WannaCry Ransomware attack – A case study

- Suraj Bhatt (17bcn7005)

What is WannaCry Ransomware attack?

This is a worldwide conducted cyberattack conducted by WannaCry Ransomware Crypt worm on 12May,2017. This attack specifically targeted Windows base Operating systems. The initial infection was likely through an exposed vulnerable SMB port, rather than email phishing as initially assumed. However, email phishing was the main method of spreading the WannaCry ransomware.

What causes infection in system?

This ransomware cyberattacks exploited a vulnerability in Windows OS called Eternal Blue (cyberattack exploit developed by the U.S. National Security Agency). This vulnerability was leaked by a hacker's group by name SHADOW BROKERS on April 14, 2017. The main victims of such cybercrime were Windows 8, 2003 and XP users, because the last released security update for XP was in April 2014, and many didn't install the newer update as of March this year. Microsoft had stopped supporting these versions of windows, but an emergency update was released for them to fight this cyber-attack. Also, there were many using an unlicensed windows software. This makes them all the more vulnerable.

The Cure

While trying to establish the size of the attack, a man named Marcus Hutchins accidentally discovered a "kill switch" coded in the malware. He registered a domain name for the DNS sinkhole (a DNS which gives false information about a domain), which stopped the spreading of the virus like a worm, thus drastically slowing down the spread of the virus, giving time to come up with defensive measures.

A man named Adrian Guinet created a "WannaKey", a solution to the WannaCry ransomware based on its flaws. He cautioned that it wouldn't work if the infected computer was rebooted or if the malware overwrote the decryption key.

Impact

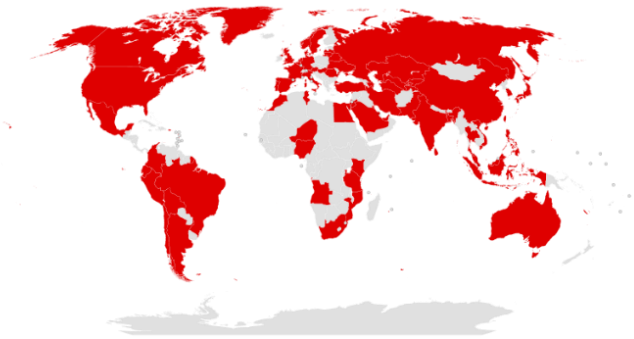

Fig. map of countries initially affected Source: Wikipedia

Some experts say that the impact of the attack would have been much disastrous if Marcus Hutchins had not found the kill switch built in by the creators or if it had been specifically targeted on highly critical infrastructure, like nuclear power plants, dams or railway systems.

According to cyber-risk-modelling firm Cyence, economic losses from the cyber-attack could reach up to US$4 billion, with other groups estimating the

losses to be in the hundreds of millions. Many major production outlets stopped their production due to this attack.

The following is an alphabetical list of organisations confirmed to have been affected:

- Andhra Pradesh Police, India[119]
- Aristotle University of Thessaloniki, Greece[120]
- Automobile Dacia, Romania[121]
- Boeing Commercial Airplanes[122]
- Cambrian College, Canada[123]
- Chinese public security bureau[124]
- CJ CGV (a cinema chain)[125]
- Dalian Maritime University[126]
- Deutsche Bahn[127]
- Dharmais Hospital, Indonesia[128]
- Faculty Hospital, Nitra, Slovakia[129]
- FedEx[130]
- Garena Blade and Soul[131]
- Guilin University of Aerospace Technology[126]
- Guilin University of Electronic Technology[126]
- Harapan Kita Hospital, Indonesia[128]
- Hezhou University[126]
- Hitachi[132]
- Honda[133]
- Instituto Nacional de Salud, Colombia[134]
- Lakeridge Health[135]
- LAKS, Netherlands [136]
- LATAM Airlines Group[137]
- MegaFon[138]
- Ministry of Internal Affairs of the Russian Federation[139]
- Ministry of Foreign Affairs (Romania)[140]
- National Health Service (England)[141][104][108]
- NHS Scotland[104][108]
- Nissan Motor Manufacturing UK[141]
- O2, Germany[142][143]
- Petrobrás[144]
- PetroChina[111][124]
- Portugal Telecom[145]
- Pulse FM[146]
- Q-Park[147]
- Renault[148]
- Russian Railways[149]
- Sandvik[128]
- Justice Court of São Paulo[144]
- Saudi Telecom Company[150]
- Sberbank[151]
- Shandong University[126]
- State Governments of India
  - Government of Gujarat[152]
  - Government of Kerala[152]
  - Government of Maharashtra[153]
  - Government of West Bengal[152]
- Suzhou Vehicle Administration[126]
- Sun Yat-sen University, China[128]
- Telefónica, Spain[154]
- Telenor Hungary, Hungary[155]
- Telkom (South Africa)[156]
- Timrå Municipality, Sweden[157]
- TSMC, Taiwan[158]
- Universitas Jember, Indonesia[159]
- University of Milano-Bicocca, Italy[160]
- University of Montreal, Canada[161]
- Vivo, Brazil[144]

Fig. alphabetical list of organizations confirmed to have been affected. Source: Wikipedia

Defensive Response

Experts quickly advised affected users against paying the ransom due to no reports of people getting their data back after payment and as high revenues would encourage more of such campaigns.

The day after the initial attack in May, Microsoft released out-of-band security updates for end of life products Windows XP, Windows Server 2003 and Windows 8; these patches had been created in February of that year following a tip off about the vulnerability in January of that year.

What happened later?

Although now this attack has somewhat slowed down, this will not mark the end of it. The hacker group “Shadow Brokers” has threatened to unleash hell in June, calling it the “Data Dump Month”.

There have been no signs of someone making the payment and having their files decrypted. The reason for this is that one’s payment cannot be linked to their computer. In addition to the above, it would require manual intervention of the hackers to decrypt any files, and thus there is no way of decrypting over 300,000 computers.

The Shadow Brokers have claimed to have access to over 75% of the US Cyber Arsenal. They also claim to have access to the Nuclear programs of North Korea, Russia, China and Iran.

In late June, hundreds of computer users reported being sent an email from someone (or multiple people), claiming to be the developers of WannaCry.[185] The email threatened to destroy the victims' data unless they sent 0.1 BTC to the Bitcoin address of the hackers. This has also happened in 2019.

Resources

https://en.wikipedia.org/ |https://ranksecure.in/