

WANNACRY DISSECTED

An in-depth analysis of the malware outbreak

\$ whoami

Daniele Ferla

Got Master's degree in Computer Engineering @
University of Bologna

Research Fellow @ CIRI ICT

Passionate about **reverse engineering, binary
exploitation** and **low-level stuff**

Tool fan!



daniele.ferla@unibo.it

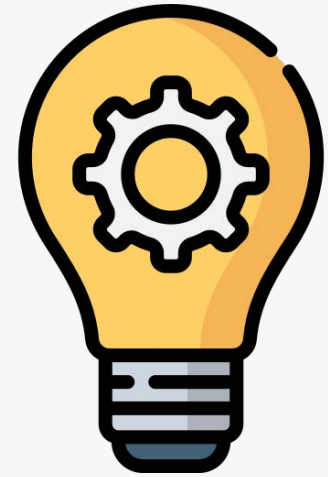


[danieleferla](https://t.me/danieleferla)

BEFORE ACTUALLY STARTING...

Types of malware (a few)

- **Virus:** self-replicating, requires user interaction
- **Worm:** self-replicating, replicates automatically exploiting vulnerabilities in software
- **Backdoor:** component purposely injected in legit software to allow remote access
- **Exploit:** leverages on program vulnerabilities in order to execute arbitrary computations
- **Trojan:** non-replicating, pretends to be legit software
- **Spyware:** tracks user activity
- **Adware:** injects custom advertising while the user is browsing the Internet
- **Rootkit:** hides itself from the operating system, very difficult to detect and remove
- **Bot:** infected hosts become part of a botnet; they are remotely controlled to perform specific actions (e.g. send spam emails, connect to a host, etc.)
- **Ransomware:** encrypts all the data on a computer, requesting a ransom (most likely in BTC) to let the user have its data back



Those features
are often
combined

BEFORE ACTUALLY STARTING...

Malware analysis jargon

- **C&C, or C2 (Command-and-control):** server used by attackers to send commands to the infected hosts
- **DDoS (Distributed Denial of Service):** an attack that aims to disrupt the correct functioning of a system, overwhelming it with an excessive amount of requests coming from a large number of hosts (botnet)
- **APT (Advanced Persistent Threat):** consists in penetrating strategic systems and install malware that remains active for large periods of time (most often with the aim of exfiltrating valuable data)
- **IoC (Indicator of Compromise):** any kind of data that can signal the presence of a malware within the network (IP addresses, domains, hashes of malware files and other artifacts)
- ...



What is it?



What is it?

Wannacry is a malware that can be logically distinguished in **two parts**:

1. **Worm**: automatically replicates itself in all the vulnerable hosts within the same network. It uses an **exploit** that leverages on a vulnerability on the SMB (Server Message Block) protocol in unpatched Windows hosts.
2. **Ransomware**: encrypts 175 file extensions and requests the equivalent of 300\$ in BTC.
 - If the payment is not issued in 3 days, the ransom goes to 600\$.
 - If in 7 days it has not been paid, all the encrypted files are lost.



A series of unfortunate events

- The NSA (National Security Agency), found a **bug** in the **SMB** protocol implemented in Windows
- They developed an exploit to trigger the vulnerability and gain **RCE** (Remote Code Execution) on target hosts.
This exploit was called **EternalBlue**.
- While the exploit was used for more than 5 year (before 2017), **NSA did not notify the issue to Microsoft**.




References: https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html

A series of unfortunate events

- The **Shadow Brokers** is a hacker group appeared for the first time in 2016.
- Main objective: **leak exploits** and other tools that targeted firewall, antivirus software and Microsoft products.
- 14 Apr 2017: in their fifth leak, **they release the EternalBlue tool** (among with others), subtracted from the NSA.

