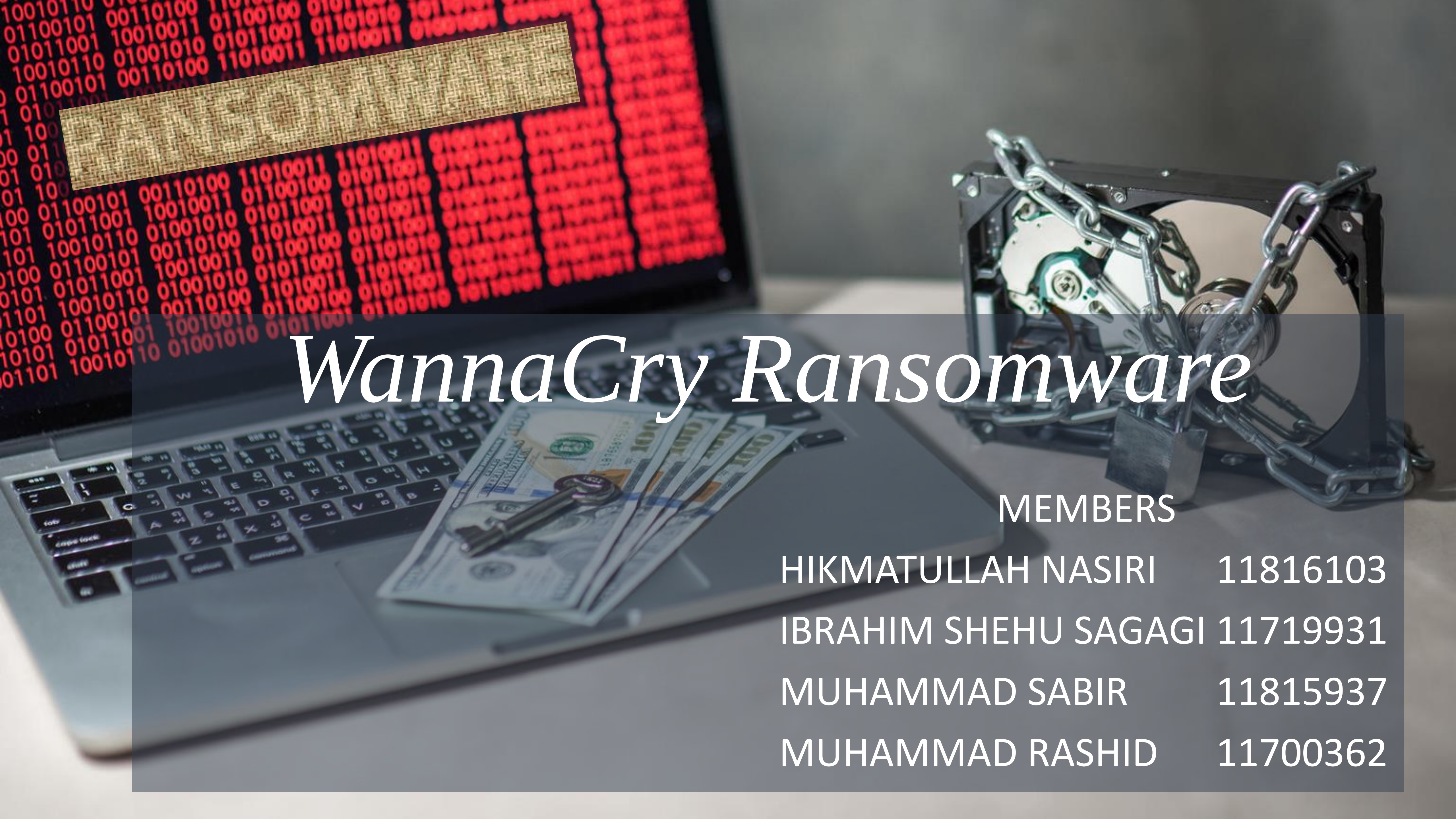


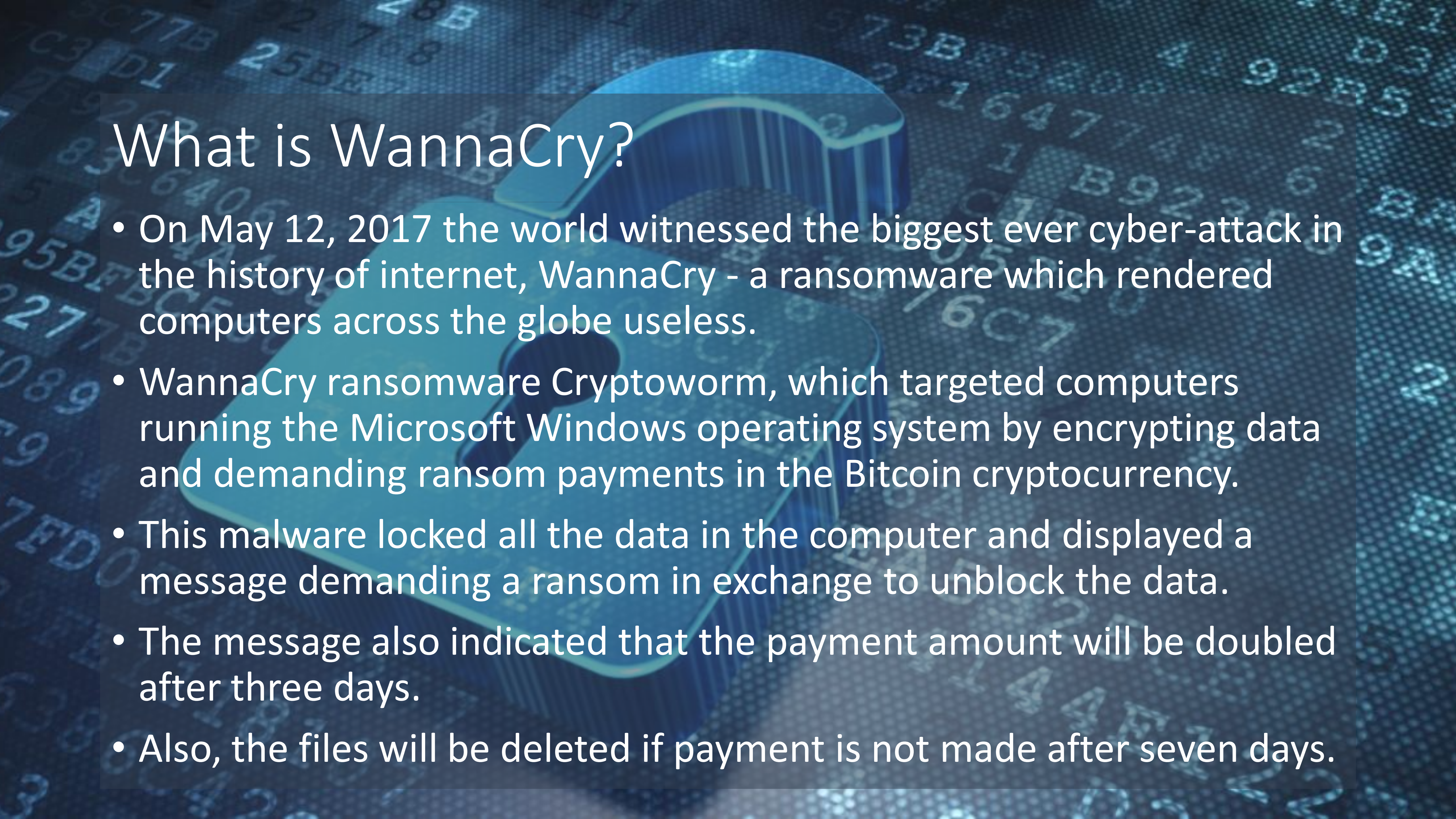
WannaCry Ransomware

MEMBERS

HIKMATULLAH NASIRI	11816103
IBRAHIM SHEHU SAGAGI	11719931
MUHAMMAD SABIR	11815937
MUHAMMAD RASHID	11700362

What is Ransomware?

