SOPHOS
Security made simple.

HOW TO STAY PROTECTED AGAINST RANSOMWARE

Businesses large and small are under threat from increasingly aggressive and brutal ransomware attacks. Loss of access to critical files, followed by a demand for payment can cause massive disruption to an organization's productivity.

But what does a typical attack look like? And what security solutions should be in place to give the best possible defense?

This paper examines commonly used techniques to deliver ransomware, looks at why attacks are succeeding, and gives nine security recommendations to help you stay secure. It also highlights the critical security technologies that every IT setup should include.

A Sophos Whitepaper May 2017

Ransomware – a brief introduction

Ransomware is 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.

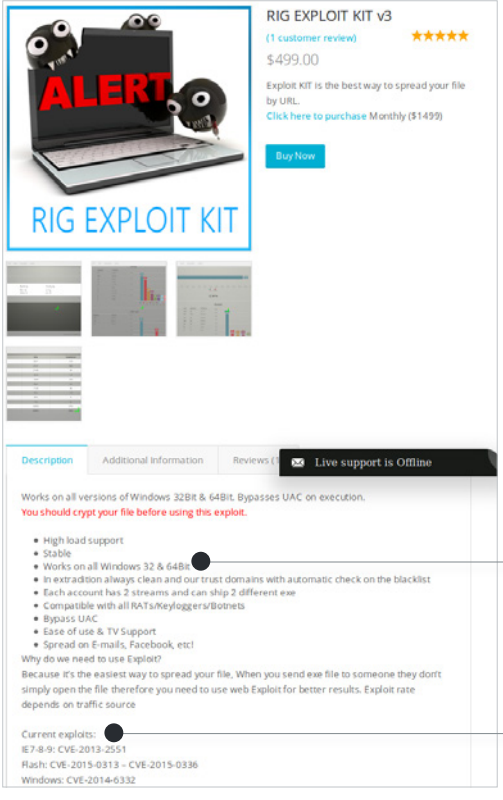
The current wave of ransomware families can have their roots traced back to the early days of Fake AV, through "Locker" variants and finally to the file-encrypting variants that are prevalent today. Each distinct category of malware has shared a common goal – to extort money from victims through social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

And the financial consequences can be severe. The Hollywood Presbyterian Medical Center reportedly paid 40 Bitcoins ($17,000) to regain access to its files, while the Kansas Heart Hospital despite paying an undisclosed sum, was faced with a second ransom demand and not given access to all of its files.

Why are ransomware attacks so successful?

Most organizations have at least some form of IT security in place. So why are ransomware attacks slipping through the net?

1. **Sophisticated attack techniques and constant innovation**
   - Access to ready-made 'Malware as a Service' (MaaS) programs is increasingly easy, making it simple to initiate, successfully complete and benefit from an attack, even for less tech-savvy criminals. Below is a MaaS program for sale.



Includes network and endpoint techniques from infecting a website, all the way to delivering an endpoint payload and selling the results.

Cross-platform and Agile developed.

Exploits automatically included.

- Skillful social engineering is used to prompt the user to run the installation routine of the ransomware. For example you may receive an email that reads something like this: "My organization's requirements are in the attached file, please provide me with a quote."
- Producers of ransomware operate in a highly professional manner. This includes providing a working decryption tool after the ransom has been paid.

