Trustwave® SpiderLabs®

2024 Education Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE BRIEFING AND MITIGATION STRATEGIES

Contents

Executive Summary

"So many of our schools across the nation are, what we call, 'target rich, cyber poor' in that they are often a frequent target for ransomware and other cyberattacks due to the extensive data kept on school networks, often without the proper protection," stated the Cybersecurity and Infrastructure Security Agency (CISA), aptly summarizing the concerning state of cybersecurity in education.

Primary school systems handle sensitive data concerning minors, while higher education institutions must safeguard intellectual property data, making them prime targets for cyberattacks. These attacks not only threaten the safety and security of teachers and administrators, but they put the privacy of students, staff, and other associated entities at risk.

With millions of students now learning through technology in hybrid, remote, or in-class settings, device security is no longer optional. It's crucial to ensure a safe and secure learning environment for everyone. Strong cybersecurity measures not only protect student data but also enable teachers to do their jobs effectively without fear of disruptions or data breaches.

These disruptions directly contradict the sector's core mission of fostering knowledge and development. As a result, educators and administrators are facing heightened concerns about cyber resilience – and recent breaches illustrate the risks.

In May 2022, Illinois' Lincoln College was forced to permanently shut down due to the impact of a ransomware attack. In March 2021, the Buffalo Public Schools District was hit by a ransomware attack and as a result, spent nearly $10 million on network security, fraud monitoring and other services. In June 2023, The University of Manchester, which has over 10,000 staff and 45,000 students, confirmed it had been successfully attacked, and data belonging to alumni and current students was accessed and removed.

There are a number of factors that make the education industry especially vulnerable to cyberattacks, including:

- **BYOD Dilemma:** The "Bring Your Own Device" culture poses security challenges by adding unmanaged devices to the network, straining IT resources.
- **Complex Infrastructure:** Diverse devices, decentralized IT management, and inconsistent security practices create a sprawling attack surface with vulnerabilities.
- **Data Trove:** Huge volumes of sensitive student data (PII, research, IP) attract attackers seeking data breaches and identity theft, amplified by online collaboration and open internet access.
- **Exposed Systems & Services:** Publicly accessible network devices like servers, building management systems, access systems, and cameras lack proper security, increasing risk.
- **Resource Scarcity:** Limited budgets hinder investments in cybersecurity software and staff, leaving critical systems under-protected.
- **Legacy Risks:** Outdated IT systems remain vulnerable to exploitation due to lack of updates and security patches.

With hundreds of security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task in looking into what leads to these breaches. We are uniquely positioned to do so, as we perform over 200,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000 to 10,000 per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, gives us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

We will begin by highlighting the significant trends currently affecting the industry: the shift towards online education, third-party security risks, and the rise of ransomware. Subsequently, we will analyze the attack flow specific to the education industry, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across education and throughout the attack chain, including:

THREAT ACTORS

- LockBit 3.0
- Rhysida
- CLOP or Cl0p
- Akira
- ALPHV aka BlackCat
- Medusa
- Vice Society
- No Escape
- Royal
- Pirat-Networks
- Bl00dy Ransomware

THREAT TACTICS

- Phishing and Social Engineering
- Exploitation of Applications and Databases
- Drive-by Compromise
- Abuse of Valid Account Credentials and Password Attacks
- Access Brokers, Auctions, and WebShells
- BYOD and IoT Risks
- Third-Party Supplier Attacks
- Powershell and User Execution Techniques
- RDP, SMB, and DCOM Lateral Movement Techniques
- Ransomware and Cryptocurrency Miners

For additional information about the most prevalent threat actors, please go to the Appendix.

Emerging and Prominent Trends

Shift Towards Online Education

The Threat

During the COVID-19 pandemic, the push towards online learning exposed educational institutions to a vast network of devices and systems. While this creates incredible opportunities for accessibility, flexibility, and personalized learning, it also presents significant challenges. Concerns range from cybersecurity and the digital divide to privacy, technical issues, and potential social isolation.

Effectively integrating online education requires careful consideration of these risks and benefits. This includes exploring specific technologies, analyzing successful case studies, staying informed about the evolving landscape, and addressing ethical considerations like algorithmic bias and data ownership. Ultimately, navigating this shift responsibly involves understanding its complexities and paving the way for a future where online and offline learning combine seamlessly to reach students everywhere.

What Trustwave SpiderLabs Is Seeing

Trustwave SpiderLabs found significant exposure of critical systems and devices such as public file servers, printers, collaboration systems, and systems storing sensitive data.

Shodan analysis and scans revealed over 1.8 million devices related to the education industry being publicly exposed. As highlighted later in this report, this number significantly dwarfs the exposure in other sectors. Trustwave SpiderLabs also found instances of misconfigured and vulnerable devices, such as publicly accessible conferencing systems and collaboration tools, which could lead to unauthorized access and data breaches.

The operational disruptions caused by data breaches in education can be severe. An example is Lincoln College, which had to permanently close its operations due to a cyberattack. The ransomware attack blocked the college from accessing data used in its student recruitment and retention, as well as fundraising efforts.

Mitigations to Reduce Risk

- Implement strict access controls for critical systems, including file servers, printer management software, and collaboration tools. Strengthen access controls to minimum necessary levels for authorized users.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control. Disable Internet access for servers that do not require it.
- Address misconfigurations in network devices and other IoT devices, ensuring firmware is updated and default passwords are changed.
- Provide ongoing cybersecurity training and awareness programs for staff and students, emphasizing the importance of security best practices.

Third-Party Security Risks

The Threat

The education sector, like many others, relies heavily on third-party vendors such as software-as-a-service, hosting providers, storage, and IT services for various functions, including learning management systems, email, and communication and collaboration tools.

These third parties pose a grave risk to the education sector because of undiscovered or un-remediated gaps in their cybersecurity controls or data breach protection.

Breaches not only impact the directly targeted institution, but can also have a ripple effect across numerous educational entities relying on the same third-party services.

What Trustwave SpiderLabs Is Seeing

Notable incidents include the breaches of Illuminate Education and Blackbaud. The Illuminate breach in early 2022 significantly impacted two of the largest US public school systems, compromising the information of approximately 820,000 students in New York City alone.

The MOVEit RCE (CVE-2023-34362) vulnerability in a third-party file transfer service led to breaches at 13 major universities. These breaches had the highest prevalence from June to August 2023, most often facilitated by the ransomware threat actor Clop.

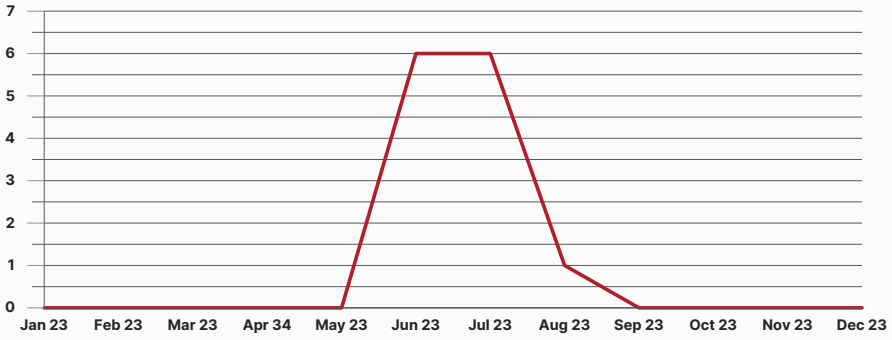


Figure 1: CVE-2023-34362 attack claims on notable universities (based on ransomware claims)

Mitigations to Reduce Risk

- Know your supply chain. Keep inventory of all critical suppliers and conduct a comprehensive security assessment before any form of engagement is initiated with a third party.
- Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, immediate breach notification, and compliance with pertinent data protection regulations.
- Encrypt all sensitive data in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- Follow industry standards and regulations like GDPR, HIPAA, FERPA, etc. for compliance with geographical location and nature of data handled by third-party vendors.
- Participate actively in cybersecurity forums of the educational sector and other information sharing platforms.

Ransomware Attacks

The Threat

Ransomware attacks have become a dominant source of breaches in education. These attacks can lead to the loss of critical educational and personal data, disrupt educational processes, and cause substantial financial and reputational damage to institutions.

To facilitate their attacks, threat actors deploy a range of malware types, including loaders/downloaders, infostealers, and RATs, to maintain control, steal information, and to facilitate the end-to-end ransomware process. Attacks targeting universities and primary education schools have led to severe operational disruptions including temporary and even permanent closures. Please refer to our later section on Ransomware for additional details.

What Trustwave SpiderLabs Is Seeing

Ransomware attacks striking the education industry are prominent and growing. For example, in 2023, Trustwave researchers monitored 352 ransomware claims against educational institutions.

The top ten ransomware groups targeting the industry were LockBit 3.0, Rhysida, CLOP (aka CL0P, Cl0p), Akira, Medusa, ALPHV, Vice Society, NoEscape, Royal, and Pirat-Networks. These groups have targeted a wide range of educational entities across different countries, predominantly in the US, but also in Canada, the UK, Australia, France, Germany. The types of institutions compromised vary from universities and colleges to public school districts, technical schools, and specific training centers.

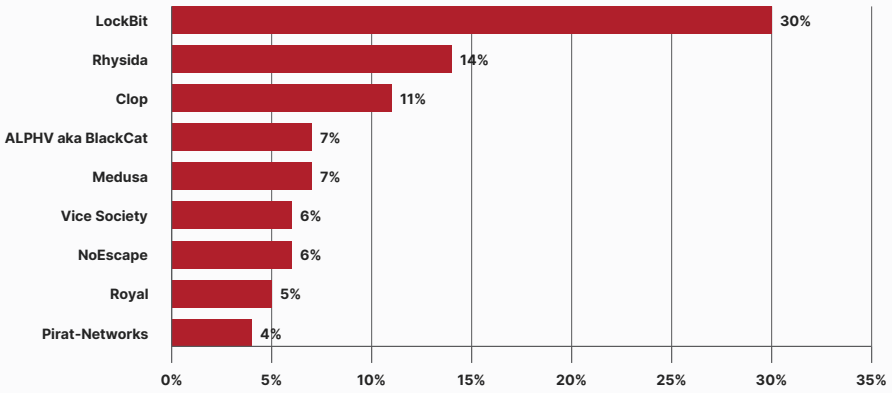


Figure 2: Top ten ransomware groups in the education sector

Mitigations to Reduce Risk

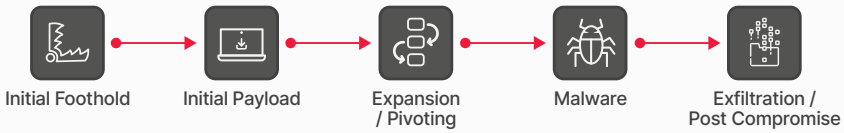
- Use host-based anti-malware tools that can assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- Establish and regularly practice a formal Incident Response process. Ensure backups are available as a contingency to recover from a worst-case scenario.
- Enable system logs on critical systems and workstations and implement network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.

Dissecting the Attack Flow for the Education Sector

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network, and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the education sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of the attack flow, the recommended mitigations provide proactive guidance to minimize the potential risks of financial, reputational, regulatory, or physical impacts to an education institution. The typical sequence of events unfolds as follows:



Attack Flow Steps

Initial Foothold

This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold into an education organization, like phishing, third party suppliers and exploitable vulnerabilities.

Initial Payload

Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target education.

Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will showcase how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.

Malware

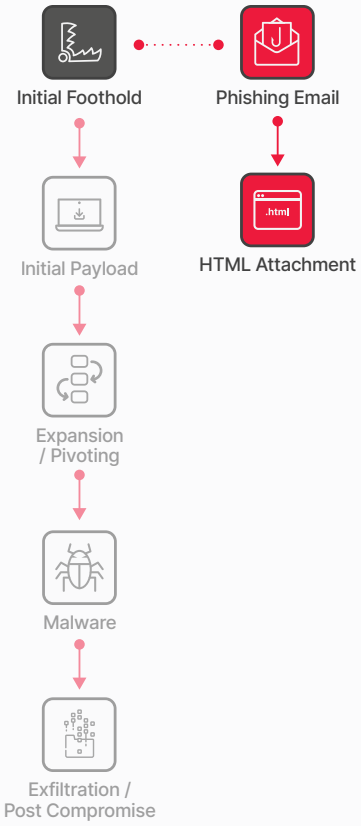
There are a variety of malware types with a myriad of uses, such as Remote Access Trojans (RATs), infostealers, ransomware, and many others.

In this section, we will focus on the types of malware pervasive in the education industry.

Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in education-related compromises. Additionally, we will present real-world examples of data breaches to provide concrete illustrations.



Initial Foothold: Phishing, Spam & Scams

The Threat

Phishing stands out as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit vulnerabilities in the software or systems on the network, attackers target staff, faculty, or others who have access to systems within the institution that can be exploited, such as finances, databases, etc.

In a typical scenario, the attacker crafts a compelling email, skillfully persuading the recipient to engage in certain actions. This could include opening an attachment, clicking a link, or executing specific instructions. Education-specific social engineering often involves sending fake university communications like offering enticing student job opportunities, which require the victim to perform certain tasks or provide sensitive information.

Typical phishing goals:

- **Credential Theft:** An example of this would be an email that appears to be from the university's administration, containing a link. When the recipient clicks this link, they are prompted to enter their login details under the pretense of accessing important information or job opportunity details.
- **Malware Insertion:** This is often executed through embedding PowerShell scripts, JavaScript, or enabling Macros in a document, which is disguised as being related to the university or a student job offer.
- **Triggering Specific Actions:** This could involve convincing the recipient to provide confidential information or perform other actions under the guise of a necessary step for a student job application or a university-related process.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team is committed to monitoring various email-based threats, such as opportunistic phishing, spearphishing, spam-based malware, and scams. In the past year, our team has noted interesting developments in the tactics and delivery approaches used in email-based attacks within education. These advancements have played a role in sustaining the continuing significance and effectiveness of these types of attacks.

In the education sector, the most common types of email attachments used for phishing and malware distribution are HTML files, executables, and PDFs, a trend that echoes observations from other industries. Notably, HTML attachments make up 82% of malicious email attachments. These attachments are primarily used in two forms: as standalone HTML pages designed for credential phishing, often featuring sophisticated obfuscation techniques, or as HTML redirectors leading to malicious sites. Additionally, Trustwave original research has also seen a preference of the use of HTML attachments in Phishing Kits.

Executable files, which make up the second most prevalent type, typically serve as either initial downloaders to facilitate further malware intrusion or act as the final payload, like Remote Access Trojans (RATs). Lastly, PDFs are commonly employed to host malicious links that initiate further malware downloads or contain deceptive text as part of a scam strategy, illustrating the diverse and evolving nature of email-based threats in education.

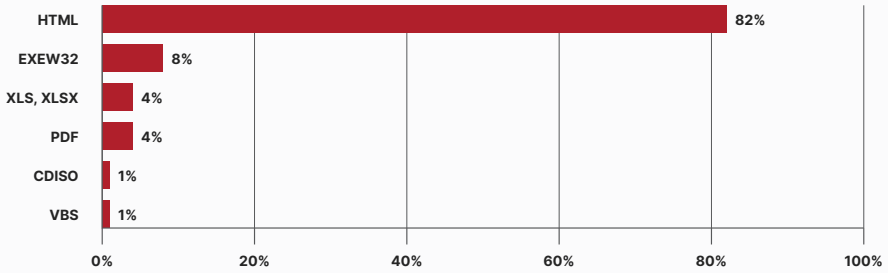


Figure 3: Top malicious attachment filetypes for the education sector

Trustwave researchers have observed that threat actors are frequently misusing specific services for these attacks. Decentralized InterPlanetary File System (IPFS) links, such as 'dweb.link,' are used to distribute phishing content, exploiting its network to avoid detection. Google Services, with domains like 'googleapis.com,' are abused for their trustworthiness to slip past security filters. Compromised WordPress sites, for example, 'howtotender.co.za,' are hijacked to host fake login pages. Cloudflare Services, including 'workers.dev,' are manipulated for their credibility to host phishing material. Additionally, free web and app hosting platforms, such as 'netlify.app,' are favored by phishers for cost-free malicious site creation.

