Protect Your Business Against Ransomware

Ransomware is a very present risk for all organisations, and indications suggest that it is not going away any time soon.

It is therefore essential to take immediate steps to secure your organisation against this type of attack.

By following both the short and longer term recommendations outlined in this document, businesses can take significant steps to protect themselves against ransomware infections.

Introduction

This document explains how to react quickly and effectively to the threats posed by ransomware such as Cryptowall, TeslaCrypt, AlphaCrypt and Locky.

It first details the mechanisms that these infections use to find their way into companies and why a large number of new infections continue to surface despite existing protective measures.

It then provides practical recommendations to protect against them, showing how these threats can be tackled using short-term and long-term technical and organisational measures.

Ransomware has become one of the most widespread and damaging threats that internet users face. Since the infamous CryptoLocker first appeared in 2013, we've seen a new era of file-encrypting ransomware variants delivered through spam messages and Exploit Kits, extorting money from home users and businesses alike.

Where does the current wave of ransomware infection come from?

Even though most companies have extensive security mechanisms in place, such as virus scanners, firewalls, IPS systems, anti-SPAM/anti-virus-email-gateways and web filters, we are currently witnessing large numbers of infections worldwide with ransomware infections, such as Cryptowall, TeslaCrypt and Locky. Files on computers and network drives are encrypted as part of these infections in order to blackmail the users of these computers to pay a sum of money, usually in the region of USD 200-500, for the decryption tool.

A common infection scenario may look like this:

A user receives an email that comes from a seemingly plausible sender with an attached document, a parcel service with attached delivery information or an external company with an attached invoice.

The email attachment contains an MS Word or Excel document with an embedded macro. If the recipient opens the document a macro will attempt to start automatically, executing the following actions: It tries to download the actual ransomware payload from a series of web addresses that only exist momentarily. If a web address cannot be reached, the next one is accessed until the payload has been downloaded successfully.

The macro executes the ransomware.

The ransomware contacts the command & control server of the attacker, sends information about the infected computer and downloads an individual public key for this computer.

Files of certain types (Office documents, database files, PDFs, CAD documents, HTML, XML etc.) are then encrypted on the local computer and on all accessible network drives with this public key.

Automatic backups of the Windows operating system (shadow copies) are often deleted to prevent this type of data recovery.

A message then appears on the user's desktop, explaining how a ransom (often in the form of bitcoins) can be paid within a time frame of e.g. 72 hours to ensure delivery of a suitable decryption tool with the private key that is only available in the attacker's system.

The ransomware will then delete itself leaving just the encrypted files and ransom notes behind.

This is just an example of how such an infection scenario may play out. While email is a popular technique to spread these threats, by no means is it the only approach. Exploit kits are also common and, for example, the Angler exploit kit has been widely used to spread CryptoWall.

The rise of malicious JavaScript attachments

As awareness of the dangers of booby trapped documents grows, hackers are increasingly turning to JavaScript attachments to spread ransomware. This approach is proving effective because:

Windows hides file extensions by default, so README.TXT.JS shows up as README. TXT, making it look mostly harmless.

Windows uses an icon for script files that looks like a scroll of paper (because scripts are stored as text files), adding to the sense of harmlessness.

Browser JavaScript has become much safer in recent years, thanks to a proactive attitude to security by browser makers, and to the "sandbox" in which web pages load and execute. As a result JavaScript is often considered safe.

Almost all email clients have blocked JavaScript inside messages for many years.

As a result, it feels as though there should be nothing to lose in opening script files. The problem is that when you launch a JavaScript file that's been saved to disk, it's no longer "sandboxed" by your email program or your browser. It can do anything that a regular application (.EXE file) can do - including downloading and running other applications, such as ransomware.

Why are ransomware attacks so successful?

