Timeline and analysis of ransomware attacks during the Covid-19 pandemic

Aim and Purpose of Project

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.

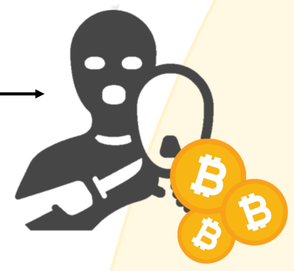
"**With this being the first pandemic since the invention of the internet, the results of this investigation will provide insight into both human and ransomware behaviour for future pandemics."**

"Global damage of ransomware increased from $8 billion in 2018 to $20 billion in 2020"

How does Ransomware work?

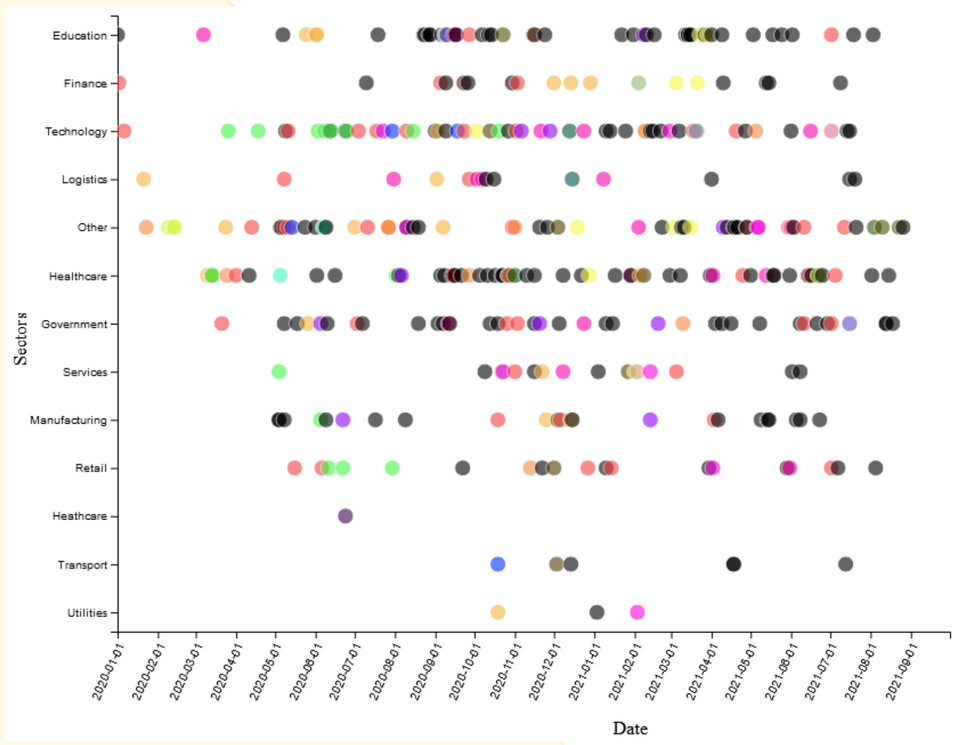
Ransomware gains access to an organisations system via Phishing/RDP vulnerabilities etc.

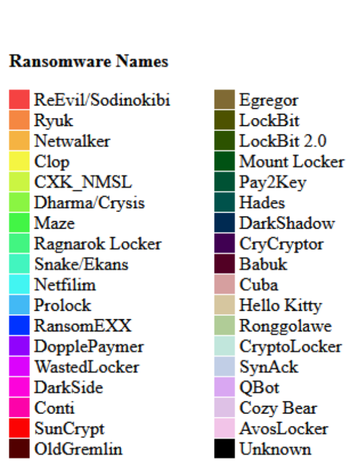
The ransomware encrypts as many files as possible as well as possibly delete backup files



Once the files are encrypted, the ransomware notifies the user to pay a ransom to return access to files and/or to prevent them being leaked into the web