In the education sector, Trustwave researchers have observed several notable phishing campaign themes:

RFQ-THEMED MALWARE SPAM

In a recent phishing scheme targeting universities, Trustwave SpiderLabs researchers observed attackers sending emails masquerading as “requests for quotations” from various educational institutions. To enhance their authenticity, these emails featured the spoofed university's logo in the message body and incorporated the institution's name in the 'From' and 'Subject' headers, as well as in the filenames of attachments.

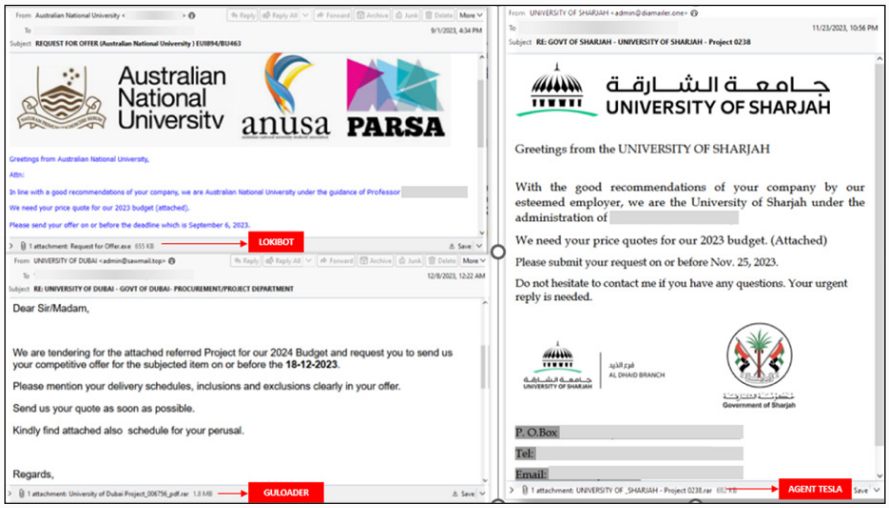


Figure 4: Sample of malicious “request for quotations” impersonating various universities

To further increase the authenticity of the attacks, the emails suggested that the quotations should align with the university's annual budget, with more details purportedly in the attached file. However, these attachments were either malicious executables or archives containing them. The threats most delivered through this phishing theme included the Lokibot Infostealer, Agent Tesla RAT, and Downloader Guloader.

FAKE UNIVERSITY COMMUNICATIONS

In another common phishing campaign, university accounts of students, faculty, and staff were targeted with fraudulent emails purporting to be official university communications.

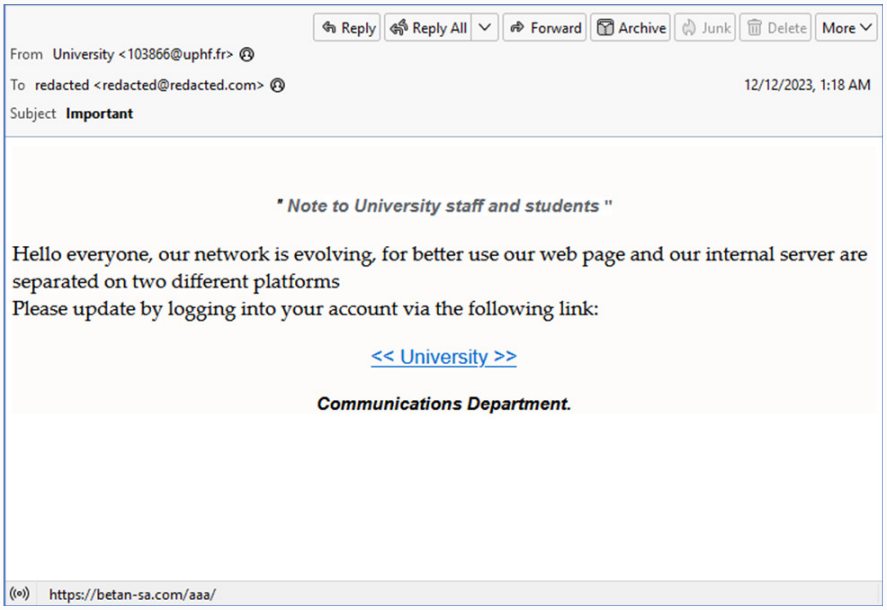


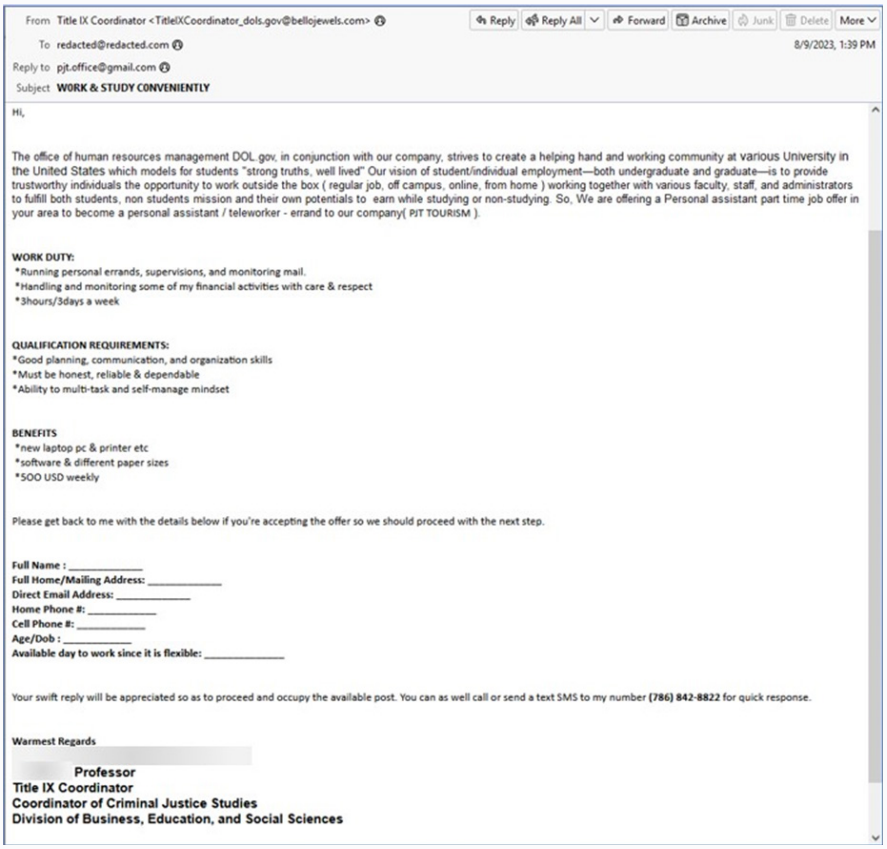
Figure 5: Sample of malicious email impersonating an official university communication that leads to a credential phishing site

These messages impersonated the university's IT department and were crafted to look authentic. They bolster their credibility by integrating the university's branding and language style, often relating to current university events or settings. The emails typically include urgent calls to action, such as requests to verify accounts or update personal information, and direct recipients to fake websites designed to harvest their credentials.

STUDENT JOB OFFER SCAMS

Trustwave researchers observed an uptick in scam messages targeting students with counterfeit job offers. These emails come unsolicited and usually present lucrative opportunities that promise high compensation for minimal effort and offer flexible working hours.

Typically, these communications initiate with a request for personal details as part of the job application process. Scammers may also demand an advance payment under the pretext of covering training expenses. In some cases, students receive a fraudulent check with instructions to deposit it and forward a portion of the funds elsewhere, only to find out later that the check is fake, rendering the student responsible for the total amount.



From Title IX Coordinator <TitleIXCoordinator_dols.gov@bellojewels.com>
Reply | Reply All | Forward | Archive | Junk | Delete | More
To redacted@redacted.com
8/9/2023, 1:39 PM
Reply to pjt.office@gmail.com
Subject **WORK & STUDY CONVENIENTLY**

Hi,

The office of human resources management DOL.gov, in conjunction with our company, strives to create a helping hand and working community at various University in the United States which models for students "strong truths, well lived" Our vision of student/individual employment—both undergraduate and graduate—is to provide trustworthy individuals the opportunity to work outside the box (regular job, off campus, online, from home) working together with various faculty, staff, and administrators to fulfill both students, non students mission and their own potentials to earn while studying or non-studying. So, We are offering a Personal assistant part time job offer in your area to become a personal assistant / teleworker - errand to our company(PJT TOURISM).

WORK DUTY:
*Running personal errands, supervisions, and monitoring mail.
*Handling and monitoring some of my financial activities with care & respect
*3hours/3days a week

QUALIFICATION REQUIREMENTS:
*Good planning, communication, and organization skills
*Must be honest, reliable & dependable
*Ability to multi-task and self-manage mindset

BENEFITS
*new laptop pc & printer etc
*software & different paper sizes
*500 USD weekly

Please get back to me with the details below if you're accepting the offer so we should proceed with the next step.

Full Name : _____
Full Home/Mailing Address: _____
Direct Email Address: _____
Home Phone #: _____
Cell Phone #: _____
Age/Dob : _____
Available day to work since it is flexible: _____

Your swift reply will be appreciated so as to proceed and occupy the available post. You can as well call or send a text SMS to my number **(786) 842-8822** for quick response.

Warmest Regards

Professor
Title IX Coordinator
Coordinator of Criminal Justice Studies
Division of Business, Education, and Social Sciences

Figure 6: Sample of a "Job Offer Scam" targeting university students

Students are prime targets for cybercriminals due to their relative inexperience with scams and eagerness for flexible, well-paying job opportunities. Their search for convenient employment can cloud judgment and makes them susceptible to offers that seem too good to be true.

HR-THEMED SPAM

Aside from the student population, the education sector has a significant workforce of personnel. Education has the 6th highest compounded rate of change in terms of employment projections out of 18 industries being tracked by the US Bureau of Labor Statistics. This high rate of increase in new staff could make the sector more attractive to threat actors.

Throughout 2023, our researchers observed a surge in phishing campaigns exploiting the ubiquitous nature of HR communications. Cybercriminals capitalized on this situation which we have observed in our spam traps and reported by Trustwave SpiderLabs in a November 2023 blog post.

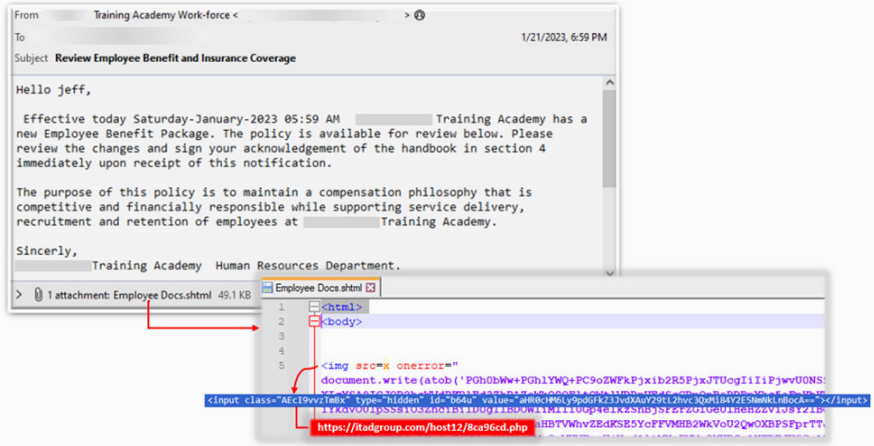


Figure 7: Sample of an HR-themed spam targeting employees of a training academy

HR-themed spam emails often lure recipients with subjects related to employee remuneration and benefits review. A notable tactic involves an HTML attachment in the email, purportedly from the organization's HR staff, presenting itself as a document for employee benefits review. However, this attachment is a credential phishing page, with malicious code obfuscated within the 'onerror' attribute of an 'img' element. The invalid image source triggers this attribute upon opening the attachment, decoding, and displaying the phishing page, thus tricking the targeted staff members into divulging sensitive information.

COMPROMISED EDUCATIONAL INSTITUTION SITES

In our research involving cyberattacks targeting educational institutions, we've observed a notable trend involving the misuse of the '.edu' domain, commonly associated with educational entities. Our spam traps identified campaigns that frequently exploit this domain, either as a top-level or second-level domain, leading to compromised websites used to disseminate threats.

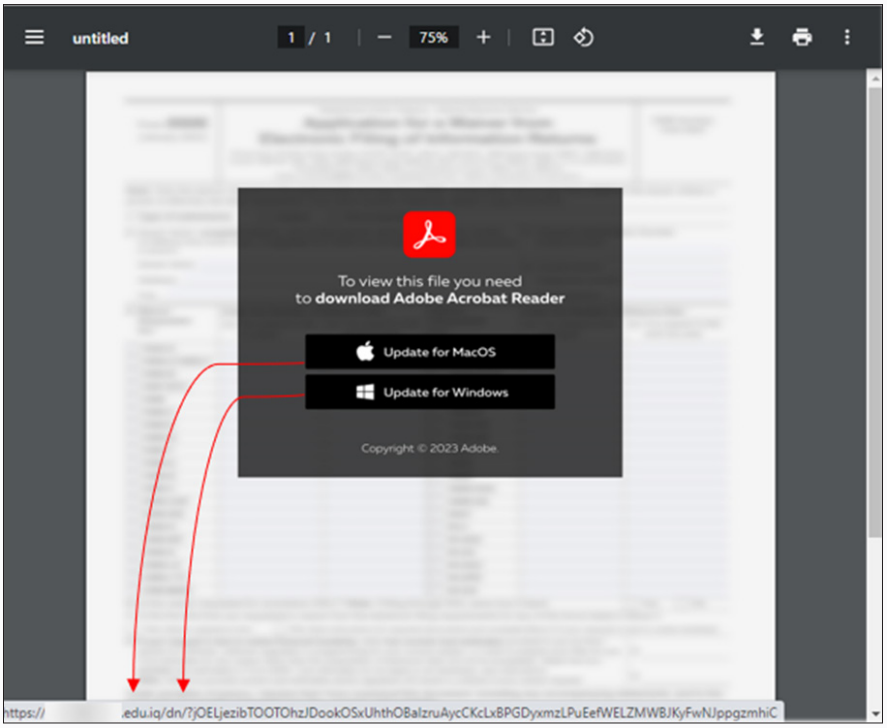


Figure 8: Sample PDF attachment leveraging an EDU domain that leads to an IcedID malware

These compromised sites are often embedded as links within the body of an email or included within the PDF files. Clicking on these links leads users to malware such as IcedID, Pikabot, and DarkGate.

WIRE TRANSFER SCAMS

In a recent Business Email Compromise (BEC) scam targeting the education space, attackers used a cleverly disguised email asking recipients to urgently process a wire transfer, allegedly for research and market development purposes. This attempt to exploit the industry's alignment with research activities is evident in the email's subject line.

