ContentKeeper

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.

Overview:

- The education sector is a leading target for ransomware attacks
- The cost of ransomware attacks in K-12 has risen dramatically
- Cyber attacks affecting schools could be 10 to 20x's greater than what's reported
- Defense-in-Depth strategies can help prevent ransomware

To proactively prevent an attack, one must understand the origins of ransomware software as well as the stages of an attack.

imperosoftware.com

Stages of a Ransomware Attack in Schools

STAGE 1:

Exploitation and Infection

The attacker establishes a foothold on a network, often through social engineering (i.e., phishing) or through exploiting a system vulnerability such as poorly written software code.

STAGE 2:

Delivery and Execution

The ransomware executable is delivered to the victim system. 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

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.

STAGE 5:

User Notification and Cleanup

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.

ContentKeeper

Impero ContentKeeper provides 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.

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.

imperosoftware.com

ContentKeeper's Defense-In-Depth Strategy

Web Filtering Malware Defense

- Malicious IP/URL protection and blocking of non-managed URL's
- Protection anywhere and on any device including off-site
- SSL/TLS decryption provides granular control and detailed reporting
- Closed-loop collaborative technology feeds real-time malware signatures for immediate categorization and prevention

Application Defense

- Identifies and blocks over 100 suspicious apps and protocols that are commonly used to circumvent school web filters
- Granular level of identification and control of specific web application functions
- Prevents students from using programs to download potentially infected files or allowing access to potential high-risk sites
- Prevents students from using VPNs to get around a school's filter and security policy

Reporting and Analytics

- Comprehensive, enterprise-class reporting to successfully monitor web use and security threats
- Live web traffic visibility and in-depth analytics
- Detailed reporting on suspicious app use and malware activity
- Intelligent dashboards to quickly analyze network and user activity for potential threats