Results and Observations





360 Attacks! (Jan 2020—August 2021)

Attacks in Healthcare, Education, Technology, and Government

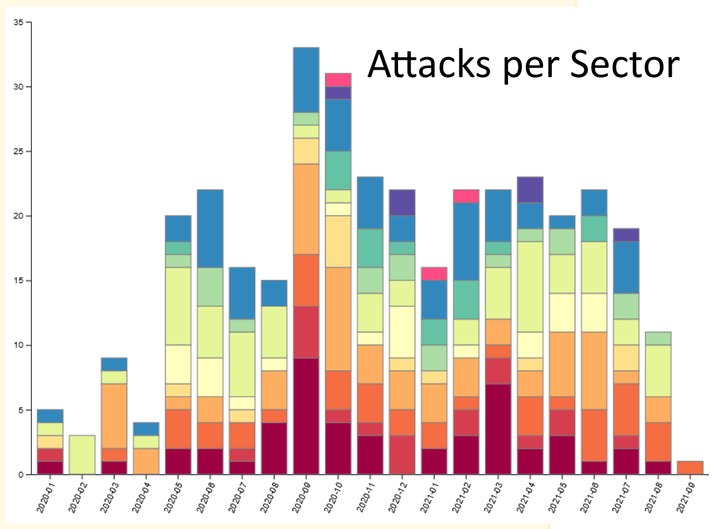
Bunches of attacks line with significant lockdown dates

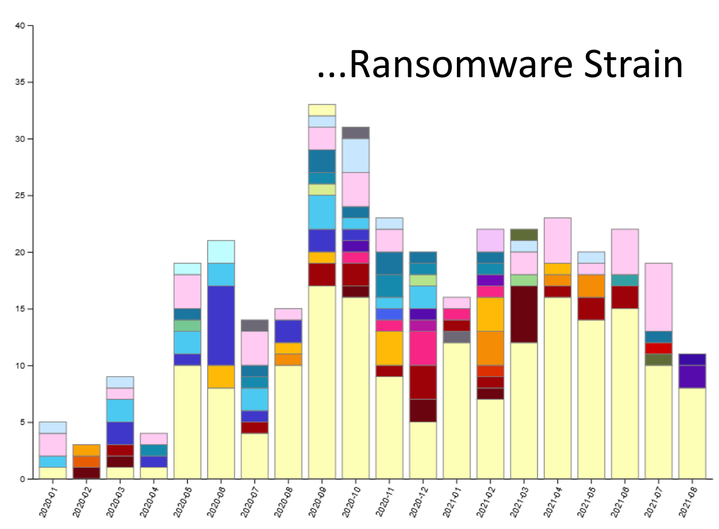
Highest amount of attacks in 2021 compared to 2020

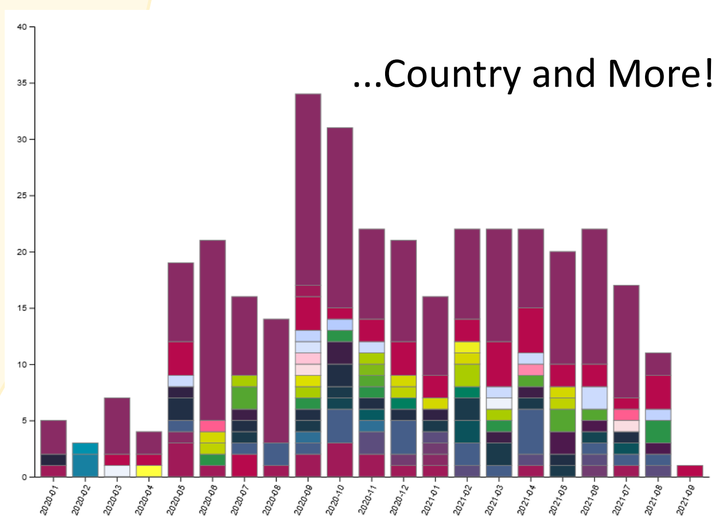
Major increase in "double extortion tactics" causing 178% in ransomware pay-out's.

Strain such as Ryuk, ReEvil, and Maze emerging as major threats.

Strains of ransomware born and died during the pandemic.







By Sophia Roscoe (sr694@kent.ac.uk)

Supervisor : Jason R.C Nurse