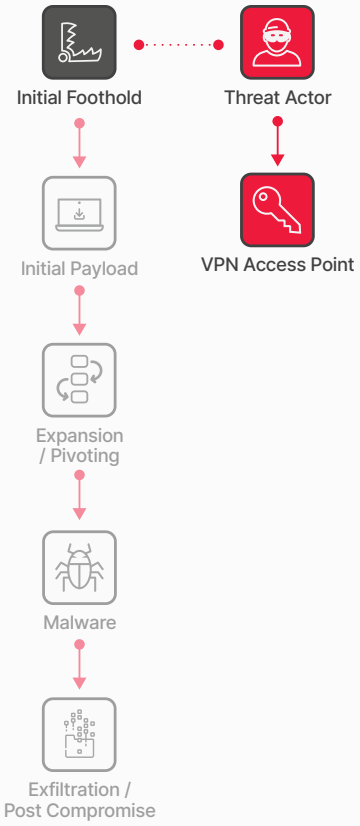
Figure 9: Sample wire transfer email scam attempting to leverage a research-related requests

However, the message contains several red flags: it artificially creates a sense of urgency by instructing the recipient to process the payment “right away,” and the sender's domain, “email.com,” is a generic free mail service, undermining the credibility of the supposed university communication.

Finally, it is worth noting that Trustwave SpiderLabs has been continually monitoring the effect of AI and Large Language Models (LLMs) like ChatGPT on phishing attacks. Many of the red flags that we teach users to identify phishing emails include items like picking out misspellings, grammar mistakes, and general clumsiness of writing that may indicate that the author is not a native speaker. The quick maturity and expanded use of LLM technology is making the crafting of these emails even easier, more compelling, highly personalized, and harder to detect.

Mitigations to Reduce Risk

- Conduct regular training and awareness programs for students, faculty, and staff, emphasizing the recognition of phishing emails, especially those mimicking university communications, HR communications, and job offers.
- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders. If feasible, consider providing the same assessment to students as well.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways.
- Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.
- Regularly monitor for the misuse of '.edu' domains and take swift action against any detected compromises.
- Perform routine security audits of university websites and IT infrastructure to identify and rectify vulnerabilities that could be exploited in phishing campaigns.
- Be vigilant about the increasing sophistication of phishing emails due to AI and LLM technologies, which can create more convincing and error-free scam messages.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Restrict the access of assets and sensitive data with the principle of least privilege in mind.



Initial Foothold: Logging in

The Threat

Threat actors can infiltrate an organization's network in various ways, including straightforward methods like using login credentials. This might happen if default device credentials remain unchanged, or if weak passwords are susceptible to brute-force attacks. But typically, threat actors gain access through methods like phishing, drive-by downloads, leveraging vulnerabilities in applications, or purchasing pre-established access to a target organization from various access brokers.

Trustwave SpiderLabs Insights

As discussed in the previous section (Initial Foothold: Phishing, Spam & Scams), phishing is the most widespread tactic to gain initial access to organizations, with attackers focusing not on software or system vulnerabilities, but rather on manipulating the individuals. Other common techniques used by threat actors are:

ACCESS CREDENTIALS AND ACCESS BROKERS

Trustwave researchers continually observe the trade of access credentials pertaining to data, networks, and systems on the Dark Web. Initial Access Brokers, which have been active in underground marketplaces and forums, were seen offering unauthorized access to various educational institutions.

Threat actors targeting universities see the potential to leverage their extensive network infrastructures for various malicious activities, such as gathering sensitive data, turning them into botnets, orchestrating DDoS attacks, or deploying ransomware. In Figure 10, the threat actor is selling alleged root access to all EC2 machines, S2 buckets, and other AWS account services of a particularly well-known US university.

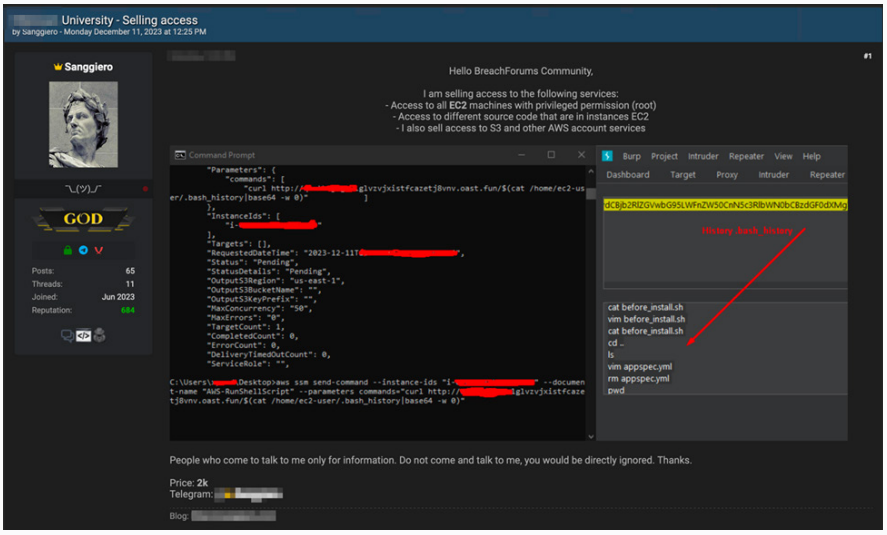


Figure 10: A threat actor selling alleged access to the AWS infrastructure of a well-known US university

In Figure 11, a threat actor is selling alleged VPN access to a university in the US. The threat actor, while vague about the victim, referenced only the university's revenue. Prices for such illicit offers vary widely, ranging from a few hundred to tens of thousands of US dollars in cryptocurrency, influenced by factors like geographical location, network size, security measures, access type, information sensitivity, and the educational facility's privilege level.

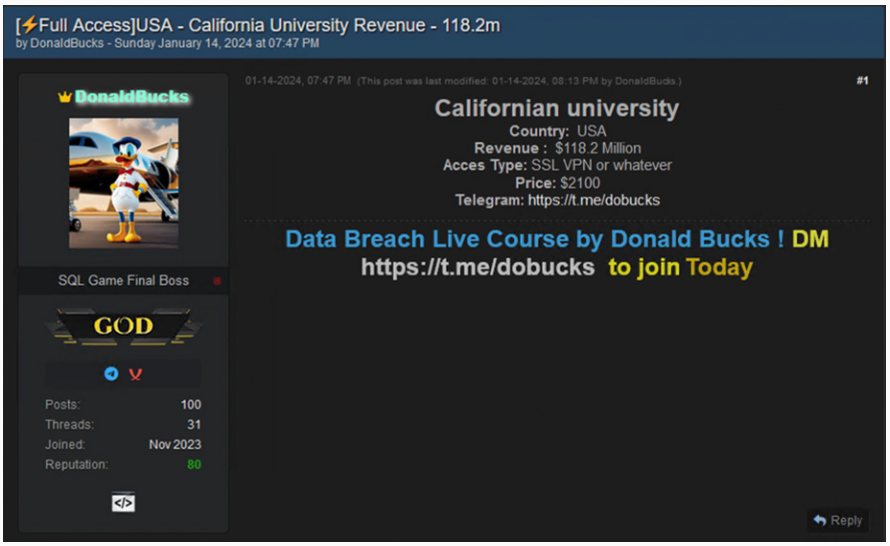


Figure 11: A threat actor selling alleged SSL / VPN access to a high revenue university in the US

Figure 12 highlights a threat actor claiming to have domain-level access to Azure and Microsoft services within a US school's network. According to the post, this access potentially allows for the management of the entire network and its numerous devices, creating a significant risk for various malicious activities originating from this institution. The actor is reportedly asking for $10,000 for this level of access.

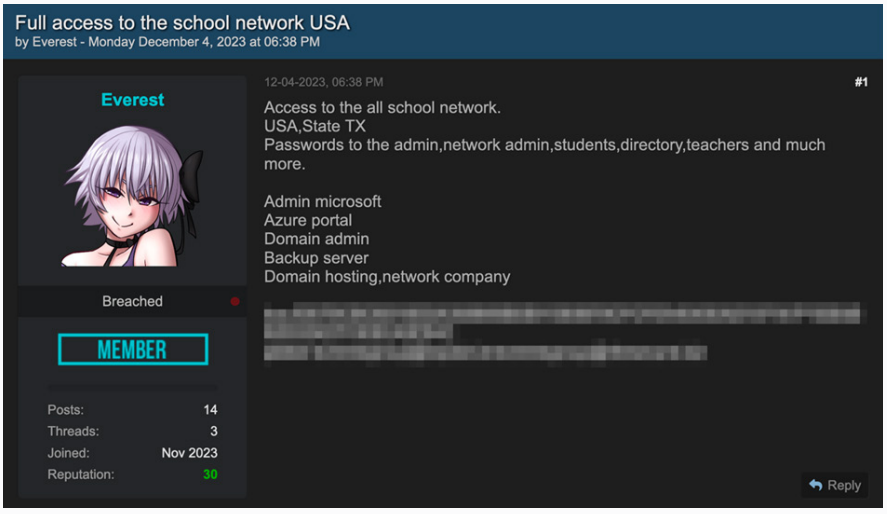


Figure 12: A threat actor selling alleged access to various Microsoft and Azure services of a school in the US

In another interesting finding, Trustwave researchers observed the "Russian Market," a marketplace known for selling data dumps, logs, and accounts, has listed over 82,000 logs mentioning the domain name mit.edu, associated with the prestigious Massachusetts Institute of Technology (MIT), in the past year. While the authenticity of these logs remains largely unverified, they predominantly contain login credentials for at least 90 subdomains of MIT. It's important to note that some of these samples might be fictitious or serve merely as examples of potential compromising methods rather than actual breaches.

EDU EMAIL ACCOUNTS

Threat actors often target education institution emails as an initial access vector due to their valuable content, including research, intellectual property, and personal and financial information of faculty and staff. The widespread use of university email addresses across various websites also makes them attractive for identity theft, phishing scams, and unauthorized access. With a large user base, these email accounts become appealing targets for hackers seeking to exploit them for malicious or financial gain.

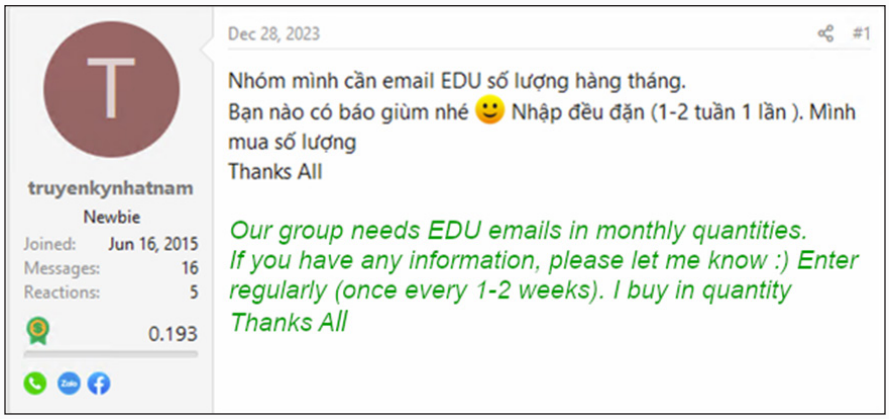


Figure 13: A threat actor in a Vietnamese forum looking to purchase EDU emails every 1-2 weeks

Email accounts from educational institutions are frequently exploited by hackers as initial access vectors to unlock various perks and benefits. This includes unauthorized access to purchasing platforms, acquiring restricted software, and taking advantage of software license discounts. The use of educational email credentials to gain entry to exclusive offers and services is a common strategy among cybercriminals. Below is an example of email access sellers:

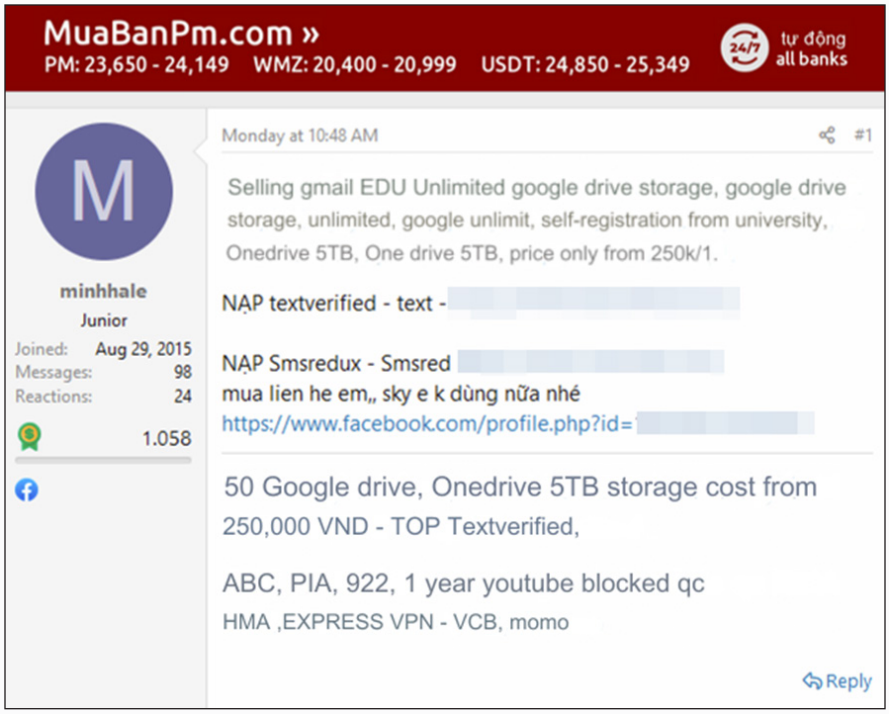


Figure 14: A threat actor in a Vietnamese forum selling various EDU Gmail accounts from a university

DRIVE-BY COMPROMISE

In the education industry, marked by academic freedom, a diverse mix of unvetted users, including students and guests, and a prevalent BYOD policy, the risk of drive-by compromises is significantly heightened.

Trustwave researchers have observed the use of drive-by compromise methods for initial network access, with SocGholish malware being a notable culprit.

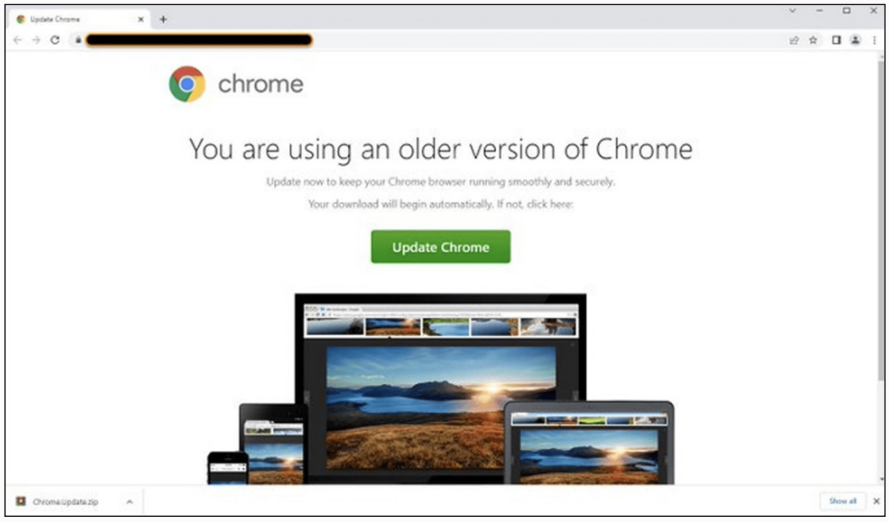


Figure 15: Sample of a Compromised WordPress website used in SOCGholish campaign. Source: heimdalsecurity.com

This malware typically disguises itself as a legitimate software browser update, exploiting the more "open" security measures in educational settings. It primarily functions as a javascript downloader, tricking users on compromised websites into downloading harmful files containing a JavaScript payload. These files, historically packaged within ZIP files, are misleadingly labeled as updates for widely used software like web browsers, or Microsoft Teams.

