CO6200 Research Project Proposal

Author: Sophia Roscoe

Research Supervisor: Jason R. C. Nurse

Title: A timeline of ransomware attacks throughout the COVID-19 pandemic and their impact

Overview

The aim for this project is to research, analyse and present the range of ransomware attacks that have taken place over the last 18 months (thus aligned with the COVID-19 pandemic). This will culminate in a detailed timeline displaying the prevalence and evolution of ransomware attacks and their targets (e.g., organisations, governments), and allow exploration of any correlation with major events during the pandemic. To conclude, I will critically reflect on the timeline, the types of ransomware attacks and the cybercriminal groups perpetrating attacks, and on how ransomware attacks may continue after the pandemic due to the change in work environment and society. This will be predominantly an analytical/research project.

Importance

The number of COVID-19 level pandemics during the computing age has been incredibly small and thus it is vital we gather and correlate information from these events. With the pandemic continuing, it is important to reflect on how the change in both the working and social environment has led to an evolution in cybercrime. This has allowed cyber criminals to exploit new avenues, ultimately leading to the pandemic being all the more traumatising for businesses and people. One example of this in February is when COVID-19 themed emails designed to entice users really installed CXK-NMSL malware [1].

One of the main culprits is ransomware. With business predominately working from home there is an increase in employers using their own systems with varying levels of security and oversight. In addition, perpetrators are using the pandemic to create ransomware disguised as government support, it is increasingly important we aim to prevent this. By researching the use of ransomware along with a timeline of the pandemic it will help us visualise the motive and targets of attacks. Such knowledge is useful in general, but also in enabling us as a society to prepare for similar threats in the future.

Methodology

To complete this project, I will need to perform extensive research on ransomware attacks throughout the last 18 months. To begin I will set myself a reasonable timeframe as to when the pandemic started to a reasonable and recent end date (~late December 2019 - ~ August 2021).

From this I shall take each month and attempt to find online articles and sources attributing to ransomware attacks. Not every article will contain all the required information so as a result I shall investigate with additional articles until the full information is found. This will ensure that there are multiple accredited proofs to support each attack.

Each case shall be compiled using Excel and other applications resulting in a data set of ransomware attacks with corresponding information (including the time of the attack and article, when/where it happened, which organisation was impacted, the group responsible and previous aliases etc). Finally, I will analyse the dataset to identify patterns throughout the last 18 months and discuss why this may be the case. This will culminate in creating a timeline of ransomware attacks similar to the one in the following article ultimately achieving the aim of my project [2].

Outputs

The final outputs of this research topic will be a technical report covering a timeline of major ransomware attacks throughout during the pandemic, a critical reflection on this timeline, and a discussion on ransomware concerns and solutions in the future.

This is in addition to the other deliverables required by the module.

References

[1] Abrams, L., 2021. *The Week in Ransomware - February 14th 2020 - Targeting MSPs*. [online] BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-february-14th-2020-targeting-msps/> [Accessed 21 September 2021].

[2] Lallie, H. S., Shepherd, L. A., Nurse, J.R.C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248 [Accessed 21 September 2021].