White Paper

For CIOs in the Education Sector, a Proactive Approach to Security is Required to Address the New Realities of Ransomware Attacks

In 2021 alone, 62 school districts experienced attacks, resulting in learning disruptions at 1,043 individual schools. The numbers are trending upwards and it's only getting worse.

K-12 school systems have become prime targets for ransomware attacks, especially with the rapid rise of mobile devices and remote learning. It's critical that a school web filter be able to scan and identify malicious protocols and websites, as well as decrypt SSL traffic to expose threats that might otherwise be hidden within encrypted tunnels. School web filters also must provide a live view of web traffic across all devices and platforms, with in-depth analytics to quickly identify potential attacks.

January 13, 2022 was no ordinary school day for Albuquerque Public Schools (APS). The largest school district in New Mexico found itself completely locked out of its mission-critical student information system (SIS) due to a cyber-attack. A malicious actor had taken possession of the SIS to hold for ransom. APS cancelled classes that day and the next over concern for student safety.[i]

Over the long holiday weekend following the cyber-attack, APS consulted with security experts and law enforcement and resolved not to pay the ransom demanded by the attacker. The district came up with a workaround to access the locked files in order to reopen the schools on January 18, with full recovery ongoing long after the attack.

This was not the first attack against a New Mexico school district. In 2019, Las Cruces Public Schools experienced a similar ransomware attack. It took months to recover, during which time the schools had to transition to non-digital teaching methods (i.e., pen and paper). The IT department had to scrub almost 30,000 devices, one by one, to ensure the malware was fully removed.[ii]

Unfortunately, these two events weren't rare occurrences. Research by the Emsisoft Malware Lab indicates the education sector is a leading target for ransomware attacks. In 2021 alone, 62 school districts experienced attacks, resulting in learning disruptions at 1,043 individual schools. The numbers are trending upwards and it's only getting worse.[iii]

The Shape-Shifting of Ransomware and What To Do About It

The Cybersecurity and Infrastructure Security Agency (CISA) defines ransomware as "a type of malicious software, or malware, designed to infect computers and encrypt files until a sum of money or other form of ransom is paid."[iv]

That's a rather simple definition of what can actually happen. In practice, the malware often destroys access to backup files before it encrypts primary files, resulting in no access to systems and complete downtime. Increasingly, sensitive data or personally identifiable information (PII) such as students' names and birth dates are being stolen and also held for ransom under threat of public exposure. According to the security consulting group Unit 42, the average ransom payment in 2021 was $570,000.[v] Paying the demanded ransom may unlock the encrypted files, but further damage could be done, such as installing persistent software that can enable a repeat attack.

It's better to be proactive in order to prevent a ransomware attack rather than deal with the fallout from an attack.

The ramifications of an attack can be extensive. As happened in New Mexico, core administrative and educational systems can be inaccessible for days, or longer, leading to cancellation of classes. Without working computer systems, schools may have to resort to old-style teaching methods. Most victim districts have to engage an outside security service to investigate the attack and ensure that no vestiges of the malware remain. If student PII has been exposed, the district becomes non-compliant with the Children's Internet Protection Act (CIPA), putting federal funding at risk. If financial data is stolen or exposed, the school district may be required to pay for credit monitoring for teachers, staff, and students' families. On top of all of this, remediation is expensive and can take weeks or months—especially if students' devices have to be re-imaged. Baltimore County Public Schools, for example, spent more than $8.1 million on recovery after an attack at the end of 2019.[vi]

The bottom line: it's better to be proactive in order to prevent a ransomware attack rather than deal with the fallout from an attack.

To Be Proactive, One Must Understand The Stages of an Attack

To proactively prevent an attack, one must understand the origins of ransomware software as well as the stages of an attack. The notion of employing a cyber-attack and holding files for ransom is big business, primarily executed by international criminal groups like REvil and nation-states such as Russia, China, Iran, and North Korea. According to Chainalysis, $1.3 billion was paid out in ransom payments in 2020 and 2021,[vii] making this a highly lucrative business for the perpetrators.