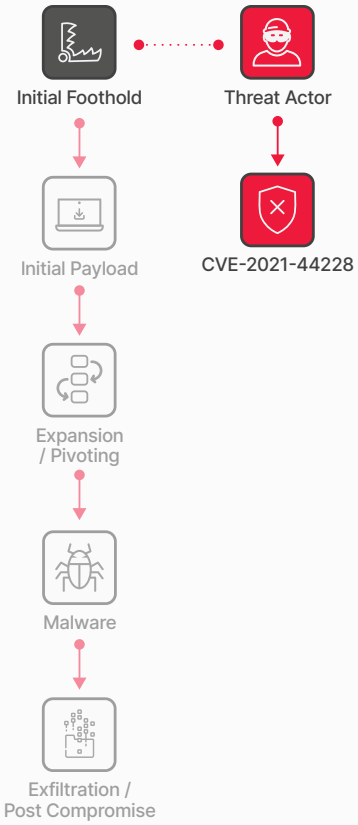
EXPLOITING PUBLIC-FACING APPLICATIONS

Educational institutions are exposed to public-facing exploits due to the nature of their operations, which involve many publicly accessible applications and systems processing information, such as student registration, enrollment, and personal information, as well as financial aid systems, crucial for storing sensitive personal details. Online collaboration sites and virtual learning platforms, which have become even more essential post-pandemic, are characterized by their vast data pools and decentralized management.

Additionally, the multiple websites and web applications of an educational institution, which are often dynamic and involve student participation, present unique security challenges. The next section will expound on specific vulnerabilities and exploits that highlight these challenges.

Mitigations to Reduce Risk

- Educate system users of the risks of phishing, drive-by downloads, and the importance of secure browsing habits.
- Update and patch all software regularly, including web browsers.
- Regularly monitor access points such as VPN and review logs for unusual activities. Educational institutions should also conduct periodic audits of their network infrastructure to identify and address vulnerabilities.
- Regular monitoring of Dark Web sites and underground marketplaces for possible breaches.
- Implement password length requirements for at least 12 or more characters to enhance security.
- Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- Restrict access to assets and sensitive data based on the principle of least privilege.
- Securely store credentials in password managers to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Audit local administrative accounts regularly and obfuscate admin accounts by not using admin in the name.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense in depth strategy



Initial Foothold: Vulnerability Exploitation

The Threat

When it comes to information security, vulnerability exploitation is often the first concept that comes to mind. This topic can encompass zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

To put it simply, a vulnerability refers to a software bug that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker takes advantage of the ability to bypass a security control and introduces a payload, such as malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring of our Trustwave Managed Services clients, Trustwave SpiderLabs identified the most common exploits targeting our clients in the education industry.

Apache Log4j (CVE-2021-44228) continues to be the most common exploit attempt against educational institutions. Apache Log4j, a notable logging library vulnerability across multiple industries, remains a threat in the education sector with its extensive ecosystem of applications, including many that are publicly accessible.

However, we also observed attacks exploiting vulnerabilities like Exchange Server RCE (CVE-2022-41040, CVE-2022-41082), which are security flaws within Microsoft Exchange Server that allow an attacker to run malicious code on the server, and Springshell (CVE-2022-22965), which are security flaws in the popular open-source application framework Spring for the Java platform.

Also, threats such as Cross Site Scripting and SQL Injection continue to target these broad and diverse educational networks and applications.

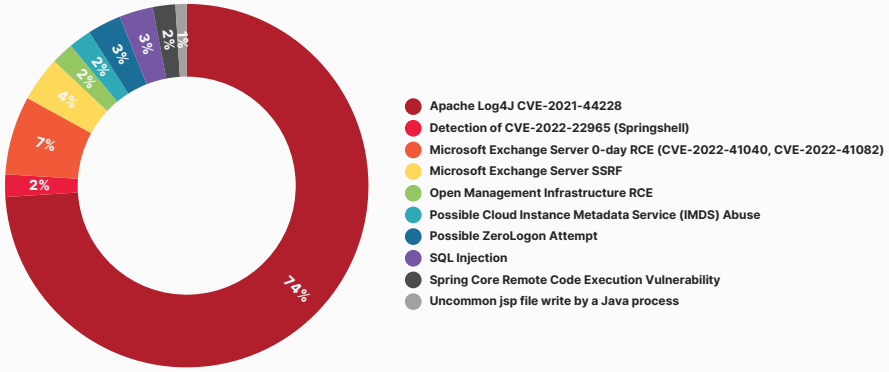


Figure 16: Exploit procedures used by threat actors

Trustwave SpiderLabs also encounters and analyzes various attacks through our specialized incident response, Open-Source Intelligence (OSINT), and Dark Web research. In a recent example, Trustwave researchers released original research showing threat actors leveraging ActiveMQ (CVE-2023-46604) to install the Godzilla WebShell to gain access to certain education organizations.

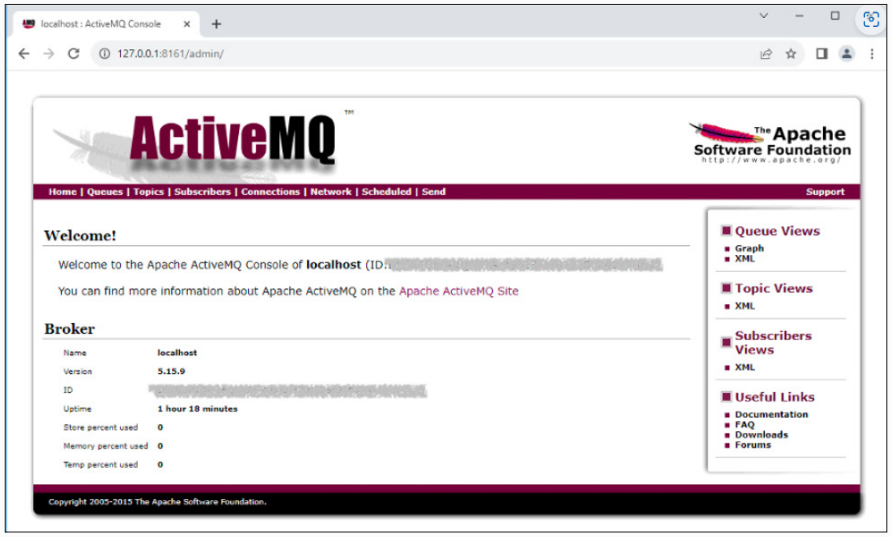


Figure 17: A malicious file containing the Godzilla Webshell was planted in the same directory of the Apache ActiveMQ admin page by leveraging CVE-2023-46604

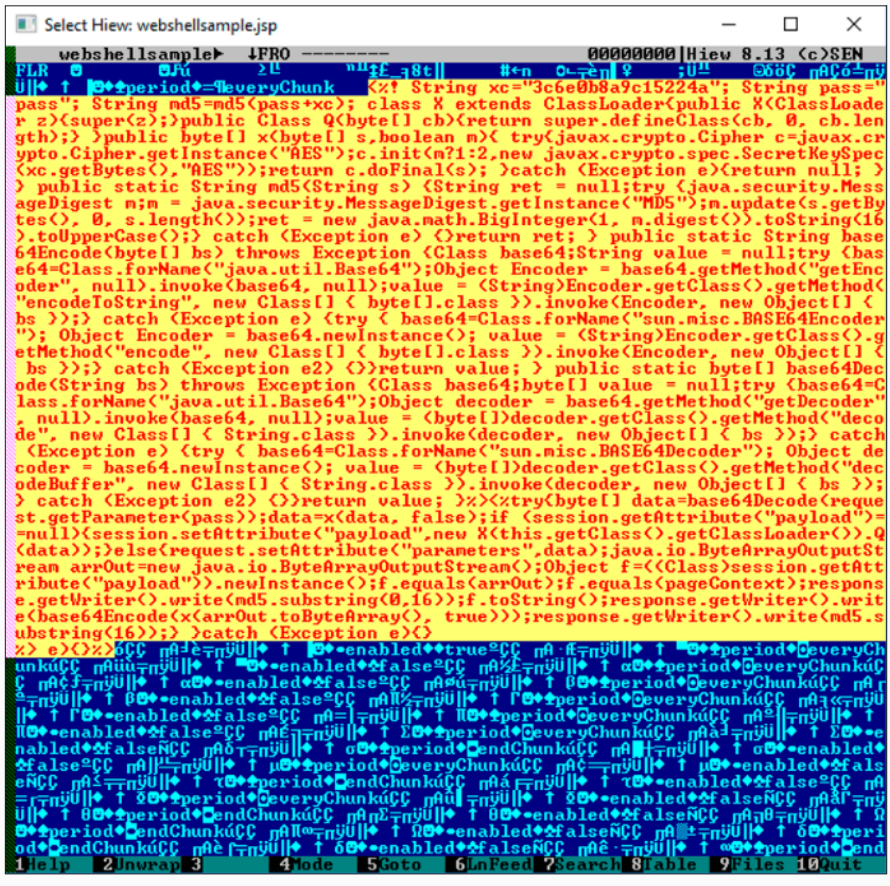


Figure 18: Examining the malicious .JSP file reveals that the malicious code containing the Godzilla Webshell was encapsulated within a binary structure of an unidentified file format, marked by the "FLR" magic header

Trustwave SpiderLabs conducted a review of Shodan, which scans all public IP addresses on the Internet. This revealed over 1.8 million devices related to the education industry. As illustrated below, this easily dwarfs the number of any of the other major verticals our team has reviewed so far. A review of these devices shows they are running mainly web services and SSH/SCP.

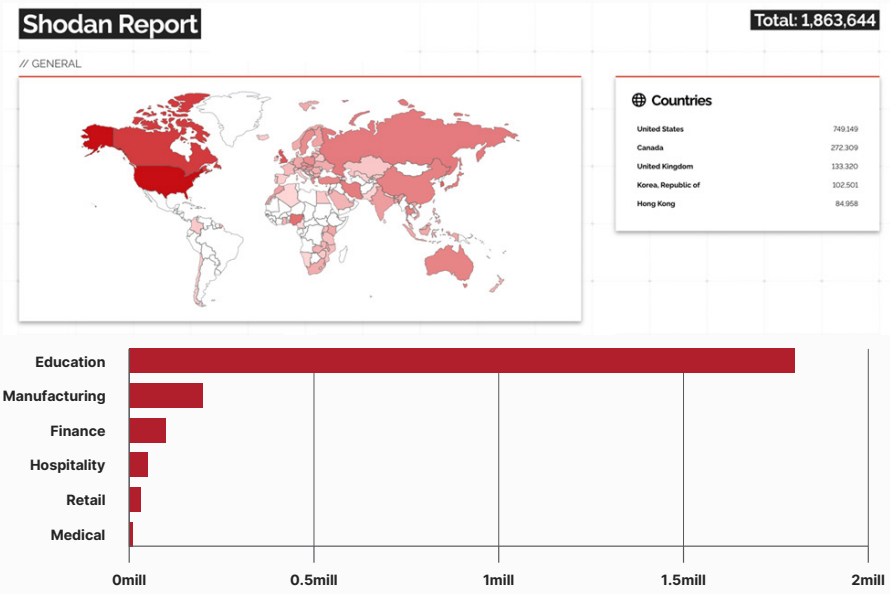


Figure 19: Based on Shodan data, the education sector had 1.8 million publicly facing devices

In the education industry, with its large number of publicly facing applications, certain vulnerabilities stand out based on Shodan. The top ten CVEs our researchers identified affecting educational systems include notable ones like CVE-2021-40438 (Apache HTTP Server SSRF), CVE-2023-44487 (HTTP/2 Rapid Reset Attack Vulnerability), and CVE-2019-0211 (Apache HTTP Server Privilege Escalation Vulnerability).

Other prevalent vulnerabilities are CVE-2012-1823 (PHP-CGI), CVE-2014-0160 (Heartbleed in OpenSSL), CVE-2019-11043 (PHP FPM), CVE-2020-0796 (Microsoft SMBv3 flaw), CVE-2020-28949 and CVE-2020-36193 (PEAR Archive_Tar), and CVE-2020-13671 (Drupal core). As expected, these vulnerabilities often involve widely used open-source software and protocols.

CVE	Number of Systems
CVE-2021-40438	69,352
CVE-2023-44487	27,164
CVE-2019-0211	24,104
CVE-2012-1823	1,805
CVE-2014-0160	1,386
CVE-2019-11043	970
CVE-2020-0796	593
CVE-2020-28949	381
CVE-2020-13671	366
CVE-2020-36193	356

Figure 20: Top ten CVEs by the total number of affected systems

It should be noted that in the analysis of publicly accessible devices, 1.8 million devices were identified, and of these devices, the ones shown in Figure 20 have vulnerabilities that show on the CISA list as "actively exploited" therefore are at higher risk.

During the review, Trustwave researchers also found some notable examples of vulnerabilities in publicly facing systems that highlight the risks that the education sector is facing. Here are some of the notable examples:

PUBLIC FILE SERVERS

Trustwave researchers found over 2,500 public file shares containing potentially sensitive data such as projects, theses, and other academic documentation. Some even contained network/website configuration and student information.

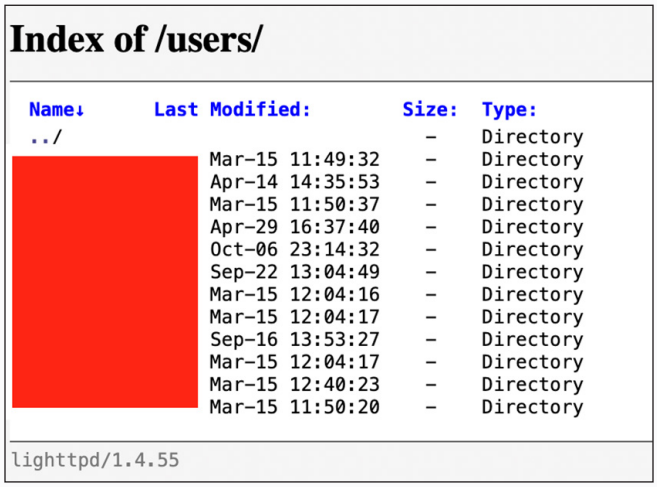


Figure 21: Example of a public file server containing various academic data

VULNERABLE PRINTER MANAGEMENT SOFTWARE

Trustwave researchers found potentially vulnerable third-party printer management software that might present a significant attack vector. In 2023, Iranian state-sponsored hackers Mint Sandstorm and Mango Sandstorm exploited an unpatched version of this software in various organizations, including universities, using CVE-2023-27350. The same vulnerability was leveraged by the Bl00dy Ransomware gang in their attacks on schools.

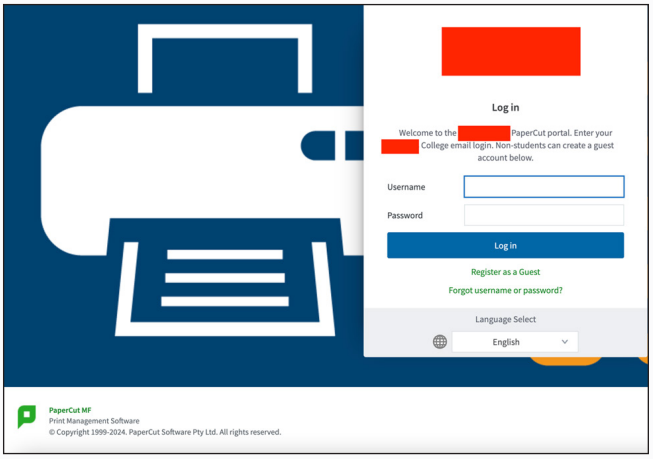


Figure 22: Example of a potentially vulnerable printer management software used by Iranian State-sponsored hackers

VULNERABLE PRESENTATION AND COLLABORATION SYSTEMS

Due to the transition to remote learning due to the pandemic, educational institutions quickly adopted various collaborative systems and devices, potentially leading to weaker security measures. For example, a Shodan search revealed a publicly accessible WolfVision Cynap device, equipped with browser and screenshare capabilities, potentially exposed due to its open access.

