SWGFL WHITE PAPER

Ransomware

Date:	October 2018
Version:	2

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

Contents

Introduction

There are various different types of malicious software (or "malware"), but all have one common purpose: to deliberately cause harm to your device, your network or your data.

The list includes viruses, worms and Trojans, with 'ransomware' one of the most prevalent types. Starting from around 2012, the number and complexity of ransomware attacks has grown internationally. IBM and Verizon (in their 2018 Data Breach Investigations Report) advise that ransom attacks were the dominant malware form in 2017, and that ransomware is increasing to become the primary attack vector of malware generally. The statistics also show that ransom attacks are beginning to target servers (rather than individual users).

This document provides an overview of the guidance from SWGfL.

For more information, please visit the information security pages on our website: www.swgfl.org.uk/security.

Ransomware Explained

Ransomware is a form of malware that interferes with data on your device, or your device itself. It enables criminals to encrypt or lock your data or your device from a remote location, and then informs you that they will not be unlocked unless you pay money (the "ransom") for their release.

Ransoms are often demanded in the form of cryptocurrency (e.g. Bitcoin) to protect the identity of the criminal.

Like other malware, ransomware targets any user, whether at home, work or school. There is also no guarantee that paying the ransom (or doing whatever else the ransomware tells you to do) will provide you with access to your device or files.

Types of Ransomware

There are different types of ransomware which behave in slightly different ways, including:

- Encrypting ransomware: the most common form of ransomware, encrypting ransomware (or "crypto ransomware) prevents access to files or data, usually by encrypting them;
- Non-encrypting ransomware: also called 'screen lock' (or 'locker') ransomware, non-encrypting ransomware prevents you from using your device, often by disabling the majority of features and enabling the user only to interact with the ransomware;
- Leakware: also called 'Doxware', leakware attacks threaten to publish information stolen from your device; and
- Mobile ransomware: specific ransomware strains have emerged that target mobile devices (since encrypted data could often be easily restored by the user through re-synchronisation of the mobile device), usually employing 'locker'-type approaches or attempting to gain access to connected 'cloud' accounts.

And whilst Microsoft Windows systems have been the main target, attackers are beginning to focus on other platforms too, including Mac and Linux, as well as Android and iOS mobile devices.

Examples of Ransomware

Well known examples include:

- CryptoLocker: emerged in 2013 and is estimated to have extorted at least $3 million from victims;
- CryptoLocker.F and TorrentLocker: a year later, in September 2014, is estimated to have infected over 20,000 devices;
- CryptoWall: emerged in 2014 and estimated losses exceed $18 million;
- Fusob: one of the main mobile ransomware families, which along with 'Small', accounted for over 90% of mobile ransomware in 2015 and 2016;
- Petya: a form of encrypting ransomware from 2016 which aimed to encrypt at the file system level, preventing systems from booting in to Windows;
- WannaCry: emerged in May 2017 on an unprecedented scale, infecting over 230,000 devices in over 150 countries; and
- SamSam: a new strain of ransomware, targeting vulnerabilities in Remote Desktop Protocol and has been behind various attacks on government and healthcare targets.

The Point of Ransomware

The distribution of ransomware is a criminal activity that generally involves someone trying to steal money or create mass disruption.

Payment is usually the intention, and the victim is encouraged to pay for the ransomware to be removed (which may or may not actually happen after payment is made), either by providing another program that can decrypt the encrypted files, or by sending an unlock sequence to the infected device to undo the payload.

The payment method is a key aspect in this process, which needs to be convenient and hard to trace. Criminals have used a range of methods, including premium-rate numbers, wire transfers, pre-paid vouchers and cryptocurrency (e.g. Bitcoin) to demand payments and protect their identities.

How Ransomware Infects your Device

The main sources of malware are:

- The Internet: visits to sites containing malicious software, downloading malicious software disguised as something useful and genuine, and downloading files through peer-to-peer networks;
- Email: malware can easily be trafficked through email, often as attachments. Opening or saving attachments can allow the payload to deploy. Email is also the primary attack method for spam and phishing;
- Software vulnerabilities: weaknesses in software (including operating systems, productivity tools, browsers, plug-ins are more) are a common target for criminal attackers;

- Removable storage: removable storage drives (including flash memory (e.g. USB) devices, memory cards and other removable drives) are at increased risk of infection as they can move easily from systems with high levels of protection to systems with low (or no) protection, become infected, and then carry the infection back inside other systems; and

- User action (or inaction): use of weak passwords, sharing of access credentials, clicking on attachments or opening files, and falling victim to 'social engineering' by attackers are all user-based vulnerabilities in systems that can be easy to exploit.

