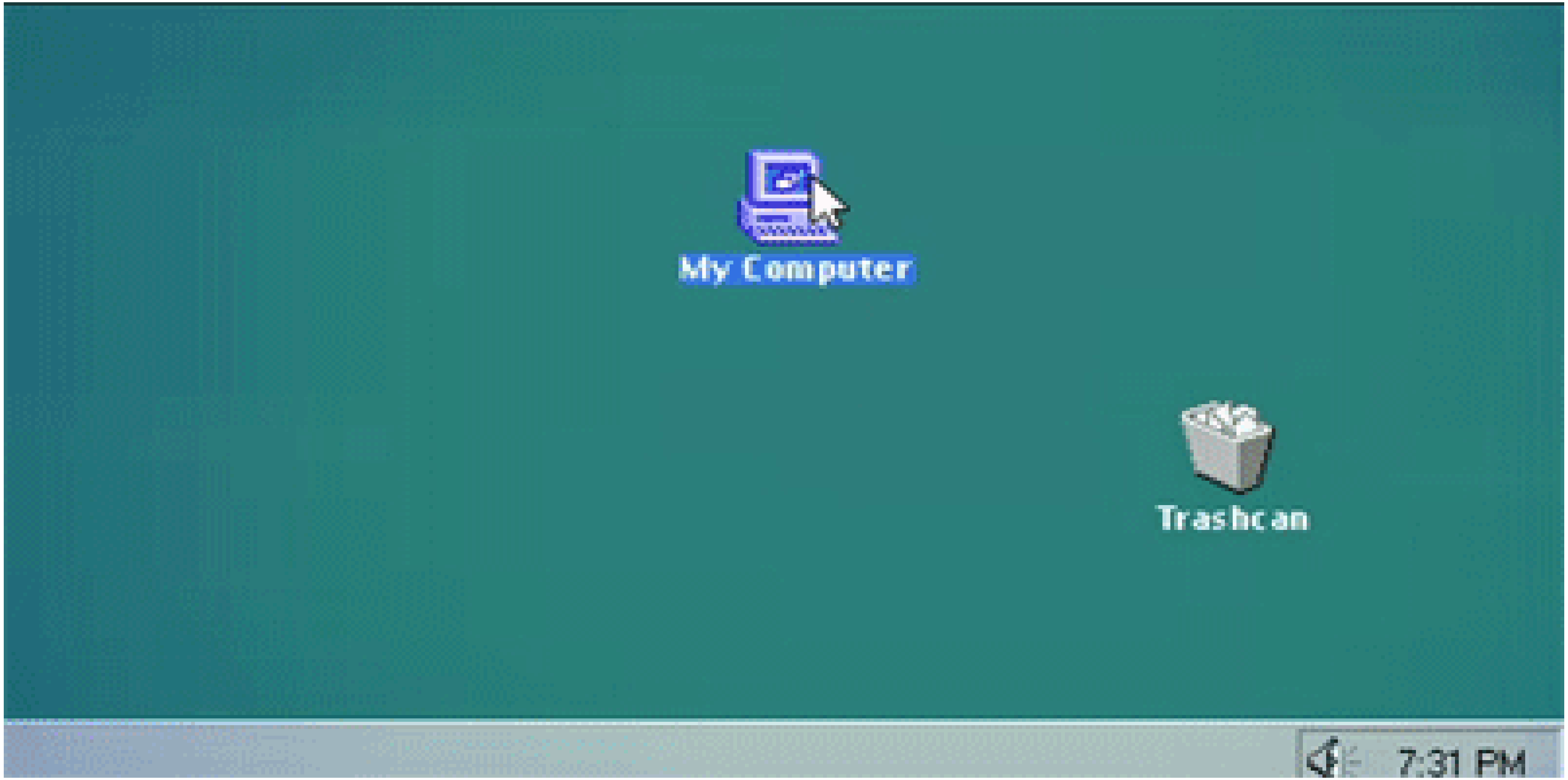
Question of the Friday (May 12) evening:
Who can share a sample of a Spam email with WannaCry?

