What cybercriminals want from your schools

Malwarebytes

Introduction

Cybercriminals target educational institutions for a treasure trove of personal and financial data.

As 21st century digital learning standards have moved from novel to classroom imperative, state governments and private companies have been leading the charge in providing US K–12 schools with educational technology hardware and software. According to the 2018 State of the States Report, 44.7 million students and 2.6 million teachers already have access to technology in their classrooms.[i] The impetus for introducing tech initiatives on campus is for improved quality of education, differentiated instruction, and the ability to engage students through familiar media, as well as more streamlined monitoring, management, assessment, and communication systems for administrators and teachers.

Yet, however much edtech may represent a promise for future classroom utopia, adoption and integration has been a massive challenge. Insufficient Internet bandwidth, unreliable Internet access, little to no provision for low-income students who don't have devices to access the Internet, and a body of teachers who may be technically challenged are some examples. Even more concerning for school IT teams, though, are the risks these technologies pose to the security of systems and student data, and how institutions can thwart criminal attempts at gaining access.

Every day, schools are exposed to cyberthreats like phishing emails, distributed denial-of-service (DDoS) attacks, insider threats, and malware—with the most disruptive coming from information-stealing Trojans and ransomware attacks.[ii] There have been 491 reported incidents of cyberattacks in schools throughout the US since 2016.[iii] If we consider reports that were not publicly disclosed, this number is likely much higher. With the ever-changing threat landscape and the growing sophistication of targeted attacks against organizations, endpoints in educational institutions need to be protected now more than ever.

> **"There have been 491 reported incidents of cyberattacks in schools throughout the US since 2016."**

For schools to effectively implement security measures unique to their environment, they must first understand why cybercriminals are trying to breach their networks. This paper identifies the top four educational institution targets for cybercriminals and the impact of their compromise on students, staff, parents, and the community. But before we get to that, let's first get to know the types of cybercriminals educational institutions face.

A bio: who attacks EDU?

In an interview with Malwarebytes[iv], Douglas Levin, founder and president of EdTech Strategies, revealed two of the most common types of cybercriminals who target education institutions: “[First], those scanning the Internet for insecure systems or soft targets, but who care little for who the target is, and [second], those who have chosen to directly target schools as institutions or even specific schools.”

Cybercriminals, being an opportunist group, are often attracted to schools because many are described as “low-hanging fruit”—easily penetrable due to outdated technological infrastructure, lack of dedicated IT and security staff, and little knowledge of basic cybersecurity hygiene and risk management.

There are also cybercriminals who specifically target K–12 schools to extract valuable data that they then sell on the black market or to extort the institutions for financial gain.

> **“Cybercriminals, being an opportunist group, are often attracted to schools because many are described as ‘low-hanging fruit’.”**

“While most people don’t think of schools as wealthy institutions, it can be easy to confound the difference between having enough money for your needs and managing a lot of money,” said Levin. “School districts manage facilities, transportation, food service, and healthcare—plus, in many communities, they are the single largest employer. We’ve seen evidence that knowledgeable cybercriminals who have targeted schools understand this difference.”

A bio: who attacks EDU?

Such targeted attacks begin with recon conducted to find key staff members, vendors, and IT systems under their employ. The threat actors then use social engineering tactics—usually in the form of phishing emails—to kick off their campaign. All it takes is for one administrator to open one malicious email attachment, and soon entire networks could be taken down by malware.

The third type of attacker may or may not be a cybercriminal, but they have the potential and the means to deal damage to educational institutions, whether with malicious intent or not: the insider threat.

Insider threats range from disgruntled former employees looking to bring chaos to their old organizations to students who are bored in class and want to cause a little mischief. Like cybercriminals, money could be a motivator, but others include getting back at colleagues and/or the organization—a tactic of current or former staff members—or making sure that they ace the semester with excellent marks—which is what cheeky but failing students do.

> **"Insider threats range from disgruntled former employees looking to bring chaos to their old organizations to students who are bored in class and want to cause a little mischief."**

Top 4 cybercriminal targets in EDU

Learn more

TARGET 1 Student and staff personally identifiable information (PII)

“Data belonging to children yields a heftier return for cybercriminals because they are, essentially, clean slates.”

