ThreatDown™
Powered by Malwarebytes

2024 K-12 RANSOMWARE *EMERGENCY KIT*

Ransomware is a clear and present danger to K-12 schools of all sizes. This emergency kit tells you what you need to know to understand the threat, how to harden your school against attacks, and what to do if your organization is experiencing an attack.

CONTENTS

UNDERSTANDING THE THREAT

Between June 2022 and May 2023, there were 190 known ransomware attacks against educational institutions, representing an 84% increase in attacks over a six-month period. Among them were high-profile attacks on Los Angeles Unified School District, Nantucket Public Schools, and Minneapolis School District.

The Vice Society ransomware gang specializes in attacking education, with almost half of its known activity (43%) directed against the sector. In 2023, we saw LockBit, Royal, Medusa, and Rhysida join Vice Society in targeting schools leading to over 6.7 million individual records breached.

The reality is that tight budgets, outdated equipment, and limited staff, make K-12 schools an easy target for ransomware attackers. The combination of these three problems spawn a host of new ones, including:

- **Lack of bandwidth and skills** can limit the ability of your team to effectively monitor and react to threat alerts.
- **Never ending cyber-attacks** continually flood schools with threat alerts.
- **Lengthy dwell times** lead to greater risk of infection.

$35.1B

What ransomware attacks on education cost the US economy

3WKS + 9MOS

For K-12 schools hit with cyberattacks

300K

Number of sensitive files leaked after Minneapolis School District refused to pay $1M ransom

ANATOMY OF A RANSOMWARE ATTACK

Ransomware is typically deployed as the last act in a sophisticated infiltration of your network by criminal hackers. Every ransomware attack is different, but they often follow a predictable pattern, which can be broken down into five phases.

Breach Attackers gain unauthorized access to one of your computers through malware; by phishing, guessing or finding a remote password; or through a software vulnerability. This can occur months before the attack phase.	The best way to stop a ransomware attack is to prevent the initial breach. This requires web protection, effective vulnerability and patch management, hardening of remote access, and users who can identify and report phishing.
Infiltration The attackers quietly explore your network and prepare their attack. They may steal data, and may try to disable security software and backups.	You can't prevent every breach, so structure and monitor your network so you can identify suspicious activity quickly and stop intruders before the attack phase.
Attack Attackers run ransomware throughout your network, often at night or the weekend. Critical business operations stop. Ransom notes explain how to negotiate with attackers.	Stopping attacks requires multiple layers of security defense, anomaly detection for unknown "zero-day" threats, and ransomware prevention technology.
Response Attackers demand a ransom, which could be millions of dollars. They will issue deadlines and may threaten to leak sensitive data.	You must restore critical operations while talking to customers, suppliers, insurance, press, lawyers, law enforcement and others. You will need offline backups and a plan.
Recovery Whether the attack is successful or not, attackers may still be on your network or there may still be lingering malware or artifacts that could cause reinfections. Your willingness to pay a ransom will have been noted.	After restoring critical operations, you must discover what happened. You will need to expel the attackers from your network, remove all traces of the breach, and harden your network against a repeat attack.

SHOULD YOU PAY THE RANSOM?

Most experts and government agencies do not recommend paying a ransom. Ransom payments incentivize further attacks and fund the continued development of ransomware, making everyone less secure.

Anyway, you might not have a choice: both North Carolina and Florida recently passed laws prohibiting public entities, including local schools, from paying the ransom.

If you are thinking of paying the ransom, you should consider the following carefully:

1. **Decryption often fails.**
   Ransomware gangs' decryption tools are poor quality and may lead to partially corrupted data. In May 2021, Colonial Pipeline paid a $4.4 million ransom. The decryption app it received was so slow it rebuilt systems from backups instead.[1]

2. **You are trusting criminals to keep their word.**
   Stolen data that's held for ransom may not be reliably deleted or properly secured. In multiple cases it has been leaked before a ransom is even discussed, or after the ransom was paid.[2]

3. **You will still incur recovery costs.**
   Even if you pay the ransom, you will need an extensive clean-up operation, and upgraded protection to prevent future attacks. The cost in downtime, lost productivity, and recovery can dwarf the ransom.

4. **Paying leads to repeat attacks.**
   Attackers will note your willingness to pay, and that you were not prepared to withstand an attack. As many as 80% of ransom payers suffer a second attack.[3]

FBI

WARNING

The FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back.