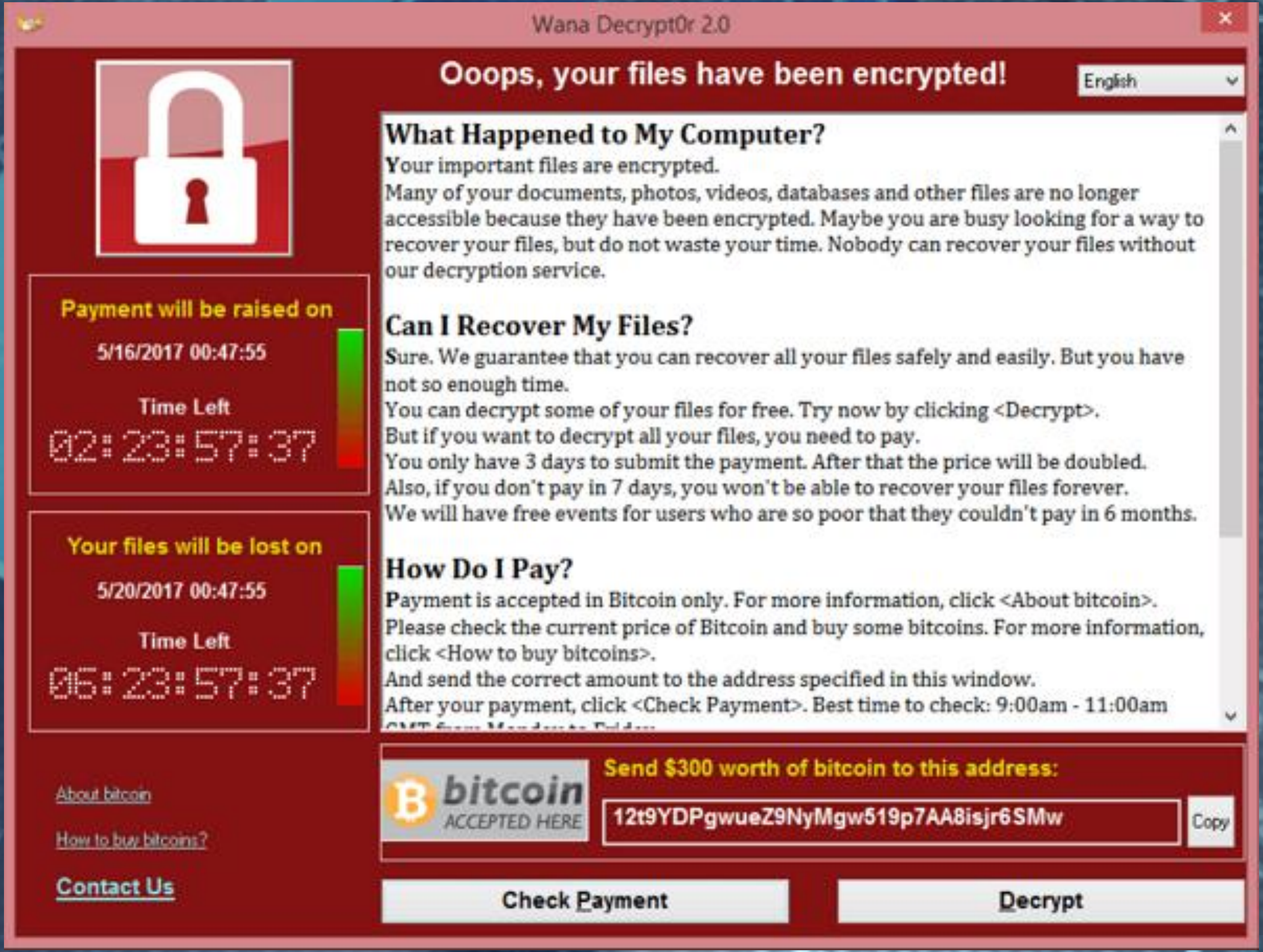
- Ransom malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
- Encrypts all data in a computer and blocks access to them
- Often, this malware masquerades as an innocent email attachment or a legitimate website link conning users to open it
- Once this malicious file is opened, it attacks the hard drive and encrypts all the files.
- A ransom is demanded for decrypting the files and if the user doesn't oblige, the files will be deleted.