Ransomware can infect your device through the same sources that any other malware can come from, but is mainly spread through email.

Typically a Trojan will enter a system through a malicious attachment or embedded link in a Phishing email. The ransomware then deploys a 'payload', which proceeds to lock the system in whichever way it works.

Some payloads are based on code designed to lock or restrict the system until payment is made, while more advanced payloads encrypt files.

Zero-day Vulnerabilities

When criminals uncover vulnerabilities, and then immediately produce and deploy malware to target those vulnerabilities, they are staging what is known as a 'zero-day' attack.

This challenges traditional anti-virus software as they generally rely on the threat first being known and then an update being sent to the anti-virus software. This is where specific anti-ransomware software becomes invaluable, as these technologies protect against zero-day vulnerabilities.

How to Reduce your Risk

In context, protecting yourself against ransomware is part of protecting yourself against malware, which in turn is part of the wider process of ensuring an appropriate level of information security.

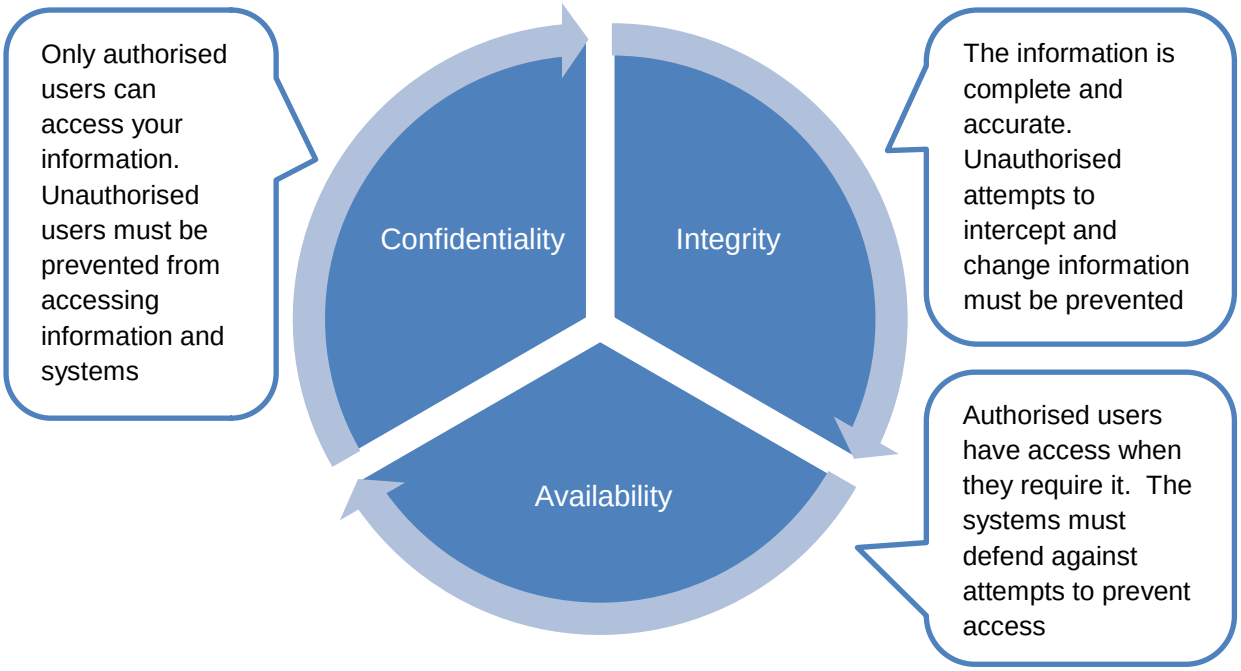
Information Security

Information security, or cyber security, is the process of ensuring that only authorised users have access to accurate and complete information, when access is required.

Information security, or "InfoSec", is an ongoing process (in the sense that continually evolving threats require continually evolving security measures) and a risk management process (in the sense that there is no perfect security, or complete security, so the organisation should assess its risk and act accordingly):

Risk (from the threat)	=	Impact (of the threat)	x	Vulnerability (to the threat)
the risk that a threat poses (i.e. the severity of it)		*the impact of the threat occurring (e.g. a ransomware attack encrypting important school data)*		*the extent to which measures are in place to protect the organisation (e.g. the anti-malware software in place)*

There are three core elements to InfoSec, referred to as the 'CIA Triad':



A thorough approach to information security requires each of these elements to be addressed.