What are the best response measures?
Disconnect machines from the network of course



Few ours later:
Ouch! It has a kill-switch which needs Internet connection

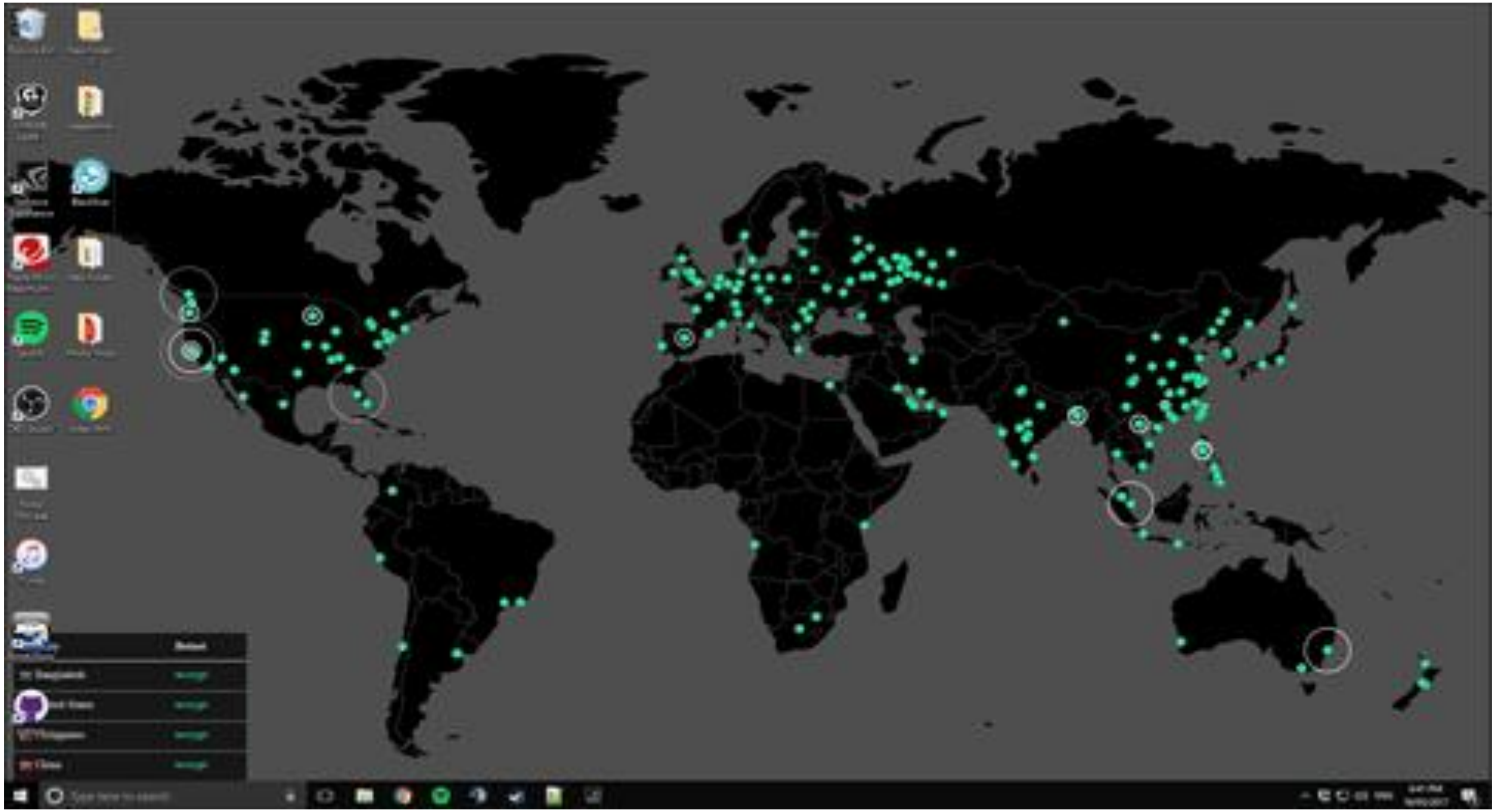
That was like …



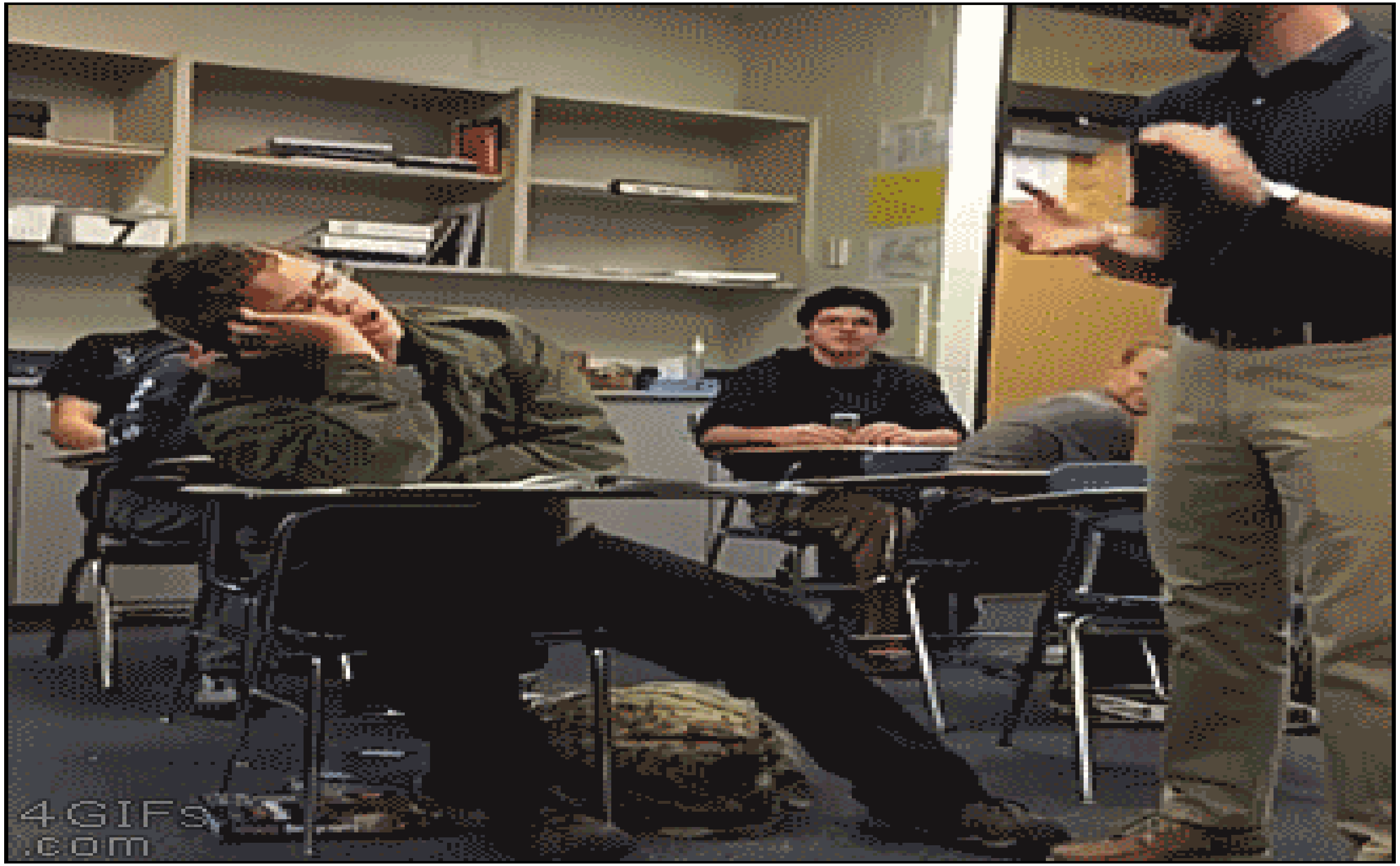
Questions for CERT-RO (especially from the media)

- How many victims are in Romania?
- Which public institutions are affected?
- Do you have any updates?
- You don’t know? Why?
- Everybody knows about a car manufacturer that was hit. How can you say you don’t know for sure?
- We know is Nord Korea. Can you please confirm? You can’t? Pfff …

And we are closely monitoring the situation
Big thanks to Marcus Hutchins



Let’s took advantage from media attention and do some awareness (again: UPDATES!)



And remember:
No good deed will remain unpunished

Questions?

CERT.RO

THANK YOU FOR YOUR TIME!

f @CERT.RO

@CERT_RO

in /certro

@cert.ro