References: <https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation>

Lost in Translation

 theshadowbrokers (60) in shadowbrokers • 3 anni fa

KEK...last week theshadowbrokers be trying to help peoples. This week theshadowbrokers be thinking f●k peoples. Any other peoples be having same problem? So this week is being about money. TheShadowBrokers showing you cards theshadowbrokers wanting you to be seeing. Sometime peoples not being target audience. Follow the links for new dumps. Windows. Swift. Oddjob. Oh you thought that was it? Some of you peoples is needing reading comprehension.

https://yadi.sk/d/NJqzpqo_3GxZA4

Password = ReeEEEEEEEEEEEEEE

theshadowbrokers not wanting going there. Is being too bad nobody deciding to be paying theshadowbrokers for just to shutup and going away. ShadowBrokers rather being getting drunk with McAfee on desert during WWII theshadowbrokers

A series of unfortunate events

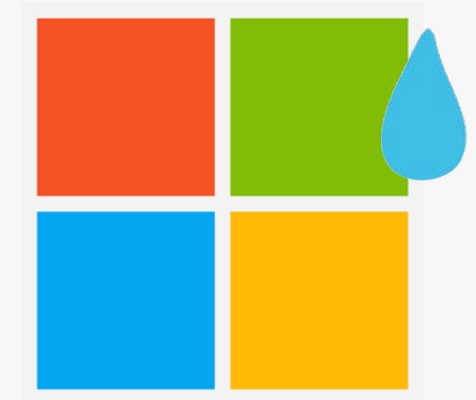
- Months before the leak, the NSA warned Microsoft after learning about EternalBlue's possible theft
- Microsoft issues a patch for the vulnerability of March 14, 2017

Doing the math, the patch was released one month before the leak.
What could possibly go wrong?



A series of unfortunate events

- The patch was released for **supported operating systems only** (from Windows 7 on), while a considerable number of hosts was still running Windows XP
- Applying security patches in the whole IT infrastructure is often **overlooked**, even in big companies



A series of unfortunate events

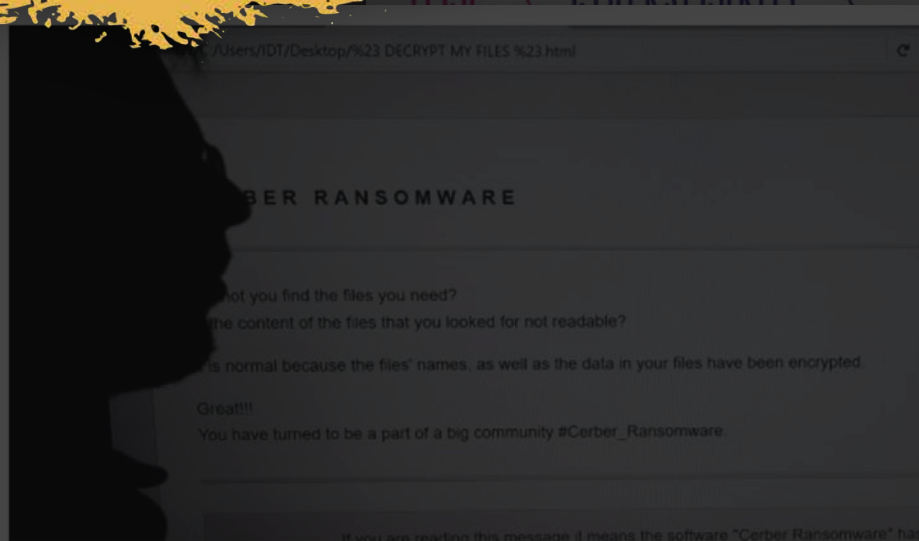
- Cybercriminals developed a ransomware that embeds the EternalBlue exploit, giving the malware the **ability to self-replicate without user intervention**.
- The North Korean **Lazarus Group** is suspected to be the main actor. Researchers found similarities between Wannacry's code and other malware previously used by the group.