The main reasons why these infections are successful are:

1. Sophisticated attack technology

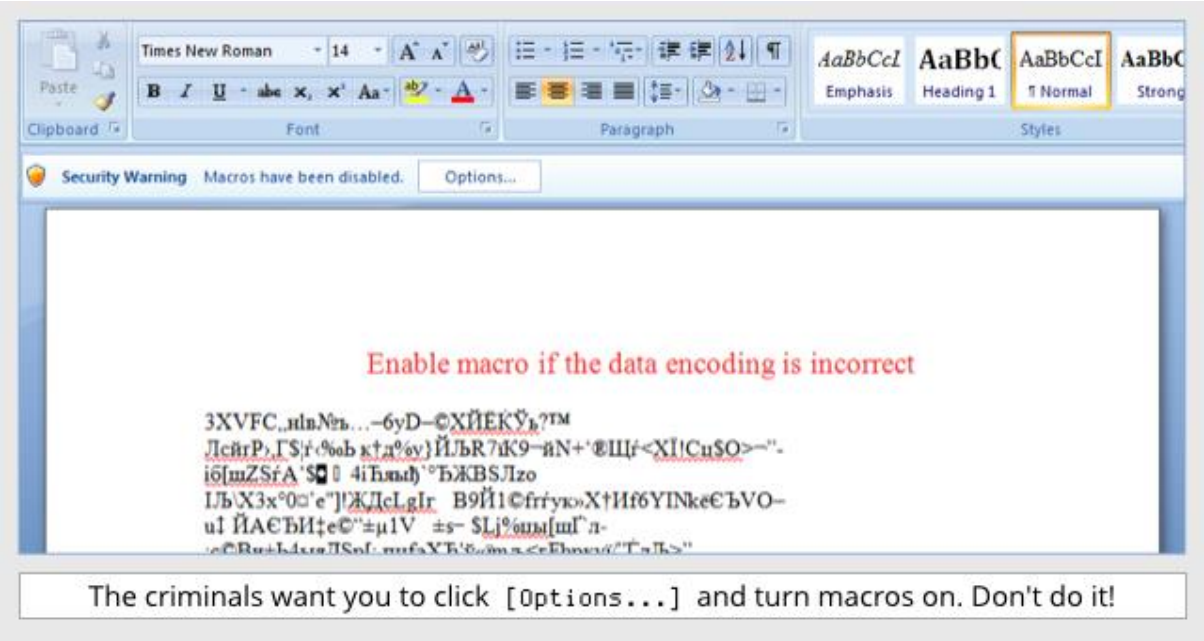
Producers of ransomware operate in a highly professional manner. This includes, among other things, usually providing an actual decryption tool after the ransom has been paid.

Skilful social engineering is employed to prompt the user to execute the installation routine of the ransomware. For example, you may get an email that reads something like this: "If the encoding of the attached Word document seems incorrect, please activate macros. This is done as follows..."

The most common way that Locky arrives is:

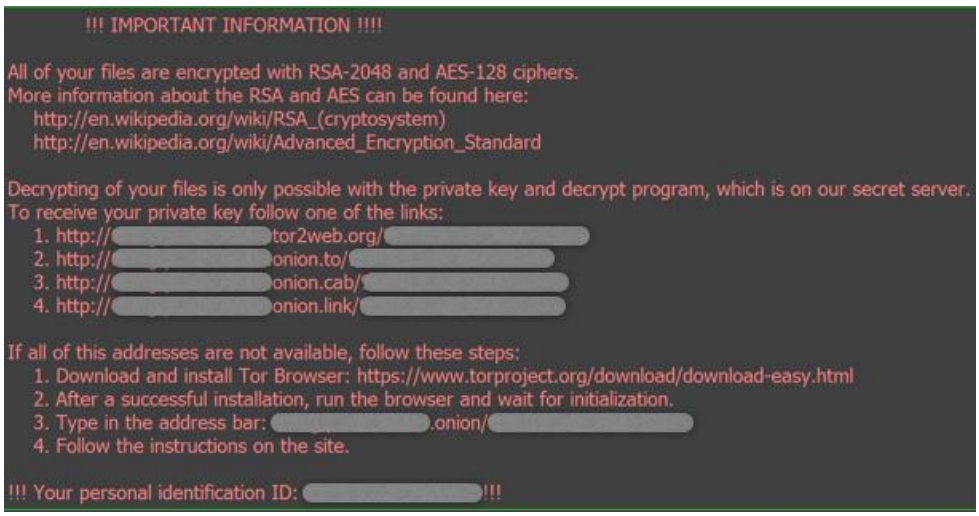
- You receive an email containing an attached document.
- The document looks like senseless gobbledegook.