[1] Forbes, Here's Yet Another Reason Ransomware Victims Shouldn't Pay The Ransom, 2021, https://www.forbes.com/sites/leemathews/2021/05/29/heres-yet-another-reason-ransomware-victims-shouldnt-pay-the-ransom/
[2] Coveware, Q3 2020 Ransomware marketplace report, 2020, https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[3] Cybereason, Ransomware: The true cost to business, 2021 https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business

RANSOMWARE PREVENTION CHECKLIST

	BREACH	INFILTRATION	ATTACK	RESTORATION	RECOVERY
Create an inventory of assets including hardware, software and data	✓	✓			
Audit your network for unknown computers and services	✓	✓			
Disable Internet-facing systems, services, and ports you don't need	✓	✓			
Perform regular vulnerability scans	✓	✓			
Patch systems regularly, prioritizing the most vulnerable and critical	✓	✓			
Ensure systems are properly configured, and security features are enabled	✓	✓			
Harden remote access with MFA, password rate limits, and password lockouts	✓				
Deploy endpoint security software to all endpoints and servers	✓	✓	✓		
Provide staff with cybersecurity awareness training	✓	✓			
Implement a process for reporting and responding to suspicious activity	✓	✓	✓		
Document your network structure and data flows		✓			✓
Use network segmentation to subdivide your computer networks		✓			
Use least-privilege access for all systems and services	✓	✓			
Use allow listing to ensure that only authorized software can run		✓	✓		
Restrict the use of legitimate tools commonly used by attackers[4]		✓			
Harden domain controllers according to the latest best practice[5]		✓			
Monitor your network and endpoints using IDS, EDR and SIEM		✓	✓		✓
Make regular, comprehensive backups, keeping at least one copy offline				✓	
Have a process for restoring computers from clean system images				✓	
Practice restoring systems from backups, so you know they work				✓	
Create an incident response plan[6] that aligns with regulations			✓	✓	
Create a critical asset list so you know what you need to restore first • Consider how you will communicate internally and externally • Make contingency plans so critical functions can continue • Understand your legal and regulatory obligations				✓	

[4] This is known as "living off the land." The Living Off The Land Binaries and Scrip (LOLBAS) project maintains a list of legitimate software used by attackers at https://lolbas-project.github.io/

[5] Domain controllers are a prime target for attackers. Microsoft maintains a guide to securing domain controllers against attack at https://docs.microsoft.com/ven-us/windows-server/identity/ad-ds/plan/security-best-practices/securing-domain-controllers-against-attack

[6] You can find a response plan template at https://github.com/counteractive/incident-response-plan-template/blob/master/playbooks/playbook-ransomware.md

10-STEP RANSOMWARE RECOVERY PLAN

If you are dealing with a ransomware incident you may be working under extreme pressure. Ransomware may still be encrypting files, attackers may have issued ultimatums, and your organization will be desperate to get up and running again. **Ask for help, prioritize your actions, communicate clearly, and take care of each other.**

We recommend you take the following actions, in order:

1. **Contain the attack.**
   Isolate infected systems or networks to limit the impact of the attack. Your priority should be containing the attack but if you can do so while also preserving evidence by leaving affected systems turned on, do so.

2. **Establish the scope of the attack.**
   Understand what systems and what kind of data are affected, and prioritize critical systems for recovery.

3. **Communicate with stakeholders.**
   Stakeholders may include senior management, PR, your legal team, cyber-insurance providers, security vendors and law enforcement.

4. **Seek assistance.**
   Consider seeking expert assistance from local and national law enforcement, vendors or other third parties familiar with ransomware recovery.

5. **Preserve evidence.**
   With the help of law enforcement and third parties, try to preserve evidence from the attack if you can.

6. **Identify the ransomware being used.**
   This will help you discover if a decryptor is available, and it will inform the specifics of containment and clean up.

7. **Contain the breach.**
   Try to identify systems and accounts used in the initial breach, and any precursor malware or persistence mechanisms left by the attackers.

8. **Rebuild systems.**
   Use known good system images and backups to restore critical systems. Take care to segregate clean systems from affected systems.

9. **Reset, patch, upgrade.**
   Reset passwords, patch and upgrade software, and instigate any additional security checks necessary to prevent a recurrence of the attack.

10. **Document lessons learned.**
    Ransomware is constantly evolving. Use what you have learned from this attack to better prepare for the next one.

SECURITY MADE EASY FOR SCHOOLS

If you're feeling overwhelmed with the amount of information we just hurled at you, then you're a human being. Continually detecting and triaging ransomware threats is tough work—it's also not a one-person job.

Protecting school devices against ransomware demands advanced protection that's also easy for small IT teams to use.

The ThreatDown K-12 Bundle simplifies staff and student device protection by combining award-winning technologies, including attack surface reduction, endpoint security and mobile security, with an expert 24x7x365 managed services team to monitor, analyze, respond to, and remediate threats on your behalf.

Protect your staff and students, preserve uptime and optimize security investments while saving time and money.

Get a quote for ThreatDown K-12 bundle

Complete protection for K-12 education
at a price that makes sense.