While some schools have opted to house pertinent data they keep on record in the cloud, many tech-enabled schools keep theirs locally. Per student—enrolled and graduated—they store a wide range of information, such as name, date of birth, current home address, their parents' information, email address, headshot photo(s), biometric information, emergency contact number(s), Social Security number (SSN), academic grades, benchmark tests, attendance, behavioral records, health records (including any testing and diagnoses for learning disorders, mental illnesses, allergies, and diseases), and geolocation information.

Schools keep most of the same information about their personnel, with the addition of employment history; designation; access rights to bank accounts, systems, and data repositories; salaries; health benefits enrollment information, and more.

Cybercriminals can sell information deemed valuable either individually or as a data set, which underground criminals refer to as “fullz”—a selling jargon that means the full identity package of a person. The form most commonly sold is the latter.

Data sets belonging to children ages 18 years and below are most sought after by cybercriminals.[v] In fact, children experience a 51 percent higher rate of identity theft than adults, and a single child's data set is worth $300, typically delivered via untraceable digital currency compared to about $10 to $25 for an adult data set.[vi] Data belonging to children yields a heftier return for cybercriminals because they are, essentially, clean slates. Children have perfect credit scores, and the younger the child the data set belongs to, the longer the criminals can keep selling, reselling, and using them for profit.

Impact of PII theft on students and staff

A cybercriminal owning a single data set of a child who goes to school or an adult working in the school can fully take over their identities by posing as them when dealing with governments and private institutions, whether that's for tax purposes or taking out a loan. They can also mix up or combine certain data to create a new identity profile. These new profiles are called "synthetic identities," which Forbes said was responsible for the $6 billion loss banks experienced in 2016.[vii]

On students

A child's SSN with its flawless credit standing alone can open several opportunities to commit fraud that miscreants no doubt go after. For example, organized criminals can open an account using the stolen child's SSN, to which they can then order a money mule to route illicit money.

Child data can also be used to threaten children and their families with violence,[viii] which was the case when a group of hackers broke into several school districts in different US states when their demands weren't met. Furthermore, this same group posted names and contact numbers of students to encourage predators to target them.[ix]

On staff

Staff data can also be used for identity theft, but often for the purpose of targeting other employees. Cybercriminals do this by impersonating a school official, such as a principal, and creating either a spear phishing email persuading a recipient to open a malicious attachment or asking a member of payroll to change the bank account linked to the principal's direct deposit,[x] thus routing the money from the principal's account to one cybercriminals control.

Impact of PII theft on educational institutions

Schools whose network is successfully breached will surely take a reputational hit, more so if the educational institution wasn't able to warn parents and staff about it early on. Yet in some cases, schools will knowingly hold off disclosing the breach as they actively investigate the matter with experts and law enforcement. Sadly, this tactic can lead to a ruined holiday for those who may have been affected by the data breach. Case in point: The San Diego Unified schools announced a compromise in their network on the cusp of a winter break.[xi] A portion of the data that may have been stolen dated back to 2008, the total victims numbering to more than half a million individuals.[xii]

> **"Schools that were not compliant might be further financially impacted by fines from the US Department of Education."**

Educational institutions also face harsh criticism from parents, guardians, and community members in response to a breach. Immense pressure to rapidly improve on current infrastructures and implement better security procedures must be reconciled with tighter budgets and lack of human resources; meanwhile schools that were not compliant might be further financially impacted by fines from the US Department of Education (ED), the Children's Online Privacy Protection Act (COPPA), state privacy or data security regulations, the Global Data Protection Regulation (GDPR), and even the possibility of Title IV funding being revoked.[xiii]

TARGET 2 Financial information

IT departments within education institutions have a demanding job, as they face the challenges of consumerization that BYOD and open campus cultures introduce. It's common for education institutions to support a combination of school-provided and student-owned devices on campus. The school's IT team may manage some devices, but most are handled directly by the user.

Allowing your students to bring their own devices provides advantages, such as reducing technology costs and facilitating a better learning experience both in the classroom and at home. However, it also introduces security risk.