What is WannaCry?

- On May 12, 2017 the world witnessed the biggest ever cyber-attack in the history of internet, WannaCry - a ransomware which rendered computers across the globe useless.
- WannaCry ransomware Cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency.
- This malware locked all the data in the computer and displayed a message demanding a ransom in exchange to unblock the data.
- The message also indicated that the payment amount will be doubled after three days.
- Also, the files will be deleted if payment is not made after seven days.

A Screenshot of the ransom note left on an infected system



Ooops, your files have been encrypted!

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

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?

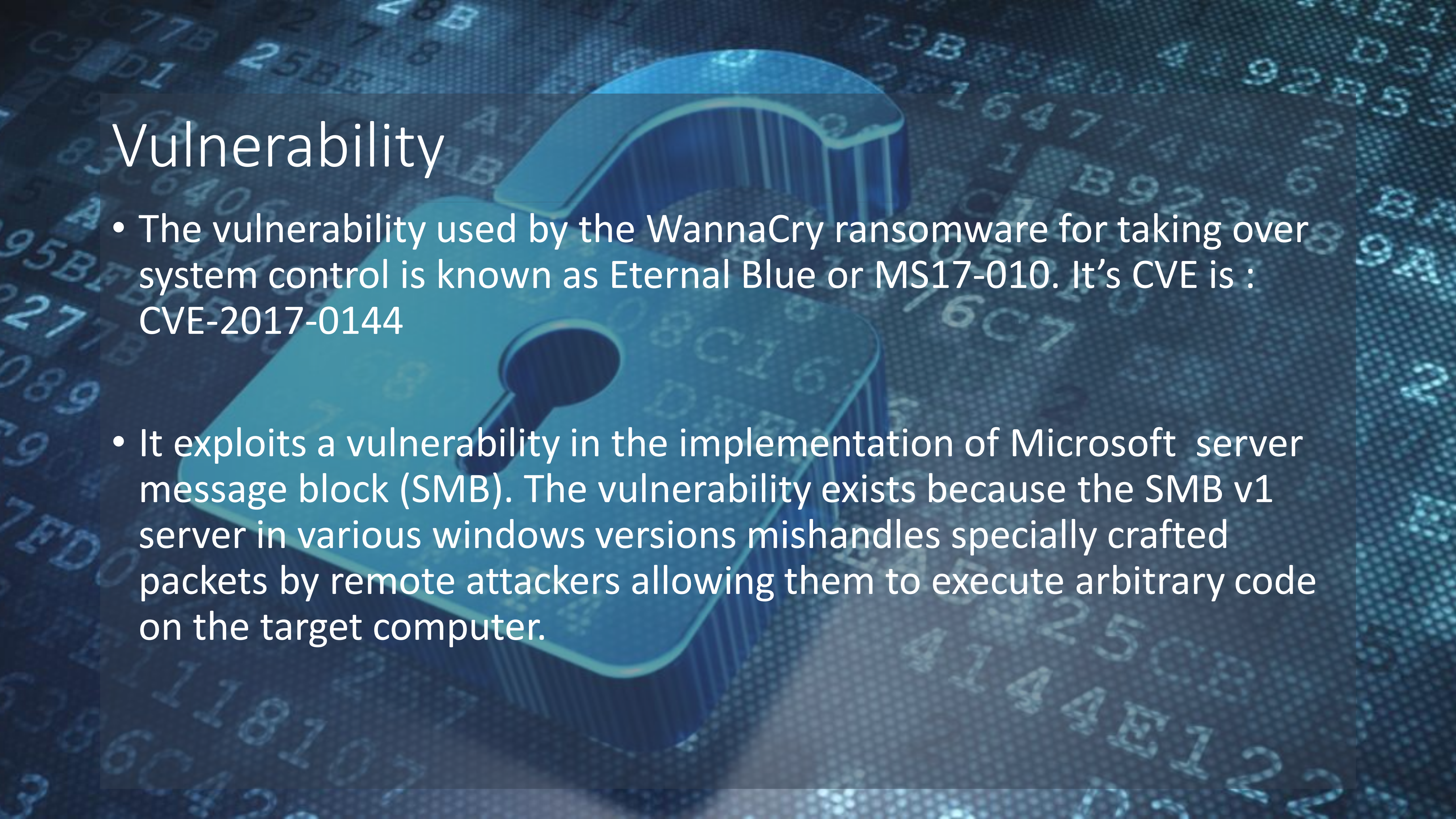
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>.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

