Bitdefender

WHITEPAPER Mar 2023

Bitdefender MDR Insights: Social Engineering Threats to Education

Contents

Key Points

- Social engineering is one of the most successful attacks that the Education industry faces because it takes advantage of potential gaps in defenses across a wide attack surface.
- Bitdefender Cyber Intelligence Fusion Cell's (CIFC) most common intelligence alerts concern typosquatting and credential leaks, with a marked increase since 2021.
- The FBI and other security organizations recommend proactive steps to mitigate the risk from social engineering attacks.
- Adopting best practices and increasing visibility on the network are important steps to adding defenses-in-depth to an enterprise.

Summary

The education industry – with its complicated ecosystem of locations, devices, people, and data – comprise a large attack surface. Even the most well-protected organization can still fall victim to an attack that uses social engineering, which manipulates people into exposing information or performing actions. Social engineering often navigates through gaps in the defenses of organizations. Monitoring indicators such as typosquatting and credential leaks, adopting best practices, and deploying security tools can benefit an organization, and act as additional layers of defense.

Details

When looking at the education industry, one must consider the vast range of internal and external assets and events influencing its threat landscape. Education encompasses multiple organizations, from primary through high schools, to higher or continuing education. The industry also includes those organizations that support the vertical, which could range from unions to government bodies, as well as publishers. To complicate matters, schools and school districts often have a large ecosystem to store data and facilitate classroom instruction across multiple physical locations; they often deal with frequent turnover as faculty and students graduate or matriculate each year.

The COVID pandemic saw an increase of geographic dispersion, as well as the adoption of cloud infrastructure and more platform- and software-as-a-service applications to support distance learning. Some of the recent technology adoptions were new for a lot of organizations, and this adoption came with growing pains for schools and districts that had never previously used these technologies. All these changes brought new factors to consider with threat modeling. In some cases, the attack surface grew and made conditions ripe for a potential attack, especially when considering social engineering threats comprised of credential leaks, typosquatting, and business email compromise (BEC). The hard part about social engineering attacks that leverage some or all these methods is that certain parts of the attack may not be immediately apparent – to systems or to people.

According to Verizon's 2022 Data Breach Investigations Report (DBIR), the education industry is under increasing threats from many sources. According to Verizon's data, educational organizations saw an increase in ransomware attacks, representing over 30% of the 1,200+ incidents they investigated. The most likely mode for attack involved an external threat actor who used system intrusion, web application attacks, or took advantage of some human factor or error, to obtain personal data and credentials—most typically with a financial or criminal goal. One of the more surprising findings from the DBIR was that over 30% of the human error was the result of an errant email that exposed sensitive data to the wrong recipients. The leading attack vector was the use of stolen credentials, which itself can lead to a variety of follow-on attacks.

Credential Leaks

At Bitdefender MDR, the Cyber Intelligence Fusion Cell (CIFC) compared internal findings with this report that seemed to support some of these findings, especially credentials. Education is the third most popular industry among Bitdefender MDR customers, representing all phases of education, and located across several regions, including North America and Europe. One of the most common intelligence alerts that CIFC investigates are those concerning credential leaks. In 2021, education customers comprised 17% of these alerts, but in 2022, that number jumped to 45% of credential leak investigations. While the most probable cause for the increase in alerts was the addition of a new intelligence source in 2022 that centers on capturing recent malware logs (which often include credential data from information-stealing malware), the increase remains concerning and will be an area CIFC continues to monitor for additional trend insight throughout 2023.

Credential leaks, especially from new malware sources, often give criminals a potentially fresh source of emails and passwords that are likely still in use. Malware logs are more dangerous than combination lists which have been frequently reposted and resold over many years. Emails alone can help target phishing or spam campaigns; meanwhile, multiple industry studies have shown that people reuse passwords across multiple platforms and applications, which increases the likelihood of many account compromises from one leaked password. The most likely sources of stolen credentials are through malicious websites that steal browser session information or are harvested from spoofed sites that might resemble login portals for popular banking or social media sites. Most often, however,

it is through spoofed sites that resemble login pages for Office 365 and similar cloud collaboration platforms. Depending on the malware, some of these credentials are bundled for sale on popular Dark Web marketplaces such as Genesis and Russian Market, which also often include browser and session information that enable access to even more accounts, as shown in Figure 1 below.

Figure 1: Stolen login information for sale on Russian Market

Besides malware and session-stealing websites, the organizations themselves can be their own worst enemies when it comes to credentials. Although it's a rare occurrence, CIFC has investigated instances where emails or full credentials and access keys were exposed on public sites like GitHub or Pastebin, often the result of academic research or coding projects completed for a course that were, in some cases, abandoned or forgotten. Most of these cases involve college courses or similar higher education; however, as STEM initiatives continue to be pushed down to younger students, the chance of exposure potentially expands to also include primary and secondary education.

