Malwares, AV & my life

{ Case studies for malwares from what I have seen

About.me

- Name: Evan Huynh - @My2ndAngelic
- Applied Mathematics Program – First year
- Vietnamese, English, Swedish (beginner) + Japanese (beginner)
- Casual guy, do a lot of things
- Pascal, Java (learning)
- No experience AT ALL in security nor dev.
- Has to do a lot of cleanup and OS reinstallations
- Microsoft Office + Windows

Case 1: Autorun.inf

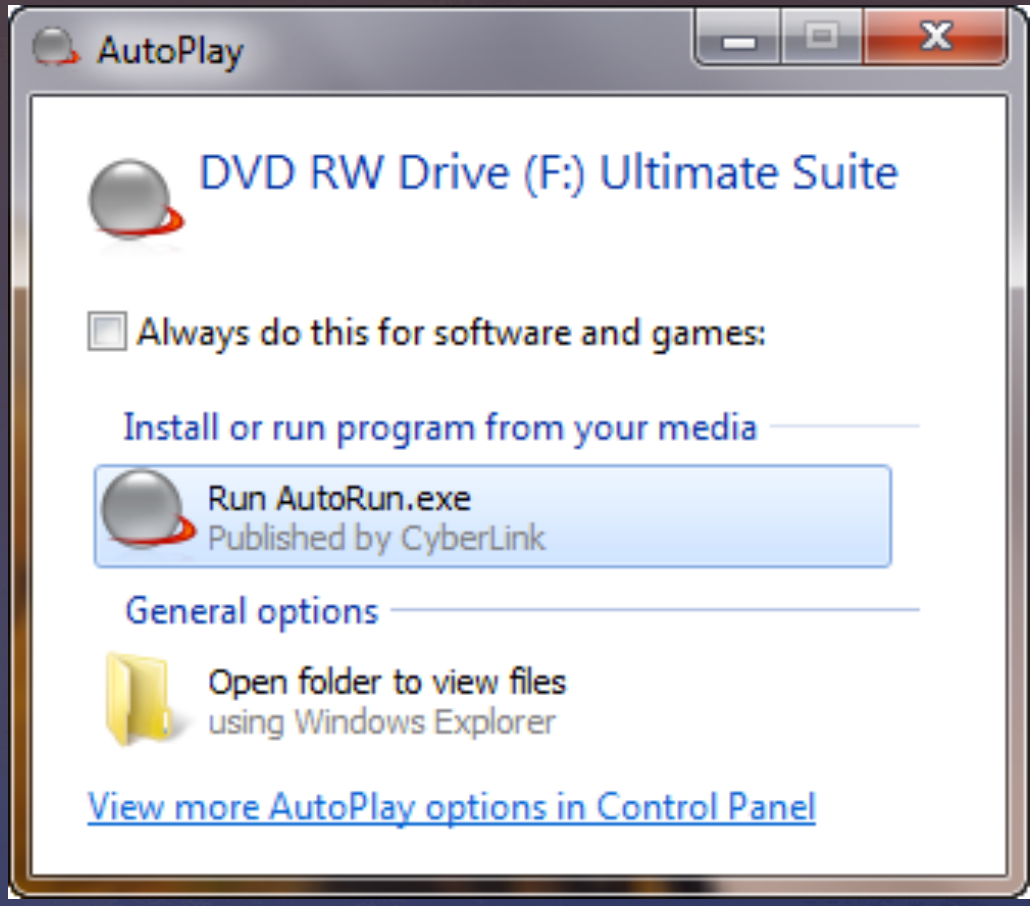
- A type of worm that infected via USB
- First appear in 2008 (?)
- Infecting using a legitimate tool in Windows (AutoPlay)
- Easy to write, easy to infect
- Personally, I encountered later than 2010.
- Really popular in Vietnam due to the widespread of Internet café. People go there and download stuffs.
- Annoyance: change disk icons, file attributions, some disallow showing hidden file and folders
- Utilize as a vector for infection
- Worm feature: infect other plugged-in USB