> **"Cybercriminals have become adept at mimicking legitimate financial emails from organizations and individuals that schools might regularly come in contact with."**

Educational institutions store data either on-premise or in the cloud. Apart from student data, educational institutions also store information about their staff, which includes viewable paychecks, pay invoices, payroll deduction information, tax deduction, names of financial institutions, account numbers, routing numbers, salary, and others like fundraising efforts and budgets for teacher training. Not all financial data from schools are useful to cybercriminals, but when they do get something they can use, they leverage it to steal from the educational institution or from the affected staff themselves.

With hundreds to thousands of Internet-connected endpoints running at the same time in an ecosystem, much like in a corporate setting, there is always the possibility of someone opening an attachment or clicking a link in a phishing email, unknowingly welcoming malware into the school system to search for financial information. In addition, cybercriminals have become adept at mimicking legitimate financial emails from organizations and individuals that schools might regularly come in contact with, whether that's a nonprofit outreach program director or a banking institution.

TARGET 2 Financial information

The Trojan Emotet impacted a district in North Carolina in this way. This malware was introduced to school networks through a spear phishing email, which was designed to look like an invoice from the antivirus vendor the school uses.[xiv] This scenario has played out countless times before, and if students and staff remain unaware of such threats and their role in keeping the school safe, it will keep on playing.

As we can see, one way cybercriminals can get their hands-on financial data housed in educational institution repositories is by using Trojans with the likes of Emotet and TrickBot, which are both designed to siphon out information. Oftentimes, a campaign is comprised of a combination of two or more sophisticated threats, which was the case when Emotet, TrickBot, and Ryuk, a ransomware that causes endpoints to freeze up by rendering files inaccessible until a ransom is paid, were seen teaming up to form a triple threat against three public schools districts in Louisiana, forcing its cybersecurity commission to declare a state of emergency.[xv]

Impact of stolen financial data

Once cybercriminals possess relevant financial information owned by the district, they can unlawfully access the account and wire money from it to accounts they own, resulting in the significant drain of taxpayer money, which further puts staff livelihood at risk. This is a terrible blow, especially to teachers who are already struggling to make ends meet. From here, the effect of insufficient funds will ripple out to affect students who are dependent on the critical programs and support the school offers, such as special needs instruction.

A financial data attack against educational institutions of this magnitude can easily be likened to incidents where schools are victimized by ransomware. In a ransomware attack, it may be necessary to temporarily cancel classes of the affected school while school IT personnel (or a third-party cybersecurity team) and law enforcement conduct their investigation and begin recovery procedures. It may also be necessary for a district to cancel other educational programs and facilities, such as after-school activities and childcare centers, respectively.

“This is a terrible blow, especially to teachers who are already struggling to make ends meet.”

The school itself isn’t the only one at risk of fraud. Even staff can be targeted individually once threat actors have copies of their W-2 tax forms, where information in them can be used to commit tax fraud. In guidance issued by Internal Revenue Service (IRS), the organization identified a tactic that phishers employ to fool certain employees of education organizations.[xvi] The social engineering aspect of the attack involves fraudsters impersonating a high-ranking school district official, such as the Superintendent, to get payroll or HR to hand over copies of staff W-2 tax forms. Unsuspecting employees, believing the ruse, could easily send the files without thinking twice. At this point, fraudsters now have a trove of data they can simply handpick from and file false tax returns under their school employee’s name.

TARGET 3 Education technology providers, vendors, or third-party suppliers

Weak security of third-party vendors in the supply chain was revealed as a new threat vector after cybercriminals breached Target through one of their refrigeration contractors in 2013. Unfortunately, educational institutions are not immune to supply chain attacks. In his work at EdTech Strategies, Levin has seen such attacks happen against schools through unsecured educational technology applications, vendors, and other suppliers. “Without adequate legal and contractual protections, some schools are finding that they have little recourse in such incidents,” according to Levin.

“Cybercriminals also target vendors directly, knowing that they, too, store information on students and staff.”

