Attacks on Online Learning - Rapidly Rising

The feds have warned that cyberattacks on the education sector are ramping up alarmingly. In an alert from the FBI and the Cybersecurity and Infrastructure Security Agency, officials said that data from the Multi-State Information Sharing and Analysis Center shows that in August and September, 57 percent of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to just 28 percent of all reported ransomware incidents from January through July. Ransomware is not the only problem, though CISA and the FBI said that trojan malwares, distributed denial-of-service attacks, phishing and credential theft, account hacking, network compromises and more have all been on the rise since the beginning of the school year. Whether as collateral for ransomware attacks or to sell on the dark web, cyber-actors may seek to exploit the data-rich environment of student information in schools and education technology services, according to the joint advisory.

"The need for schools to rapidly transition to distance learning likely contributed to cybersecurity gaps, leaving schools vulnerable to attack. In addition, educational institutions that have outsourced their distance learning tools may have lost visibility into data security measures. "On the ransomware front, malicious cyber-actors have been adopting tactics previously leveraged against business and industry, while also stealing and threatening to leak confidential student data to the public unless institutions pay a ransom. " The five most common ransomware variants identified in incidents targeting K-12 schools this year are Ryuk, Maze, Nefilim, AKO and Sodinokibi/REvil, the feds noted.

Unfortunately, K-12 education institutions are continuously bombarded with ransomware attacks, as cybercriminals are aware, they are easy targets because of limited funding and resources. government is aware of the growing need to protect the schools and has put forth efforts to provide the proper tools for education institutions. A bill has been introduced called the K-12 Cybersecurity Act of 2019, which unfortunately has not been passed yet. "Meanwhile, other malware types are being used in attacks on schools 0with ZeuS and Shlayer the most prevalent. "

"Attackers also are continuing to exploit the evolving remote learning environment, officials warned, often using exposed Remote Desktop Protocol services to gain initial access for further attacks. " Cyber-actors likely view schools as targets of opportunity, and these types of attacks are expected to continue through the 2020/2021 academic year, according to the joint alert.

Recommendation

While schools and IT professionals may focus on acquiring the technology to prevent phishing emails from entering the teachers and staff mailboxes, it will be necessary to educate them properly. Implementing a robust security awareness program will be essential to help educate staff, teachers, and administration to effectively spot a phishing email and report to their IT departments to handle swiftly.

References

https://www.ciol.com/5-indian-government-provided-free-online-courses-with-certificates-lockdown/

https://threatpost.com/feds-k12-cyberattacks-rise/162202/

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/online-learning-still-struggles-especially-with-security.html

https://core.ac.uk/download/pdf/54844947.pdf