Six Steps to Stopping Ransomware in Schools and Governments

Local governments and educational institutions are disproportionately targeted and impacted by ransomware, but they usually lack the resources to mount aggressive countermeasures. Fortunately, although there are hundreds of ransomware families with multiple variants each, they share similar attack methods. Focusing on thwarting these common methods will stop most ransomware attacks as well as lay a security foundation that limits the harm from tomorrow's ransomware—or prevents it from succeeding altogether.

Successful Ransomware Follows Multiple Steps

Like all cyberattacks, ransomware executes a series of steps on a target over the course of minutes or weeks. Ransomware starts by exploiting a vulnerability, delivering a payload, and installing on one or more computers or servers. It then establishes a command-and-control (C2) channel with one or more external servers, enabling attackers to send commands to the infected system or systems. Attackers typically attempt to move through the network to deliver payloads to other systems, with the eventual goal of encrypting many important files to extract the largest possible ransom.

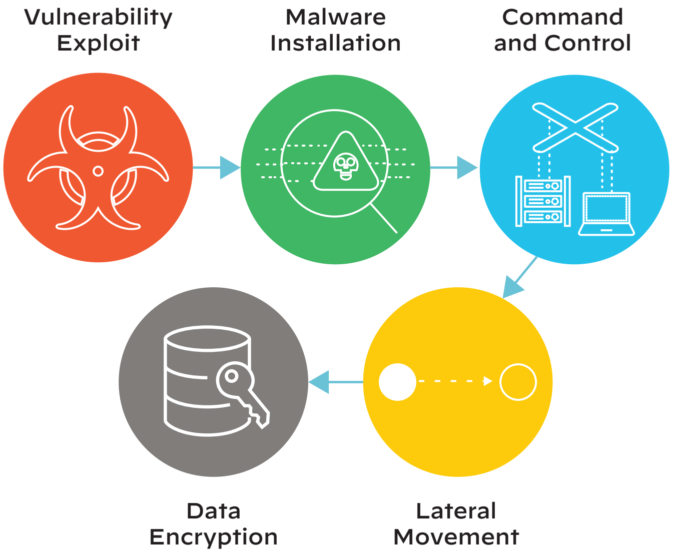

Figure 1: Ransomware attack lifecycle

Once files are encrypted, it's almost impossible to reverse the damage without the decryption key. To get files back, organizations often have to either pay the ransom or painstakingly restore machines from backups. Let's explore ways you can use technology to disrupt the attack lifecycle so you don't have to resort to these outcomes. The more ways you can disrupt the lifecycle, the less likely it is that ransomware will impact your organization.

1. Maintain Traffic Awareness

Because governments and school districts operate such a diverse range of networks and devices, identifying and patching or fixing cybersecurity vulnerabilities can be difficult. A surefire way to identify malicious activity is to gain visibility into what normally happens in your environment. Ideally, your security operations center (SOC)—or your security or network team—is aware of and has catalogued the users, applications, devices, and traffic patterns that should normally be on your network. This will make it easier to identify anomalies. Other steps you can take to maintain awareness include:

- **Decrypt anomalous traffic**. The first step of a ransomware attack often occurs over an encrypted channel, such as HTTPS. Develop an SSL decryption policy that maintains your employees' privacy while decrypting traffic from unknown or suspicious web and email servers.
- **Build daily traffic reports**. Understanding your organization's daily traffic snapshots helps quickly identify anything that is anomalous.

2. Disable the Delivery

Most ransomware attacks start with a phishing email delivering a malicious file to an unsuspecting user or directing them to a malicious website. In the context of ransomware, the goal of a phishing attack is to get a victim to either download a malicious payload to their computer or divulge their corporate login credentials to an attacker.

While training is an important aspect of preventing successful phishing, today's sophisticated attackers often create fake emails and websites that are difficult to distinguish from the real thing. The best defense is to prevent these types of communications from ever reaching an employee to begin with. Tactics that disable delivery include:

- Identify and block ransomware files or malicious links in emails.
- Ensure security enforcement points can recognize and repel new ransomware variants.
- Prevent your employees from entering their corporate credentials into fake websites.