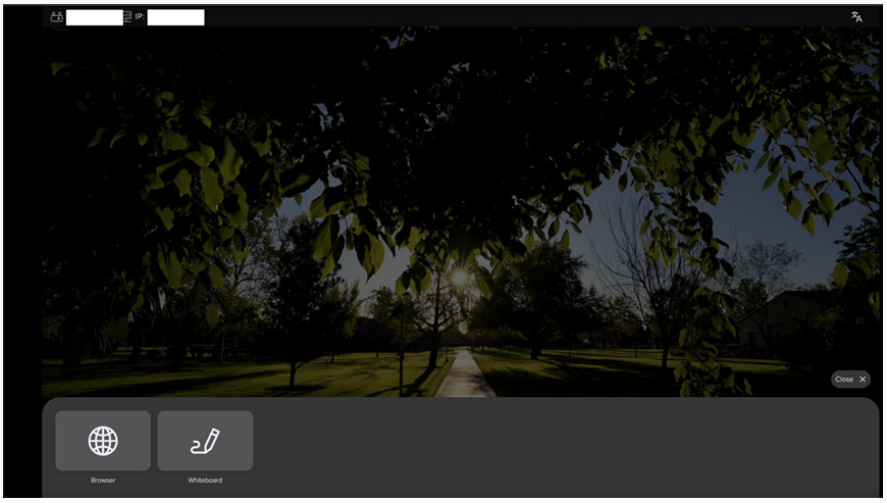


Figure 23: Example of a WolfVision Cynap device with Open Access

UNSECURED NETWORK DEVICES

Trustwave researchers identified multiple examples of misconfigured network devices in the education industry. Examples include critical vulnerabilities like CVE-2023-25717 in Ruckus admin panels leading to AndoryuBot malware infections for DDoS attacks, widespread use of default passwords in Cisco IP and Poly phone devices, and a Remote Code Execution vulnerability (CVE-2022-3236) in Sophos XG firewalls. These issues are exacerbated by outdated firmware requiring manual updates. Furthermore, a Netgear GS108PE switch at a prominent university was found publicly accessible with hard-coded login credentials, highlighting the urgent need for improved security practices and regular updates in educational institutions' network management.

Figure 24: Example of a vulnerable Ruckus device with a critical CVE-2023-25717 vulnerability

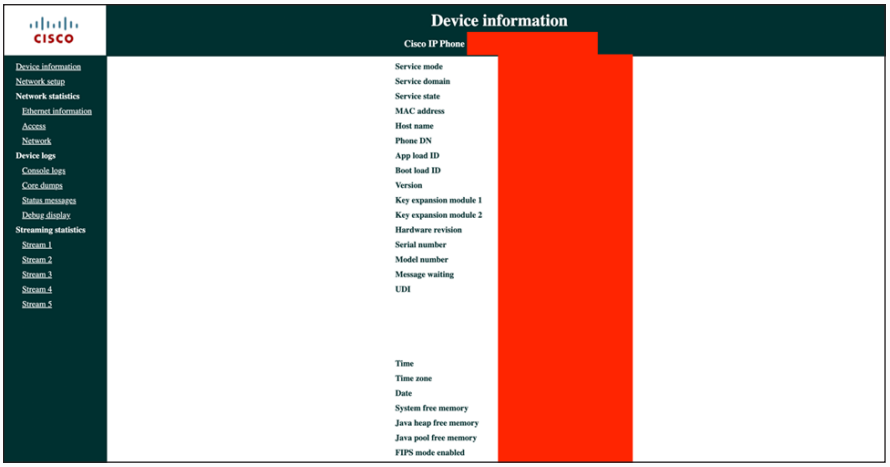


Figure 25: Example of a Cisco device with open access

Figure 26: Example of a Sophos XG firewall vulnerable to CVE-2022-3236

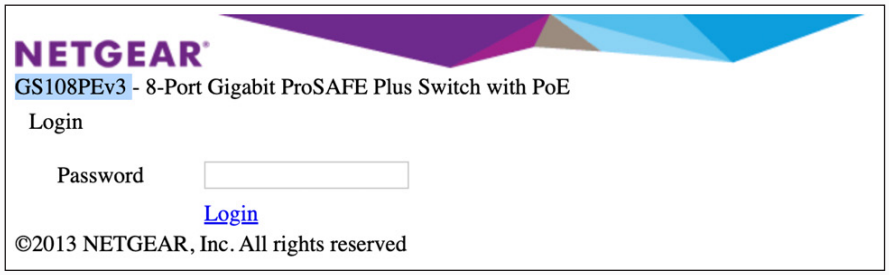


Figure 27: A Netgear switch in a prominent university with hard-coded passwords

CRYPTO MINERS

The widespread use of Internet-connected systems in educational environments, coupled with the BYOD policies and liberal browsing practices, significantly increases the risk of getting infected with malware. Crypto miners are not only limited to institutional equipment but are also found on devices possibly owned by students.

Figure 28: Example of a Nanominer found in a compromised device

PASSWORD MANAGERS

Trustwave researchers observed there were publicly accessible, self-hosted password managers exposed in various educational organizations. It should be noted that recent breaches, such as AutoSpill on Android and LastPass's 2022 source code theft underscore the risks that unsecured deployment of these services present.

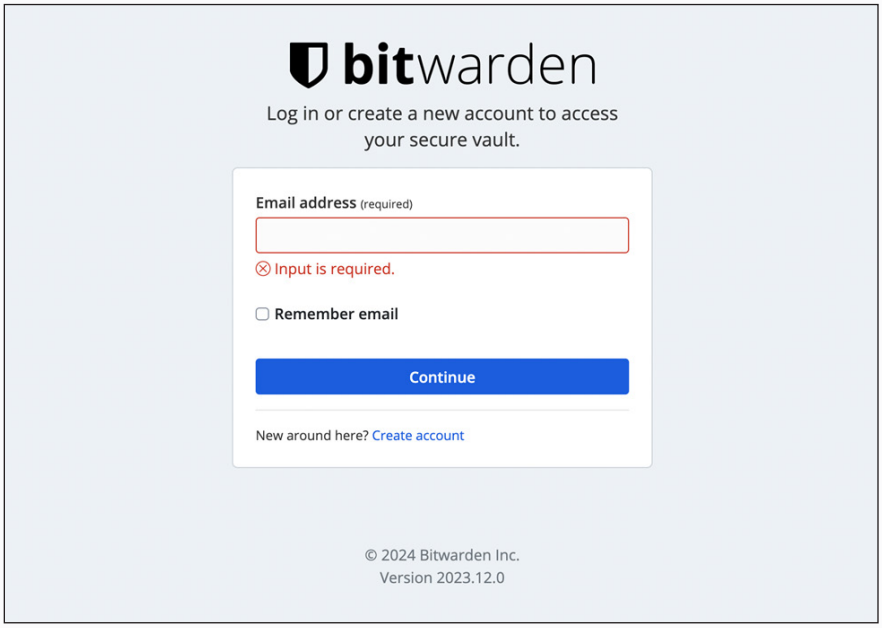


Figure 29: Example of a publicly accessible password manager

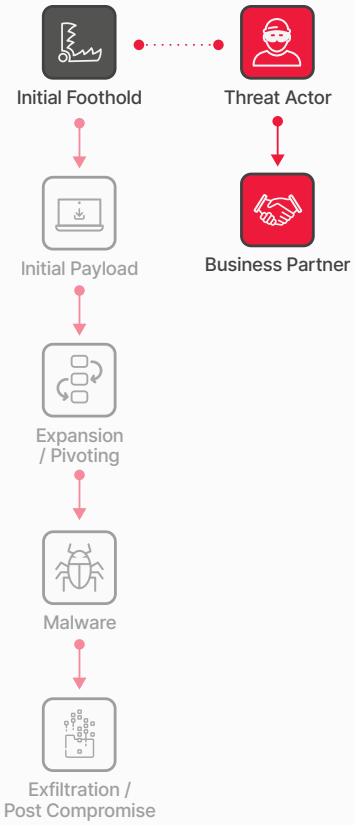
OPEN SECURITY CAMERAS

Trustwave researchers observed that unsecured security cameras, including live feeds of critical infrastructure, were accessible in multiple educational institutions due to security misconfigurations.

Figure 30: A school security camera with open access

Mitigations to Reduce Risk

- Regularly update and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems.
- Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Utilize vulnerability assessments and penetration testing to identify vulnerable servers.
- Implement strict access controls for critical systems, including file servers, printer management software, and collaboration tools. Strengthen access controls to minimum necessary levels for authorized users.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control. Disable Internet access for servers that do not require it.
- Address misconfigurations in network devices and other IoT devices, ensuring firmware is updated and default passwords are changed.
- Provide ongoing cybersecurity training and awareness programs for staff and students, emphasizing the importance of security best practices



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly widespread. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents encountered in headlines.

Trustwave SpiderLabs Insights

The education sector, like many others, relies heavily on third-party vendors such as software-as-a-service, hosting providers, storage, and IT services for various functions, including learning management systems, email, and communication and collaboration tools.

Cybercriminals commonly prefer to attack these third parties in a flanking maneuver—if the attack succeeds, they gain access to the targeted company's data. These third parties pose a grave risk to the education industry because of undiscovered or un-remediated gaps in their cybersecurity controls or data breach protection.

Previous supply chain attack headlines, like SolarWinds and 3CX, underscore the exposure third-party vendors can create for the education vertical For example, Trustwave research on ransomware claims noted at the minimum, there were breaches of 13 major universities directly attributable to the MOVEit RCE (CVE-2023-34362) vulnerability, a popular third-party file transfer service. These breaches had the highest prevalence from June to August 2023, most often facilitated by the ransomware threat actor Clop.

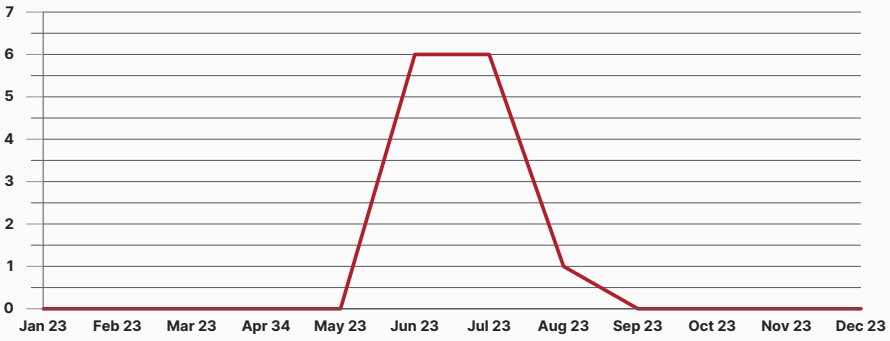


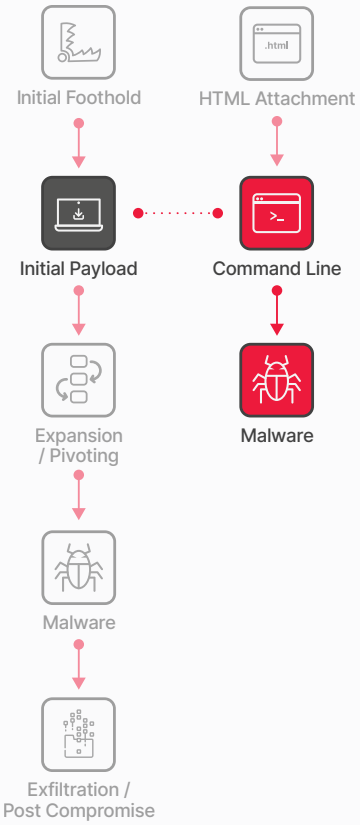
Figure 31: CVE-2023-34362 attack claims on notable universities (based on ransomware claims)

Aside from the aforementioned software, there were several prominent third-party education services providers that were affected by cyber breaches, such as Illuminate Education, a prominent provider of K-12 technology systems used for tracking grades, attendance, and other critical student data. The breach's magnitude highlighted the vulnerability and far-reaching consequences of third-party breaches in education.

Another third-party supplier example worth highlighting is the Blackbaud breach of May 2020. Blackbaud is a cloud service provider schools and universities use for administrative tasks such as record keeping, fundraising, and financial management. The Blackbaud ransomware breach exposed sensitive personal data of millions of people from 13,000 educational institutions and non-profits worldwide. The breach was also a notable example of third-party security risks as Blackbaud initially failed to disclose the full extent of the breach including the threat actor's access to unencrypted banking and social security information. This ultimately led to a series of legal and financial repercussions including lawsuits and substantial settlement by the third party.

Mitigations to Reduce Risk

- Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. This will involve assessing the cybersecurity policy being deployed, existing and tested incident response plans, and compliance with related standards.
- Ensure that third-party vendor contracts have strict cybersecurity clauses. This could include mandating the conducting of regular security audits, immediate breach notification, as well as ensuring compliance with the pertinent data protection regulations.
- Periodically conducting audits and reviewing the security practice of third-party vendors. This involves a periodic review of the service provider, vulnerability assessments, as well as penetration testing to identify and remediate any weak points in security.
- Encrypt all sensitive data both in transit and at rest. Restrict the access of sensitive data to the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.
- Ensure following of the industry standards and regulations like GDPR, HIPAA, FERPA, etc., for compliance to geographical location and nature of data handled by third-party vendors.
- Participate actively in cybersecurity forums of the educational sector and other information sharing platforms.



Initial Payload

The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Execution techniques of initial payloads observed through active monitoring mostly involved the use of command and scripting interpreters and user execution. Command and scripting interpreters like VBA and Powershell can be used to execute commands and scripts on compromised systems, as well as to download and run malicious payloads. Another popular technique used by adversaries to deliver initial payloads simply relies on a user opening a malicious file to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution. Figure 32 showcases real-world cases concerning education institutions or providers that highlight the various methods that initial payloads are downloaded and executed.

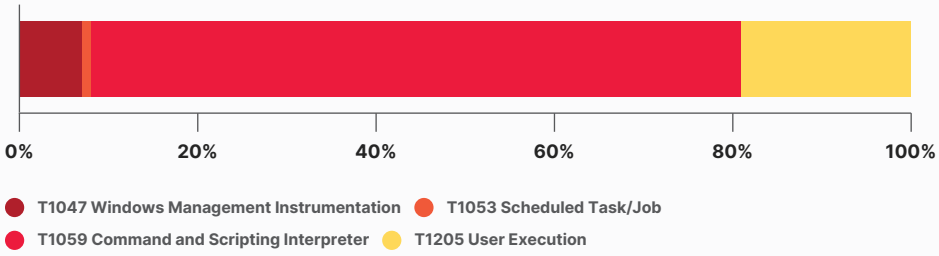


Figure 32: Execution techniques used by threat actors

In a case involving an attack on a company specializing in university and college multimedia, a VBA (Visual Basic for Applications) macro was used to deliver a malicious payload. The attack used a malicious Office document featuring a VBA macro that had a lure urging the user to enable or "unlock" the content.

Once activated, the macro discreetly deployed a DLL file onto the victim's system using the rundll32.exe process. The DLL was intended to execute further harmful activities. However, the complete functionality and impact of the malware could not be fully ascertained, as the URL intended for downloading additional malicious components was non-functional, cutting off further investigation. This incident highlights the use of VBA, a widely recognized command and scripting interpreter, in executing the initial phase of a cyberattack.