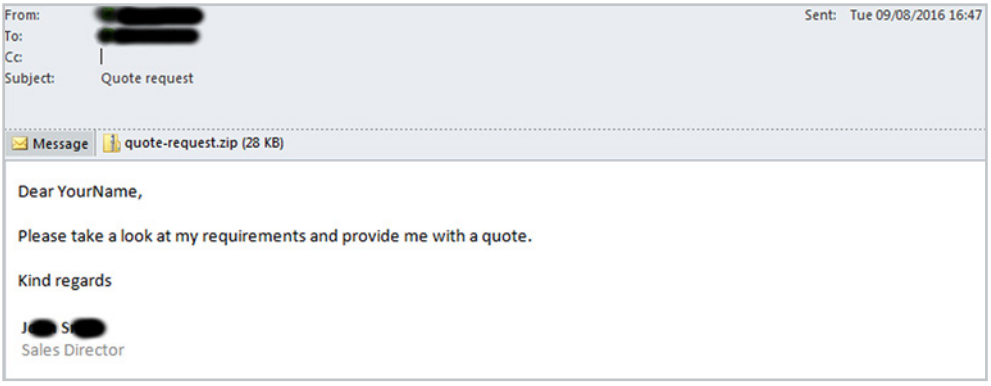
2. **Security holes at affected companies**
   - Inadequate backup strategy (no real-time backups, backups not offline/off-site).
   - Updates/patches for operating system and applications are not implemented swiftly enough.
   - Dangerous user/rights permissions (users work as administrators and/or 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 IT security knowledge (.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…").
3. **Lack of advanced prevention technology**
   - Many organizations have some form of generic protection.
   - Ransomware is constantly being updated to exploit and avoid this protection. For example, deleting itself so quickly after encrypting files that it can't be analyzed.
   - Solutions need to be designed specifically to combat ransomware techniques.

How does a ransomware attack happen?

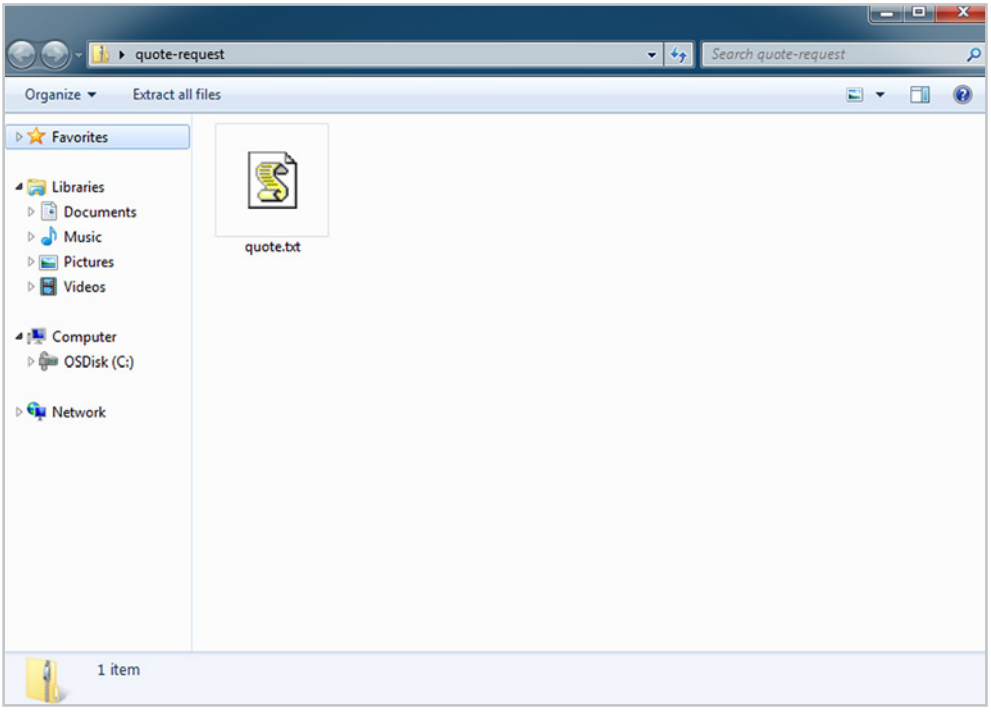
There are two main ways that a ransomware attack starts. Via an email with a malicious attachment, or by visiting a compromised (often a legitimate, mainstream) website.

Malicious email

Today's criminals are crafting emails that are indistinguishable from genuine ones. Grammatically correct with no spelling mistakes, and often written in a way that is relevant to you and your business.