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

How much was demanded? Why in bitcoins?

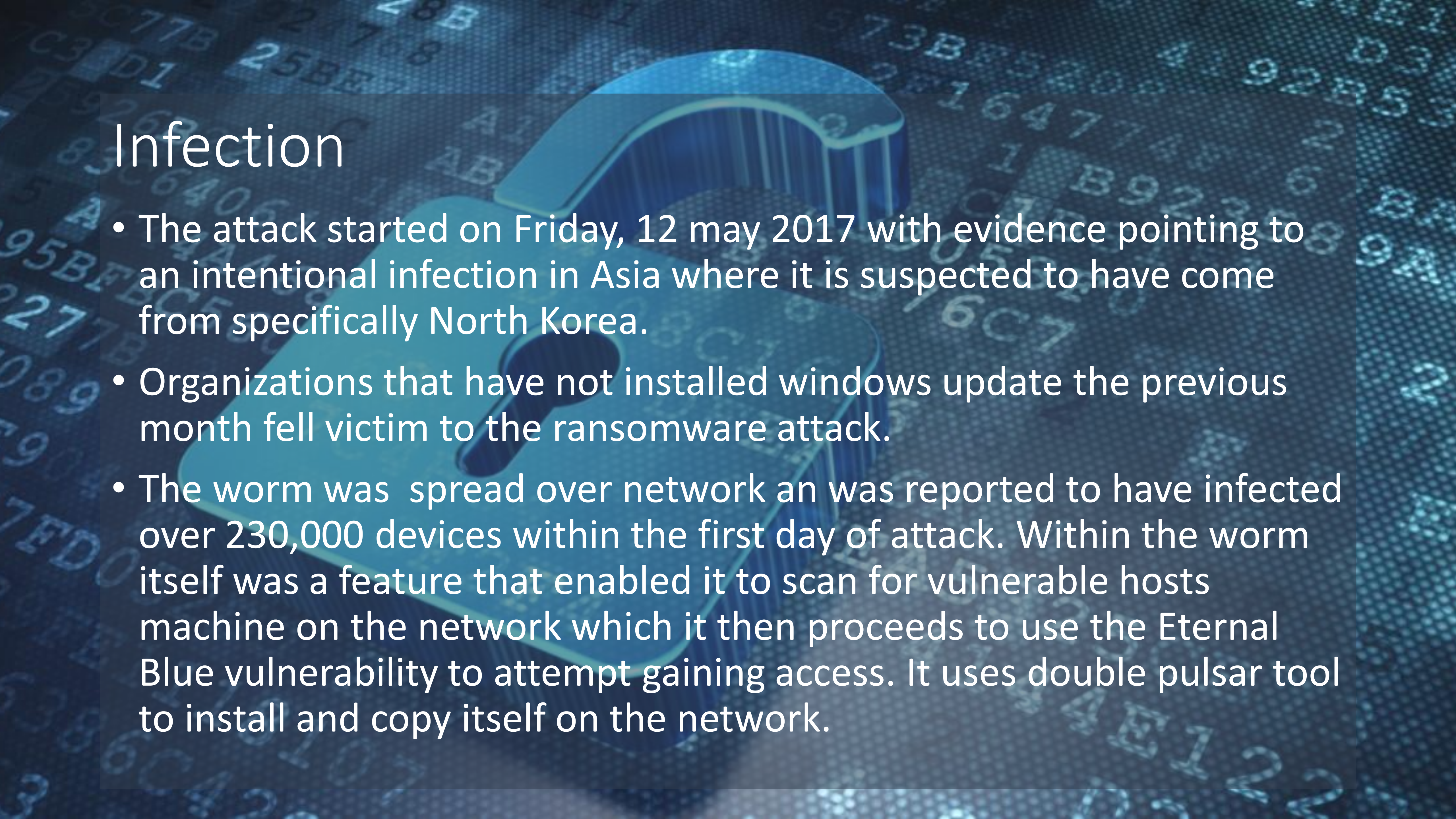
- WannaCry ransomware demanded $300 worth of the crypto-currency Bitcoin to decrypt the contents of the affected computers.
- The payment was demanded in bitcoins as this digital currency, popular among cybercriminals, is decentralized, unregulated and impossible to trace.
- The more important cost - the time lost, the files damaged beyond repair and other unexpected collateral damage caused by the malware, will be very difficult to ascertain.



