1 WannaCry Ransomware Attack

1.1 The Attack

WannaCry was a crypto ransomware attack that occurred in May 2017. The attack basically encrypts every file on the system including any usb or drive storage connected with symetric encryption (AES algorithm) and then encrypts the secret key used by AES with public (or asymmetric) encryption [1]. However, it was not just a simple ransomware attack. First, the user gets infected by clicking something he shouldn't but after that, the next users don't even need to click anything to get infected. Once it affects one machine it spreads over that machine's network and infects all the computers connected to it that have the SMB Windows vulnerability. These users get all his files encrypted without even clicking or installing anything. To reverse this attack, the hackers demanded a payment to certain bitcoin addresses in five days, otherwise the files would be lost forever [2].

1.2 Source Causes

National Security Agency (NSA) discovered a vulnerability on the SMB (Server Message Block) protocol in Windows machines and developed a tool to exploit it called EternalBlue. This tool was stolen by a group of hackers some months before the attack took place. It was used to spread the virus through the network taking advantage of that vulnerability that so many computers had. Although Microsoft patched this vulnerability in all Windows operating systems, due to user negligence, a lot of people didn't update their systems right away or at all so the attack was allowed to keep spreading. NSA knew about this windows vulnerability and didn't warned Microsoft until it was too late. When Microsoft acknowledged it, they did what was in their power to patched it the fastest way. In my opinion, NSA is the main organization to be blamed when we talk about WannaCry.

1.3 The Impacts

Because of this attack, millions and millions of files were encrypted and lost. It is estimated that the hackers only gained 108 thousand pounds in bitcoins [3], which is irrelevant when compared to the estimated value of 4 billion dollars of losses [4]. For example, only the National Health System of United Kingdom calculated over 90 millions pounds in losses due to the fact that 19 thousand appointments were cancelled [5]. Besides the money, enormous amounts of sensitive data were lost. On the other hand, cyber-security awareness raised a lot because of this attack.

1.4 How it could have been prevented

In the first place, this attack wouldn't have the growth it had if NSA shared with Microsoft the vulnerability that they discovered in time, so that Microsoft could have fixed it and release security updates. On a second approach, there's always the users that prefer to not update the systems and to be vulnerable to every type of attacks. In 2019, more than two years later, it is expected that still more than a million machines are vulnerable to EternalBlue (this numbers were warned by Microsoft) [6]. This just proves, that although Microsoft released the security patches to this vulnerability straightaway, there's a lot of people or organizations that don't update their systems (sometimes because of legacy software, it happens a lot in the medical field). In my opinion, this attack could have been prevented if NSA collaborated with Microsoft and if users would care more about their systems before it was too late (this means, until the system gets infected).

References

[1] COMPUTERPHILE. *How WanaCrypt Encrypts Your Files*. 2017.

[2] COMPUTERPHILE. *Wana Decrypt0r (Wanacry Ransomware)*. 2017.

[3] GUARDIAN, T. *WannaCry: hackers withdraw £108,000 of bitcoin ransom*. 2017.

[4] NEWS, C. *WannaCry ransomware attack losses could reach $4 billion*. 2017.

[5] TELEGRAPH. *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled*. 2017.

[6] VERGE, T. *Microsoft warns 1 million computers are still vulnerable to major Windows security exploit*. 2019.