AutoPlay mechanism

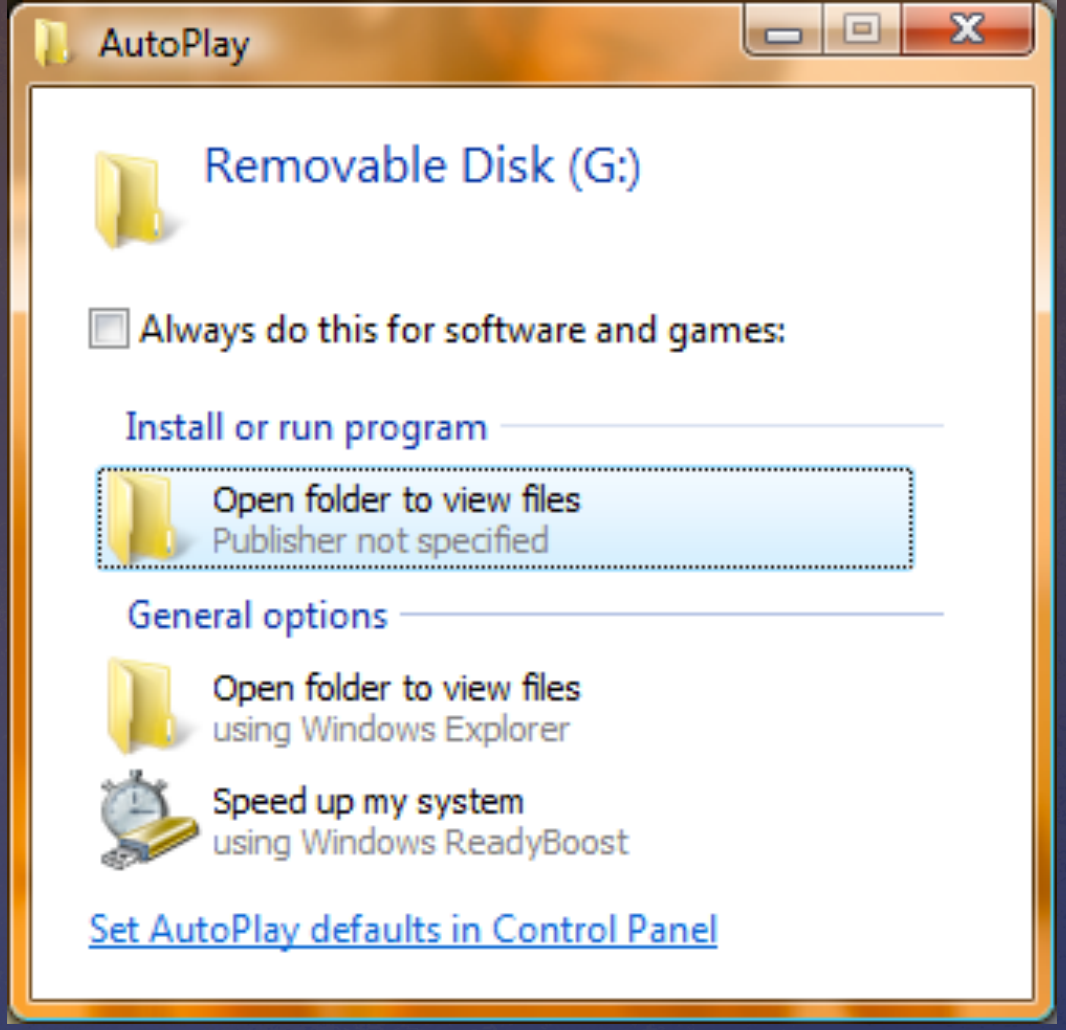
1. User insert media (software/game installation)
    1. Windows XP does not support removable media such as USB flash drive
    2. Windows Vista and later support this
2. Autorun.inf is read (automatically)
3. AutoPlay popup prompt what to do (?).
4. AutoRun do the action

[autorun]
open=AutoRun.exe
icon=AutoRun.exe,0
label=Run AutoRun.exe

Source: Autorun.inf – Wikipedia.