- The document advises you to enable macros “if the data encoding is incorrect.”
- The hackers want you to click on the 'Options' button at the top of the page. DON’T DO IT!



They use technologies to spread infections that are permitted in many companies and in which malicious code can easily be disguised (Microsoft Office macros, JavaScript, VBScript, CHM, Flash, Java).

Once you click Options, Locky will start to execute on your computer. As soon as it is ready to ask you for the ransom, it changes your desktop wallpaper:



2. Security weaknesses in affected companies

Quite often, affected businesses may have some or all of the following flaws in their organisation:

a) Inadequate backup strategy (no real-time backups, backups not offline/off-site)
b) Updates/patches for operating system and applications are not implemented swiftly enough
c) Dangerous user/rights permissions (users work as administrators and/or have more file rights on network drives than necessary for their tasks)
d) Lack of user security training ("Which documents may I open and from whom?", "What is the procedure if a document looks malicious", "How do I recognise a phishing email?")
e) Security systems (virus scanners, firewalls, IPS, email/web gateways) are not implemented or are not configured correctly. Inadequate network segmentation can also be included here (servers and work stations in the same network)
f) Lack of knowledge on the part of administrators in the area of IT security (.exe files may be blocked in emails but not Office macros or other active content)
g) Conflicting priorities (e.g. "We know that this method is not secure but our staff need to get their work done...")

Setting priorities

The argument that "security only disrupts the users ... they have to get on with their work" often prevents many useful safety-related measures from being implemented. In many cases, this argument does not apply if the safety-related measures are planned with due care and adjusted to the situation of the employees and the company.

In some cases, for example when an email is received or when Office documents with macros are used internally, businesses need to be aware of what is more important for the company:

Example 1:

Every user can receive Office documents from the Internet and can also execute them with macros on corporate computers.

Example 2:

Only the users of the specialist departments who have to work with Office macros (order processing, accounting, sales) have authorisation to execute Office macros in line with the company's central policy.

If an individual sends an email with an Office document to recipients in the company, then this email is placed in quarantine. The recipient is informed of this and is asked to confirm with the sender of the email that he or she actually sent it. After doing this, the employee can then remove this email from quarantine automatically. Alternatively, he or she can ask the individual to pack all future documents into a password-protected ZIP archive whose password they both create during this conversation. Such password-protected ZIP archives are never placed in email quarantine; future emails will always arrive immediately and the transfer via email will now also be encrypted.

Example 1 is definitely the simplest from an administration perspective. In Example 2 you first have to find out which specialist departments have to receive Office documents from external individuals; you have to define the appropriate group guidelines and train the employees of the specialist departments. Nevertheless, implementing Example 2 is of course the more logical step if you want to improve security significantly by using technical measures and by minimising changes to employees' working behaviour.

In keeping with this example, the following recommended measures should always be taken into account, considering what the consequences of non-implementation would be and how these measures could be implemented so that they affect the user only as much as is necessary.

Best practices to apply immediately

Backup regularly and keep a recent backup copy off-site. There are dozens of ways other than ransomware that files can suddenly vanish, such as fire, flood, theft, a dropped laptop or even an accidental delete. Encrypt your backup and you won't have to worry about the backup device falling into the wrong hands.

Don't enable macros in document attachments received via email. Microsoft deliberately turned off auto-execution of macros by default many years ago as a security measure. A lot of malware infections rely on persuading you to turn macros back on, so don't do it!

Be cautious about unsolicited attachments. Hackers are relying on the dilemma that you shouldn't open a document until you are sure it's one you want, but you can't tell if it's one you want until you open it. If in doubt, leave it out.

Don't give yourself more login power than you need. Most importantly, 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 have administrator rights.

Consider installing the Microsoft Office viewers. These viewer applications let you see what documents look like without opening them in Word or Excel itself. In particular, the viewer software doesn't support macros at all, so you can't enable macros by mistake!