When considering that each academic year (and sometimes each semester), new faculty, staff, and students are on- and offboarded, the potential pool of victims ebbs and flows – and so does the attack surface. This is where it becomes critical to ensure that access is shut down as quickly as possible when no longer needed; alternatively, if a password is discovered in the wild, that it's reset in a timely manner. To mitigate the damage of a potential credential leak, it's good to audit account accesses from the beginning and use least-privilege principles wherever possible. It shouldn't have to be said, but it might be worthwhile to make occasional gentle reminders to not mix business and school emails with personal use. Frequently, CIFC has seen official work emails exposed in breaches of social media, gaming, e-commerce, and other non-business websites.

Finally, while it may be cost-prohibitive to adopt certain tooling across the entire organization, adopting multifactor authentication (MFA) for a few may also be a good step, especially for those who have more privileged access to sensitive information or administrative access to devices on the network. Deploying endpoint protection tools also adds visibility of users and devices connected to the network, while also protecting against malware or criminal tools with information-stealing capabilities, such as RedLine or Raccoon, which are popular on criminal marketplaces.

Typosquatting

The tactic of typosquatting remains popular for spammers and phishing campaigns that attempt to take advantage of unsuspecting users. Like phishing itself, typosquatting is a low-tech method that requires minimal investment and offers potentially large returns. More importantly, when combined with attacks like phishing, typosquatting still works and remains part of top attack vectors every year.

For example, criminals are betting on that moment when b1tdefender.com looks exactly like bitdefender.com for just a split-second, long enough to conduct fraud. Advanced nation-state actors have also improved their typosquatting tactics over the years and still use them to add legitimacy to their attacks; thankfully, Microsoft and other vendors have worked quickly to shut down these domains. To further complicate matters, malicious phishing and spam domains often have a lifespan measured in hours, making it hard for defenders to share information or react quickly.

To stay ahead of attackers, CIFC monitors typosquatting across all customers by investigating new domain registrations and comparing them to known good customer information and alerting customers for further review, if needed. While the team has investigated over 1,000 typosquatting alerts since the beginning of 2022, the number of suspicious domains forwarded for customer review was under 10%, and actual malicious domains seen in the wild were far less.

Monitoring domain changes is a cost-effective way to ensure the brand or organization is not being targeted, especially considering how much a single domain registration may cost on popular top-level domains (TLD), such as .com, .net, or .edu. If an organization tries to purchase all the possible misspellings and related domains to redirect users – or that take advantage of newer TLDs such as .info, .education, .academy, and similar – it becomes another expense and one more thing to maintain and remember to renew. Considering there are nearly 1,600 TLDs available, this can become unmanageable and requires budget efficiency, especially for smaller organizations who may not have limitless budgets or personnel.

Organizations should not only audit domains they own on a regular basis, but they should also make sure to communicate to users which domains are the correct ones to use. If a typosquatting event occurs, administrators should take steps to block known bad domains as quickly as possible at the mailbox level, and at the network or proxy level. Information-sharing organizations and

intelligence threat feeds can also complement existing email or network security tools to help identify suspicious or malicious domains, as well as the ability to block these quickly at scale.

Business Email Compromise

As discussed in the introduction, a major security factor at play is the human factor, and business email compromise (BEC). BEC attacks may be one result of credential theft and spearphishing that take advantage of implied trust between coworkers or vendors. If phishing is an extremely broad, untargeted attack, BEC is its laser-focused, shadowy sibling. More dangerous than spearphishing, BEC attacks stem from a position of trust. While it is most often discussed in the context of business, BEC can show up in educational settings. The attack surface expands and contracts regularly with educational institutions, and it doesn't help that human factors come into play, or that there are always new users who don't know the correct processes.

There are a few ways an attacker might perform BEC. The FBI warns of several scenarios: invoice fraud, CEO or executive fraud, attorney or client/vendor impersonation, or data theft. Threat actors may spoof a domain to resemble a partner or vendor, or an otherwise legitimately related business. They may obtain access from a partner or vendor and intrude into the middle of an email chain, representing themselves as someone legitimate. Once in the conversation, there are ways they can work with replies to send malware or build trust to facilitate other attacks. In a lot of often-cited cases, it's an executive impersonation attempting to obtain financial or personal information, or to send a fraudulent payment. Emails to your organization might be a product of scraping company email addresses from social media or other publicly available websites, or purchased from a third party, such as a marketing company or from illicit forums or marketplaces.