References: <https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group>

	
WANTED BY THE FBI	
PARK JIN HYOK	
Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)	
	
DESCRIPTION	
Aliases: Pak Jin Hek, Jin Hyok Park	
Place of Birth: Democratic People's Republic of Korea (North Korea)	Hair: Black
Eyes: Brown	Sex: Male
Race: Asian	Languages: English, Korean
REMARKS	
Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.	
CAUTION	
Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.	
Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company - Chosun Expo Joint Venture, also known as Korea Expo Joint Venture - was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).	
If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.	
Field Office: Los Angeles	

WannaCry: hackers withdraw £108,000 of bitcoin ransom

Consequences were **catastrophic**



By Russell Brandom | May 12, 2017, 11:36am EDT

How malware can be analysed

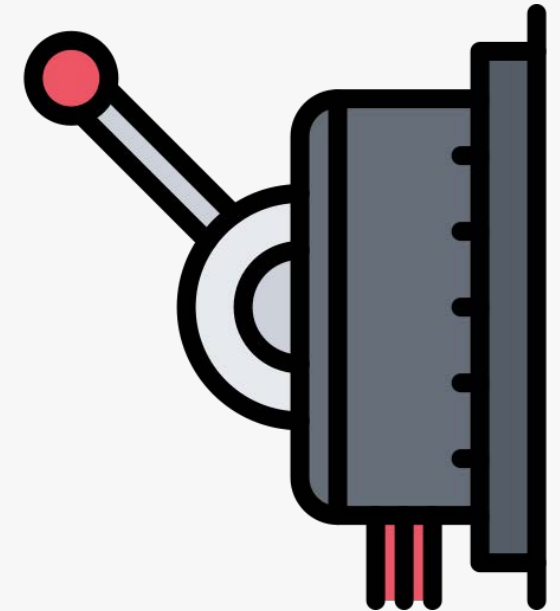
- Malware analysts have to use **reverse engineering** techniques to figure out what does the malware do.
- Reverse engineering can take place using **two different approaches**:
 - **Static analysis**: malware code is analysed without being executed. If malware is a binary program, disassemblers and decompilers can be used to obtain a higher level representation of what the program does.
 - **Dynamic analysis**: malware is executed in a protected environment (Virtual Machine or sandbox). Behaviour is inferred by looking at how the malware interacts with the environment (system/library calls, modified files, network activity, etc.)



IDA Pro, Ghidra and
Cuckoo sandbox are
commonly used tools

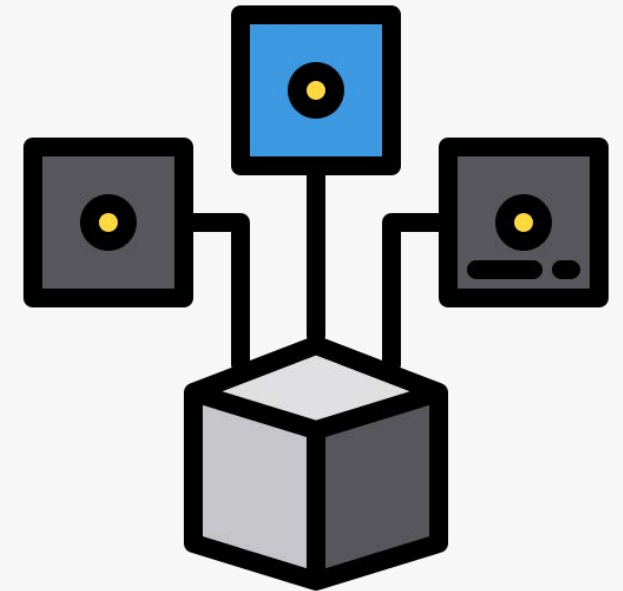
Startup

- The very first action performed by the malware is trying to connect to the following domain:
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
 - If the connection succeeds, the malware exits
 - Otherwise, it continues its execution
- This is a **kill switch**: if attackers wanted to avoid the malware to further spread itself on the Internet, they had to register that domain.
- A security researcher [discovered](#) this behaviour and registered the domain, preventing further infections.
- After three variants of Wannacry, with three different kill switch domains, another [variant without kill switch](#) began to spread.



