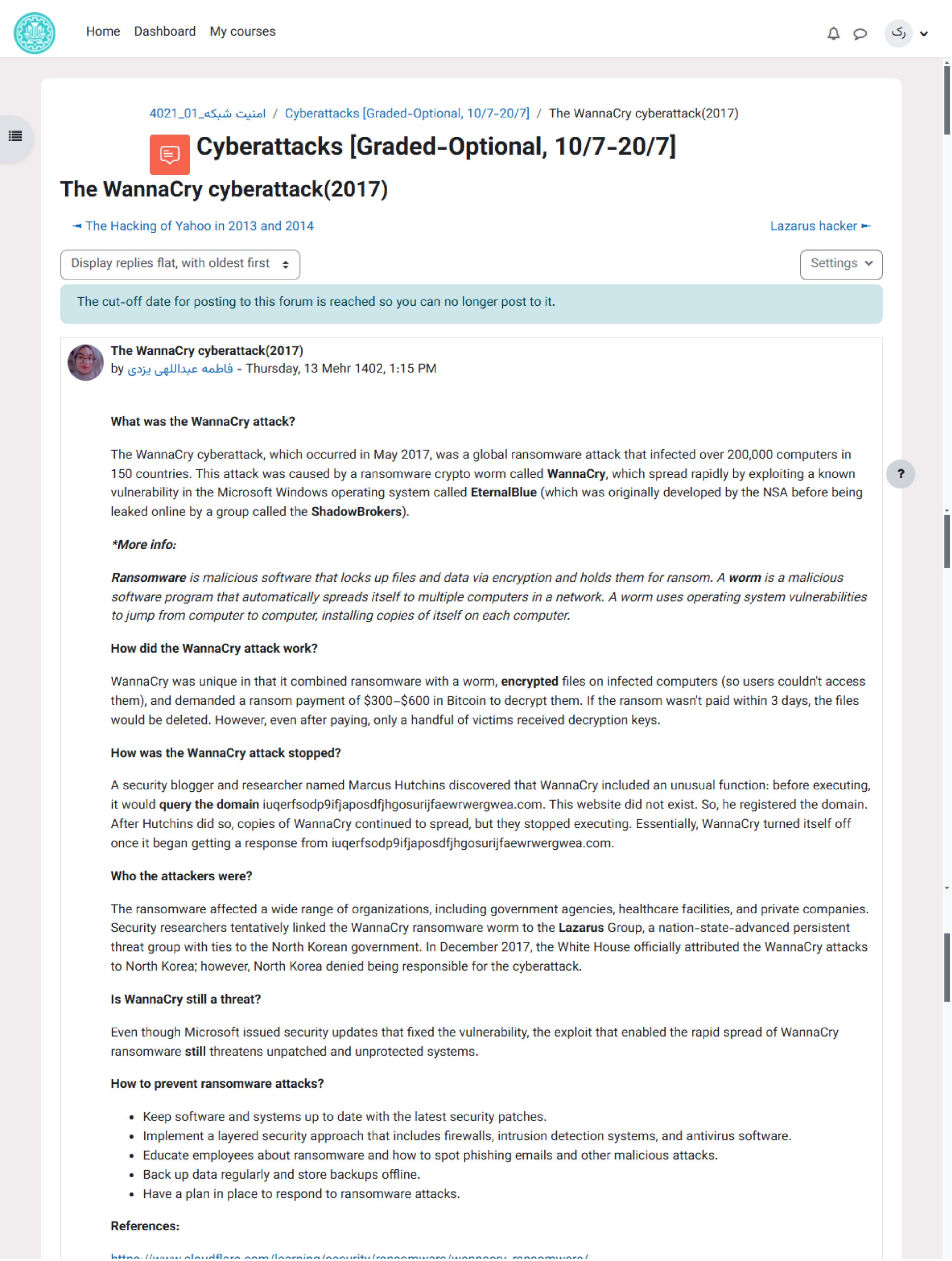


امنیت شبکه_4021_01 / Cyberattacks [Graded-Optional, 10/7-20/7] / The WannaCry cyberattack(2017)

Cyberattacks [Graded-Optional, 10/7-20/7]

The WannaCry cyberattack(2017)

◄ The Hacking of Yahoo in 2013 and 2014

Lazarus hacker ►

The cut-off date for posting to this forum is reached so you can no longer post to it.

The WannaCry cyberattack(2017)
by فاطمه عبداللهی یزدی - Thursday, 13 Mehr 1402, 1:15 PM

What was the WannaCry attack?

The WannaCry cyberattack, which occurred in May 2017, was a global ransomware attack that infected over 200,000 computers in 150 countries. This attack was caused by a ransomware crypto worm called **WannaCry**, which spread rapidly by exploiting a known vulnerability in the Microsoft Windows operating system called **EternalBlue** (which was originally developed by the NSA before being leaked online by a group called the **ShadowBrokers**).

More info:

Ransomware *is malicious software that locks up files and data via encryption and holds them for ransom. A* ***worm*** *is a malicious software program that automatically spreads itself to multiple computers in a network. A worm uses operating system vulnerabilities to jump from computer to computer, installing copies of itself on each computer.*

How did the WannaCry attack work?

