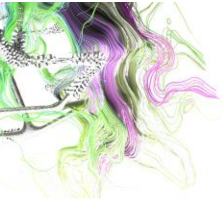


Ransomware 101: Protecting the education sector from damaging outages and data theft

***** This information is a collaborative piece produced by TrendMicro, Phoenix Software and SWGfL.

To this day, there remains no silver bullet solution to tackle the ransomware threat that can infiltrate the education sector. While commodity attacks are still commonplace, a growing threat is from more sophisticated actors who may spend weeks or even months performing reconnaissance on targets before using advanced techniques to covertly compromise and then deploy the malware for maximum effect. Increasingly these multi-stage attacks also include data theft, adding an extra dimension of risk to victim organisations, especially if student data or sensitive research is taken.

The education sector has been particularly badly hit. It is often seen as an easy target and one where there is huge pressure on schools, colleges and universities to keep services online. The start of the new 2020-21 academic year saw Newcastle and Northumbria universities hit by major ransomware-related outages, while countless others have been affected by a combined data stealing/ransomware attack on service provider Blackbaud—highlighting the threat from the digital supply chain.

There have been numerous threats to the education sector including phishing emails along with attackers sabotaging backup devices and using certain forms of technology to stay hidden. The National Cyber Security Centre recently announced an increase in attacks targeting the UK education sector. These attacks are noted as being more complex than normally associated with ransomware.

The current COVID-19 crisis is making things more challenging still for the sector. This is not just financially, but also in terms of its risk exposure through digital infrastructure and the ability of IT teams to respond promptly to incidents.

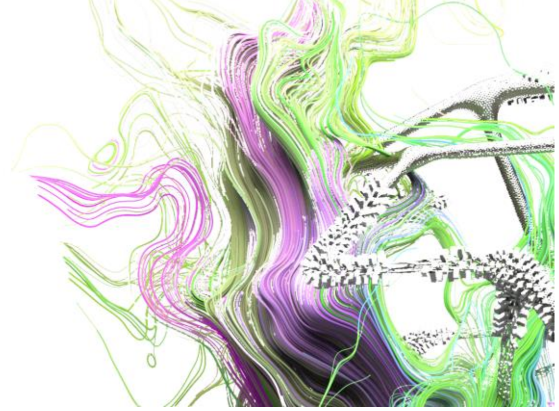
However, the good news is that there are things your school can do to mitigate the threat from ransomware - minimising the financial and reputational fallout and, most importantly, the impact on staff and students.

Building a shield: preventing ransomware from entering your IT system

As with any form of online threat, safeguarding entry points is key. Here is a security checklist for preventing ransomware from infecting the school/college/university network:

- **Back up critical data regularly.** Cybercriminals bank on the fear of losing access to key files and documents, thereby forcing victims to pay the ransom. Although many groups have also started to steal sensitive data before encrypting it, making backups of your important files is still good practice. It means critical data will be kept in a secure location, allowing your organisation to bounce back quickly after an incident.

  Practice the 3-2-1 rule: create 3 backup copies on 2 different media with 1 backup offsite. Some ransomware variants have been known to go after backup data found on a shared network drive,



which makes it important to set a backup on a separate location, which isn't connected to the company network.

Include this in business continuity planning and regularly test such plans to make sure everyone knows what they're doing.

- **Turn on ransomware detection/protection features**.
- **Implement application whitelisting to block all unknown and unwanted applications.** Allow only the apps you need to run, blocking new apps by default (this is known as whitelisting and is managed by your IT support service)
- **Develop a security-oriented network segmentation plan**. Segment your network. This means only allowing data to be stored or accessed by those who are authorised to access it. Keep the most valuable data accessible to only those who need it.

By compartmentalising areas of a network specific to a department or a team's needs, a potential attacker will not be able to move laterally and infect other parts of the network. Using the least-privilege principle in assigning user profiles makes it more difficult for perpetrators to gain administrative rights. Staff and students should be on separate networks where possible or segmented using firewalls/IPS and possibly network anomaly/breach detection monitoring.

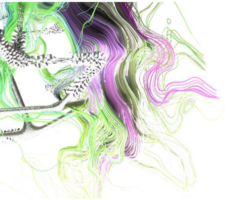
- **Educate users on the dangers and signs of social engineering.** Both staff and students should be taught good email and internet safety practices like downloading attachments, clicking URLs or executing programmes only from trusted sources. It is also important to encourage users to alert the IT security team if they spot anything suspicious, creating an effective first line of defence.
- **Regularly apply software patches from OS and third-party vendors.** Unpatched applications and servers are often exploited as an entryway for pushing malware such as ransomware into a system. To counter this, regularly patch and update software. Carefully scrutinise your patching processes to identify and eliminate roadblocks in the timely rollout of necessary updates. Virtual patching can protect vulnerable servers from ransomware threats, even if the relevant patches have not been rolled out by vendors.
- **Ensure your security products are up-to-date and perform periodic scans.** A cybercriminal only needs to find one crack in your cyber-defences to get in. Make sure that any security solutions you have in place are regularly updated, to close down any avenues of attack.

Stopping the bleeding: containing the damage

Ransomware attacks can happen frighteningly fast. It could take just minutes from an accidental click on a malicious link to the display of the ransom note. However, this gap is crucial in identifying and containing an infection and any subsequent damage. Here are some notes to include in your security checklist:

- **Identify and isolate compromised machines from the network**. While ransomware tactics vary, most attacks involve establishing communication with a command-and-control (C&C) server in order to receive further instructions.

  Once alerted to any unusual behaviour, IT admins should act fast to keep the infection isolated to as few resources as possible. Disconnect the infected machine from the network to prevent any



attempts to propagate to other systems. If the need arises, shut down the network until the incident is controlled.

- **Establish a real-time incident response team.** An incident response team will monitor system activity and any behavioural anomalies. In doing so, it can establish proactive control of the incident and prevent an infection from spreading.
- **Encourage users to report unusual system behaviour.** IT admins should proactively educate staff and students connected to the network to keep an eye on signs that could indicate a compromise.

  A noticeable system slowdown could signal extra (malicious) processes happening in the background, for example, providing a vital early warning to the IT response team.

Preventing the aftershock: recovering from infection
Even if your system gets infected with ransomware, all is not lost. The key is to quickly spot, respond, and remediate to keep damage to a minimum. Most importantly, to avoid being forced to pay the ransom. Here's a checklist of things you can do after an infection:

- **Find decryption tools.** A wealth of free decryption tools that can detect and remove certain ransomware variants are now readily available free-of-charge online.
- **Implement a comprehensive data backup and recovery plan.** Developing a backup and recovery plan is a useful insurance policy against ransomware, assuming data is not also stolen by attackers. With this in place, you will at least be able to resume operations as quickly as possible.
- **Conduct post-incident analysis**. Once the incident has been properly dealt with, investigate and scope the breadth and magnitude of the infection. More importantly, analyse the source of the infection to identify vulnerabilities and system weaknesses that can be addressed to prevent recurrence.

In different cases, a sandbox analysis of the ransomware in question could help determine the malware's behaviour. This could also be used to identify Indicators of Compromise—from its capabilities, routines, and tactics employed—that would improve detection and develop ways to prevent future incidents.

Don't underestimate the harm ransomware can do to your organisation. A multi-layered approach to security is vital to mitigate the risks associated with a serious attack.

Ransomware solutions:
SWGfL, Phoenix & Trend Micro offer different solutions to protect your school and to help minimize the risk of getting infected by ransomware:

You can find all of the products here at Trend Micro™ Security Services

In collaboration with

SWGfL Safe, Secure, Online

PHOENIX