SOPHOS
Security made simple.

How to stay protected against ransomware

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

It also includes optimal configuration settings for Sophos solutions to protect against ransomware.

Introduction

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.

The current wave of ransomware families can have their roots traced back to the early days of FakeAV, through "Locker" variants and finally to the file-encrypting variants that are prevalent today. Each distinct category of malware has shared a common goal – to extort money from victims through social engineering and outright intimidation. The demands for money have grown more forceful with each iteration.

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.

Why are ransomware attacks so successful?

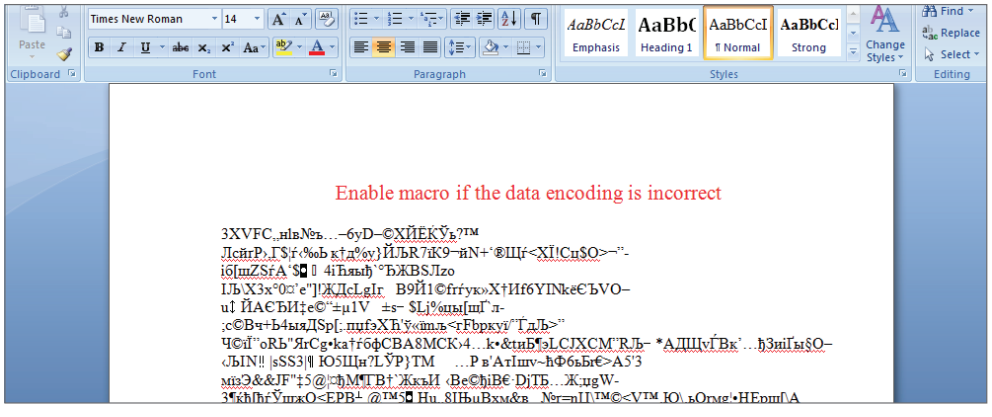
The main reasons why these infections are successful are:

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.
- Skillful 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..."

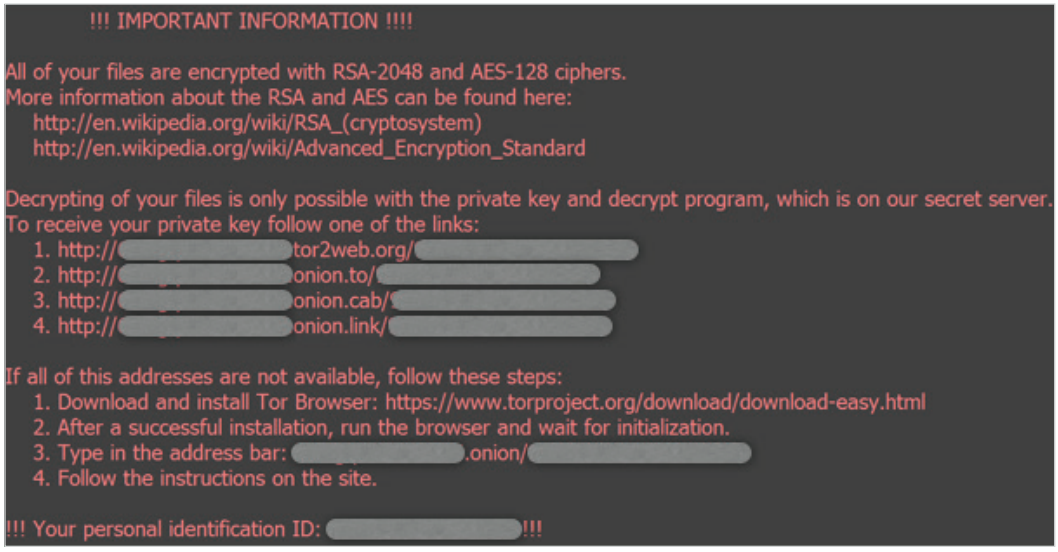
The most common way that Locky arrives is:

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



- 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

- Inadequate backup strategy (no real-time backups, backups not offline/off-site)
- Updates/patches for operating system and applications are not implemented swiftly enough
- Dangerous user/rights permissions (users work as administrators and/or have more file rights on network drives than necessary for their tasks)
- 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 recognize a phishing email?")
- 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)
- 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)
- Conflicting priorities ("We know that this method is not secure but our people have to work...")