Patch early, patch often. Malware that doesn't come in via document macros often relies on security bugs in popular applications, including Office, your browser, Flash and more. The sooner you patch, the fewer open holes remain for hackers to exploit. In 2015 it emerged that a recently patched Adobe Flash flaw (CVE-2015-3113) was being exploited to drop CryptoWall on machines. Always keep up to date with software and OS security updates.

Keep informed about new security features added to your business applications. For example, Office 2016 now includes a control called "Block macros from running in Office files from the internet" which helps protect you from external malicious content without stopping you using macros internally.

Open .JS files with Notepad by default. This helps protect against JavaScript borne malware by enabling you to identify the file type and spot suspicious files.

Show files with their extensions. Malware authors increasingly try to disguise the actual file extension to trick you into opening them. Avoid this by displaying files with their extensions at all times.

Keep anti-malware up-to-date – new ransomware is being developed all the time so it pays to be able to stop the latest threats.

Additional measures to secure against ransomware

Install the right products

A layered approach using several different cyber security solutions to work together can reduce the likelihood of an attack on your networked system. A good firewall in particular is the first layer and acts as a 'border' between the outside world and your internal network. Unified Threat Management (UTM) from WatchGuard is the industry's highest-performing, all-in-one network security platform. This is a full-featured, take-no-prisoners, super-fast security appliance that scales with your business, and is easy to distribute across every network you manage. APT Blocker and Malwarebytes Endpoint Security will further protect your business.

Employee awareness/training

In addition to the immediate measures described above , it's important that employees receive regular IT security training.

Segmentation of the company network

Security measures at the gateway are rendered useless if a computer that is introduced to the network without authorisation (private notebook, computer belonging to the service provider, company notebook with outdated virus protection) is allowed to infiltrate these measures. Network Access Control (NAC) solutions for example, can help against the threat of an unauthorised device in the network by only allowing known computers access to the network.

Therefore, in general, the principle that each system only has access to those resources that are necessary to fulfil the relevant tasks should also apply to the network design.

In the network area, this also means that you separate functional areas with a firewall, e.g. the client and server networks. The relevant target systems and services can only be accessed if this is really necessary. The backup servers can then only be accessed from the work stations, for example, via the port required by the backup solution, not via Windows file system access.

As a result, you must also consider applying a client firewall to work stations or servers because there is usually no reason for work stations or servers to have communication with each other, unless it relates to known services. This method can also help to prevent waves of infection within a network.

Encrypting company data

Suitable encryption of company documents can help to prevent malware from obtaining unencrypted access to confidential documents. This prevents damage caused by the outflow of business-relevant documents.

Think of security as a layered system

In many companies, security components (e.g. firewall, VPN, IPS, endpoint security, encryption, web security, email security, mobile management, WLAN management) run alongside each other in parallel without these components communicating with each other, correlating results or being able to trigger automatic countermeasures when potential security incidents arise.

However, if these security components were able to communicate with each other and trigger automatic actions to safeguard the entire system in the event of potential security incidents - that is, act as a system - then the overall security of the infrastructure would be increased significantly.

A synchronised security approach enables you to share intelligence in real time between your endpoints and firewall. By automating threat discovery, investigation, and response, synchronised security gives you unparalleled protection against advanced threats.

Use security-analysis tools

Even if you implement all of the above measures, you can never guarantee with 100% certainty that security incidents/infections in company computers will be prevented in the future.

However, if an incident does occur, it is vital that the source of the infection and any potential effects on other company systems are identified as quickly as possible and contained. This can help to reduce the time and effort required to identify and correct the affected systems and restore functionality to the IT infrastructure drastically. In addition, by identifying the source and the method of infection, potential vulnerabilities in the security concept can be highlighted and eliminated.

IT Security Best Practices

Many of the measures proposed in this document are “Best Practices” in IT security and should in fact be long established in the company, just like some other measures that have not been mentioned here, e.g. strong passwords. We recommend regular security check-ups/ health checks to identify potential security deficits and to be up to date when it comes to technical and organisational options for protecting your IT infrastructure.

If you would like any further advice or information regarding the security of your IT infrastructure, please contact 3C Technology Ltd:

Head Office Tel (Essex): 01206 790060
Hertfordshire: 01442 863388

Email: info@3ctech.co.uk

Web: www.3ctech.co.uk