NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

Education Sector: An Attractive Target for Cyber-Attacks

February 7, 2018

TLP: **WHITE** | ***The NJCCIC assesses with high confidence that educational institutions across the globe will remain attractive targets for a range of cyber-attacks designed to disrupt daily operations, steal sensitive data, instill fear in the community, and hold critical operational data for ransom.*** In October 2017, the US Department of Education issued an updated Cyber Advisory warning schools about a new method of cyber extortion impacting institutions across the country. In recent attacks, cyber-criminals demanded large ransom payments in exchange for sensitive student record information obtained via schools' compromised networks. In some instances, cyber-criminals made direct threats to the safety of students and staff members via SMS messaging. According to Verizon's 2017 Data Breach Investigations Report, the education sector was impacted by approximately 455 security incidents in 2016, with at least 73 of these events involving the disclosure of data. As the use of technology within the classroom is increasingly required for educational purposes, more schools are implementing Bring Your Own Device (BYOD) policies, allowing students and employees to connect their personal computers, tablets, and mobile phones to their networks. Unfortunately, if BYOD is not implemented with security in mind, schools could be exposing their networks and sensitive data to an increased risk of compromise created by vulnerable and infected devices. Sophisticated and profit-motivated threat actors are cognizant of this fact and will continue to target universities and school districts as many of them do not have adequate resources, funding, or staffing to properly protect and defend their networks.

- The NJCCIC recently alerted its education sector members to a cyber-extortion campaign targeting educational institutions in Florida. In this targeted attack, emails were sent to the presidents of several colleges and universities threatening mass shootings and bombings if a payment of 1.2 Bitcoin, approximately $18,000 USD at the time, was not received. The emails originated from *onlyfair[@]protonmail.com* and reportedly contained threats of imminent violence against students and staff.

- In November 2017, SchoolDesk, a company that provides website hosting solutions for schools, suffered a breach by a hacking group known for distributing ISIS propaganda videos. The breach resulted in the defacement of the Bloomfield Public School District website, where an ISIS-sponsored video was displayed for approximately two hours before being detected and removed. Although no sensitive information was accessed or released, the ability of threat actors to gain remote access to web servers highlighted the impact that third-party vendor vulnerabilities can have on educational institutions.

- A group known as *The Dark Overlord* claimed responsibility for the breach of numerous school districts in several states across the US in late 2017, including the Johnston Community School District in Iowa, the Splendora Independent School District in Texas, and the Columbia Falls School District in Montana. The breaches stemmed from compromised servers that exposed confidential information including names, phone numbers, and addresses of students, parents, and staff. In some instances, students and parents received violent, threatening messages from the attackers resulting in school closures and canceled extracurricular programs.

Recommendations

The NJCCIC advises our education sector members to take proactive steps to reduce their cyber risk, beginning with comprehensive audits of their networks to identify and patch existing vulnerabilities in outdated operating systems, applications, servers, and websites. Continuously monitor systems for indicators of compromise by running reputable and up-to-date antivirus software and maintain network traffic logs in accordance with your data retention policy. Limit user privileges to only those systems and files required by one's job functions, and implement strict authentication policies incorporating mandatory password resets, minimum character requirements, and multi-factor authentication for email, web services, and remote access tools. Additionally, encrypting systems and databases that contain sensitive personal data, financial information, and user credentials can mitigate the impacts of data breaches and render stolen data useless. Have an incident response plan in place and report cyber-attacks to your local police department, the FBI, and the NJCCIC.