Setting priorities

The last point pertaining to priorities must be challenged in particular. 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, one has 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 authorization to execute Office macros in line with the company's central policy.

If business partners send 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 business partner 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 business partners in the Internet; 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 minimizing changes to employees' working behavior.

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.** The crooks 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 the crooks to exploit.

Configuration settings for Sophos solutions

Sophos technologies protect and block malicious files and web traffic used by ransomware. To enable your protection to work effectively, it's important to configure your solutions correctly.

Sophos Endpoint Protection

If you manage **Sophos Endpoint Security and Control** via Sophos Enterprise Console, ensure that the following settings have been made in the AV policy of all work stations and file servers/ terminal servers:

- On-access-scan: on
  - Check files on Read, Rename, Write: on
  - Scan system memory: on
- Download scans: on
- Block access to malicious websites: on
- Sophos Live Protection: on
- Behavior monitoring: on
  - Detect malicious behavior: on
  - Detect malicious traffic: on
  - Detect buffer overflows: on

If you use **Sophos Cloud Endpoint Protection,** then the following settings must be made for all users:

- Real-time scanning: on

If you use **Sophos Cloud Server Protection**, configure your server as follows:

- Real-time scanning – local files...: all switches on
- Real-time scanning – Internet: all switches on
- Real-time scanning - Options:
  - Detect malicious behavior: on
  - Live protection: on
- Activate the “Server Lockdown” functionality

Configure email gateway correctly

A virus scan and a SPAM scan of all inbound and outbound emails must first be set up on the email gateway, configured in accordance with the manufacturer's Best Practices.

If your email gateway provides sandboxing technology to analyze attachments, then activate this function. The **Sophos Email Appliance** provides this function from Version 4.0; **Sophos UTM** provides it from Version 9.4.

Also configure your email gateway in such a way that no executable attachments are allowed through from incoming emails from the Internet, including Office documents, VBS, JavaScript, Java, ActiveX, CHM.

Sophos recommends in particular that you quarantine files types with the following extensions (.ade, .adp, .bas, .bat, .chm, .cla, .class, .cmd, .com, .cpl, .exe, .hlp, .hta, .inf, .ins, .js, .jse, .lnk, .msc, .msi, .mst, .ocx, .pcd, .pif, .reg, .scr, .sct, .shb, .shs, .url, .vb, .vbs, .vbe, .wsf, .wsh, and .wsc). It is also important to scan unencrypted archives for these files and place them in quarantine if necessary.

There is a predefined rule for this with the **Sophos Email Appliance** - “Threat Protection -> SophosLabs Suspect Attachments to all”.

Emails with these types of attachments should be placed in quarantine and the recipient should be notified that a corresponding email is in quarantine (e.g. by replacing the original attachment with a message explaining that the attachment is in quarantine and how you should now proceed).

If you use the Sophos Email Appliance enable the 'Delay queue' in "Policy -> SMTP Options -> Delay Queue". When turned on, the appliance will delay suspected spam that was not caught on the first round of scanning between 10 - 60 mins, and rescan it afterwards. This will help prevent spam campaigns from being delivered on initial arrival.

Depending on the email solution, the organization and the training that the employees have received, the emails can be released from quarantine either by the email administrators or by the original recipients of the email - after the recipient in question has verified (e.g. after calling the sender of the email) that it is a valid email.

Configure web gateway

Configure your web gateway in such a way as to scan all downloads for viruses and block known web addresses and mechanisms for communication with command & control servers. Activate the scanning of SSL connections in each case. If your web gateway provides **sandboxing** technology to analyze downloads, then activate this function.