Vulnerability

- The vulnerability used by the WannaCry ransomware for taking over system control is known as Eternal Blue or MS17-010. It's CVE is : CVE-2017-0144

- It exploits a vulnerability in the implementation of Microsoft server message block (SMB). The vulnerability exists because the SMB v1 server in various windows versions mishandles specially crafted packets by remote attackers allowing them to execute arbitrary code on the target computer.



Infection

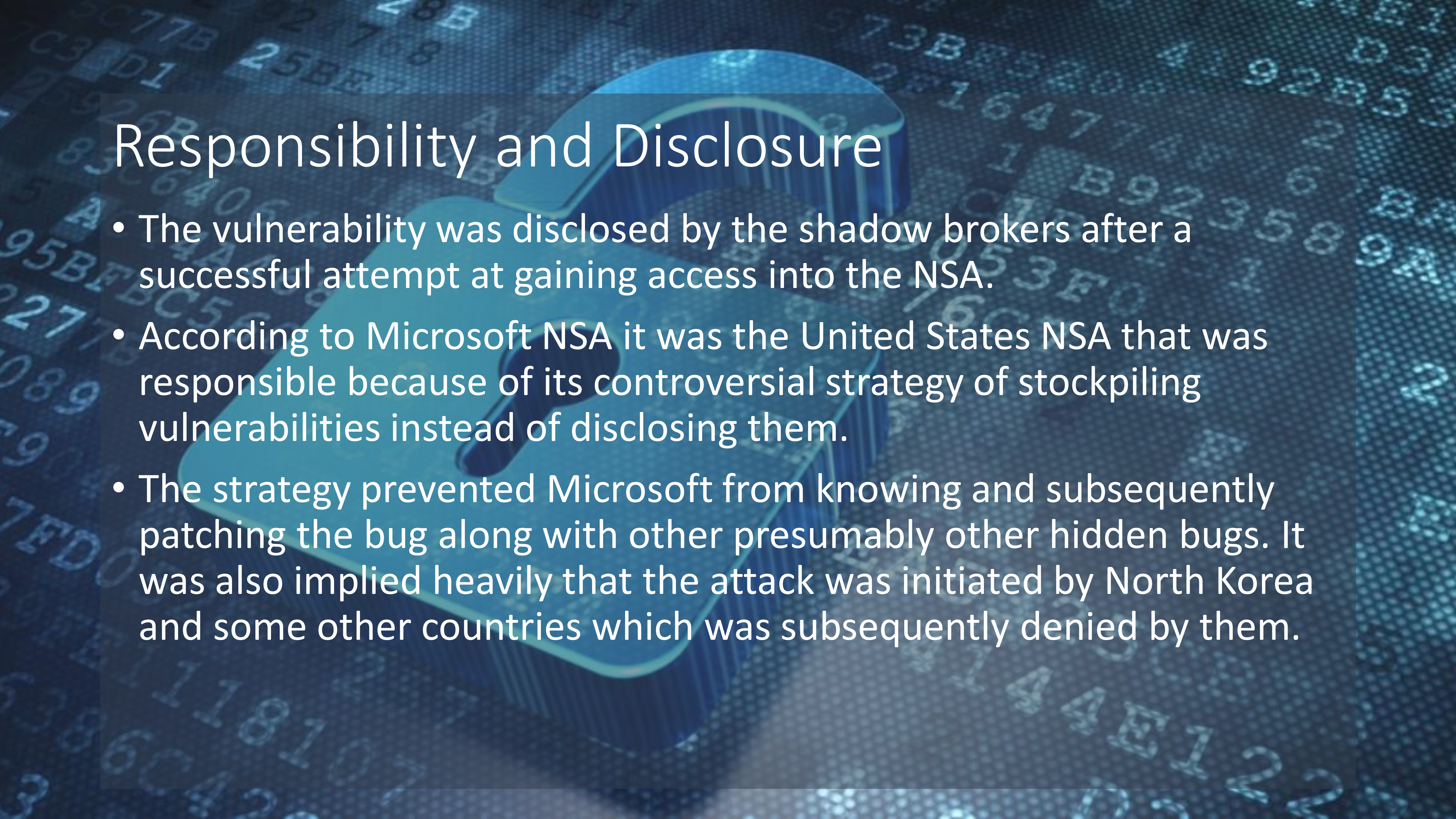
- The attack started on Friday, 12 may 2017 with evidence pointing to an intentional infection in Asia where it is suspected to have come from specifically North Korea.
- Organizations that have not installed windows update the previous month fell victim to the ransomware attack.
- The worm was spread over network an was reported to have infected over 230,000 devices within the first day of attack. Within the worm itself was a feature that enabled it to scan for vulnerable hosts machine on the network which it then proceeds to use the Eternal Blue vulnerability to attempt gaining access. It uses double pulsar tool to install and copy itself on the network.

