The evolving menace of ransomware: A comparative analysis of pre-pandemic and mid-pandemic attacks

The Evolving Menace of Ransomware: A Comparative Analysis of Pre-pandemic and Mid-pandemic Attacks

Michael Lang, Lena Yuryna Connolly, Paul Taylor, Phillip J. Corner

Digital Threats Research and Practice, August 2022, ACM (Association for Computing Machinery)
DOI: 10.1145/3558006

What is it about?

In recent times, ransomware has emerged as a major challenge to both public and private entities, consistently ranking high in alerts from cybersecurity companies, governmental bodies, and police departments. Its tactics are ever-changing and there's been a significant surge in the number of attacks. This piece delves into the evolution of ransomware assaults post the onset of the COVID-19 crisis. We analyze data from 39 incidents, with 26 happening just before the pandemic (from 2017 to 2019) and 13 during the pandemic years (2020 to 2021).

Why is it important?

The digital transformation of workplaces got a rapid boost due to the COVID-19 pandemic, resulting in countless global employees adapting to makeshift home offices with suboptimal security conditions. Initially, many organizations weren't ready for the security challenges that came with remote work, lacking proper cybersecurity protocols. As a result, there was a marked increase in cybercrime aimed at home-based workers during the pandemic. With social engineering posing a significant threat to remote workers, it's essential for businesses to establish strong Security Education, Training, and Awareness programs. Yet, employees at home often forget about security protocols due to the relaxed environment, leading to a phenomenon termed "security amnesia."

In the past few years, the "bring your own device" (BYOD) trend has gained momentum, allowing staff to utilize company IT assets for personal use. This has muddled the distinction between professional and personal life, creating concerns not just about work-life balance and "techno-stress," but also IT security. The combination of BYOD, the forced shift to remote work by COVID-19, and stricter data protection laws (like EU's GDPR and California's CCPA) creates a complex environment for IT security experts. They face an ever-growing number of potential attack points, while also needing to ensure data protection across various systems and devices. Ransomware criminals have eagerly exploited these chaotic conditions.

Ever since ransomware emerged around 2013 as a significant threat, there's been a surge in related academic writings. Numerous studies and reviews on ransomware attacks exist, but most of them emphasize the technical aspects. There's limited focus on the social-technical dynamics or the real consequences for the affected parties.