Rise of Ransomware Attacks on the Education Sector During the COVID-19 Pandemic

Malware has existed for decades. Ransomware has become one of the most financially devastating types of malware attacks and poses a serious threat to agencies, school districts and other organizations. The objective of ransomware attacks is to gain unauthorized access to files containing sensitive information while restricting access to the files by authorized users and demanding a ransom payment to release the restriction.

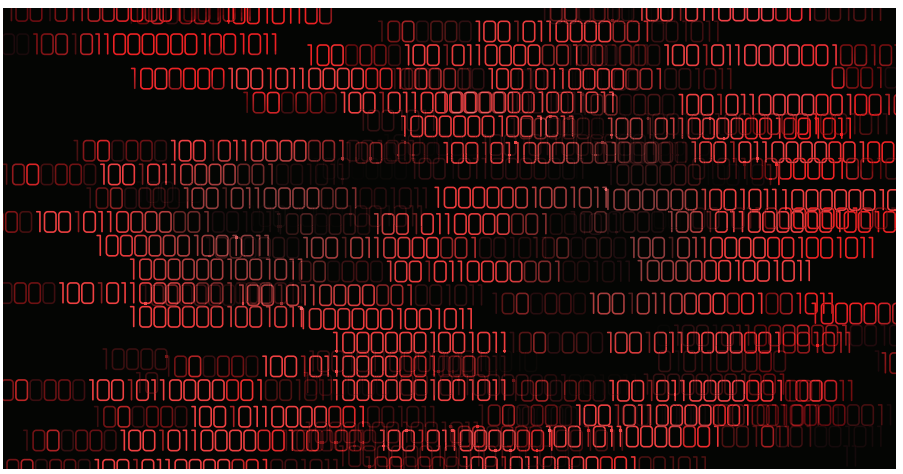
The number of ransomware attacks has increased tremendously given the expanding threat landscape. The COVID-19 global pandemic has further expanded the threat landscape with employees, consumers, teachers and students having to work, shop and learn from home. More digitally connected than ever before, school systems have been particularly vulnerable to the threat of ransomware attacks during the pandemic. Platforms such as Google Classroom, Zoom and other distance learning solutions were used by many educational institutions to continue learning for students after the suspension of in-person learning. This has its benefits and challenges, including excessive screen time and technical difficulties. Although some of the distant learning solutions are not as vulnerable to ransomware attacks for infrastructure, they have their own drawbacks, affecting both students and faculty.

Examining the rise of ransomware attacks on schools and identifying attack vectors during the emergence of the COVID-19 pandemic can offer recommendations such as the adoption of a security framework and mitigation strategies to address these issues and curtail this type of attack.

Rise of Ransomware Attacks

According to a report by Skybox Security, the creation of new ransomware samples increased by 72 percent during the first half of 2020, with 77 ransomware campaigns being observed during the first few months of the COVID-19 pandemic.[1]

The attack vectors of ransomware come in the form of malicious emails, compromised websites and infected file downloads. School districts and colleges worldwide were not immune nor prepared for the surge in ransomware attacks during the start of the global pandemic. At the genesis, the majority of school districts and colleges immediately put a stop to in-person learning for most students. Most institutions, and especially budget-challenged school districts, were unprepared for the immediate shift from in-person instruction to remote learning for their student and teacher populations. This made schools and colleges easy targets for malicious actors. The reliance on virtual learning, which put further burdens on limited technical



James G. Koomson
Is a doctoral student in cybersecurity at the School of Business and Technology (SBT) at Marymount University (Arlington, Virginia, USA). He can be reached at Jgk35311@marymount.edu.

resources, made these institutions more vulnerable. In the United Kingdom, due to the rise of attacks, the National Cyber Security Centre (NCSC) issued a warning that the education sector was being targeted specifically for ransomware attacks.[2] Also recognizing this vulnerability, the US Federal Bureau of Investigation (FBI) issued a warning to all K–12 schools to expect an increase in ransomware attacks during the COVID-19 pandemic and urged school districts to take extra precautions to secure their networks.[3]

On 16 July 2020, Ambrose University in Calgary, Alberta, Canada, received notification from Blackbaud of a ransomware attack that occurred. Malicious actors stole data from Blackbaud, one of the world's largest providers of education administration, fundraising and financial management software for nonprofits, to extort funds.[4]

On 4 September 2020, Newcastle University in Tyne, England, had its systems breached by the DoppelPaymer ransomware gang, exposing the data of staff and students.[5]

On 28 September 2020, Clark County, a Las Vegas, Nevada, USA, school district serving 320,000 students, became the largest school district to fall victim to a ransomware attack since the beginning of the COVID-19 pandemic.[6]

On 29 October 2020, a ransomware attack occurred against Las Cruces, a public school system in New Mexico, USA, which shut down computers and networks across the district. The school district's IT teams reportedly reacted quickly, shutting down all computers immediately after detecting the attack to evaluate the extent of the damage and develop a remediation plan.[7]

In March 2020, the Sheldon Independent School District in Texas, USA, which is home to 10,000 students, experienced a ransomware attack and paid nearly US$207,000 in ransom after hackers locked officials out of critical software systems, blocking access to emails, important staff data and security cameras.[8] Based on searches of hacker sites on the dark web, *The Wall Street Journal* has documented nearly three dozen ransomware attacks against school districts in the United States since March 2020.[9]

Effects

While there is a continued increase in the amount of ransomware attacks during the pandemic due to the expansion of the threat landscape from the shift to virtual learning, the effects on educational institutions that fall victim can be staggering in many ways. Ransom demands from attacks can be a major financial blow to institutions that already have budget challenges. On 3 June 2020, the University of California (San Francisco, USA), which has helped with COVID-19 research, paid a US$1.14 million ransom demand after NetWalker threat actors infected several servers in the university's School of Medicine with ransomware.[10]

Financial loss is not the only effect of ransomware attacks on academia—the unauthorized access to confidential and personally identifiable information (PII), which can contain financial details, names, addresses and Social Security numbers, has major implications if it is accessed by the wrong people. The compromised PII of students and faculty can lead to identity theft and lawsuits by victims, against the schools, for not exercising due care of their information or failure to remediate the damage caused by the data breach.