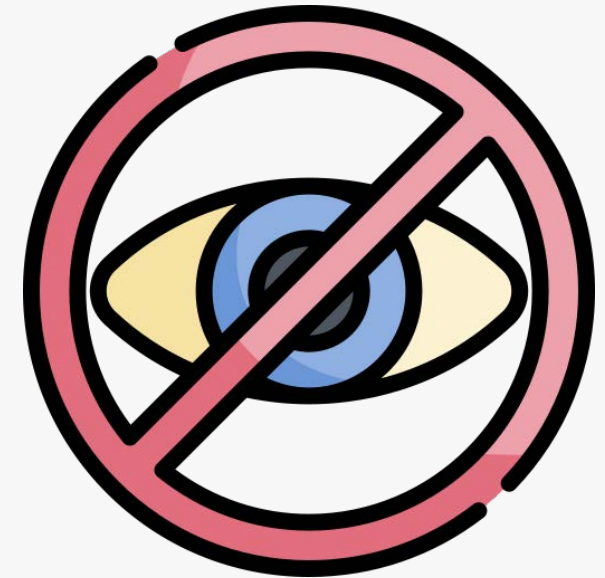
Spreading across the network

- WannaCry spawns several threads, with the aim of **enumerating** network interfaces and all the other reachable hosts in the network.
- **A thread for each IP** in the subnet is created. Each of which tries to connect to **port 445**, where the SMB service listens to.
- **SMB (Server Message Block)** is a protocol designed to share files and printers over the network. SMBv1 is the outdated version, vulnerable to EternalBlue.
- If the connection succeeds, the exploit is launched and the remote host is infected.