Configure the **Sophos UTM** as follows:

- ATP: Network Protection -> Advanced Threat Protection: on
- Web Filter Profile -> Filter Action -> Anti-Virus -> Anti-Virus Scan: Dual Scan
- Web Filter Profile -> Filter Action -> Anti-Virus -> Sandstorm: on (from UTM 9.4)
- Web Filter -> HTTPS -> Decrypt and Scan
- Block web filter categories:
  - Anonymizers
  - Browser exploits
  - Dangerous downloads
  - Malicious sites
  - Phishing
  - SPAM URLs
  - Program data is anonymized (also anonymizing utilities)

Configure the **Sophos XG/SF-OS Firewall** as follows:

- ATP: On the dashboard -> go to the right column and click “Advanced Threat Protection” -> Configure -> “Advanced Threat Protection: on”
- Web Content Filter -> Scanning: Dual Anti-Virus
- In each relevant policy rule -> Malware Scan -> Decrypt & Scan HTTPS: on
- In each relevant policy rule -> Web filter policy with blocked categories:
  - Anonymizers
  - Command & Control
  - Phishing & Fraud
  - SPAM URLs

Configure the **Sophos Web Appliance** as follows:

- Global Policy -> HTTPS Scanning: on
- Global Policy -> Sandstorm: on
- Block web filter categories: Proxies & translators
  All other malicious URLs (phishing, spyware, SPAM, high risk sites) are blocked by default and the virus scan is activated.

Configure firewall/intrusion prevention system

A dedicated IPS or an IPS integrated into a firewall/UTM should be configured in such a way that the command & control communication is blocked.

In the **Sophos UTM** you use the IPS policy to block communication:

- Network Protection -> Intrusion Prevention -> Attack Pattern
  - Malware

In the **Sophos XG/SF-OS Firewall** you use the IPS policy to block communication:

- Policies -> Intrusion Prevention Category
  - Malware Communication

Additional measures to secure against ransomware

Employee awareness/training

In addition to the immediate measures described above , it's important that all employees receive regular IT security training. The success of these measures should also be checked regularly.

Sophos provides a number of free tools to help educate employees on security threats, including **IT Security DOs and DON'Ts** and the **Threatsaurus**. See the further reading section at the end of this paper for links to these resources.

Segmentation of the company network

Security measures at the gateway are rendered useless if a computer that is introduced to the network without authorization (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 unauthorized 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 fulfill 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

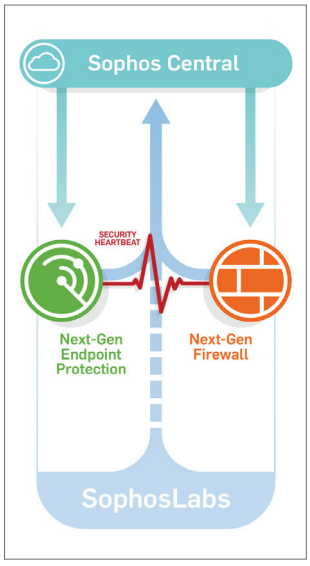
Suitable encryption of company documents can help to prevent malware from obtaining unencrypted access to confidential documents. This prevents damage caused by the outflow of business-relevant documents.

Think of security as a 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.

Sophos' synchronized security approach enables you to share intelligence in real time between your endpoints and firewall. By automating threat discovery, investigation, and response, synchronized security gives you unparalleled protection against advanced threats. To find out more visit www.sophos.com/heartbeat



Deploy malicious traffic detection capabilities

It's essential to react quickly to new threats. Malicious Traffic Detection, which is available in Sophos Endpoint Protection, detects communications between a compromised endpoint and an attacker's servers. The Malicious Traffic Detection automatically identifies offending software and stop it from running to prevent potential damage or data loss.

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 organizational options for protecting your IT infrastructure.

Ransomware is a very present risk for all organizations, and indications suggest that it is not going away any time soon. It is therefore essential to take immediate steps to secure your organization against this type of attack. By following both the short and longer term recommendations outlined in this document, organizations will take significant steps to protect themselves against ransomware infections.

Further reading

Sophos technical whitepaper on ransomware

Sophos blog post on Locky

Sophos blog post on ransomware

IT Security DOs and DON'Ts

Threatsaurus

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, GB | Boston, USA

03/16.NP.wpna.simple

SOPHOS