"THE COMPROMISED PII OF STUDENTS AND FACULTY CAN LEAD TO IDENTITY THEFT AND LAWSUITS BY VICTIMS, AGAINST THE SCHOOLS."

Prevention

Since 2019, more than 1,000 educational institutions have fallen victim to ransomware.[11] Coupled with the fact that ransomware attacks are surging during the COVID-19 pandemic, this indicates that ransomware attacks plaguing US educational institutions are not slowing down

anytime soon. Therefore, educational institutions must be proactive in implementing preventive measures to reduce the risk of ransomware attacks. Security awareness training for both faculty and students helps users know how to identify phishing emails and suspicious links. Creating and storing backups of official school data at an offsite location are also vital in the event of a ransomware attack, as those remote files do not get compromised.

Another effective measure for schools is to implement strong passwords, which include a combination of special characters and numbers and are required to be changed frequently. Vulnerability scanning and patching is very effective in identifying weaknesses that need to be mitigated on the school's network. This reduces the likelihood of threat actors exploiting the weaknesses to gain unauthorized access to the network.

School districts and universities should consider cybersecurity insurance in addition to implementing measures to reduce the risk of ransomware attacks. Procuring cybersecurity insurance is essential for the education sector in the event of an attack on a school's network, which can result in data being lost, compromised or stolen. Insurance assists with remediation of ransomware and other cyberattacks or incidents and mitigates a school's liability for damages caused to students and faculty.

Conclusion

If significant action is not taken, ransomware attacks will continue to plague the education sector more frequently with the expanded threat surface as a result of distance learning during the COVID-19 pandemic. Although many schools have limited budgets, measures can be taken to show due care and protect the PII of their student and faculty populations. There is no silver bullet to protect against cybersecurity events such as ransomware attacks. However, implementing a defense-in-depth layered approach and adopting a security framework, such as the US National Institute of Standards and Technology (NIST) Cybersecurity Framework, will likely reduce the risk of future attacks. In the future, cybersecurity experts could examine the common types of ransomware attacks on schools and conduct a comparative analysis of how two school districts in different cities, states or countries with different operating budgets respond to ransomware attacks on their school environment.

"INSURANCE ASSISTS WITH REMEDIATION OF RANSOMWARE AND OTHER CYBERATTACKS OR INCIDENTS AND MITIGATES A SCHOOL'S LIABILITY FOR DAMAGES CAUSED TO STUDENTS AND FACULTY."

Endnotes

1 Skybox Security, *Tear Up the Cybersecurity Rule Book: Pioneer a New Approach to Vulnerability Management*, USA, 2020, *https://lp.skyboxsecurity.com/WICD-2020-11-VTM-POV_Asset.html*

2 National Cyber Security Centre (NCSC), "Cyber Security Alert Issued Following Rising Attacks on UK Academia," USA, 17 September 2020, *https://www.ncsc.gov.uk/news/alert-issued-following-rising-attacks-on-uk-academia*

3 Bernstein, J. A.; T. G. Vare; B. J. McGinnis; M. Arango; "Ransomware Attack on Nevada School District Highlights Newest Hacker Targets," *The National Law Review*, 2 October 2020, *https://www.natlawreview.com/article/ransomware-attack-nevada-school-district-highlights-newest-hacker-targets*

4 Ambrose University, Calgary, Alberta, Canada, "Ambrose Response to Blackbaud Data Breach," 20 July 2020, *https://ambrose.edu/ambrose-response-blackbaud-data-breach*

5 Martin, A.; "Newcastle University Students' Data Held to Ransom by Cyber Criminals," Skynews, 8 September 2020, *https://news.sky.com/story/newcastle-university-students-data-held-to-ransom-by-cyber-criminals-12066081*

6 *Op cit* Bernstein

7 Foresman, B.; "Ryuk Ransomware Shuts Down New Mexico School District a Second Time," EdScoop, 26 February 2020, *https://edscoop.com/ryuk-ransomware-shuts-down-new-mexico-school-district-second-time/*
8 Willey, J.; "Sheldon ISD Forced to Pay Nearly $207K After Hackers Targeted Servers," ABC 13, Houston, Texas, USA, 15 October 2020, *https://abc13.com/sheldon-isd-ransom-school-district-hacking-from-hackers-online/7036662/*
9 Hobbs, T. D.; "Schools Struggling to Stay Open Get Hit by Ransomware Attacks," *The Wall Street Journal*, 13 November 2020, *https://www.wsj.com/articles/my-information-is-out-there-hackers-escalate-ransomware-attacks-on-schools-11605279160*
10 Davis, J.; "UCSF Pays $1.14M to NetWalker Hackers After Ransomware Attack," Xtelligent Healthcare Media, 29 June 2020, *https://healthitsecurity.com/news/ucsf-pays-1.14m-to-netwalker-hackers-after-ransomware-attack*
11 Spadafora, A.; "Over a Thousand Schools Hit by Ransomware in 2019," *TechRadar*, 18 December 2019, *https://www.techradar.com/news/over-a-thousand-schools-hit-by-ransomware-in-2019*