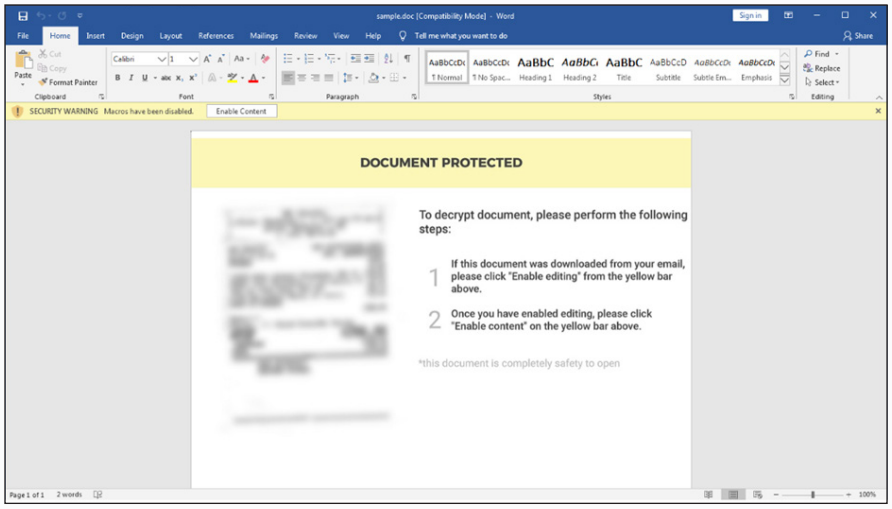


Figure 33: Malicious document leveraging a VBA macro to deliver a malicious DLL file

User execution is a common and very effective method to deliver the initial payload. Trustwave researchers often observe deceptive MSI (Microsoft Software Installer) files being leveraged to trick users. For example, in one of the cases our researchers investigated, a deceptive MSI file presented as a PDF viewer installer, but instead installed a repackaged Chromium-based browser, "Launch Browser," from SecureBrowser.io. This instance of social engineering led users to unknowingly install unwanted programs and adware, potentially violating their consent. The case highlights the use of MSI files and user execution as a deceptive delivery method, exploiting social engineering techniques to trick users into installing unwanted software.

In another particularly interesting case, the Apache ActiveMQ RCE vulnerability (CVE-2023-46604) was exploited to deliver a Godzilla Webshell payload. Trustwave researchers discovered a .jsp file containing malicious code, which turned out to be a sophisticated JSP webshell known as Godzilla. This open source webshell boasts various features like remote code execution and server info retrieval. Notably, the Jetty JSP engine within Apache ActiveMQ processed and executed this embedded code, converting the webshell into Java code for execution, highlighting a critical security concern in the processing of unverified code.

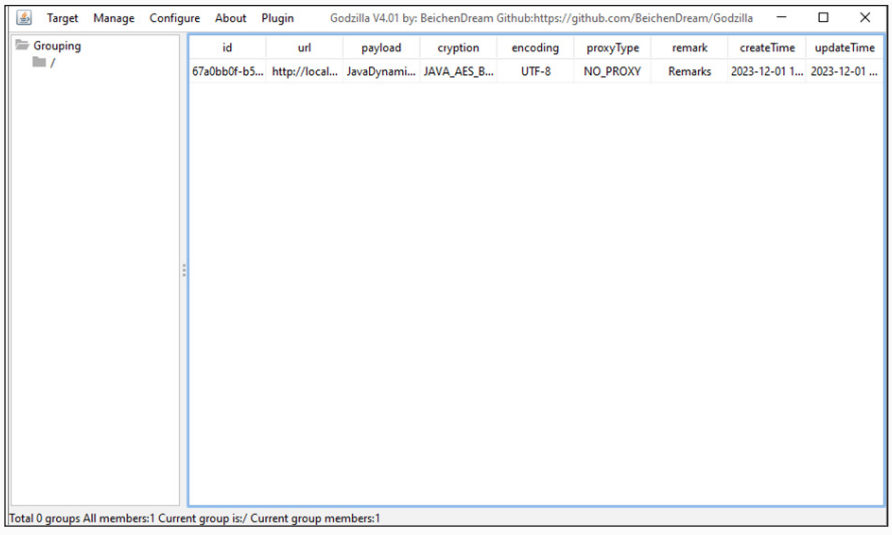
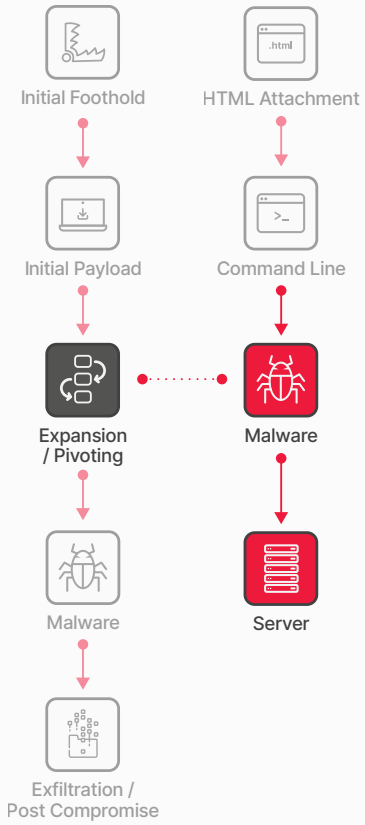


Figure 34: Godzilla webshell payload delivered via CVE-2023-46604

Trustwave researchers uncovered certain downloaders, malware specifically designed to download payloads onto a compromised system, often used in malicious campaigns directed at educational institutions. Downloaders like GuLoader, GootLoader, and SocGholish have been frequently observed being delivered through malicious email campaigns or through drive-by compromise. These malware types primarily serve as initial infection vectors, tricking users into downloading them under the guise of legitimate applications or updates. Once installed, these downloaders execute their primary function: to facilitate the download and execution of additional, often more damaging payload onto the victim's system. Their effectiveness lies in their ability to initiate multi-stage attacks discreetly, paving the way for more sophisticated cyber threats.

Mitigations to Reduce Risk

- Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help them identify and avoid phishing attempts and social engineering tactics.
- Implement policies to restrict or monitor the execution of scripts like VBA and Powershell. This can be done using tools like Windows Group Policy. Microsoft also has what it calls attack surface reduction (ASR) rules.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Conduct regular audits of all applications operating within the environment.
- Implement highly granular “allow lists” of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- Apply additional privilege restrictions to prevent unprivileged sources from running different command shells.



Expansion / Pivoting

The Threat

Since the initial foothold typically occurs on a low-value workstation, such as the laptop of a phishing victim, or a network appliance like a VPN endpoint, the attacker now is going to target higher-value accounts and systems with the appropriate tools at their disposal. These can include Domain Admins, Root Accounts, Active Directory Systems, and Database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party, the goal of the threat actor is privilege escalation and expansion. This step is often referred to as "pivoting" or "lateral movement."

As an initial step, threat actors will typically try to obtain credentials to facilitate lateral movement. Credential access tends to be easier once initial access or foothold has been obtained as security tends to fall off internally. Often this is due to the mentality of "it's behind a firewall," so there isn't a need to prioritize security controls. We used to refer to this as "crab security," a hard shell with a soft interior.

Based on Trustwave active monitoring, credential access techniques observed in the attacks against education organizations relied mostly on password brute-force attempts, but also OS credential dumping, authentication process modification, stealing or forging Kerberos tickets, and forced authentication.

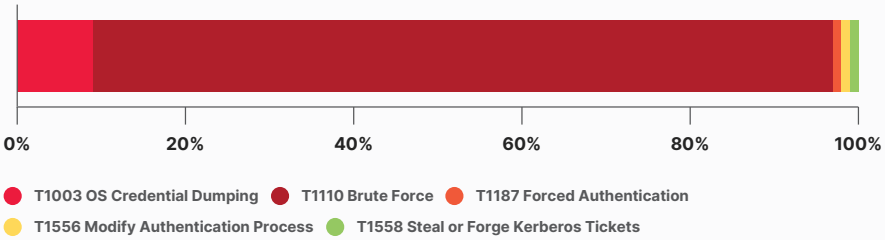


Figure 35: Credential access techniques by threat actors

Once an initial foothold has been acquired, threat actors then obtain valid credentials, by using various lateral movement techniques to gain further access within the organization. Trustwave researchers observed the lateral movement techniques utilized by attackers in educational institutions relied mostly on Remote Desktop Protocol (RDP), SMB/Windows Admin Shares, and DCOM. Use of Alternate Authentication Material (Pass the Ticket) was also observed. Additionally, investigations show that Lateral Tool Transfer indicators were mostly related to Bloodhound, Cobalt Strike, and Solorigate.

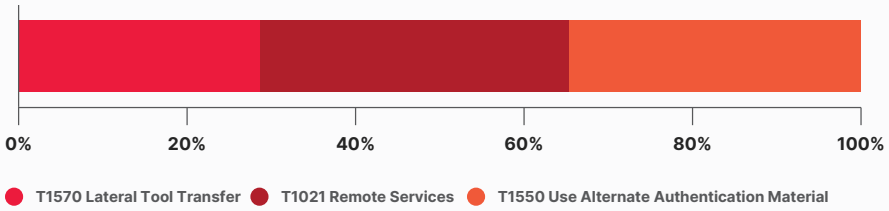


Figure 36: Lateral movement techniques by threat actors

As threat actors continue to move laterally across the organization, they tend to increase their privileges as they pilfer various compromised systems and high-value assets. Based on our active monitoring of educational institutions, privilege escalation techniques observed in security incidents mostly involved the use of Valid Accounts where attackers use legitimate credentials to access systems, applications, and data.

During threat hunts for education institutions, Trustwave researchers often encounter scenarios involving the use of custom scripts to escalate privileges. In this situation, passwords are frequently either hardcoded into the scripts or used in clear text. This practice makes these clear text passwords a prime target for malware, which is often designed specifically to collect and exfiltrate these credentials. This method demonstrates a typical approach where attackers exploit weak security practices to gain higher access levels within a system.

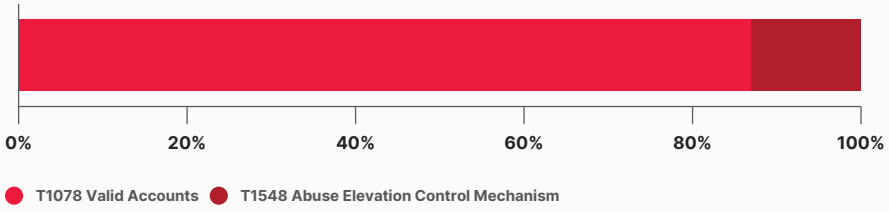


Figure 37: Privilege escalation techniques by threat actors

It is also during this stage when the threat actors will try to establish persistence in the network so attackers can share access with others on their team or come back at a future time to continue the attack. Investigations by Trustwave researchers into incidents in education institutions show that persistence techniques predominantly utilized Account Manipulation, which includes adding accounts to privileged groups, changing permissions, setting accounts to not expire, or even altering login scripts. Other techniques seen were Boot or Logon AutoStart Execution and Event-Triggered Execution. Valid Accounts and other techniques were also observed.

To further highlight this, in our threat hunting activities, Trustwave researchers also often see the use of Scheduled Tasks for Persistence purposes. Like local user accounts, these scheduled tasks tend to become unmanaged and forgotten over time. This neglect can be a significant vulnerability, as it allows threat actors or malware to surreptitiously create new scheduled tasks, establishing backdoors or maintaining malware execution.

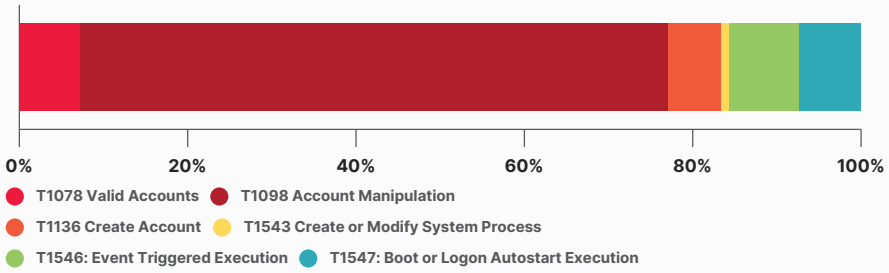


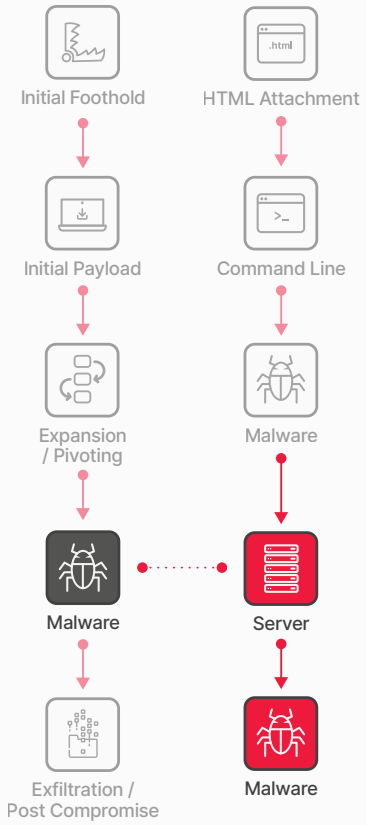
Figure 38: Persistence techniques by threat actors

Trustwave SpiderLabs®

Trustwave SpiderLabs conducts 200K hours of pentesting each year

Mitigations to Reduce Risk

- Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- Adopt strong password policies and implement continuous monitoring for credential dumping and authentication manipulation techniques.
- Monitor the use of unusual connections in RDP, SMB/Admin Shares, DCOM, and other open services using anomaly and behavior-based detection techniques.
- Implement robust host-based security controls including detailed "allow list" of applications on designated hosts to minimize exposure. Pay special attention to Lateral Tool Transfer indicators.
- Impose additional restrictions on privileges to prevent unauthorized execution of commands from unprivileged sources.



Malware: Loaders, Infostealers and RATs

The Threat

Malware is an essential tool used by threat actors to gain access, steal information, and maintain control of their victim's environment. Among the multitude of malware strains, Loaders/Downloaders, Infostealers, and Remote Access Trojans (RATs) are among the most important types of malware to facilitate threat actor activities.

Loaders/Downloaders specialize in delivering other types of malware onto a compromised system, often acting as the initial step in a multi-stage attack by installing threats like RATs and infostealers to execute their respective tasks. Infostealers focus on extracting sensitive information, targeting stored data (like passwords and contacts), and data entered during online activities, often via malicious browser plugins. RATs, on the other hand, provide backdoor access to a system, allowing attackers to perform a range of activities from downloading files to capturing data, like infostealers, and even activating webcams.

Trustwave SpiderLabs Insights

Trustwave SpiderLabs gains insights into malware in our clients' environments through the delivery of our managed services, threat hunts, DFIR, and malware analysis teams. Trustwave is in a unique position to detect and analyze distinctive malware threats focusing on specific industries. Through our various services, our researchers have identified some of the more notable malware particularly active in education institutions.

GULOADER:

This loader malware has been around since 2019 and specializes in deploying RATs and infostealers. GuLoader is interesting as it uses cloud storage for hosting malicious payloads which complicates detection. It spreads mainly via phishing emails and leverages encryption methods for defense evasion. Trustwave researchers have observed GuLoader in RFQ-themed malicious spam campaigns targeting various education institutions.