3. Prevent Ransomware Installation

If ransomware manages to get past your perimeter defenses, it must successfully install on a computer or server to inflict any damage. With new ransomware variants being created all the time, your endpoint security needs to stay ahead of the latest ransomware techniques, especially if your computers and servers are not up to date with the latest patches. Ideally, your endpoint security does not rely on signatures. Instead, it should use multiple methods on the endpoint, as well as intelligence gained from other sources, to detect and block the installation of ransomware. For an endpoint security checklist, read 10 Requirements for Securing Endpoints.

4. Disable the Command-and-Control Channel

In the past, command-and-control (C2) channels used a single domain or web address to communicate with infected hosts. Now, attackers take advantage of DNS to further ransomware attacks. According to Unit 42, the Palo Alto Networks threat research team, almost 80% of malware uses DNS as a way to establish communications with a C2 server. To understand the common ways adversaries abuse DNS, read Stop Attackers from Using DNS Against You.

5. Prevent Lateral Movement

Once a ransomware attacker has gained a foothold, the next objective is to exploit any network-based vulnerabilities to gain access to other systems and infect them. Attackers typically succeed because most governments and schools grant users with verified credentials access to all environments, even if they don't have credentials for a particular system. A Zero Trust security strategy, based on a "never trust, always verify" approach, is a good tactic for preventing lateral movement, even for attackers with stolen credentials. Your organization identifies valuable data, assets, applications, and services (DAAS), creates a microperimeter around it, and defines the combination of users, devices, and applications that can access those valuable assets.

6. Employ Automation

Once you've detected and successfully stopped a ransomware attack, automatically disseminating that threat intelligence across your cybersecurity tools will help your organization quickly detect and repel future attacks. Security orchestration tools collect data from multiple cyber data sources, extract indicators of compromise (IOCs), and enable security teams to respond to incidents quickly and effectively.

Preventing Ransomware with Palo Alto Networks

Palo Alto Networks integrated innovations work together to automatically prevent ransomware in government and education. For more information, visit our ransomware page for government and education or contact your account team.

Table 1: Palo Alto Networks Technology vs. Ransomware

Ways to Stop the Ransomware Attack Lifecycle	How Palo Alto Networks Helps
Maintain Traffic Awareness	Our Next-Generation Firewalls, both physical and virtual, offer deep visibility into the applications, users, and traffic—even encrypted traffic—on your network without hindering performance or overburdening your network and security professionals. For more information, read 13 Things your Next Firewall Must Do.
Disable the Delivery	Next-Generation Firewall capabilities protect your network and cloud environments with advanced analysis, machine learning, shared intelligence, and automated protections. WildFire® malware prevention service detects evasive ransomware, automatically creates new protections against them, and updates security enforcement on your endpoints and in your cloud and network environments. URL Filtering includes credential phishing prevention you can use to block incoming phishing attempts and outgoing transmission of credentials to unrecognized domains.
Prevent Ransomware Installation	Cortex XDR™ blocks ransomware on computers and servers by combining local AI- and behavior-based analysis with data from other endpoints as well as cloud and network environments. Endpoints also benefit from automatic protection delivered by WildFire. Cortex dashboards offer holistic views into traffic across your endpoints and network.
Disable the Command-and-Control Channel	DNS Security for Next-Generation Firewalls applies predictive analytics and machine learning to identify malicious domains and DNS traffic, blocking C2 channels. Next-Generation Firewalls also take advantage of the latest intelligence on malicious websites, while DNS sinkholing pinpoints infected hosts attempting to communicate with C2 servers.
Prevent Lateral Movement	Palo Alto Networks has been named a Leader in The Forrester Wave™ Zero Trust eXtended (ZTX) Ecosystem Providers, Q4 2019. This is our second consecutive year as a Zero Trust Leader. Read the report.
Employ Automation	Cortex™ XSOAR is a security orchestration, automation, and response (SOAR) solution that helps your security teams manage alerts, standardize threat hunting processes, and automate response to attacks, including ransomware.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com