Implementing and maintaining an appropriate level of information security is a non-trivial undertaking. Whilst certain measures need to be managed internally (e.g. governance and policy), schools may require support and assistance in doing so. Other measures may be best implemented by external organisations (e.g. firewall management and configuration, or penetration testing), but often the existing supply chain lacks the specialist knowledge to provide genuine assistance.

SWGfL can support schools in developing and maintaining information security and data protection. If you have queries or require support, please contact us at infosec@swgfl.org.uk.

Defence in Depth

Defence in depth is a concept within information security in which multiple security layers are implemented throughout the ICT systems. A good approach will combine security controls from three areas:

1. Physical security: anything that prevents unauthorised physical access to systems or data (e.g. perimeter fences, locked doors, CCTV).

2. Technical security: the hardware and software used to protect your systems and data (e.g. firewalls, disk encryption, Windows account permissions).

3. Administrative security: the policies, procedures and guidance set out to help ensure the right level of information security (e.g. recruitment practices, data protection policy and user account management processes).

It should also be recognised that no individual security device, software or approach is 100% effective, 100% of the time, so it's important to take a 'defence in depth' approach as part of information security risk management.

12 Steps to Protect against Ransomware

For ransomware specifically, the following provisions will help to improve your level of protection (and/or recoverability, should you suffer an attack):

1. Backup:

Backup your data regularly (ideally daily); keep a recent copy off-site and off-line (i.e. not connected 'live' to the network); and test your backups (which lots of people forget to do, until it's too late).

If you can restore your data easily and quickly, the impact of a ransomware attack will be lessened. Some types of ransomware can encrypt files on external storage that is connected to your device, so as part of a backup strategy ensure that certain backups are disconnected once the backup is complete.

Data replication is different to data backup. Whilst replication can be useful for retrieving files under normal circumstances, it's possible that ransomware would infect the replicated data location too. A true backup is a copy of the data at a point in time, which (on the assumption it is working correctly) can be restored to the source at a later time.

2. Update and up to date:

Vendors like Microsoft release patches frequently, so make sure they are downloaded and installed without delay. Also, make sure you are only running versions of software that are supported by the vendors.

Ransomware typically exploits vulnerabilities in popular software, applications and plug-ins (e.g. Microsoft Windows, Microsoft Office, browsers, Flash Player etc.) so it's important to keep yours up to date with the latest version.

In some cases it's also important that you uninstall older versions when you install the new ones, so that the vulnerabilities are closed (e.g. Java).

It is also advisable to consider the configuration of software. Some malware is deployed via features in operating systems and applications that many users do not require, so disabling or removing them (or not installing them in the first place) can improve security.

3. Update security products too:

Having security is essential, but so too is keeping it up to date and well configured. Software (e.g. anti-virus) needs to be updated with the latest info, and things like firewalls need to be configured and managed by specialists to be fully effective.

It's also advisable to consider specific anti-exploit software to provide additional protection against 'zero-day vulnerabilities', including ransomware.

It is also advisable to check the extent to which your security software is deployed (i.e. the number of devices) and whether any issues have been detected (i.e. malware detected) regularly. Certain anti-malware solutions provide a 'console' allowing these checks to take place easily.

4. Be cautious:

Email is still one of the major attack methods, so don't click on links that you are not certain are genuine and trustworthy; and do not open unsolicited email attachments or attachments to emails that don't look right (e.g. emails purporting to be official but that are incorrectly formatted, contain poor spelling or grammar).

Microsoft Office viewers allow the viewing of attachments without opening them (https://support.microsoft.com/en-us/help/979860/supported-versions-of-the-office-viewers).

Check whether your email platform is using good spam filtering, and that the settings are correct. This can prevent phishing emails and malicious attachments from reaching users.

5. Manage accounts carefully:

Do not set up accounts to give more 'power' than is necessary, as these accounts allow malicious code to run more easily. A security software company, Avecto, found a couple of years ago that a huge percentage of vulnerabilities are based on use of 'local admin' rights.

It's common for malware to need elevated permissions to do real damage to a device, and gets this through 'administrator' level accounts.

Don't give yourself more permission than you need. Don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you are logged in with administrator rights.

6. Look after passwords:

The basics: don't ever reveal your full password; don't write it down (unless you're storing it securely); and use sufficiently long and complex passwords to avoid easy routes in.

A lot of malware still spreads as a result of user action (or inaction). A common cause is the use of poor passwords (e.g. very short passwords or the use of the same password by the same user across numerous different services).

7. Check out those files:

Enable visible file extensions so you can see what a file actually is from the extension (e.g. ".exe"). If you're using mobile tech, particularly Android, it's also worth making sure devices only use Google Play Store (as alternative sources may lack any attempts to screen apps for malware).

