Amanda Gonzalez
Computer Networking
15 September 2022

Current Event

Educations for Ransom

Hackers recently infiltrated the network of the Los Angeles Unified School District (LAUSD), with a ransomware attack on various network applications. The LAUSD is one of the largest school districts in the US, so news of the attack promptly followed FBI and CISA (Cybersecurity and Infrastructure Security Agency) involvement. These authorities have noted that the education sector, namely grades K-12, are becoming increasingly targeted by hacking groups due to their vulnerable connectivity and information accessibility ("Update on the Los Angeles Unified School District ransomware attack. Spyware update. Data breaches and ransomware."). So much so that the Russian hacking group Vice Society has claimed recognition for this attack, which follows with their previous targeting of school systems.

Patterns of Vice Society attacks start with exploits of SonicWall products or other internet application vulnerabilities (Arntz). After gaining access, the attackers take their time to extort the most information possible and broaden their control. They will then plant malware on devices and use ransom techniques to take over a network. So knowing their tactics, what can be done to prevent these types of attacks in schools? First, security education should be mandatory for all faculty, students, and families of a school district. Technology can seem abstract to many of these individuals, so it is important to teach them about how to identify irregularities and maintain their devices/applications. Secondly, device/application monitoring and regulation should be implemented. This means data securities, multilayered authentication, and defensive software. Investing in knowledgeable individuals and teams to oversee these security measures can largely protect the privacy and security of so many individuals, although this comes at a cost. Lacking the resources and time to undertake such tasks may limit the security schools can have in place, and thus, become a concern for a majority of schools in the nation.

Since schools are becoming increasingly interconnected, security becomes even more of a threat; however, it may not be met with equal force. Access to security resources, or even technology as a whole, is very disproportionate across school districts in the United States. Where a district like the LAUSD can flag for immediate FBI intervention, other school districts may not even notice security breaches or have the means to recover from them. This can put

the security of families at risk, and worse, because they lack the privileges of other communities, their information could be exploited and lead to greater problems. Therefore, cybersecurity needs to become a larger national concern, so threats can be prevented.

Works Cited

Arntz, Pieter. “Warning issued about Vice Society ransomware targeting the education sector.” *Malwarebytes*, 7 September 2022, https://www.malwarebytes.com/blog/news/2022/09/authorities-issue-warning-about-vice-society-ransomware-targeting-the-education-sector. Accessed 12 September 2022.

“#StopRansomware: Vice Society | CISA.” *US-CERT*, 6 September 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-249a. Accessed 13 September 2022.

“Update on the Los Angeles Unified School District ransomware attack. Spyware update. Data breaches and ransomware.” *CyberWire*, 12 September 2022, https://thecyberwire.com/newsletters/privacy-briefing/4/175. Accessed 13 September 2022.

Security Review

TikTok...Time to Address this New Social Media App

Originally capturing the talents of young users as the app Musical.ly, TikTok became the most downloaded app in the United States in 2018 ("TikTok surpassed Facebook, Instagram, Snapchat & YouTube in downloads last month"). Suddenly, children and celebrities alike were choreographing 15 second videos to audio from popular movies, songs, and more. These personalized videos grace upon a "For You" page curated uniquely for each person, with videos reaching up to millions of people. Both the ease of virality and eerily personal For You page have become a cause of concern, so much so that political figures and the president have debated taking executive action. But what makes TikTok so different from other social media platforms, like Facebook or Twitter?

TikTok is owned by the Chinese company ByteDance that was created in 2012 by software engineers Zhang Yiming and Liang Rubo. They centered their company around algorithmic personalization using AI, which followed with much success from their content and information sharing apps. Their ingenuity has challenged the way we view social media and its underlying effects on all aspects of society.

Assets:

- TikTok is the first social media app that doesn't require you to be social! You don't need friends, a following, or event posts to engage with the app. However, their personalized services come at a cost. They collect everything from keystroke patterns to location data that could easily become intercepted (confidentiality).
- User's find themselves absorbed by the selection of videos curated for them, so much so that some claim the app has mastered the art of "distractions". But its influence can easily become a tool for malice (integrity).

Threats:

- Officials in the U.S are already skeptical about China intervening in the app, although some may claim their worries are rooted in nationalism while others point out that all countries tend to meddle in social media all the time. But as a whole, government powers continue to be a concern to national security should they introduce micro propaganda or monitor the population of their adversaries.
- TikTok in itself is a threat to the user. Their vague data collection policies put the users at risk to be manipulated by their algorithms, sold out to companies or organizations, or be hacked at any moment.
- Any common individual could use the personal information uploaded on TikTok against their prey. They could easily stalk, harm, or release private information from the data they gather.

Weaknesses:

- Vague and technical app policies could be overlooked by users causing them to be unaware of opt out or data removal privileges.
- TikTok has a vast amount of data, but like any other software company their grasp on it can only be so tight. If data leaks occur, it could be more detrimental because of its specificity.

Defenses:

- TikTok has international headquarters to ensure their data is distributed and secured under regional standards. This makes international interference less of a threat.
- Transparency about data and privacy standards has shown that TikTok is following any technical legislation and maintaining neutrality. This helps users and legal enforcement understand the technical processes used by TikTok.

Risks:

Much like any other social media app, loses of data can be a huge threat to users world wide. However, in a different sense, the influence of TikTok does raise some concerns of potential manipulation if they or other groups try to direct the content of users. Although, in a broader sense, this has/could happen to other social media sites as well, so the concern should only remain level. In total, legislation and guidance surrounding technology and social media should be reevaluated first if changes should be made across the board. This includes being more transparent about data processes and stricter security measures.

Conclusions:

Social media has transformed the social landscape of everything from national diplomacy to local trends and continues to make itself more relevant in day-to-day life by the second. The issues that arise with the newfound popularity of TikTok are only remnants of those bound to all of the other media sites we use today. If anything, concerns about TikTok should be an example for national and international security groups to take social media more seriously. In the end, a balance between a users' expression and their security should be more apparent, thereby giving new social media platforms an example to follow by.

Works Cited

Newman, Lily Hay. "It's Time to Get Real About TikTok's Risks." *WIRED*, 6 September 2022, https://www.wired.com/story/tiktok-nationa-security-threat-why/. Accessed 12 September 2022.

Smith, Ben. "How TikTok Reads Your Mind." *The New York Times*, 5 December 2021, https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html. Accessed 13 September 2022.

"TikTok surpassed Facebook, Instagram, Snapchat & YouTube in downloads last month." *TechCrunch*, 2 November 2018, https://techcrunch.com/2018/11/02/tiktok-surpassed-facebook-instagram-snapchat-youtube-in-downloads-last-month/. Accessed 13 September 2022.