National Cyber
Security Centre
a part of GCHQ

Alert: Targeted ransomware attacks on the UK education sector by cyber criminals

Version: 1.0

17 September 2020

Summary

This alert details recent trends observed in ransomware attacks on the UK education sector. It also provides mitigation advice to help protect this sector from attack.

This alert is designed to be read by those responsible for IT and Data Protection at education establishments within the UK. Where these services are outsourced, you should discuss this alert with your IT providers.

Introduction

Since August 2020, the NCSC has been investigating an increased number of ransomware attacks affecting education establishments in the UK, including schools, colleges and universities.

Due to the prevalence of these attacks, you should be sure to follow NCSC's recently updated mitigating malware and ransomware guidance. This will help you put in place a strategy to defend against ransomware attacks, as well as planning and rehearsing ransomware scenarios, in the event that your defences are breached.

Ransomware

Ransomware is a type of malware that prevents you from accessing your systems or the data held on them. Typically, the data is encrypted, but it may also be deleted or stolen, or the computer itself may be made inaccessible.

Following the initial attack, those responsible will usually send a ransom note demanding payment to recover the data. They will typically use an anonymous email address (for example ProtonMail) to make contact and will request payment in the form of a crypto currency.

More recently, there has been a trend for cyber criminals to also threaten to release sensitive data stolen from the network during the attack, if the ransom is not paid. There are many high-profile cases where the cyber criminals have followed through with their threats by releasing sensitive data to the public, often via "name and shame" websites on the darknet.

Ransomware attacks can have a devastating impact on organisations, with victims requiring a significant amount of recovery time to re-enable critical services. These events can also be high profile in nature, with wide public and media interest.

Common ransomware infection vectors

Ransomware attackers can gain access to a victim's network through a number of infection vectors. Indeed, it can be hard to predict how a compromise will begin, as cyber criminals adjust their attack strategy depending on the vulnerabilities they find. However, in recent incidents, the NCSC has observed the following trends:

- **Remote Desktop Protocol (RDP)** is one of the main protocols used for remote desktop sessions, enabling employees to access their office desktop computers or servers from another device over the internet. Insecure RDP configurations are frequently used by ransomware attackers to gain initial access to victims' devices. Often, the attacker has previous knowledge of user credentials, through phishing attacks, from data breaches, and credential harvesting. User credentials have also been discovered through brute force attacks because of ineffective password policies.

- **Vulnerable Software or Hardware**: Unpatched or unsecure devices have commonly been used by ransomware attackers as an easy route into networks.
- **Phishing emails** are frequently used by actors to deploy ransomware. These emails encourage users to open a malicious file or click on a malicious link that hosts the malware.

Upon initial access to a network, an attacker will attempt to move around the network and to increase their privileges and seek out high-value systems, often using additional tooling to assist with this. They will also attempt to cover their tracks so that any subsequent investigation will be more difficult.

Recently, attackers have also been seen to:

- sabotage backup or auditing devices to make recovery more difficult
- encrypt entire virtual servers
- use scripting environments (i.e. PowerShell) to easily deploy tooling or ransomware

Mitigations

The NCSC recommends that organisations implement a ‘defence in depth’ strategy to defend against malware and ransomware attacks. This section lists a number of important defences practices and techniques

Your organisation should also have an incident response plan, which includes a scenario for a ransomware attack, and this should be exercised.

Further details are can be found in the NCSC’s recently updated guidance on ‘Mitigating Malware and Ransomware’.

Disrupting ransomware attack vectors:

- Effective **vulnerability management** and **patching** procedures (See Vulnerability Management)
- Secure **RDP** services using **Multi Factor Authentication**.
- Install and enable **Antivirus software**
- Implement mechanisms to prevent **Phishing** attacks
- Disable or constrain **scripting environments** and **macros**

Enable effective recovery:

- Having up-to-date and tested **offline backups**. Offline backups are the most effective way to recover from a ransomware attack (See the NCSC's Offline backups in an online world blog)
- **Exercise** your response to ransomware and other cyber attacks. (See the NCSC's Exercise in a Box)

The following supplementary NCSC resources may be useful:

- Top Tips for Staff
- 10 steps to cyber security
- School governor questions
- Cyber Security in Schools: Practical Tips
- Helping school staff to work safely online

Disclaimer

This report draws on information derived from the NCSC based on our observations of this activity as well as partners and victim organisations. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.