

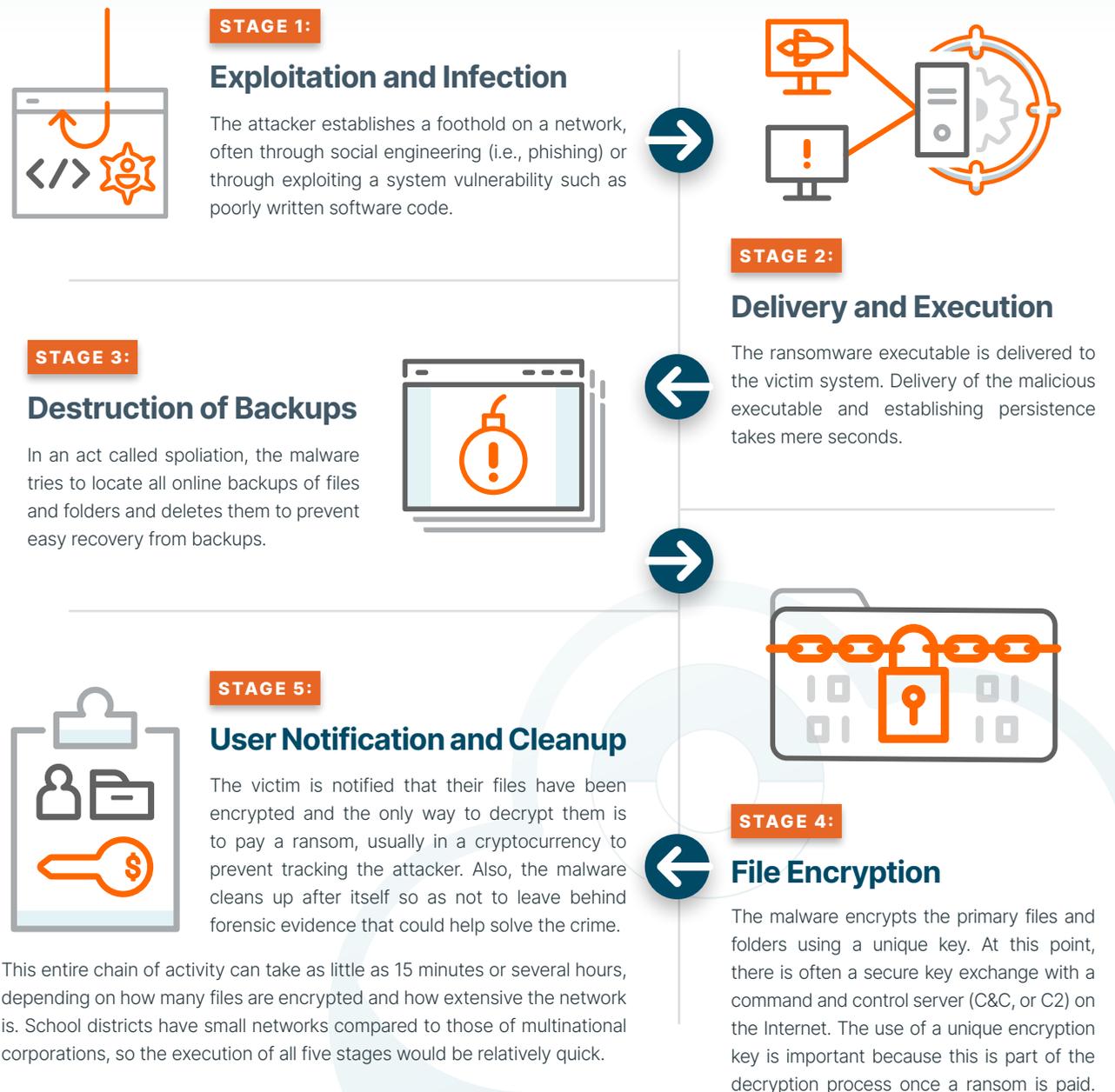
K-12 school systems have become prime targets for ransomware attacks, especially with the rapid rise of mobile devices and remote learning. It's critical that a school web filter be able to scan and identify malicious protocols and websites, as well as decrypt SSL traffic to expose threats that might 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.

Stages of a Ransomware Attack in Schools





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.

contentkeeper.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 90 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