When opened, the zip file appears to contain an ordinary .txt file.



However, when the file is executed the ransomware is downloaded and installed onto your computer. In this example it's actually a JavaScript file disguised as a .txt file that's the Trojan horse, but there are many other variations on the malicious email approach, such as a Word document with macros, and shortcut (.lnk) files.

Malicious websites

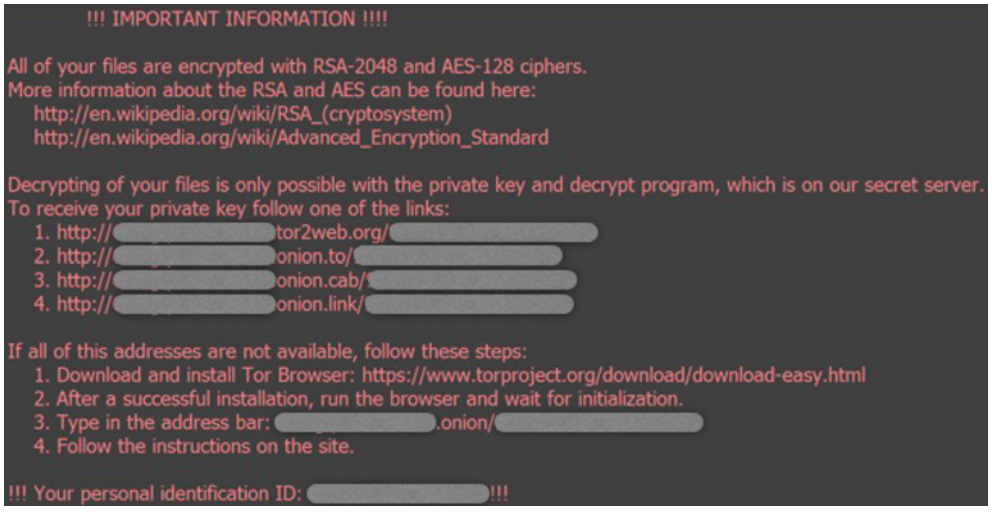
Another common way to get infected is by visiting a legitimate website that has been infected with an exploit kit. Even popular, mainstream websites can be temporarily compromised. Exploit kits are black market tools that hackers use to exploit known or unknown vulnerabilities (such as zero-day exploits).

You browse to the hacked website and click on an innocent-looking link, hover over an ad or in many cases just look at the page. And that's enough to download the ransomware file onto your computer and run it, often with no visible sign until after the damage is done.

What happens next?

After initial exposure such as via the email and web examples, the ransomware takes further action:

- It contacts the attacker's Command & Control server, sending information about the infected computer and downloading an individual public key for it.
- Specific file types (which vary by ransomware type) such as Office documents, database files, PDFs, CAD documents, HTML, XML, etc., are encrypted on the local computer, removable devices and all accessible network drives.
- Automatic backups of the Windows operating system (shadow copies) are frequently deleted to prevent data recovery.
- A message appears on the desktop explaining how the ransom can be paid (typically in Bitcoins) in the specific time frame.



- Finally, the ransomware deletes itself leaving the encrypted files and ransom note behind.

Wanna Decrypt0r 2.0 ransomware outbreak

Wanna (aka WannaCry, WCry, WanaCrypt, WanaCrypt0r and Wana DeCrypt0r) is a fast spreading piece of ransomware that began causing global disruption on 12th May 2017.

Analysis seems to have confirmed that the attack was launched using suspected NSA code that was leaked by a group of hackers known as the Shadow Brokers. It uses a variant of the ShadowBrokers APT EternalBlue Exploit (CC-1353) and uses strong encryption on files including documents, images and videos.

Unusually, Wanna was able to exploit a remote code execution (RCE) vulnerability that allowed it to infect unpatched machines without users doing anything. Due to this Wanna was able to rapidly spread, similar to decade old worm outbreaks such as Slammer and Conficker.