An attack goes through several stages and understanding them presents the opportunity to defend against a successful attack.

Stage 1: Exploitation and Infection

This is the phase where an attacker establishes a foothold on a network, often through social engineering or phishing, or through exploiting a system vulnerability such as unpatched or out-of-date software. Once the foothold is established, the attackers can leverage their position to deploy their payload: ransomware software.

Stage 2: Delivery and Execution

Next the ransomware executable is delivered to the victim system and put into action. One of the first things it does is establish persistence, meaning it won't go away even if the host machine is rebooted or

attempts are made to remove the software. Delivery of the malicious executable and establishing persistence takes mere seconds.

Stage 3: Destruction of Backups

In an act called spoliation, the malware tries to locate all online backups of files and folders and deletes them to prevent easy recovery from backups.

Stage 4: File Encryption

Once the backups are thoroughly dispatched, the malware encrypts the primary files and folders using a unique key. At this point, there is often a secure key exchange with a command-and-control server (C&C, or C2) on the Internet. The use of a unique encryption key is important because this is part of the decryption process once a ransom is paid. Ransomware uses strong encryption methods to prevent the victim from breaking the encryption without paying the ransom.

Stage 5: User Notification and Cleanup

Last but not least, the victim is notified that their files have been encrypted and the only way to decrypt them is to pay a ransom, usually in a cryptocurrency to prevent tracking the attacker. Also, the malware cleans up after itself so as not to leave behind forensic evidence that could help solve the crime.

This entire chain of activity can take as little as 15 minutes or several hours, depending on how many files are encrypted and how extensive the network is. School districts have small networks compared to those of multinational corporations, so the execution of all five stages would be relatively quick.

Impero's ContentKeeper Web Filtering and Security Solution Fits into a Defense-in-Depth Strategy

No single cybersecurity solution can offer complete protection. A Defense-in-depth strategy layers multiple solutions to maximize the chance that any attack will be stopped. ContentKeeper is a full-featured web filtering and security solution that supports all platforms, devices, and web browsers. This solution plays a crucial role in protecting K-12 online environments from ransomware and other cyber threats. Let's explore how ContentKeeper can help prevent a ransomware attack.

The two most common threat vectors that allow ransomware to gain a foothold on a school district's network are phishing attacks and drive-by downloads from malicious applications and websites.

Phishing is a social engineering tactic whereby an individual is tricked into revealing sensitive information, credentials, or clicking a malicious link, usually by being led to believe that a fraudulent website or email message is genuine. The fraud can look very authentic. For example, a teacher could be sent an email that appears to come from the school principal, with instructions to follow a link to view the agenda for the upcoming in-service day. Of course, the principal's email address has been spoofed and the hyperlink goes to a server that relays malware – and not the meeting agenda – to the teacher's device. And just like that, the ransomware has a foothold on the school's network.

Another major threat vector stems from, shall we say, curious students who try to do things they shouldn't be doing, like going to BitTorrent to download files, or using Psiphon to access blocked websites and services. In these scenarios, students are going to parts of the Internet where threats are rampant, and they are quite likely to accidentally download malware without knowing it.

Activities like these, whether innocent or intentional, provide the infection vectors that get the whole ransomware chain of events started. Fortunately, ContentKeeper provides layers of protection that proactively defend against harmful activities and stop ransomware before it gets into the school networking environment.

Application Defense with App Defender

Students and others on the network may try to access applications that are known conduits for malware, for example, UltraSurf, Tor, BitTorrent, and Psiphon. Unfiltered Internet access granted through rogue applications such as these provides an effective gateway for malware infection. Shutting down these apps protects school networks and users from these threats.

NextGen firewalls (NGFWs) can identify applications based on port or reputation, but ContentKeeper provides a more granular level of identification and control of specific web application functions. App Defender identifies and blocks over 90 suspicious apps and protocols that are commonly used to circumvent school web filters. App Defender can prevent students from accessing the Dark Web or using programs to download potentially infected files, two common sources for all kinds of virus-infected content, including ransomware. App Defender also prevents students from using virtual private networks (VPNs) to get around a school's filter and security policy, even when the VPN application is run from a live-boot flash drive or on a bring-your-own-device (BYOD) access device.