Mitigation

- Security professionals advised users against paying the ransom as those that paid initially failed to get back their data and paying such ransoms will fuel future campaigns/attacks like this one which should be avoided at all cost. Organizations that have not installed windows update the previous month fell victim to the ransomware attack.
- Marcus Hutchins a security researcher in the UK made the one single contribution to stopping the attack by identifying a domain name hardcoded and embedded within the worm itself which was intended to be used as a kill switch by the attackers before it got out of hand.
- The worm comes online it makes a request to the domain name when it gets nothing back it proceeds to activate other features otherwise it halts and kills itself hence the kill switch term.

Impact of this Attack

- WannaCry hit more than 200,000 organizations from over 150 countries, shutting down everything from telecoms in Spain to the Interior ministry of Russia, and affecting 47 NHS trusts in United Kingdom.
- This kind of ransomware attack was unprecedented and unheard of.
- 230,000 infected computers over a 150 countries.
- One of the most hit organization was the NHS in UK where over 70,000 devices including oxygen generators MRI scanners etc. were infected by the worm.
- Nissan motors halted production due to the infection and to curtail it
- . A total of 327 payments were made totaling up to 130,000 US dollars
- while the economic loss of the entire attack is valued at around 4 billion US dollars.



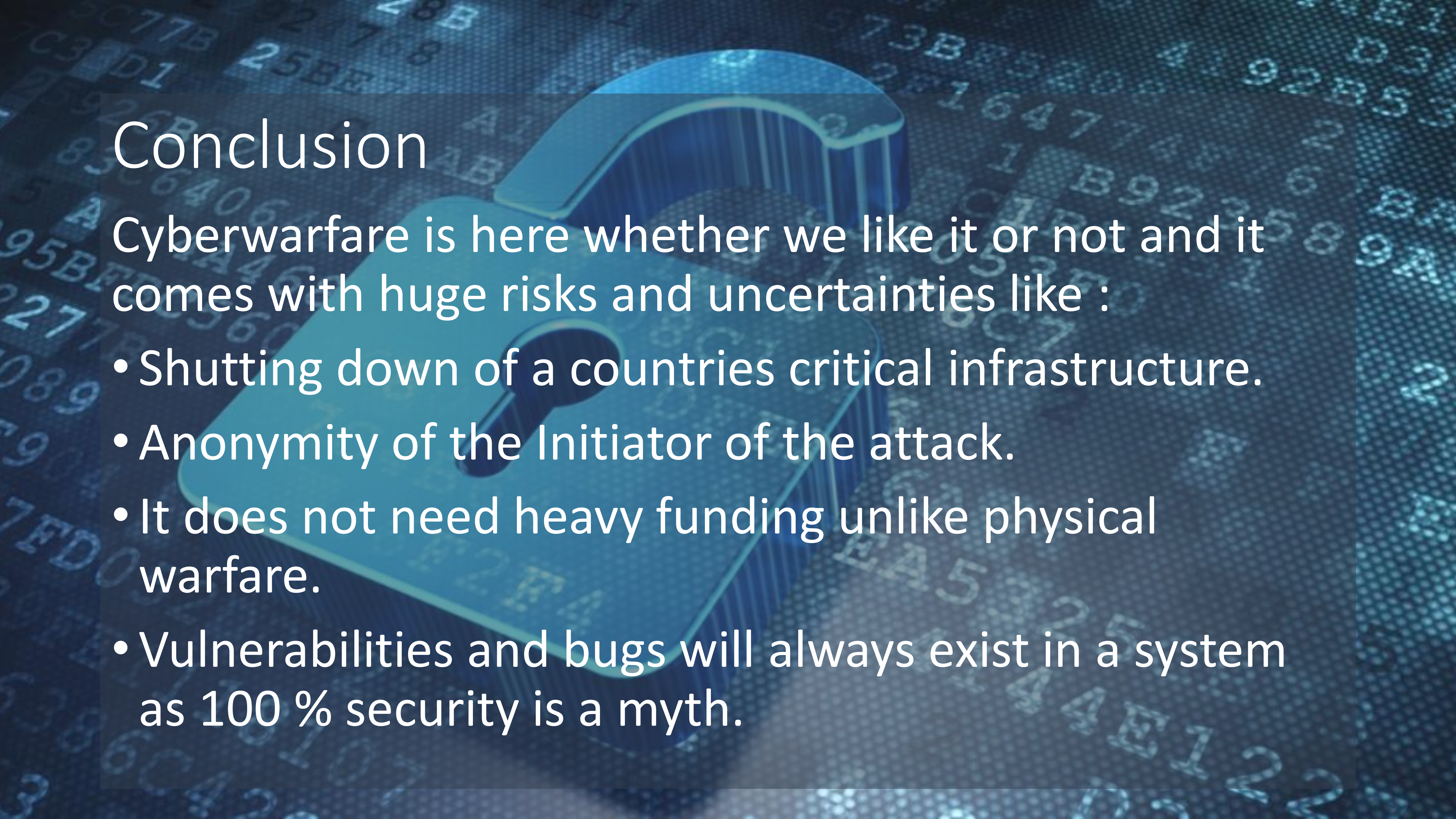
Responsibility and Disclosure

- The vulnerability was disclosed by the shadow brokers after a successful attempt at gaining access into the NSA.
- According to Microsoft NSA it was the United States NSA that was responsible because of its controversial strategy of stockpiling vulnerabilities instead of disclosing them.
- The strategy prevented Microsoft from knowing and subsequently patching the bug along with other presumably other hidden bugs. It was also implied heavily that the attack was initiated by North Korea and some other countries which was subsequently denied by them.

How to protect yourself?

Here are few Security Recommendations:

- Keep your Windows Operating System and antivirus up-to-date.
- Install internet security software
- Regularly back-up your files in an external hard-drive.
- Avoid unknown USBs
- Enable file history or system protection. In your Windows 10 or Windows 8.1 devices, you must have your file history enabled and you have to setup a drive for file history.
- Use OneDrive for Consumer or for Business.
- Beware of phishing emails, spams, and clicking malicious attachment.



Conclusion

Cyberwarfare is here whether we like it or not and it comes with huge risks and uncertainties like :

- Shutting down of a countries critical infrastructure.
- Anonymity of the Initiator of the attack.
- It does not need heavy funding unlike physical warfare.
- Vulnerabilities and bugs will always exist in a system as 100 % security is a myth.

THANK YOU