In some cases, threat actors target third parties as a means to an end, looking for a less secure, easier entry into school district networks. For example, cybercriminals might first compromise a third-party and lay dormant on their network, pouncing at the first opportunity to grab login credentials to the school network. In cases where Levin saw districts targeted, criminals lodged social engineering attacks against school personnel pretending to be an authorized vendor with the intent to redirect huge sums of money from vendor accounts to their own.

On the other hand, cybercriminals also target vendors directly, knowing that they, too, store information on students and staff. This is especially true of edtech companies and learning management systems, which store student and parent emails, logins, and assessments, and may also offer threat actors a way into home networks. This was what happened to online educational platform Edmodo in 2017, when crooks stole the data of more than 77 million student, teacher, and parent users, including emails and hashed passwords.[xvii]

Impact of vendor compromise on schools

In scenarios where educational institution vendors, providers, or partners are breached for school district data, the K–12 schools themselves are not liable to pay any post-breach costs. Sadly, the result is still the theft and sale of data about staff, students, and their parents in underground markets in the dark web with the risk of identity theft and account takeovers becoming high.

In addition, schools already on tight budgets might need to come up with additional cash to pay the real vendors if criminals stole from vendor accounts. Finally, students connecting to compromised educational technology platforms at home can endanger their home networks and infect additional devices.

> **“Students connecting to compromised educational technology platforms at home can endanger their home networks and infect additional devices.”**

In addition, school districts can find themselves at the receiving end of blame and criticism. As data owners, it’s important for them to ensure that they know how technology providers store, process, secure, and use the data they share before deciding to use their products. It is also the school’s responsibility to inform parents and caretakers about a breach to a vendor’s product they use. But more notably, school staff members themselves spend a lot of time and effort communicating follow-ups to parents, and administrators are often bogged down in legal work. Such vendor-related breach cases should serve as a wake-up call to educational institutions who may be ill-equipped to assess third-party risks. This is a nascent concern, especially for K–12 schools who have adopted edtech and those who are planning to do so.

TARGET 4 Public communication channels and the school system

“Distributed Denial of Service (DDoS) attacks to shut down the school’s Internet for the day-the modern-day equivalent of pulling the fire alarm.”

Not everyone who attacks school networks are looking for data or profit. And not all attackers are outside the school campus.

Every now and then, there are stories of students using keyloggers—a malicious program that captures and records the keys pressed on a keyboard—to hack into teachers’ computers to change grades. Or sometimes, bored or mischievous students might launch Distributed Denial of Service (DDoS) attacks to shut down the school’s Internet for the day—the modern-day equivalent of pulling the fire alarm.[xviii]

Students, current and former, aren’t the only ones capable of becoming insider threats. Disgruntled or opportunistic staff, parents, former employees, or volunteers can also cause damage, especially if they still have unrevoked access or working credentials they can use to amass personal data. In one case, a former teacher was able to access the school’s records and make extensive changes to it.[xix]

While there are hacker groups who compromise official school social media accounts,[xx] there have also been instances when insiders were able to hijack such accounts to make violent threats,[xxi] often times with no known motivation.

Impact of tampering with operations, school records, and social media accounts

On operations

Students or other insiders looking to disrupt the school day by compromising technology can do a number on instructional hours, which would be severely impacted by a DDoS attack. Any use of the Internet, computer labs, or other devices would be prohibited, and lessons that were formerly differentiated or made more engaging through technology would have to be revised on the spot. In addition, potential media coverage of the event could distract students and teachers even further. This may seem petty compared to having PIIs leaked, but the outcome—severe disruption of the school's normal day-to-day operations—remains the same.

On social media

Social media channels have given educational institutions opportunities to communicate with students, staff, and parents in real time that were never available before. However, using them also puts the reputation, spirit, and values of the school at risk.

A hijacked social media account, if not given back to its rightful owner quickly, could be used to promote content that is inaccurate or misrepresentative of the school, bullies its students or teachers, or promotes hateful language or philosophies. Worse, it could be used to lead followers to visit dangerous sites, such as a scam page, a phishing page, or a page housing malware.