The exploited RCE vulnerability was a flaw in the Windows Server Message Block (SMB) service, which is used by Windows computers to share files and printers across local networks. Microsoft had addressed it with the MS17-010 bulletin in March 2017, but systems that hadn't installed the update or were running versions of Windows that are no longer supported were still vulnerable.

In response to the outbreak Microsoft took the rare step of releasing the security update for platforms in custom support (such as Windows XP) to everyone. It is strongly recommended to install this update as soon as possible.

For more information see the Sophos KB article: www.sophos.com/kb/126733

Nine best security practices to apply now

Staying secure against ransomware isn't just about having the latest security solutions. Good IT security practices, including regular training for employees are essential components of every single security setup. Make sure you're following these nine best practices:

1. **Backup regularly and keep a recent backup copy off-line and 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.

2. **Enable file extensions**

The default Windows setting is to have file extensions disabled, meaning you have to rely on the file thumbnail to identify it. Enabling extensions makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript.

3. **Open JavaScript (.JS) files in Notepad**

Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.

4. **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 infections rely on persuading you to turn macros back on, so don't do it!

5. **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.

6. **Don't give yourself more login power 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 have administrator rights.

7. **Consider installing the Microsoft Office viewers**

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

8. **Patch early, patch often**

Malware that doesn't come in via a document often relies on security bugs in popular applications, including Microsoft Office, your browser, Flash and more. The sooner you patch, the fewer holes there are to be exploited.

9. **Stay up-to-date with new security features in 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 against external malicious content without stopping you using macros internally.

Protection technologies to help keep you secure against ransomware

To stop ransomware you need to have effective, advanced protection in place at every stage of an attack.

Securing your endpoints

Intercept X utilizes the unique CryptoGuard technology to stop ransomware attacks in their tracks. It works by detecting and stopping ransomware from encrypting your files, including the recent Wanna ransomware outbreak. Intercept X complements your existing security, blocking processes that attempt to make unauthorized modifications to your data.

Stopping email threats

The best defense against booby-trapped emails is your email gateway. Anti-spam technologies stop ransomware emails, while antivirus scans for and blocks email-borne threats. Blocking emails with macro attachments can help you avoid another common ransomware technique. Time-of-Click technology stops you and your users from clicking through to infected websites – even if they were clean when the email entered your inbox.

Stopping web threats

Web threats are neutralized at the firewall and web gateway. URL filtering blocks websites hosting ransomware, as well as their command and control servers. And by enforcing strict controls you can stop ransomware-related files from being downloaded at all.

Cloud sandboxing at both the email and web gateway blocks zero-day advanced threats, including ransomware. It's like having your own private malware lab that runs suspicious files to determine behavior.

Protecting your servers

Server whitelisting and lockdown keep your servers secure by whitelisting authorized applications and identifying what they can change and update – all other attempts to make changes are automatically blocked, stopping ransomware from taking action. Malicious traffic detection stops ransomware from contacting command & control servers and downloading its payload. Sophos Server Protection also includes CryptoGuard technology that stops ransomware from encrypting your files.

Security Heartbeat

Your security products are great individually, but even better when they work together. By enabling your endpoint and firewall to share security information and proactively respond to threats you get unparalleled protection against advanced threats.

Make sure you're using the best practice settings for your Sophos solutions.

www.sophos.com/kb/120797

Try Sophos Intercept X for free at sophos.com/free-trials

More than 100 million users in 150 countries rely on Sophos as the best protection against complex threats and data loss. Sophos is committed to providing complete security solutions that are simple to deploy, manage, and use that deliver the industry's lowest total cost of ownership. Sophos offers award winning encryption, endpoint security, web, email, mobile, server and network security backed by SophosLabs – a global network of threat intelligence centers. Read more at www.sophos.com/products.

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

North America 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

2017-05-16 WP-NA (2619-DD)