National Cyber Security Centre
a part of GCHQ

Further targeted ransomware attacks on the UK education sector by cyber criminals

Alert

Version 2.1
What's new?

Updated with new information on March 2021 activity

19 March 2021

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

Updated information for the education sector

Update March 2021

The NCSC is responding to further targeted ransomware attacks on the education sector by cyber criminals.

Since late February 2021, **an increased number of ransomware attacks have affected education establishments in the UK, including schools, colleges and universities**.

The NCSC previously acknowledged an increase in ransomware attacks on the UK education sector during August and September 2020. The NCSC has therefore updated this Alert in line with the latest activity.

The NCSC urges all organisations to follow our guidance on 'Mitigating malware and ransomware.' This details a number of steps organisations can take to disrupt ransomware attack vectors and enable effective recovery from ransomware attacks.

The NCSC has produced a number of practical resources to help schools and other educational institutions improve their cyber security.

Introduction

The NCSC continues to respond to an increased number of ransomware attacks affecting education establishments in the UK, including schools, colleges, and universities.

This report details recent trends observed in ransomware attacks on the UK education sector. This encompasses trends observed during August and September 2020, as well as the more recent attacks since February 2021. 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.

It is also important that senior leaders understand the nature of the threat and the potential for ransomware to cause considerable damage to their institutions in terms of lost data and access to critical services

Due to the prevalence of these attacks, you should be sure to follow NCSC's 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 towards cyber criminals also threatening 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.

“In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing.”

Impact

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

In recent incidents affecting the education sector, ransomware has led to the loss of student coursework, school financial records, as well as data relating to COVID-19 testing.

It is therefore vital that organisations have up-to-date and tested offline backups.

For further information see the NCSC’s Offline backups in an online world blog as well as the NCSC’s guidance on backing up your data)

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 identify. However, in recent incidents, the NCSC has observed the following trends:

Remote access

Attackers frequently target organisations' networks through remote access systems such as remote desktop protocol (RDP) and virtual private networks (VPN). They regularly exploit:

- weak passwords,
- lack of multi-factor authentication (MFA),
- unpatched vulnerabilities in software.

Remote Desktop Protocol (RDP) remains the most common attack vector used by threat actors to gain access to networks. 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 or credential harvesting. User credentials have also been discovered through brute force attacks because of ineffective password policies. Compromised credentials and remote access are frequently sold by cyber criminals on criminal marketplaces and forums on the dark web.

VPN vulnerabilities: Since 2019, multiple vulnerabilities have been disclosed in a number of VPN appliances (for example Citrix, Fortinet, Pulse Secure and Palo Alto). Ransomware actors exploit these vulnerabilities to gain initial access to targeted networks.

The shift towards remote learning over the past year has meant that many organisations have rapidly deployed new networks, including VPNs and related IT infrastructure. Cyber criminals continue to take advantage of the vulnerabilities in remote access systems.

Phishing

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.

Other vulnerable software or hardware

Unpatched or unsecure devices have commonly been used by ransomware attackers as an easy route into networks. For example, on 11 March 2021 Microsoft reported that cyber criminals have exploited vulnerabilities in Microsoft Exchange Servers to install ransomware on a network.

Lateral movement and privilege escalation

Having acquired initial access to a network, an attacker will typically seek to navigate around the network, increase their privileges and identify high-value systems, often using additional tooling (such as Mimikatz, PsExec, and Cobalt Strike) to assist with this. They may also attempt to conceal their actions so that any subsequent investigation will be more difficult.

Recently we have also observed attackers seeking to:

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

Mitigation

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 defence 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 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 NCSC has produced a number of practical resources to help schools and other educational institutions improve their cyber security:

- Cyber Security for Schools
- Top Tips for Staff
- 10 steps to cyber security