8. Prevent code from running:

Disable macros in document attachments received by email; and open potentially risky files like JavaScript (.JS) files in a simple text editor (like Microsoft Notepad). Also, make sure 'on-access scanning' or 'real-time protection' is enabled in your anti-virus software.

9. Don't do as you're told:

If an email or document tells you to turn off security features (e.g. enable macros), don't (and definitely don't without checking out the validity first). Most items can be viewed with the security features in place.

10. Network security and segmentation:

Consider network design and network access carefully.

Where wireless local area networks (WLANs) are used to transmit sensitive or personal data, appropriate security protocols should be in place. Wi-Fi Protected Access II (WPA2) is recommended.

Where it is necessary to support remote working, consider the security implications. Remote Desktop Protocol (RDP) can be easy to set up, but can also (if not sufficiently hardened) open up the network to a range of attacks.

Separate different nodes on the local network (e.g. servers and workstations), and generally wired and wireless traffic too. This will help to limit further movement across the network if unauthorised access is gained.

11. Train:

Raise awareness amongst staff and users of the importance of information security.

Keep staff and users up to date with security training, and what your organisation is doing. Even advising users on what to look out for in a phishing email can prevent a problem from occurring.

A lot of malware requires an action from a user in order to deploy (e.g. clicking to open an email attachment).

12. Plan:

Plan and document measures to take if anything goes wrong; when something does happen, organisations that have clear plans are able to recover more quickly and effectively, and as a consequence, usually with less pain (i.e. reduced data loss and cost).

This could include:

a) Developing a clear and workable business continuity and data recovery (BCDR) plan will help everyone understands what needs to be done in the event of an issue.
b) Building a clear data protection policy will help to make sure that the right data is kept safe.
c) Establishing a breach management process with a clear protocol for informing the ICO if any personal data has been compromised.
d) Setting out a clear communications plan to keep all users and stakeholders informed.
e) Considering whether any of the cyber-risks can be covered by insurance.

This is not a complete list of information security tasks, but a guide to certain fundamental steps that can be taken (or checked) to help ensure a base level of control is in place.

For more information, please visit the information security pages on our website: www.swgfl.org.uk/security.

What to Do if Infected with Ransomware

If ransomware has infected your device(s) or system(s), the following guidance applies. We strongly recommend the undertaking of these steps before paying any ransom demanded by the ransomware.

There is no guarantee or assurance that payment of the ransom will result in restoration of your data or device(s). Additionally, payment of the ransom reinforces the actions of the criminals and will serve to support the continued production of ransomware for commercial gain. It should be noted that, in some cases, victims that have paid have been targeted again, or have been required to pay more than the original payment in order to restore their data or systems.

1.	Implement your plans:	If you've developed plans, this is the point to implement them. A BCDR plan should set out how data is backed up, which data, and how to restore it. Am information security plan should set out the steps to take when a security incident occurs.
2.	Isolate the infected device(s):	Any infected systems should be physically disconnected from the network immediately to prevent infections from spreading further.
3.	Isolate any affected devices:	Any systems that may be affected, but have not yet been completely infected, should be physically disconnected from the network and powered off. This may prevent the infection from worsening.
4.	Secure backups:	Any on-site online backups should be taken offline immediately, by physically disconnecting the device from the network if necessary. If possible, perform checks on the backup data to ensure they are free of malware.
5.	Contact law enforcement:	Contact local Police and Action Fraud (0300 123 2040) without delay to report the crime.
6.	Change account passwords:	If possible, change passwords for all network accounts without delay. It will be necessary to change passwords again when the malware has been removed, but changing them at this stage may limit the spread of the malware.
7.	Contact specialist support:	If you have a specialist security support provider, contact them without delay. If you have an IT support provider, and particularly if they have knowledge of security incidents, or have advised or undertaken work on your backup procedures or anti-virus software, contact them without delay.
8.	Escalation:	To the extent that the internal management team is not aware of the incident, escalate the incident to them without delay and advise of the steps taken so far.
9.	Analysis:	Commence analysis of the incident, supported by specialist security support provider/IT support provider. Identify the initial cause of the infection. Consider the impact on the organisation and on the affected users. Prepare resolution plan.
10.	Communication plan:	Commence internal and external communications in alignment with the plans, management instructions and proportionate to the severity of the incident.

For more information, please visit the information security pages on our website: www.swgfl.org.uk/security, or if you need assistance, contact us at infosec@swgfl.org.uk.