App Defender allows an administrator to determine the best course for handling a rogue application, such as monitoring its use in passive mode, blocking it completely, or creating a quarantine for the person trying to use the app. In addition to the security benefits, disallowing BitTorrent and other rogue applications can save valuable bandwidth that is needed for teaching and learning.

Web Filtering Defense

Phishing campaigns are designed to trick people into clicking on a URL that takes them to a malicious website that may try to steal user credentials or auto-download malware to the user's device. ContentKeeper protects against malicious links that are found in phishing emails; URL protection is a powerful tool included with Impero's ContentKeeper Cloud Filtering and Security Platform. ContentKeeper uses sophisticated technology to evaluate the harmful status of both apps and URLs/IP addresses. Thus, a student or other user on the school network will never get to the sites that host the malware or ransomware because they are blocked.

ContentKeeper technology provides consistent and reliable filtering for all sources of K-12 web traffic and platforms including Chromebooks, Windows, Mac, iOS, IoT, BYOD, and guest networks. ContentKeeper is able to decrypt both Secure Socket Layer (SSL) and Transport Layer Security (TLS) protected web traffic at very high speeds in order to inspect it. The solution has real-time alerting of suspicious online activity. Moreover, the solution's cloud architecture allows schools to filter off-site devices without having to send traffic back to the school's network. This means that students using their school-managed device over a home Internet connection are still protected from malicious links, apps, and websites, making the transition to remote learning more secure.

Reporting and Analytics with ReportCentral

Visibility and measurement are critically important for school districts that want to understand how well they are doing in terms of security policy enforcement. After all, it's hard to control what can't be seen

or measured. Thus, ContentKeeper provides comprehensive, enterprise-class reporting and analytics to successfully monitor web use, security threats, and student safety.

ReportCentral's comprehensive reporting features include a live view of web traffic and in-depth analytics. CIO dashboards allow administrators to quickly analyze network and user activity to detect potential threats. The live viewer allows security teams to analyze traffic in real time to monitor and mitigate security incidents. ContentKeeper App Defender is fully integrated into ReportCentral to detect security circumvention attempts and preventions.

Being able to "fingerprint" the environment, and know who is using what device, and what browser, is very important. Knowing the categories of content that students and staffers are trying to get to is important. Knowing what kinds of applications the students are using, and what they are searching for, is very important. Visibility into all these things helps the district create a very informed cyber policy against threats like ransomware.

Conclusion

Ransomware is a serious threat to all school districts, and the threat grows stronger as organized criminals and rogue nation-states seek the easy payouts of ransom by desperate school administrators who want to avoid schedule disruptions. Ransomware has very serious ramifications, from complete loss of critical systems to expensive payouts and weeks of IT repair and recovery. Thus, prevention strategies are an absolute must.

K-12 schools are required by law to use web filtering techniques to keep students away from harmful websites and online content. Impero provides a leading solution for content filtering that has the additional benefit of heading off ransomware and other malware threats.

Learn more and request a demonstration at https://www.imperosoftware.com.

---

[i] Brad Dress, The Hill, Albuquerque schools remain closed for second day following cyber attack, January 14, 2022

[ii] Stephanie Chavez, KQRE, APS working to recover from ransomware attack (krqe.com), January 14, 2022

[iii] Emsisoft Malware Lab, The State of Ransomware in the US: Report and Statistics 2021, January 18, 2022

[iv] CISA, Reduce the Risk of Ransomware Awareness Campaign, January 2021

[v] GRC World Forums, Ransomware demands soar by 518% in 2021, 13 August 2021

[vi] Amy Simpson, Fox45News, BCPS ransomware recovery efforts come with $8.1 million price tag, June 15, 2021

[vii] Chainalysis Team, As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict, February 10, 2022