WannaCry ransomware attack

Introduction

Previously you were introduced to cyberattacks, and you learned what a cyberattack is and some of how cybercriminals use them.

Nowadays, computers and mobile phones are increasingly used to save valuable information like pictures, documents, videos, and passwords. With this increasing use of technology, cyber threats have become more sophisticated and dangerous. One of the most significant cyber threats faced today is ransomware attacks. Welcome to the digital age!

Ransomware is a type of malware that takes control of a victim's files and encrypts them, then demands payment in exchange for a decryption key that restores access to the files. Ransomware attacks have become a major concern for both individuals and businesses in recent years. These malicious programs can even lock victims out of their computer systems. One of the most notable examples of ransomware attacks is the WannaCry ransomware, which affected computer systems worldwide in May 2017.

The image below shows the steps of how Ransomware takes place; from receiving the malware through to the ransom demand.

In this reading, you'll focus on the WannaCry ransomware attack in detail and discover:

- how the ransomware attack came about,
- how it was resolved,
- and the lasting impact it has had.

What is WannaCry?

The WannaCry ransomware attack was a global incident that caused substantial damage in May 2017. It's considered one of the most significant cyberattacks in recent history, affecting more than 200,000 computers across 150 countries and causing billions of dollars in damage. The attack targeted the Microsoft Windows operating system, exploiting a vulnerability known as EternalBlue. Once it infected a machine, it encrypted data and demanded payment in cryptocurrency for the data to be restored.

Some high-profile organizations affected by WannaCry ransomware were:

- UK's National Health Service (NHS),
- and the Health Service Executive in Ireland.

It also affected companies like:

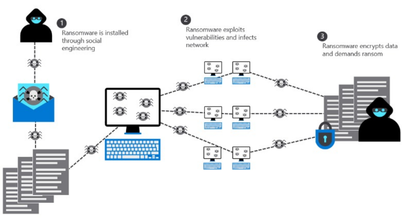
- Renault,
- FedEx,
- Telefonica,
- and the German railway company Deutsche Bahn.

How did it start?

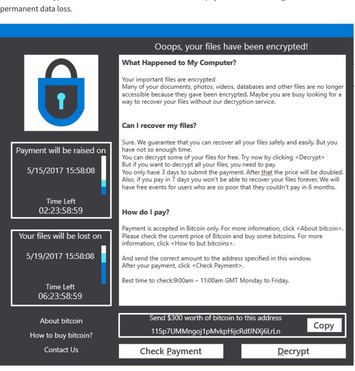
The WannaCry attack began when hackers used a vulnerability in Microsoft's Server Message Block or SMB protocol, which is used for file sharing. The vulnerability, known as EternalBlue, was discovered by the US National Security Agency (NSA),and was later stolen and leaked by a group of hackers known as "The Shadow Brokers." Once the vulnerability was exposed, the WannaCry ransomware started spreading like wildfire. The hackers behind WannaCry were able to use EternalBlue to spread the ransomware from one system to another very quickly.

The ransomware was spread through malicious attachments in emails and infected websites, as well as computers connected to a network. When the malware infected a machine, it encrypted all the data on that machine and displayed a message demanding payment in Bitcoin to unlock the data. The ransom demanded was initially $300 in Bitcoin, which increased if the payment was not made within a certain period.

The image below shows the steps of how WannaCry took place. From receiving the malware through to the ransom demand.



The image below displays the WannaCry ransomware attack message victims received when the ransomware successfully infected their systems. The message demands payment in Bitcoin in exchange for a decryption key to unlock the encrypted files. It warns the victim that failure to pay the ransom in the given timeframe will result in permanent data loss.



The impact of WannaCry

The WannaCry ransomware attack was devastating and had a massive impact on individuals and businesses across the world. For individuals, the attack resulted in a loss of personal data, and work files, as well as an inability to access important files.

The impact on business was even more severe, resulting in significant financial losses, reputational damage, and a reduction in trust. Companies lost access to critical systems and data, resulting in lost revenue and productivity. Many businesses were forced to shut down their operations temporarily, while others had to pay a hefty ransom to regain access to their systems.

Hospitals, government agencies, and businesses were among the most affected. Hospitals were forced to shut down their systems which resulted in canceled appointments and delayed non-urgent surgical procedures. The attack also highlighted the lack of critical security infrastructure. Businesses such as hospitals were forced to shut down and turn away patients due to the ransomware attack.

The image provides a visual representation of the global reach and scope of the WannaCry attack.

How was it stopped?

You might ask yourself; how did the world stop the ransomware attack?

WannaCry was diagnosed by a 22-year-old cybersecurity researcher named Marcus Hutchins, who discovered a kill switch within the code. The kill switch was surprisingly simple as it was just a domain name. WannaCry was designed in such a way that if it could contact this domain name from the affected computer, it will stop encrypting the files on that system. So, no further damage would be done to that computer if the ransomware was able to communicate with that domain.

This domain name was ***iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com***.

Hutchins registered that domain name and accidentally activated the kill switch for WannaCry, which halted the ransomware from damaging the system. This also averted a potential worldwide catastrophe that may have occurred if the kill switch hadn't been turned on in time.

Aftermath

While WannaCry had a massive impact across the world, it also highlighted the risks of cyberattacks to organizations and businesses of all sizes. It showed that businesses which lacked proper security measures were particularly vulnerable to attack. The incident underscored the importance of proactive measures to protect against cyber threats, including implementing robust security protocols and ensuring regular data backups.

Governments and businesses around the world started taking steps to improve their cybersecurity measures. Microsoft also released a patch to fix the EternalBlue vulnerability that caused the WannaCry ransomware to spread so rapidly.

Conclusion

As you may have concluded, the WannaCry ransomware attack was a wake-up call for everyone! It highlighted the importance of cybersecurity and the need to take proactive measures to prevent cyberattacks. It showed that no one is safe from cyber threats and cybercriminals are always looking for vulnerabilities to exploit. The best defense against such attacks is to stay vigilant, keep software up-to-date, and have a solid backup system in place.

In this reading, you explored the WannaCry ransomware attack in detail, you discovered how it started, the impact it had, and what individuals and businesses learned because of it.

Mark as completed