WannaCry

the worldwide cyberattack

MARIA-ELENA LIVITCHI
individual assessment in Confident Project

Mind map:

Topics Covered

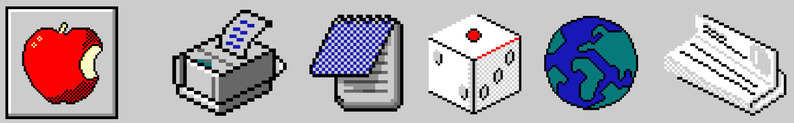
- what is **WannaCry**?
- the affected **information** resource
- the **modus operandi** of the threat
- threat **actors**
- related **protection** measures

Start

WannaCry -

the worldwide cyberattack

The WannaCry **ransomware attack** was a worldwide cyberattack in May 2017 by the WannaCry ransomware cryptoworm, which **targeted computers running the Microsoft Windows** operating system by **encrypting data** and **demanding ransom payments in the Bitcoin** cryptocurrency.




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

the modus operandi of WannaCry ransomware

WannaCry **spreads via a flaw** in the Microsoft Windows implementation of the Server Message Block (**SMB**) protocol. The SMB protocol helps various nodes on a network communicate, and an unpatched version of Microsoft's implementation could be tricked by **specially crafted packets into executing arbitrary code, an exploit known as EternalBlue**.

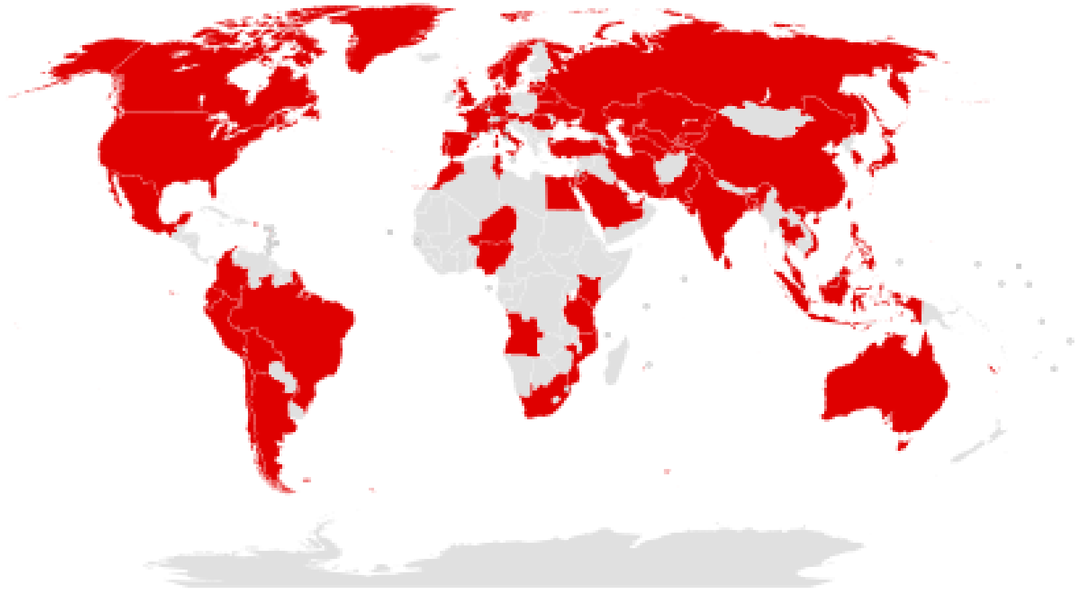
The WannaCry threat actors:

The security firm Symantec believed that the code behind this malware might have a **North Korean origin**.

They believe that the **Lazarus Group** are the culprits behind WannaCry, a hacking group that has been tied to North Korea.

The WannaCry cyberattack impact:

Approximately 190,000 computers in **over 150 countries** have been affected. **European Critical infrastructure operators** (health, energy, transport, finance and telecoms), **manufacturers and service providers** have been affected.



According to Kaspersky Lab, the four most affected countries were Russia, Ukraine, India and Taiwan.

How was WannaCry ransomware attack stopped?

A **kill switch** for WannaCry was discovered by the British security researcher **Marcus Hutchins**, who inadvertently **stopped the attack by registering a web domain found in the malware's code**.

Kill switch - a computer function for disabling software or a device remotely. If it received a response from the domain, it shut down. If not, it continued to work. So when Marcus Hutchins (known also as MalwareTech) registered the domain, it effectively activated the kill switch.

Protection

proactive measures

- ensure that your **operating systems**, regardless of their cost or developers, are **updated** to the **latest security patches**
- use the latest version of the operating systems
- regularly carry out **backups of important data** and **store** them in a safe and secure manner, **independent of the machine** from which the data is being backed up
- also ensure that you **do not open** any suspicious emails or **files from physical and network** mediums, erring on the side of caution.

Protection

reactive measures

- people who are using machines at the risk of infection, especially unsupported operating systems (like Windows XP), should **download the special patch issued by Microsoft** to close the vulnerability that enable the attack and **backup any important files** as well
- Victims who are already infected by the attack should **contact a security agency or developer immediately** and investigate means to recover the data while putting into place back up computers to carry out critical tasks while data recovery can take place.

The only real, long term solution, however, remains **increasing education around security best practices** and ensuring operating systems are patched frequently by end users.

Back to Agenda Page

WEB bibliography:

- https://www.**enisa**.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level
- https://en.**wikipedia**.org/wiki/WannaCry_ransomware_attack
- https://www.**kaspersky**.com/resource-center/threats/ransomware-wannacry