GOOTLOADER

This malware is a combination of loader and infostealer. Gootloader emerged around 2020 starting off as a banking Trojan. This malware has gained notoriety due to its exploitation of compromised WordPress sites for malware distribution and its utilization of SEO poisoning techniques to achieve high rankings in web search results. Trustwave researchers often observe this malware as part of malicious email campaigns targeting various education institutions.

SOCGHOLISH

SocGholish is primarily a loader and has been active since early 2020. It is distributed through compromised websites, tricking users into downloading fake browser updates. SocGholish can deliver various payloads, including RATs. Trustwave researchers have often observed SocGholish as part of drive-by compromise attacks in education institutions.

MACRO MALWARES

These are typically loaders and infostealers. Macro malware is particularly dangerous in environments like schools and universities due to the frequent exchange of documents. Trustwave researchers have investigated notable cases where macros written in VBA have been used to download and execute malicious payloads.

PUPS (POTENTIALLY UNWANTED PROGRAMS)

Though not always malicious, PUPs can include adware and other unwanted software. These often come bundled with legitimate software, making them common in various sectors, including education. Trustwave researchers have investigated notable cases where deceptive MSI files and browser extensions were used to download unwanted software in education institutions.

ICEDID:

Since 2017, IcedID has implemented a range of delivery methods, but favors email as its initial access vector. It started as a banking trojan targeting financial institutions but has since evolved into a dropper of additional malware payloads, like ransomware, and has become an initial access provider for other threat actors seeking to establish a foothold on a target system. The malware leverages sophisticated HTML Smuggling methods to deliver its payload. Additionally, Trustwave researchers have often found malicious PDFs hosted in compromised EDU sites that ultimately leads to the IcedID malware.

PIKABOT

Pikabot is a RAT distributed through phishing and malicious downloads. Pikabot can steal information and control infected systems. Similar to IcedID, Trustwave researchers have often found malicious PDFs hosted in compromised EDU sites that lead to the Pikabot malware.

DARKGATE

DarkGate is a hybrid loader, infostealer, and RAT that gained popularity in June 2023 when the tool was advertised in a Dark Web forum. Spam campaigns leading to this threat utilized highjacked email threads. Of note, after the Qakbot takedown by the FBI, Trustwave researchers observed campaigns using similar email structures as those delivering Qakbot. By analyzing the Indicators of Compromise (IOCs), our researchers identified the same email campaigns were now being leveraged by the DarkGate malware.

ANDORYUBOT

AndoryuBot is a RAT with infostealer capabilities. It often spreads through spear-phishing and exploits vulnerabilities in software commonly used in educational institutions. Trustwave researchers found vulnerable Ruckus access points in various educational institutions that were notorious as hosts for the AndoryuBot malware. These infected devices were often used as staging points for DDoS attacks.

AGENT TESLA:

Known since the mid-2010s, Agent Tesla is a sophisticated RAT and infostealer. It is typically deployed via phishing emails with archive or even disc image attachments. Agent Tesla includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a flexible command and control channel and can connect to the C2 via HTTP, HTTPS, Email, or a Telegram channel. Trustwave has seen Agent Tesla delivered through various RFQ-themed malicious email campaigns targeting education institutions.

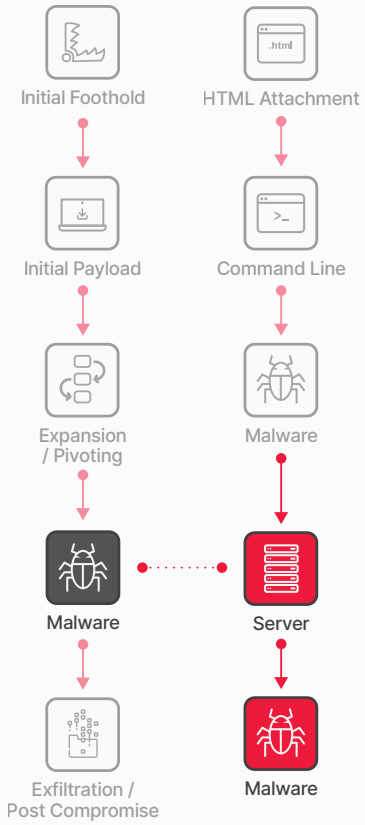
LOKIBOT

LokiBot is an infostealer that has been active for several years. It specializes in infiltrating systems and harvesting sensitive data. It is disseminated through phishing campaigns and exploit kits. Trustwave researchers have seen many spam messages with this malware attached, including RFQ themed malicious spam campaigns targeting universities. Trustwave has also observed LokiBot payloads hidden inside PNG files.

TRUSTWAVE MDR ELITE OFFERS AN MTTA OF 15 MINUTES AND MTTR OF <30 MINUTES

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- For OT and IoT devices that may not have the capability to run host-based anti-malware tools, ensure that compensating controls are in place such as network-based monitoring / prevention systems and network isolation and segmentation.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

Ransomware is a type of malware that typically encrypts or locks data and then demands the victim pay a ransom to provide access to that data again. Modern ransomware campaigns prevent recovery by also attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data before deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom isn't paid, the threat actors still have a dataset they can turn around and sell. This is commonly referred to as a double-extortion tactic.

Threat actors also use triple extortion in which case the attacker will strategically deploy a DDoS attack as a third-layered extortion tactic. Worse yet, is when they target the victims of the breach and threaten to release their data if they don't pay.

Trustwave SpiderLabs Insights

In 2023 alone, Trustwave researchers monitored 352 ransomware claims against educational institutions. The top ten ransomware groups targeting the industry were LockBit 3.0, Rhysida, CLOP (aka CL0P, Cl0p), Akira, Medusa, Alphv, Vice Society, NoEscape, Royal, and Pirat-Networks. These groups have targeted a wide range of educational entities across different countries, predominantly in the US, but also in Canada, the UK, Australia, France, Germany, and others. The types of institutions compromised vary from universities and colleges to public school districts, technical schools, and specific training centers.

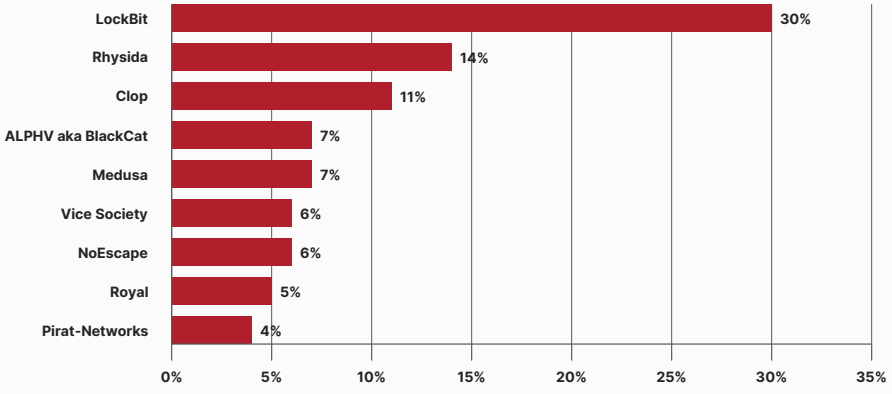


Figure 39: Top ten ransomware groups in the education sector

The timeline of ransomware attacks and breaches in 2023 shows varying levels of activity throughout the year. There were spikes in ransomware activity in the middle of the year, particularly during June to August 2023, which coincided with the height of the exploitation of the MOVEit (CVE-2023-34362) vulnerability. Other months like March and April 2023 were comparatively quieter.

The geographical spread and diversity of the institutions targeted underscore the global threat posed by these ransomware groups. As the top six ransomware groups claim more than 40% of all the breaches in the education sector for 2023, the following analysis will focus on ransomware claims from those groups.

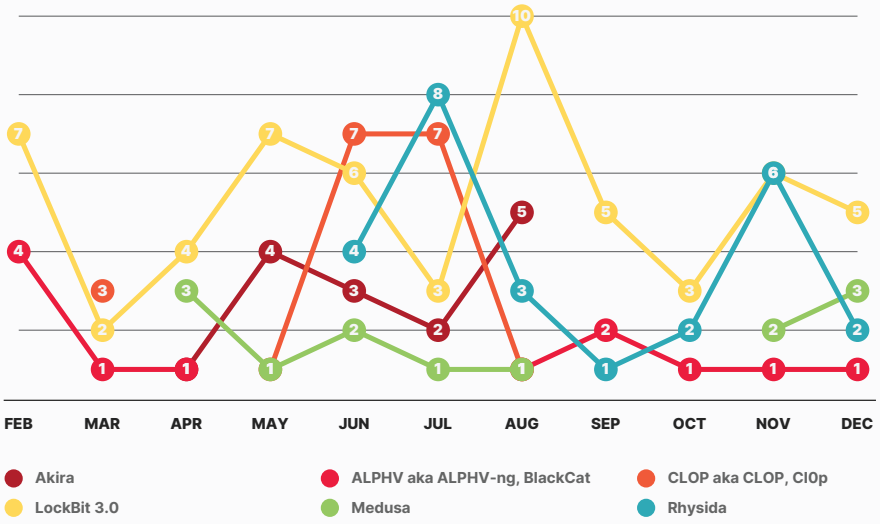


Figure 40: Breach trends of the top six ransomware group claims in the education industry

LockBit 3.0 Ransomware: Lockbit had the most claims among all ransomware groups, alleging to have breached multiple and diverse public schools and universities globally. These included the likes of Richmont Graduate University, Shore Regional High School District, Northern Ontario School of Medicine University, and Olympia Community Unit School District (CUSD), among others. On a rather unusual note, the ransomware gang supposedly issued an unconditional apology for targeting school children in the Olympia CUSD. The threat actor also admitted it felt "ashamed" and said it would provide a free decryptor to victims. The group was active throughout all of 2023 and had the highest activity during August.

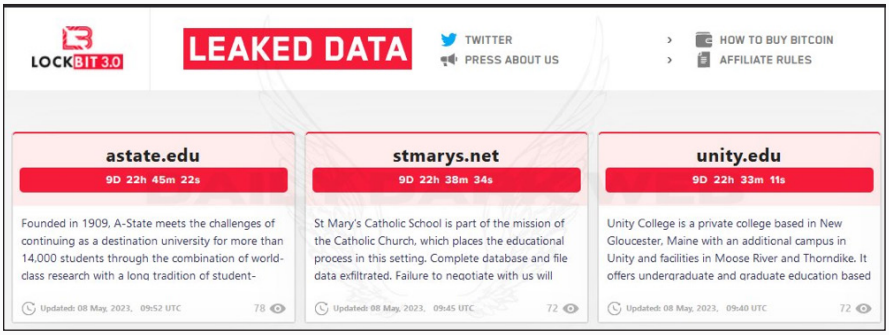


Figure 41: Samples of schools claimed to have been breached by LockBit

CLOP aka CL0P Ransomware: Clop targeted and claimed notable and well-known universities such as University of California Los Angeles (UCLA), Johns Hopkins University, University of Rochester, University of Georgia, and Medical College of Wisconsin, among others. The breaches often exploit third-party vulnerabilities like CVE-2023-34362 (MOVEIt). The group was most active during June and July 2023.

Medusa Ransomware: Medusa's targets were diverse, including claims for Uniondale Union Free School District, Glendale Unified School District, St. Landry Parish School Board, and Atlantic International University Inc. (AIU), among others. Medusa had a low victim count but was relatively consistent for most of the year with a small spike around November and December 2023.

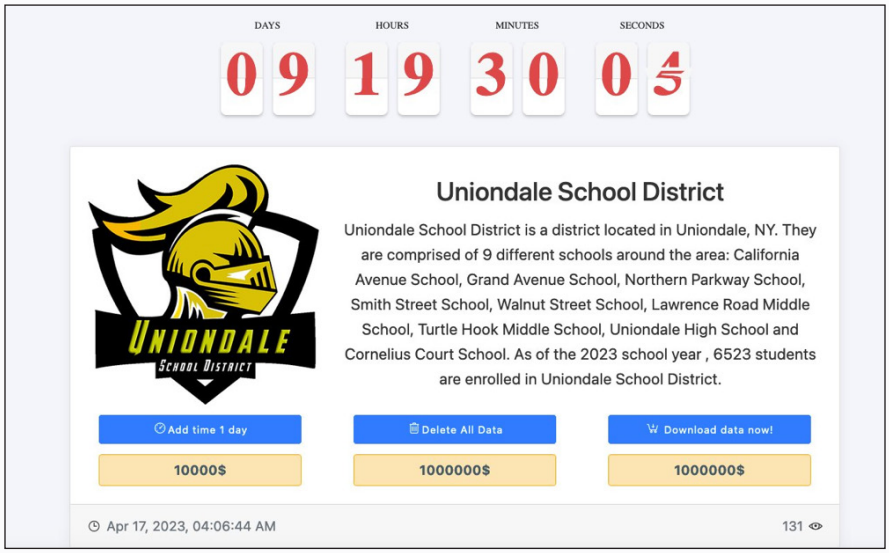
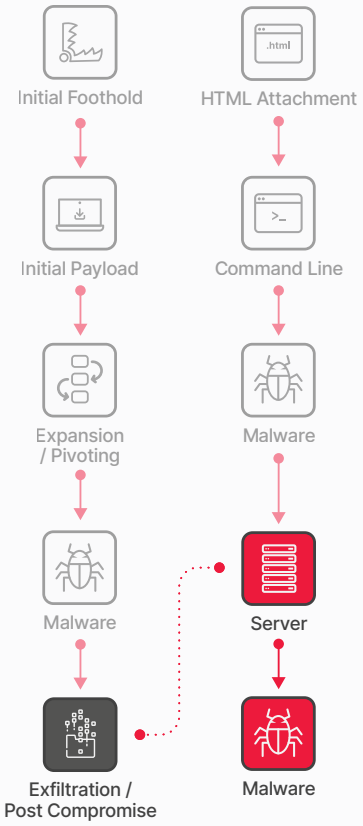


Figure 42: Sample of a Medusa ransomware breach claim of a school district

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining ransomware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security controls to protect against ransomware distributed via email. Educate users on the risks of malicious email attachments and phishing attempts. Enhance vigilance and implement email filtering and monitoring systems.
- Establish and regularly practice a formal Incident Response process. Ensure that backups are available as a contingency to recover from a worst-case scenario.
- Enable system logs on critical systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.
- Ensure enforcement of least privilege, data cannot be encrypted if the exploited user does not have access to it.
- Instill multiple levels of security, or defense in depth, including varying anti-malware scanners from multiple providers at different layers.



Exfiltration / Post Compromise/ Impact

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

Based on active monitoring, Trustwave researchers observed that the technique most often used was data encryption related to unspecified ransomware activity and network denial of service.

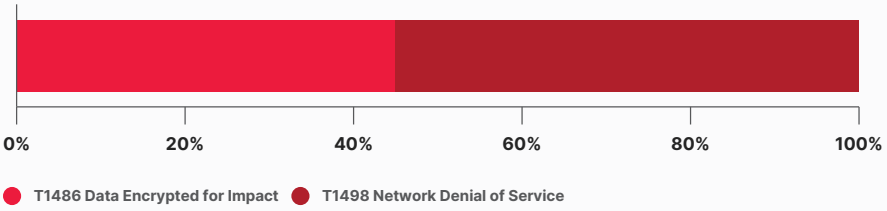


Figure 43: Impact techniques used by threat actors

Ransomware attacks have become the dominant source of breaches for the education sector and are exacerbated by large-scale breaches of third-party education providers such as Blackbaud and Illuminate.