Example



Case 2: Conficker & Stuxnet

What does Conficker do?

- Botnet (it's also a worm)
- Microsoft offers $250,000 reward for information lead to the arrest of the worm author.
- It utilize a vector of infection using Autorun (and other CVE)
- It has been theorize for using a massive DDOS campaign, but that has never happened
- Also it does have AutoUpdate function

Ability to weaponize

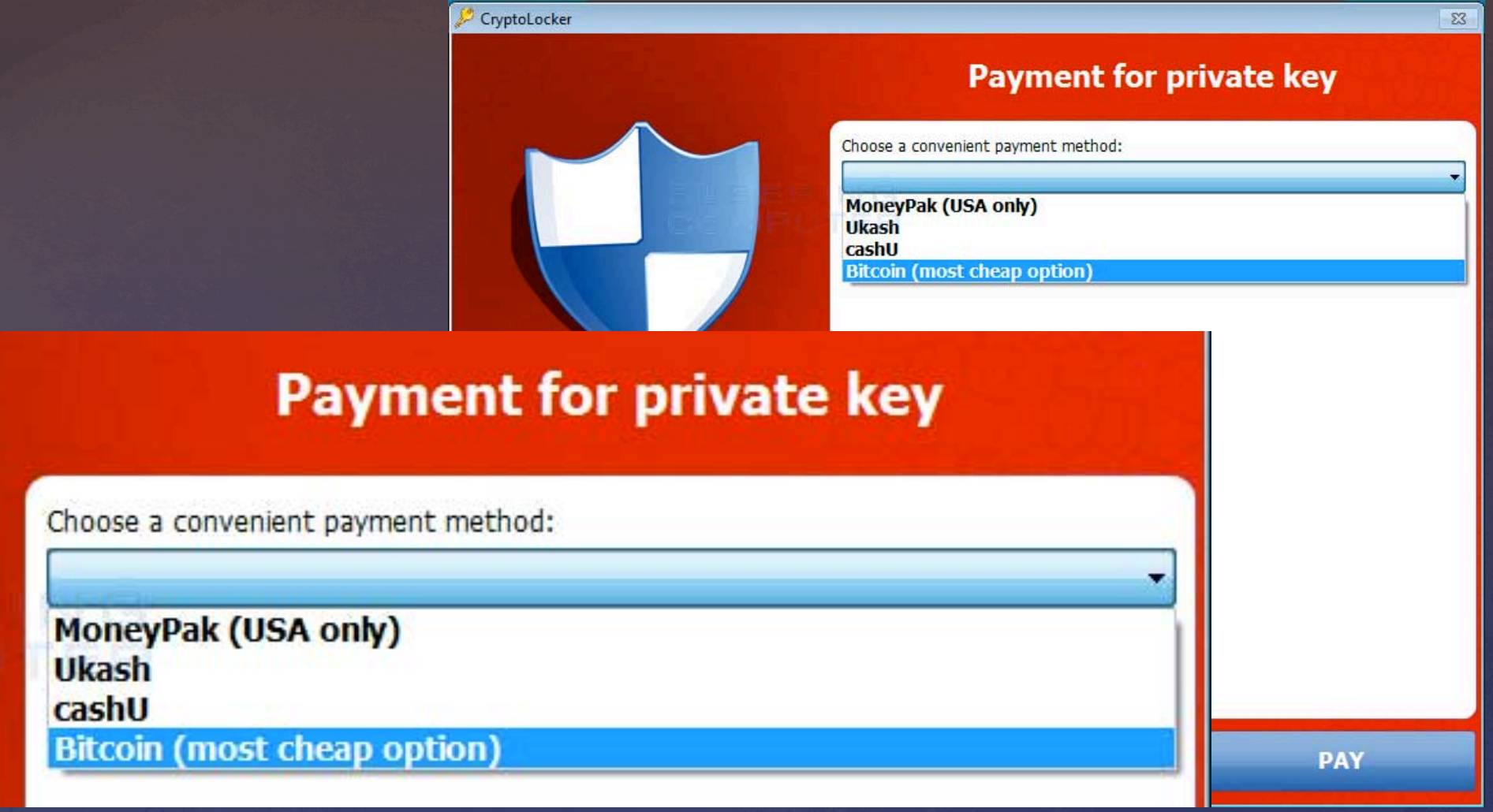
- Stuxnet incidence: again, using USB as a vector (and P2P)
- Specialized for embedded system
- Take over Iranian nuclear controller system (mainly Siemens Simatic PLC)