WannaCry was unique in that it combined ransomware with a worm, **encrypted** files on infected computers (so users couldn't access them), and demanded a ransom payment of $300–$600 in Bitcoin to decrypt them. If the ransom wasn't paid within 3 days, the files would be deleted. However, even after paying, only a handful of victims received decryption keys.

How was the WannaCry attack stopped?

A security blogger and researcher named Marcus Hutchins discovered that WannaCry included an unusual function: before executing, it would **query the domain** iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. This website did not exist. So, he registered the domain. After Hutchins did so, copies of WannaCry continued to spread, but they stopped executing. Essentially, WannaCry turned itself off once it began getting a response from iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

Who the attackers were?

The ransomware affected a wide range of organizations, including government agencies, healthcare facilities, and private companies. Security researchers tentatively linked the WannaCry ransomware worm to the **Lazarus** Group, a nation-state-advanced persistent threat group with ties to the North Korean government. In December 2017, the White House officially attributed the WannaCry attacks to North Korea; however, North Korea denied being responsible for the cyberattack.

Is WannaCry still a threat?

Even though Microsoft issued security updates that fixed the vulnerability, the exploit that enabled the rapid spread of WannaCry ransomware **still** threatens unpatched and unprotected systems.

How to prevent ransomware attacks?

- Keep software and systems up to date with the latest security patches.
- Implement a layered security approach that includes firewalls, intrusion detection systems, and antivirus software.
- Educate employees about ransomware and how to spot phishing emails and other malicious attacks.
- Back up data regularly and store backups offline.
- Have a plan in place to respond to ransomware attacks.

References:

https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

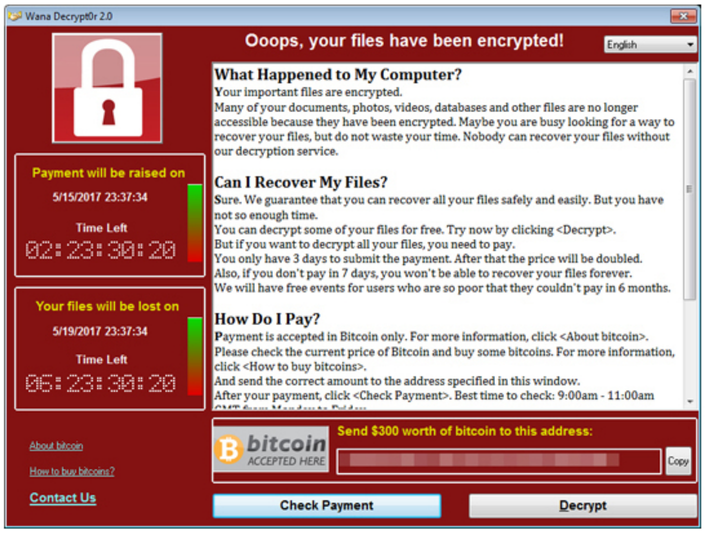
https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware/

https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry/

Permalink

What is SMB and how WannaCry used it to spread

by رسول کاماکار - Thursday, 13 Mehr 1402, 2:34 PM



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

Server Message Block (SMB)

The Server Message Block Protocol (SMB Protocol) is a client-server communication protocol used for sharing access to files, printers, serial ports, and data on a network. It can also carry transaction protocols for authenticated inter-process communication.

SMB was originally designed by Barry Feigenbaum at IBM in 1983 with the aim of turning DOS INT 21h local file access into a networked file system and was originally designed to run on top of NetBIOS over TCP/IP (NBT) using IP port 139 and UDP ports 137 and 138.

What are Ports 139 and 445?

SMB is a network file sharing protocol that requires an open port on a computer or server to communicate with other systems. SMB ports are generally port numbers 139 and 445.

Port 139 is used by SMB dialects that communicate over NetBIOS. It operates as an application layer network protocol for device communication in Windows operating systems over a network. For example, printers and serials ports communicate via Port 139.

Port 445 is used by newer versions of SMB (after Windows 2000) on top of a TCP stack, allowing SMB to communicate over the Internet. This also means you can use IP addresses in order to use SMB like file sharing.

Are Open Ports Dangerous?

While port 139 and 445 aren't inherently dangerous, there are known issues with exposing these ports to the Internet. Open ports are necessary to communicate across the Internet. However, an open port can become a security risk when the service listening to the port is misconfigured, unpatched, vulnerable to exploits, or has poor network security rules.