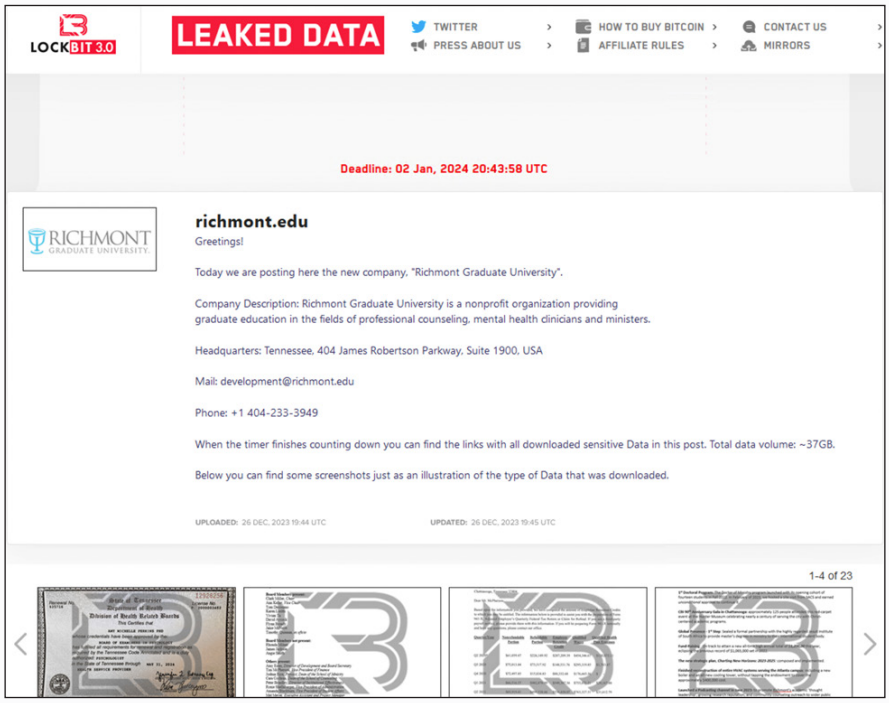


Figure 44: A ransomware threat actor claiming a breach of a university with potentially sensitive health information

Another notable impact observed in our active monitoring is Network Denial of Service. This observation is supported by events highlighting the significant increase in DDoS attacks on educational institutions in the past few years. This result was particularly notable during the pandemic due to the transition to remote learning in most countries. DDoS attacks have led to considerable network disruptions, causing downtime, and interrupting online classes.

Notably, these attacks were not only carried out by professional cybercriminals, but also by students using easily accessible online DDoS tools. For example, the National Crime Agency in the UK identified students as young as nine years old deploying such attacks.

Additionally, straightforward intellectual property and identity theft can also be considered one of the important impact factors in the education industry. Universities and research institutions have a significant amount of intellectual property and research. Education institutions involved in research collaborations with government or military agencies where breaching university systems might provide access to sensitive governmental or military information are particularly vulnerable.

Identity theft is another important potential impact as breaches of education databases could potentially expose personal details of students, faculty, and staff. Threat actors commonly exploit this data for illicit activities such as selling stolen information on the various Dark Web forums and marketplaces such as the one shown below.

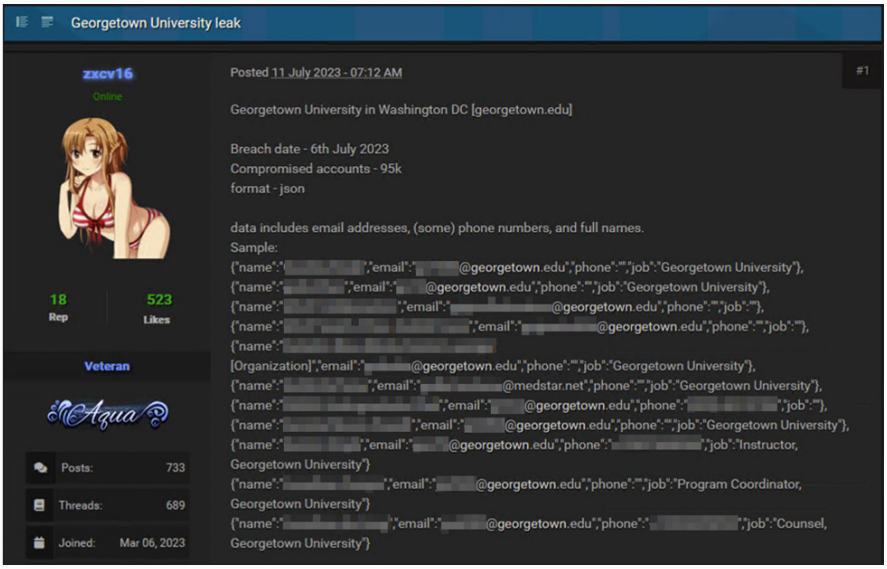


Figure 45: Sample posting of a threat actor selling personal information of personnel from a well-known US university

Lastly, the impact of cyberattacks on educational institutions can be profound. Cyberattacks and breaches could have significant impact in their operational capabilities and status. For example, Buffalo Public Schools experienced major operational disruptions due to such attacks. More drastically, Lincoln College had to close its operations permanently, highlighting the severe consequences cyberattacks can have on educational institutions.

100%

OF TRUSTWAVE'S ADVANCED CONTINUAL THREAT HUNTS RESULT IN THREAT FINDINGS

Mitigations to Reduce Risk

- Databases that store sensitive data should be a priority for robust security controls. Database security tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Ensure appropriate segmentation, segregation, and apply Zero Trust principles. Review if the database needs to be accessible to the whole network, or if it can be hidden behind certain applications.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you. Train staff on ransomware recognition to decrease time of response and remediation.

Key Takeaways and Recommendations

Although the education sector isn't alone in facing an elevated threat landscape, the consequences of attacks in this industry can be quite severe. Attackers are highly motivated by financial gains and continually adapt their methods to outpace defenses. Education has some unique challenges due to the nature of the industry, including:

- **Extensive Online Infrastructure:** The education sector faces unique challenges due to its extensive infrastructure. These include a wide range of devices and systems that could potentially be vulnerable to cyberattacks. As educational institutions continue to shift towards online education, there is an escalating exposure of networked devices and systems. Furthermore, decentralized IT management, and in some cases, limited cybersecurity resources often lead to inconsistent security policies and inadequate controls.
- **Data Trove:** Education institutions and their third-party suppliers store large volumes of personal data, which increases the risk and impact of data breaches and identity theft. Their heavy reliance on digital communication and online collaboration platforms increases the risk of phishing and social engineering attacks. The risk is further heightened by typical open internet access policies and BYOD practices in these institutions.
- **Collaboration and Intellectual Property:** The involvement of many educational institutions in research and their possession of sensitive intellectual property makes these institutions attractive targets for cybercriminals and state actors. Collaborative activity with entities like the government and military increases their risk exposure, and with the continuing evolution of cyber threats creates challenges their cybersecurity preparedness.

As demonstrated in our attack cycle, threat actors often employ multiple vectors to persistently target education organizations. While the technical aspects of these attacks may change over time, the underlying tactics tend to remain consistent. Some of the key points to consider in the education industry are as follows:

- **Phishing and Social Engineering Threat Vectors:** Phishing and social engineering are the most exploited methods for gaining initial access within organizations. These attacks typically pose as legitimate university communications, often leveraging relevant topics such student job offers and research related RFQs.
- **Malicious Email Attachments:** The education sector frequently encounters malware through email attachments. HTML files are particularly common and used for credential phishing and redirecting to malicious sites. Research shows this is facilitated through misuse of reputable services (e.g., Google Services, Cloudflare) and compromised websites to distribute malicious content.
- **Vulnerability Exploitation:** Apart from phishing, threat actors continue to exploit vulnerabilities in public-facing applications and use techniques like drive-by downloads to gain initial access to educational institutions' networks. Attackers continue to rely on vulnerabilities in often targeted publicly exposed services including, but not limited to Log4J, MOVEIt, and ApacheMQ.
- **Exposure of Publicly Accessible Systems and Services:** There is significant exposure of educational institutions' networked devices. These include highly sensitive systems such as public file servers, printers, collaboration systems, password managers, network devices, and security cameras.
- **Malware and Ransomware Attacks:** Ransomware, as with other sectors, is a significant threat to educational institutions. To facilitate the attacks, threat actors deploy a range of malware types, including loaders/downloaders, infostealers, and RATs, to maintain control, steal information, and to facilitate the end-to-end ransomware process. There have been attacks targeting universities and schools that have led to severe operational disruptions and data exposure.
- **Access Brokers and the Dark Web:** Access Brokers in the Dark Web and various underground marketplaces continue to sell and trade unauthorized access credentials to a diverse number of educational institutions' networks and systems.

- **Third-Party Supplier Risk:** Educational institutions are vulnerable through third-party suppliers. Attacks against software and IT service providers can lead to compromised severe security and operational impact within the institutions themselves as illustrated in the Blackbaud and Illuminate breaches.
- **DDoS Attacks:** Educational institutions are particularly susceptible to DDoS attacks, which can cause significant network disruptions and interrupt critical online activities, including remote learning and administrative functions. There have been reports that DDoS attacks have been carried out by students themselves.

As a result, preventative measures remain the most effective defense against all types of cyberattacks. As shared earlier in the previous sections of the attack cycle, the following chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.

Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- ❑ Conduct regular training, awareness, and mock phishing tests programs for students, faculty, and staff, emphasizing the recognition of phishing emails, especially those mimicking university communications, HR communications, and job offers. Educate the education community about the risks of phishing, drive-by downloads, and the importance of secure browsing habits.
- ❑ Implement robust anti-spoofing measures, including deploying technologies on email gateways. Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- ❑ Regularly conduct vulnerability scanning and patch systems to protect against known vulnerabilities. Promptly patch critical vulnerable systems. Update and patch all software regularly, including web browsers.
- ❑ Enforce account and password hygiene. Regularly rotate passwords (e.g., every quarter) to mitigate issues related to valid accounts. Implement password complexity requirements to enhance security. Enable multi-factor authentication (MFA) to provide an additional layer of protection for accounts.
- ❑ Databases that store sensitive data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- ❑ Conduct a comprehensive security assessment before any form of engagement is initiated with a third party. This will involve assessing the cybersecurity policy being deployed, existing and tested incident response plans, and compliance with related standards.
- ❑ Periodically conduct audits and reviewing the security practice of third-party vendors. This involves a periodic review of the service provider, vulnerability assessments, as well as penetration testing to identify and remediate any weak points in security.
- ❑ Encrypt all sensitive data both in transit and at rest. Restrict the access of sensitive data to only those coming from the principle of least privilege. Carry out regular monitoring of the access logs so that activities of unauthorized or suspicious nature may be detected.

Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Educate users about the dangers of opening unknown files and links. Regularly conduct security awareness training to help them identify and avoid phishing attempts and social engineering tactics.
- Implement policies to restrict or monitor the execution of scripts like VBA and PowerShell. This can be done using tools like Windows Group Policy.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Implement granular "allow list" of applications on specific hosts to minimize exposure. Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- Apply additional privilege restrictions to prevent unprivileged sources from running different command shells.
- Conduct regular audits of all applications in the environment to combat the adoption of custom applications that could result in vulnerabilities.
- Adopt strong password policies and implement continuous monitoring for credential dumping and authentication manipulation techniques.
- Monitor the use of unusual connections in RDP, SMB/Admin Shares, DCOM, and other open services using anomaly and behavior-based detection techniques.

Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- Enhance email security measures and educate users about the dangers of malicious email attachments. Increase vigilance against phishing campaigns and scrutinize email attachments. Implement robust email filtering and monitoring systems.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations and implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous. Additionally, establish and regularly practice a formal Incident Response process.
- Perform ongoing underground and Dark Web monitoring for information leakage that may have been missed.

Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Databases that store sensitive data should be a priority for robust security controls. Database security tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Ensure that up-to-date backups are available as a contingency to recover from a worst-case scenario.
- Use advanced email filtering solutions like Trustwave MailMarshal to detect and block malicious emails that may contain harmful attachments or links.
- Employ comprehensive endpoint protection solutions that include antivirus, anti-malware, and behavior-based threat detection to identify and mitigate threats.
- Monitor the Dark Web regularly for potential compromises and have a robust incident response process to contain and manage incidents.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you. Train staff on ransomware recognition to decrease time of response and remediation.

Appendix/Reference

Threat Groups

Akira:

- First detected in March 2023, the Akira ransomware has primarily targeted companies in the US and Canada. While code similarities suggest links to the notorious Conti ransomware group, tracing their exact connection is difficult. Akira takes a unique approach to double extortion. Unlike most groups, they steal sensitive data before encrypting files, giving them leverage beyond just data loss. However, instead of demanding payment for both decryption and data deletion, they offer victims a 'choice': pay to decrypt files or pay to have data deleted, but not both.

ALPHV aka BlackCat:

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. According to the FBI, ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

Bl00dy Ransomware:

- Bl00dy ransomware gang began their operations in May 2022 by targeting healthcare organizations in New York. Compared to other ransomware groups, Bl00dy appears to conduct their ransomware operations manually and does not develop their own ransomware independently.
- Instead, Bl00dy uses leaked ransomware builders and source codes of other ransomware payloads such as Babuk and Conti. In September 2022, Bl00dy ransomware group came up with a new ransomware variant that uses the leaked LockBit 3.0 ransomware builder.

Clop or Cl0p:

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023- 34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

LockBit 3.0:

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

Medusa:

- MedusaLocker is a ransomware strain that emerged in 2019 and has since spawned various versions, though core functionalities remain unchanged. Alterations include modified file extensions for encrypted data and variations in the appearance of the ransom note. Ransom payments from victims are typically divided between the affiliate (55-60%) and the developer.
- This ransomware often infiltrates victim systems via vulnerable Remote Desktop Protocol (RDP) setups, alongside employing email phishing and direct attachment of the ransomware to emails in spam campaigns for initial access.

No Escape:

- Emerging in May 2023, No Escape is a financially motivated cybercriminal enterprise, and employs tactics like double extortion, striking fear into victims across diverse industries like healthcare, finance, and education. Their custom-built malware encrypts files and pilfers sensitive data, holding it hostage with threats of public exposure unless ransoms are paid.

Pirat-Networks:

- The "Pirat" ransomware group has been observed using a Chaos ransomware variant to attack individual devices, including both personal and business machines. While identified in multiple countries, its activity does not seem as widespread as other ransomware actors employing more complex tactics like multiple encryption, lateral movement, and double extortion.
- Upon successful compromise, Pirat encrypts files and appends them with random 4-character extensions. A ransom note demanding 300 US dollars in Bitcoin is left along with a cryptocurrency wallet address and email contact.

Rhysida:

- Emerging in May 2023, the Rhysida ransomware has infected nearly 50 organizations globally. Operating under a RaaS model, this financially motivated threat rents or sells its attack tools to other cybercriminals. Beyond encryption, they employ double extortion, stealing sensitive data and threatening public release unless a ransom is paid.
- Rhysida casts a wide net, targeting sectors like government, healthcare, education, and technology.

Royal:

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).

Vice Society:

- The Vice Society ransomware group gained attention between late 2022 and early 2023 due to a series of high-profile attacks, including one affecting San Francisco's rapid transit system. While primarily focused on education and healthcare, evidence indicates they are also often targeting the manufacturing sector, suggesting a diverse industry penetration approach through compromised credentials procurement.
- Initially known for exploiting the PrintNightmare vulnerability, Vice Society utilized ransomware strains like Hello Kitty/Five Hands and Zeppelin. Recently, they developed their own ransomware builder and adopted stronger encryption techniques. A joint advisory by FBI, CISA, and MS-ISAC in September 2022 highlighted the group's disproportionate targeting of the education sector, with expectations of heightened attacks coinciding with the 2022-23 school year.