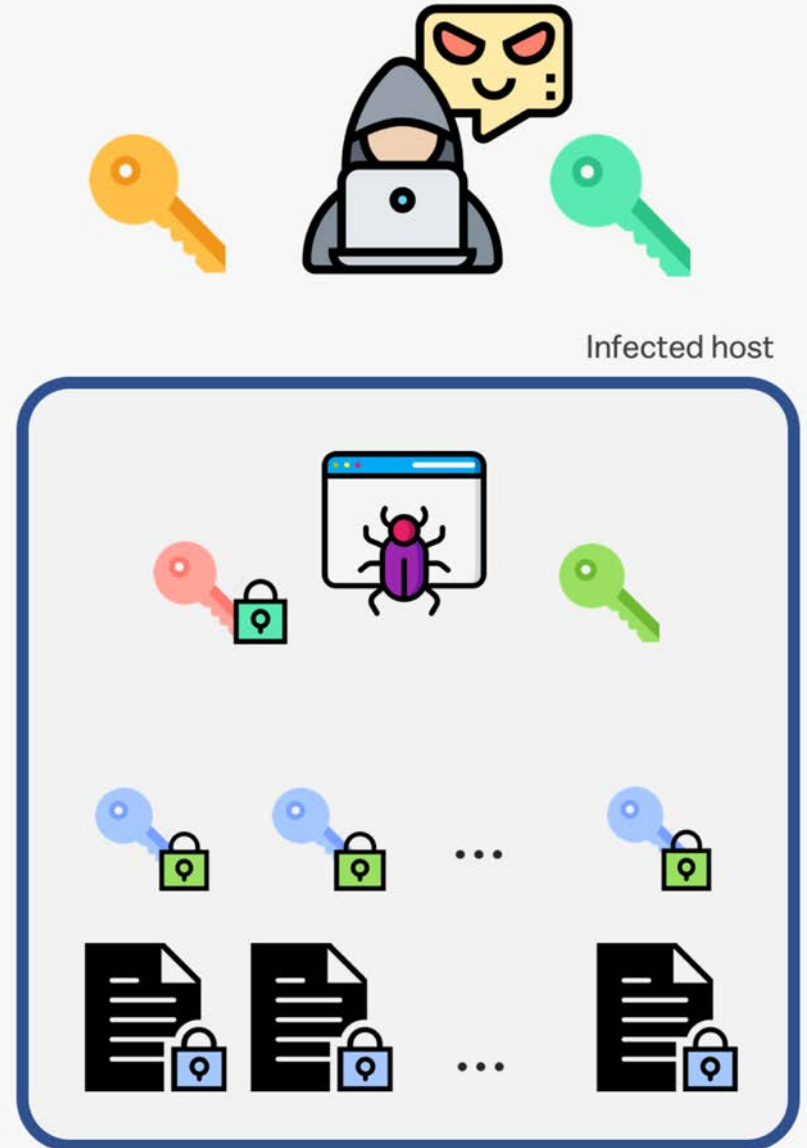
Settling down

- WannaCry obtains **persistence**: it creates a new service (named `mssecsvc2.0`), copies itself in `C:\Windows` and writes in the Windows Registry to be launched at every startup.
- Hides its files, assigning them the “hidden” attribute (same as adding “.” at the beginning of the file name on *nix systems).
- Obtains all the privileges for all its subdirectories.
- A thread scans every 3 seconds if a new drive has been plugged in. In that case, it tries to infect it as well.



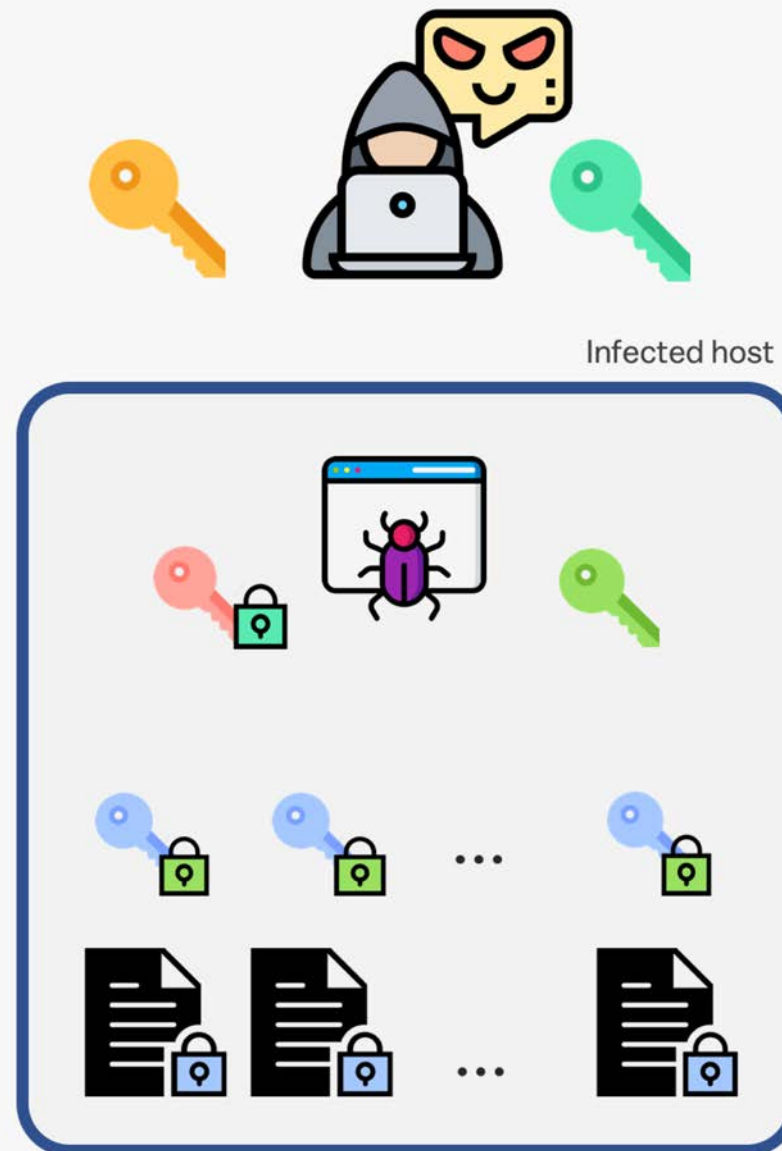
Encryption scheme

- WannaCry generates a new 128-bit **AES key** for **each file**, so that all the files are encrypted with a different key. The encryption uses CBC mode, with NULL initialisation vector.
- It generates a 2048-bit **RSA key pair** for the **infected host**. Then encrypts all the AES keys with **the host public key**.
- Finally, the **host private key** is encrypted with the **attacker's public key**, which comes embedded in the malware