- Crypto + Malware = $$$

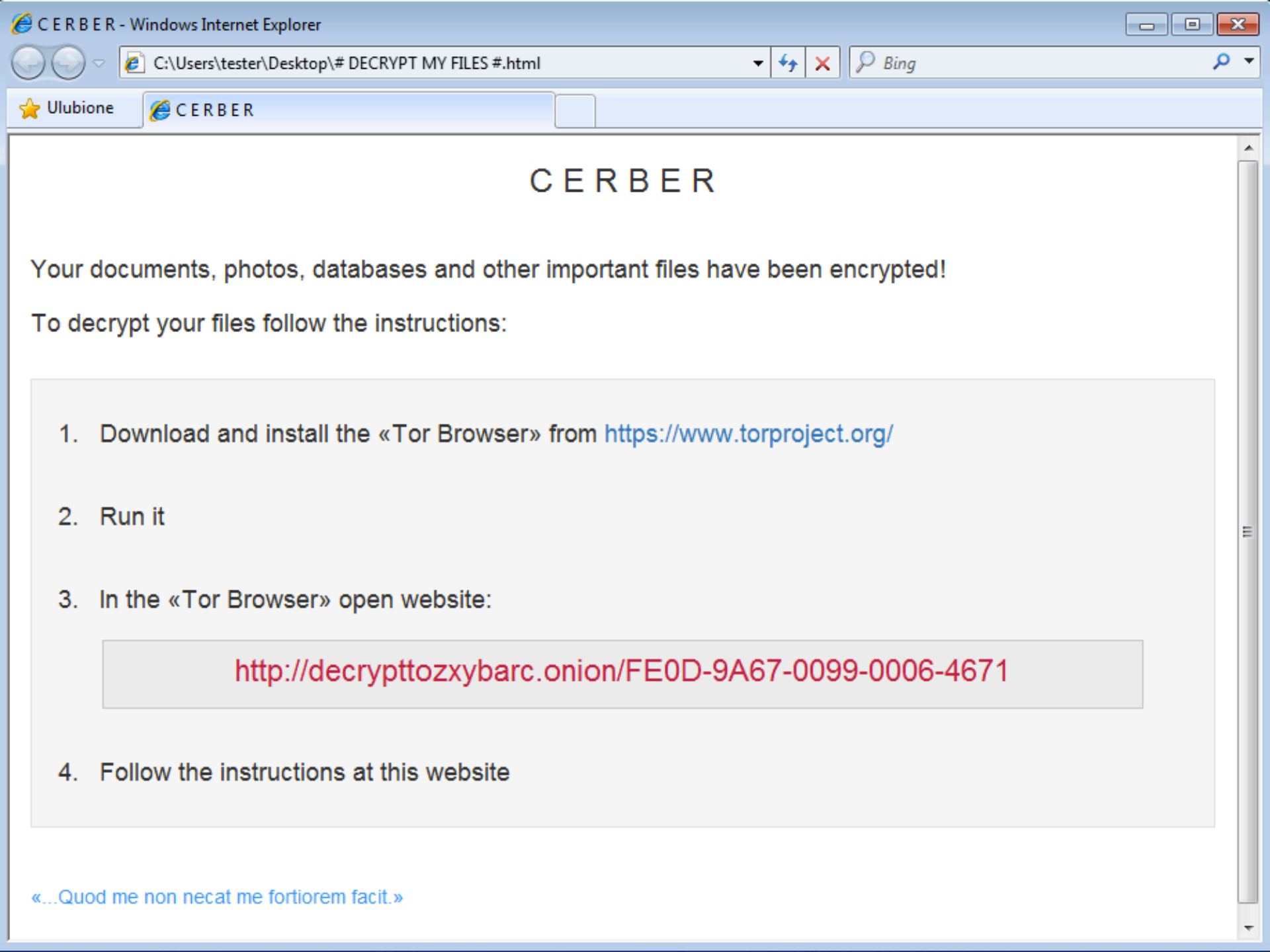
Case 2: Ransomware

1. Spam campaign/0-day exploit: ransomware ran on victims' computer
2. Generate ID/Password/Private key on victim's machine
3. Contact Command and Control (C&C) server for sending private key (can be done after encrypting)
4. Start encrypting files (according to provided list)
5. Ransom notes on victim's machine
6. Wait for money
7. Send decryption key/program if payment is received (most likely never)

Case 2: Ransomware



CryptoLocker


CERBER - Windows Internet Explorer
C:\Users\tester\Desktop\# DECRYPT MY FILES #.html
Bing
Ulubione
CERBER
CERBER
Your documents, photos, databases and other important files have been encrypted!
To decrypt your files follow the instructions:
1. Download and install the «Tor Browser» from https://www.torproject.org/
2. Run it
3. In the «Tor Browser» open website:
http://decrypttozxybarc.onion/FE0D-9A67-0099-0006-4671
4. Follow the instructions at this website
«...Quod me non necat me fortiorem facit.»


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

- Link: https://www.youtube.com/watch?v=IEAtGCkbq5Y

WannaCry heatmap

WannaCry

- First ransomware equipped with worm functionality, spreading quickly via SMB using EternalBlue & DoublePulsar exploit kit by the NSA.
- Affect over 150 countries

Not so good news

- NSA exploits, exploits and exploits are still a great vector to attack networks
- Everything-as-a-service: from software to infrastructure to ransomware

Current state

- What timeline are we on?
