2017 Ukraine Ransomware Attacks

Summary

In 2017, a series a cyberattacks occurred, overwhelming Ukraine corporate websites of banks, ministries, utility companies, etc.

At the same time, similar infections began to pop up in other countries such as France, Germany, Poland, Australia, and the U.S. However, it was estimated that 80% of all infections occurred within Ukraine.

One day after the initial assault, the Ukraine government declared that the attack was halted. The belief, sourced by the AP, was that this was the Petra virus masquerading as ransomware while the main intent was to create maximum damage within Ukraine.

Source

The root of the infection was believed to be within a Ukraine accounting package call MeDoc, a widely used service across the country. Apparently, an automatic software update was infected, pushing the malware out to business and government agencies alike. The company, Intellect Service, claimed no involvement in the hack.

Security experts eventually found that the code which infected the company's website had a backdoor built in to potentially be used to launch future attacks.

Damage

The malware or in this case Ransomware, infected a computer resulting in the data on the computer to be encrypted. It then required the user to send hundreds of dollars in Bitcoin to decrypt the data. It managed to abuse a vulnerability in Microsoft Windows. Microsoft issued patches in 2017 to address this vulnerability in all of its post-Windows 7 operating systems.

The suspicious element was that often the malware ended up destroying the data, causing complete loss. Because of this, the attack was seen more of a ploy to cripple the Ukraine infrastructure, most likely by its hostile neighbor, Russia. Other coincidences included the event happen on the eve of the Ukrainian Constitution day and the assassination of a senior intelligence officer.

The Ukraine government seized the equipment of the Intelligent Service where the virus was source and held the staff responsible because of lax security and lack of effort to prevent such attacks.

2017 Ukraine ransomware attacks - Wikipedia