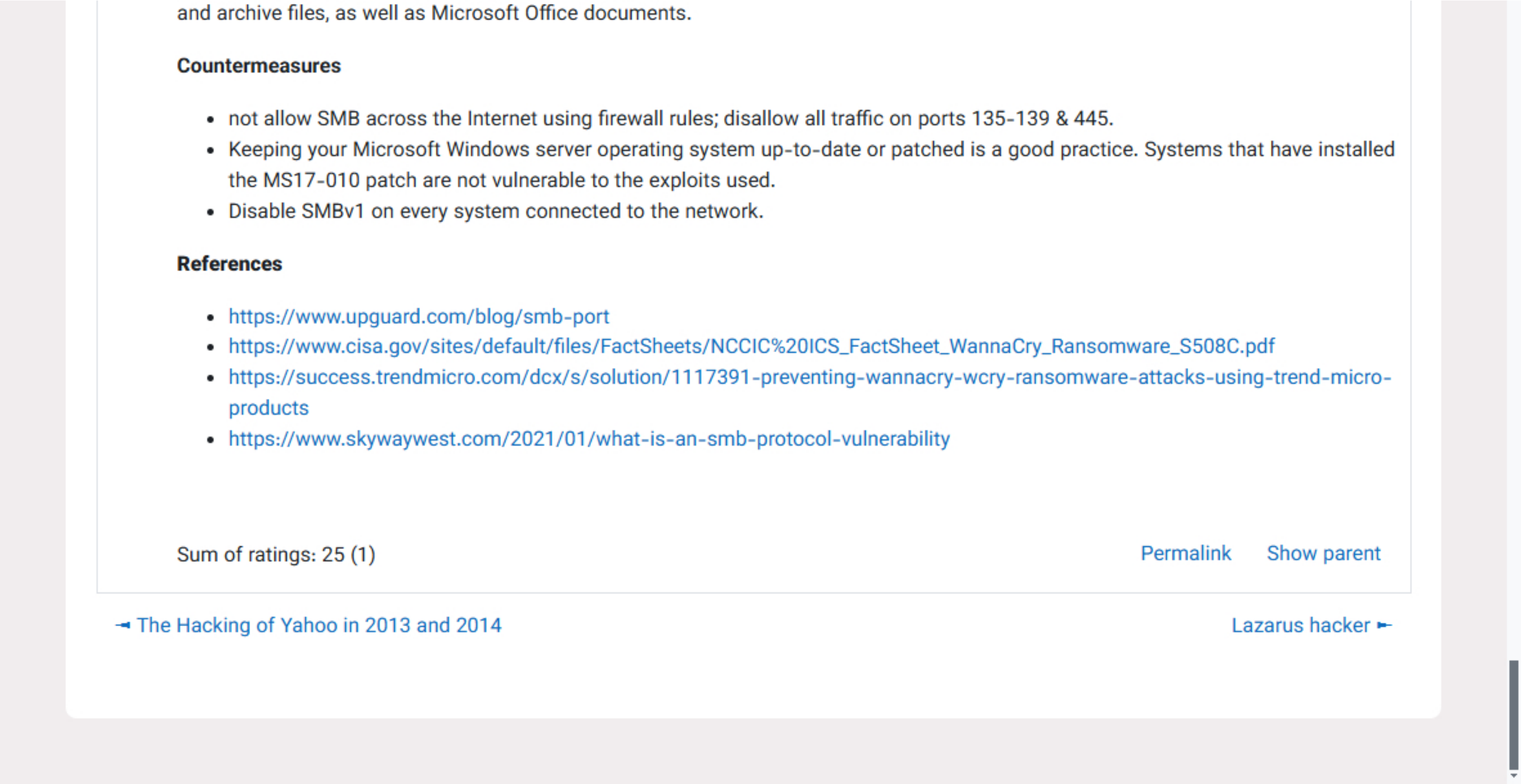
WannaCry Exploiting SMB

Early versions of the SMB protocol were exploited during the WannaCry ransomware attack through a zero-day exploit called EternalBlue. WannaCry exploited legacy versions of Windows computers that used an outdated version of the SMB protocol

WannaCry is a network worm with a transport mechanism designed to spread itself automatically. The transport code scans for systems vulnerable to the EternalBlue exploit and then installs DoublePulsar, a backdoor tool, and executes a copy of itself.

An infected computer will search its Windows network for devices accepting traffic on TCP ports 135-139 or 445, indicating the system is configured to run SMB. It will then initiate an SMBv1 connection to the device and use buffer overflow to take control of the system and install the ransomware component of the attack. This means WannaCry can spread automatically without victim participation.

WannaCry ransomware targets and encrypts 176 file types. Some of the file types WannaCry targets are database files, multimedia



and archive files, as well as Microsoft Office documents.

Countermeasures

- not allow SMB across the Internet using firewall rules; disallow all traffic on ports 135-139 & 445.
- Keeping your Microsoft Windows server operating system up-to-date or patched is a good practice. Systems that have installed the MS17-010 patch are not vulnerable to the exploits used.
- Disable SMBv1 on every system connected to the network.

References

- https://www.upguard.com/blog/smb-port
- https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf
- https://success.trendmicro.com/dcx/s/solution/1117391-preventing-wannacry-wcry-ransomware-attacks-using-trend-micro-products
- https://www.skywaywest.com/2021/01/what-is-an-smb-protocol-vulnerability

Sum of ratings: 25 (1)

➟ The Hacking of Yahoo in 2013 and 2014

Lazarus hacker ➻