Ukraine Ransomware

A ransomware attack involves the encryption of files and folders in a system, rendering them inaccessible until a ransom is paid to get the access key. The Ukrainian attack was no different. It was identified as a variant of the Petya ransomware. The malware was designed to encrypt user’s files or lock the master file table (MFT) of the computer, making the system inaccessible. This would then require a ransom to be paid for the decryption key (Wakefield, 2017).

The vulnerability was discovered when a global cyber-attack affected various companies worldwide. The ransomware was identified as spreading through MEDoc, the Ukrainian tax-filing software. The update system of the software was compromised, which led to malware being executed instead of obtaining the legitimate software updates (Wakefield, 2017). It is from this software update process that most of the initial infections to various company systems was traced.

To exploit the software vulnerability the attackers hijacked the update mechanism of the software. Through this, they were able to propagate the malware without the knowledge of the software users as they saw it as a legitimate software update. Upon successfully breaching an organization, the software used the ExternalBlue exploit, which is a windows vulnerability that was discovered by the NSA and leaked online. It also leveraged stolen IT credentials and admin tools such as PsExec and WMIC to further spread within the infected network. Through this method, the malware was able to spread rapidly across different systems throughout the world.

There are preventive measures that could have been taken and implemented in an effort for prevent the occurrence of such an attack. One such measure includes regularly updating software, and verifying updates’ integrity by use of advanced tools such as anti-ransomware. Also, regular application of security patches to the system on known vulnerabilities like SMB protocol exploited in Eternalblue could have protected companies from the attack (Shabut et.al 2016).

References

Shabut, A. M., Lwin, K. T., & Hossain, M. A. (2016, December). Cyber attacks, countermeasures, and protection schemes—A state of the art survey. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)* (pp. 37-44). IEEE.

Wakefield, J. (2017 June 8). Tax software blamed for cyber-attack spread. BBC. Retrieved from <https://www.bbc.com/news/technology-40428967>