On school system records

Depending on how extensive the changes to student records, remediation could range from as simple as ordering the student or staff to change the data back to the arduous (and expensive) process of attempting to restore hundreds of deleted, manipulated, or generally vandalized student records.[xxii] In this event, classes may be suspended for days or weeks until the restoration process is finished and the school can function as normal.

World regulations protect school data

Below is a list of current regulations that are enforced in the US and other countries to ensure that student data in K–12 and/or primary schools is protected, secured, and used responsibly:

- US: Child Online Privacy Protection Act (COPPA)
- US: Family Education Rights and Privacy Act (FERPA)
- European Union (EU): General Data Protection Regulations (GDPR)
- The Philippines: Data Privacy Act of 2012 (DPA)
- Bermuda: Personal Information Protection Act of 2016 (PIPA)
- Australia: Privacy Act

Conclusion

When it comes to making a buck out of stolen information, cybercriminals have always targeted vulnerable systems and people, whether it's local government bodies, healthcare institutions, nonprofits, or grandmas and grandpas who are not technically savvy. Cybercriminals don't discriminate. And unfortunately, educational institutions today are all vulnerable.[xxiii]

It is important for education boards and IT professionals to be reminded that they have a fiduciary responsibility to ensure that student and staff PII, including financial information, are protected; educational ecosystems run as normal; and teaching hours are continuous. Fortunately, there are several tactics they can take to fulfil these.

Because cybercriminals have adopted a multi-vector offensive technique—a mixture of malware, social engineering, and hacking—implementing a multi-vector defensive stance to protect endpoints is the next logical step. This is done by combining good security hygiene practices and technologies that provide layered protection and detection.

Take your first step to endpoint protection

For more information about how Malwarebytes protects school endpoints from malware, visit:

www.malwarebytes.com/education

[i] EducationSuperhighway. 2018 State of the States Report. October 2018.

[ii] Malwarebytes Labs. What K-12 schools need to shore up cybersecurity. February 2019.

[iii] The K-12 Cybersecurity Resource Center. The K-12 Cyber Incident Map. Active January 2016.

[iv] The interview was conducted on 5 June 2019 via email.

[v] Carnegie Mellon University's CyLab. Child Identity Theft. March 2011.

[vi] CNN Money. Infant Social Security numbers are for sale on the dark web. January 2018.

[vii] Forbes. The Battle Against Synthetic Identity Fraud Is Just Beginning. February 2018.

[vii] IC3. PSA: Education Technologies: Data collection and unsecured systems could pose risks to students. September 2018.

[ix] The Washington Post. Education Department warns of new hacker threat as 'Dark Overlord' claims credit for attacks on school districts. October 2017.

[x] The K-12 Cybersecurity Resource Center. OH: Scam targets school districts' direct payroll deposits. March 2019

[xi] YouTube. Data breach at San Diego Unified School District. December 2018.

[xi] The K-12 Cybersecurity Resource Center. The State of K-12 Cybersecurity: 2018 year in review. February 2019.

[xii] Patterson Belknap. Education Department Toughens Tone on Cyber and Threatens to Pull Funding for Non-Compliance. February 2018.

[xiv] WebTitan. Emotet Malware Infection Cost Rockingham School District $314,000 to Resolve. January 2018.

[xv] Ars Technica. Louisiana declares state of emergency in response to ransomware attack. July 2019.

[xvi] IRS. Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others. February 2017.

[xvii] EdSurge. Hacker Steals 77 Million Edmodo User Accounts. May 2017.

[xviii] YouTube. Police: Teen Hacked Secaucus School's WiFi. April 2019.

[xix] YouTube. Disgruntled employee accused of hacking student records at Detroit school. April 2018.

[xx] EdWeek. Hacked Twitter Accounts a New Headache for Schools. September 2017.

[xxi] YouTube. School Threats Increasing In North Texas Since Florida School Shooting. February 2018.

[xxii] YouTube. Disgruntled employee accused of hacking student records at Detroit school. April 2018.

[xxiii] EdSurge. Report: A New Cybersecurity Incident Strikes K-12 Schools Nearly Every Three Days. February 2019.