- Ransomware as a service
- Malware criminals operate like legitimate businesses, even better support than the legitimate one
- Threats and exploits everyday
- Flash & Java (seriously)

Read more

- Wikipedia about those malwares
- YT channel: Tom Scott, Computerphile, TPSC, danooct1, Colin Hardy, quidsup
- Tw: @malwarehunterteam, @MalwareTechBlog, @Malwarebytes
- Trusted sources: Bleeping Computer, Malwarebytes Blog, Naked Security (Sophos), Krebs on Security, SecureList (Kaspersky), TheHackerNews, WeLiveSecurity (ESET), EMSISoft blog

Prediction for the future

- Weaponized-ransomware? (Stuxnet + WannaCry)
- DDOS could take down the global internet
- More sophisticated threats
  - AV turns against us by zero-day attacks
  - Bootkit ransomwares (also on BIOS/UEFI)
  - Malware-free attacks
- Education: public awareness

- Do you want?
- Demo: Autorun.inf, HiddenTear, KeRanger (?)
- WannaCry disassembling
- Due to (whatever) reasons, I cannot get all the malware samples that I have been talking today. Please let me apologize for that.

Demonstration time

Bibliography

- Some random images from Google
- Malware samples: some random source
- Reading Wikipedia, Malwarebytes blog, TheHackerNews
- Sample credit: theZoo, VirusTotal, contagio
- All YouTubers for great videos regarding this
- BitCoin chart price by blockchain.info
- Autorun mechanism provided by MSDN

Bibliography

- Screenshot source:
  - AutoPlay: Wikipedia & CyberLink
  - CryptoLocker: BleepingComputer
  - Cerber: Malwarebytes Labs
  - WannaCry: Malwarebytes, Wikipedia