A timeline and analysis of ransomware attacks during the COVID-19 pandemic

By Sophia Roscoe

Supervised by: Jason R.C Nurse

Project description

Ransomware is a type of malware designed to access, block, and encrypt the victim's personal data until a request is fulfilled. With the estimated average global damage of ransomware increasing from $8 billion in 2018 to $20 billion in 2020 it is not a surprise that there was a significant increase in the number, complexity and severity of attacks during the COVID-19 pandemic despite the technology only being ~33 years old. The aim of this project was to research all ransomware attacks during the COVID-19 timeline using various news and scientific research outlets to ensure validity and correlate them to a visual timeline of attacks. These statistics are then used to identity trends and patterns in attacks related to significant COVID-19 dates. Being the first pandemic since the invention of the internet, the results of this investigation will provide insight into both human and ransomware behaviour for future pandemics.

Results

I have found that there was a large amount of attacks in certain sectors such as Government (41), Education (48), Technology (54), and Healthcare (58). This compared to other sectors such as Retail (16) and Services (19) possibly show a focus on these particular sectors. One reason for this targeting could be to acquire and disrupt valuable Covid-19 research as well as exploit new vulnerabilities created by remote learning. There are also very distinct bunches of attacks in these sectors such September 2020 – December 2020 which seem to coincide with noticeable Covid-19 news and dates. There was a noticeable increase in the use of "double extortion" tactics by ransomware groups[1] such as Maze causing a 178% in ransom payouts. Finally one interesting observation is that certain ransomware gangs such as Ragnarok[2], Avaddon[3], Darkside[4], and noticeably Maze emerged and shut down during the Covid-19 timeframe.

References:

[1] Cognyte. 2022. *Global Threat Intelligence Report - The Ransomware Landscape*. [online] Available at: <https://www.cognyte.com/resources/the-ransomware-landscape/#> [Accessed 13 February 2022].

[2] Techcrunch.com. 2022. *TechCrunch is part of the Yahoo family of brands*. [online] Available at: <https://techcrunch.com/2021/08/30/ragnarok-ransomware-gang-shuts-down-and-releases-its-decryption-key/> [Accessed 13 February 2022].

[3] Itpro.co.uk. 2022. [online] Available at: <https://www.itpro.co.uk/security/ransomware/359859/avaddon-hackers-release-decryption-keys> [Accessed 13 February 2022].

[4] Tripwire, I., 2022. *Maze Ransomware Gang to Shut Down Operations*. [online] The State of Security. Available at: <https://www.tripwire.com/state-of-security/security-data-protection/maze-ransomware-gang-to-shut-down-operations/> [Accessed 13 February 2022].