Thankfully, lots of good advice exists to protect the organization from BEC. Because the cost to business has ranged from millions to billions of dollars in losses each year, the FBI has issued alerts and advisories about major events and good practices to adopt. Some of the most basic steps are similar to solutions to other security problems, such as regular patching and being vigilant about email security, especially paying attention to the sender and the message. Another tip that makes sense is using out-of-band communication methods or secondary verification steps to ensure the payment being requested is legitimate. Finally, ensure credentials, financial information, and other sensitive data are not being sent to unknown parties via text, chat, or email.

Another aspect of business email compromise to consider requires some additional critical thinking on the part of the targeted user; this is where specialized training and awareness can come into play. If someone suspects foul play, there needs to be validation or confirmation mechanisms that involve secondary communication means or points of escalation. As with phishing, looking at the message itself and how it's presented can be great indicators of something amiss:

- Is there high pressure to conduct a transaction immediately?
- Is the message coming from the sender's actual, known email address(es)?
- Do the invoice amounts or services requested make sense on the part of the sender?
- Would this transaction be conducted via email normally? Is there a customer or vendor portal, or other process that would normally be used?
- Would this person normally make this type of request? Conversely, would the targeted employee be the one who would normally handle such a request?
- Is there pressure to keep this transaction confidential?
- Does the language and tone of the email sound like the person? Also, do the language and grammar seem right for the person (if known)?

The bottom line is that if something doesn't look right, then it should be reported to leaders or security teams. The organizational culture should emphasize security and ensure that there are processes that protect the employees and the business. Finally, these measures should be documented and communicated for the benefit of everyone.

Conclusion

Adversaries will continue trying new tactics to take advantage of the human factor, and threat actors are experts at probing weaknesses and finding security gaps. Understanding where the threats lie and how they might attack prepares everyone for a potential attack. The problem with social engineering attacks such as these is that they can bypass traditional security tooling and processes in the initial phases, or attack where no defenses exist. This is where a combination of tooling and best practices can help add defense-in-depth to an educational institution, especially one with complicated factors of technology, location, and people to consider.

MDR Actions Taken

- Bitdefender Labs constantly looks for new malware signatures and updates GravityZone tooling regularly. This is due in part to our global support of popular security websites such as VirusTotal, but also due to research on various sources and millions of customer endpoints that enable visibility on a wide variety of emerging and ongoing campaigns.
- MDR analysts perform regular threat hunting and investigate both behavioral and indicator anomalies to determine if activities in an environment are legitimate or require further investigation.
- CIFC researches the latest indicators to develop follow-on intelligence hunts that may capture new or altered adversary tactics and signatures, including known breached or compromised emails that could indicate unauthorized access.
- CIFC monitors domain registration changes and typosquatting and credential leaks based on known customer information that is confirmed through questionnaires, daily operations, and customer communications.

Recommendations

Review and implement the Center for Internet Security's Critical Security Controls (CSC) to standardize best practices across the enterprise. Verizon's DBIR recommends that organizations in the education industry focus on CSC 4 (Secure Configuration of Enterprise Assets and Software), CSC 6 (Access Control Management), and CSC 14 (Security Awareness and Skills Training). CIS offers guidance on applicable training, programs, and frameworks that can support these endeavors.

Consider using least privilege policies for users, especially when considering a user's ability to install and remove software, run scripts or execute files, or make changes to the default configuration of work devices.

Identify high-risk employees or teams, such as finance, human resources, IT administrators, or leadership who would be targeted in social engineering schemes. Consider using more specialized situational training for these teams, and employing hardening techniques, such as multifactor authentication or approval processes, as well as recognizing social engineering tactics that could be used telephonically, via email, and via social media. Regular cybersecurity awareness training, especially around phishing scenarios, can be beneficial to all users.

Check emails and passwords against public databases such as HaveIBeenPwned and enforce regular password changes, as well as policies for complex user passwords. Consider using multifactor authentication and password managers to guard against reused passwords, especially for more at-risk users.

Consider adopting acceptable use policies on when to use official email addresses and what types of user activity are allowed on the network. These policies may also include requirements to regularly complete security awareness training.

Install security tooling that can monitor or block activity on user devices and ensure all assets on the network have some level of security visibility. Email security can complement endpoint security tools to provide an extra layer of visibility to provide extended detection and response (XDR) capabilities for a security team.

Ensure user devices are regularly patched and updated to the latest secure versions to prevent exploitation of any software or hardware vulnerabilities.

Use industry-specific information-sharing frameworks, such as information sharing and analysis centers (ISAC), or intelligence feeds to stay aware of suspicious or malicious activity, such as phishing and BEC or typosquatting campaigns. Block known bad domains and IP addresses and ranges. Geofencing and web application firewalls can bolster defenses at the application level.

For more information, visit https://www.bitdefender.com.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-CIFC-MDRInsights-SETE-creat6589-en_EN
CreaDate_01Mar23 • Updated_02Mar23