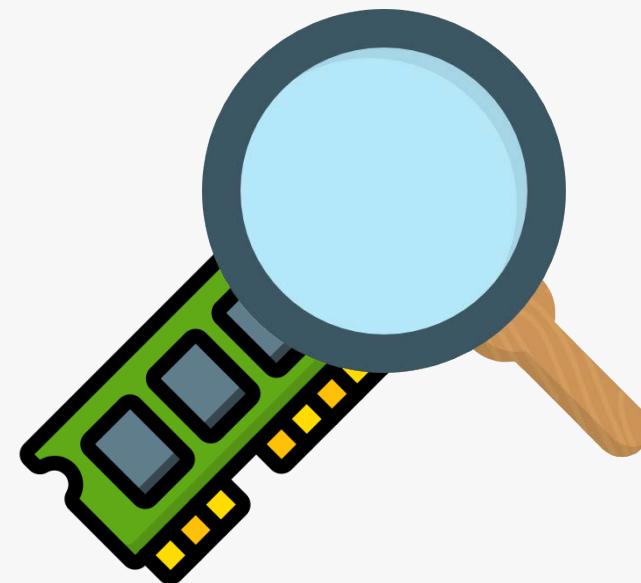
Encryption scheme

- To decrypt all the data, WannaCry sends the **encrypted host private key** to the attacker's C&C server via covert channel (TOR)
- The user also sends the unique ID of his Bitcoin wallet, in order to let the attackers identify his payment.
- If the payment is confirmed, the attackers return the **decrypted host private key**.



Recovering the keys

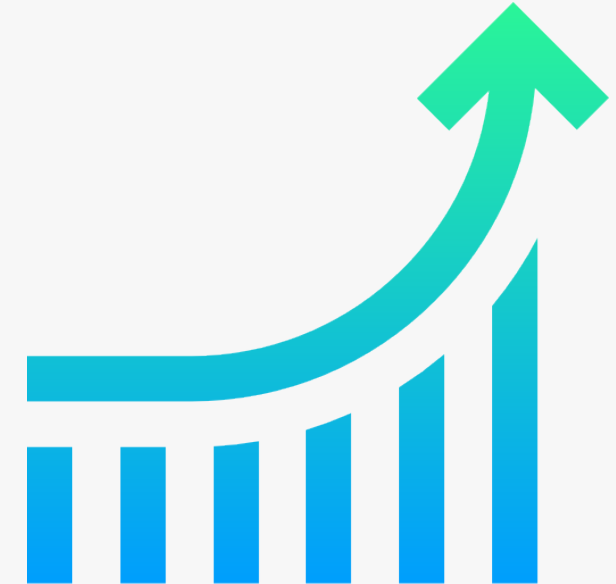
- To implement Wannacry's cryptographic features, the attackers took advantage of the **Crypto API** available on Windows systems.
Right choice for them: never do your own crypto!
- However, researchers discovered that, on Windows XP and 7, that two of the exposed functions were flawed: CryptReleaseContext and CryptDestroyKeys freed memory where the prime numbers were stored, **without properly erasing it**.
- If the infected host hasn't been rebooted, it is possible to recover the prime numbers from memory using a [tool](#).



References: <https://blog.comae.io/wannacry-decrypting-files-with-wanakiwi-demo-86bafb81112d>

What happened next?

- There were roughly **300.000 infected computers**
- Economic losses due to the attack: about **\$4 billion**
- How much money did the attackers make?
 - Bitcoin is a pseudo-anonymous payment network
 - Using data from [blockchain.com](https://www.blockchain.com) it is possible to figure out how much money was sent to the three wallets attributed to WannaCry attackers
 - These wallets received a total of 54,38 BTC == 500.000 \$



References:

<https://www.blockchain.com/btc/address/13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94>,
<https://www.blockchain.com/btc/address/115p7UMMngo1pMvkhHjcRdfJNXj6LrLn>,
<https://www.blockchain.com/btc/address/12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw>

Conclusion

- Ransomware are becoming a trend
- When coupled with powerful exploits, they can cause excessive damage
- The most effective solutions are prevention measures:
 - always backup data
 - apply the latest software updates as soon as it is possible