How to Avoid & Prevent Ransomware

No business is immune from the threat of ransomware.

The best way to stop ransomware is to be proactive by preventing attacks from happening in the first place. In this article, we will discuss how to prevent and avoid ransomware.

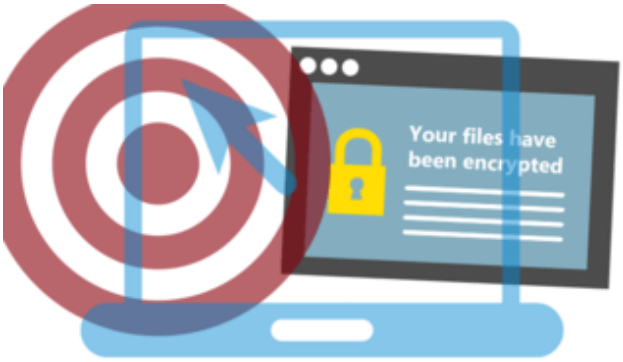
A string of ransomware attacks that began in 2016 (Locky, Petya and WannaCry), have been a wake-up call for many businesses regarding how important a comprehensive approach to IT security is.

These types of attacks can have a devastating impact, from losing precious business data to shutting down hospital services in the middle of emergency procedures.

Businesses must deploy the right technologies to prevent ransomware attacks from happening in the first place and have an effective backup strategy in place to help you recover quickly in the event of a data breach.

In this document, we examine the most commonly used techniques to deliver ransomware. We also look at why attacks are increasingly devastating, and provide you with some simple, easy to adopt security recommendations to help protect your business from malicious threats and ransomware.

We'll also highlight our recommended security services and technologies that every business should look at adopting in order to provide a **multi-layered defence model**.



What is Ransomware?

Ransomware is a type of malware. It is one of the most widespread and damaging threats that businesses currently face.

It is spread when an unsuspecting user opens a document (or javascript file), which looks like gibberish. The document recommends enabling macros "if the data encoding is incorrect." Once macros were enabled, the malicious macro would download an executable file and start to encrypt files, wreaking havoc on your network.

Back in May 2017, around forty NHS hospitals were simultaneously hit by WannaCry ransomware, which affected huge numbers of businesses and IT networks across the world.

A Freedom of Information request by Citrix published in December 2016 found that 90% of England NHS Trusts continue to rely on PCs installed with Windows XP, Microsoft's 15-year-old desktop operating system. Microsoft stopped providing extended support for XP in April 2014 but continued to provide the NHS with updates and security patches under a contract that cost an estimated £5.5 million.

Ironically, there was already a patch made available by Microsoft for all affected Windows systems since March 2017. This demonstrates how seldom security updates and patches are carried out.

Why are ransomware attacks so successful?

Most organisations have at least some form of IT security service or software in place. But why is this no longer enough, and why does there seem to be more and more ransomware attacks slipping through the net? There are several reasons for this:

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.

   Producers of ransomware now operate in a highly professional manner, running cyberattacks as an extremely profitable business. Skilful social engineering is used to prompt unsuspecting users to run the installation of ransomware. For example, you may receive an email that reads something like this: "My organisation's requirements are in the attached file, please provide me with a quote."

2. **Security holes within an organisation**

   Businesses that have suffered a breach often have some or all of the following:

   - Inadequate backup strategy (no real-time backups, or backups are not offline/off-site).
   - Updates/patches for operating system and applications are not implemented swiftly enough.
   - Risky user/rights permissions. For example, users work as administrators and/or have more file rights on network drives than necessary for their tasks.
   - Lack of user security training; Employees should recognize the signs of a phishing attack. Keep yourself and your employees up-to-date on the latest cyberattacks and ransomware. Make sure they know not to click on executable files or unknown links.
   - Security systems such as virus scanners, firewalls, IPS, sandboxing, email/web gateways are not implemented or are not configured correctly.
   - Conflicting priorities ("We know our methods are not secure but our staff need to work uninterrupted…").

3. **Lack of advanced prevention technology**

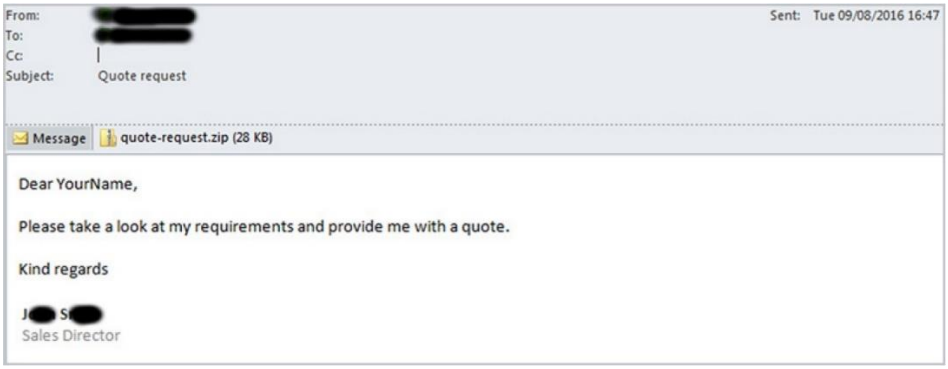
Ultimately, it is becoming increasingly clear that a single layered approach to fighting viruses that relies on signature-based technology is no longer sufficient.

A layered approach is the best bet when it comes to cyber security.

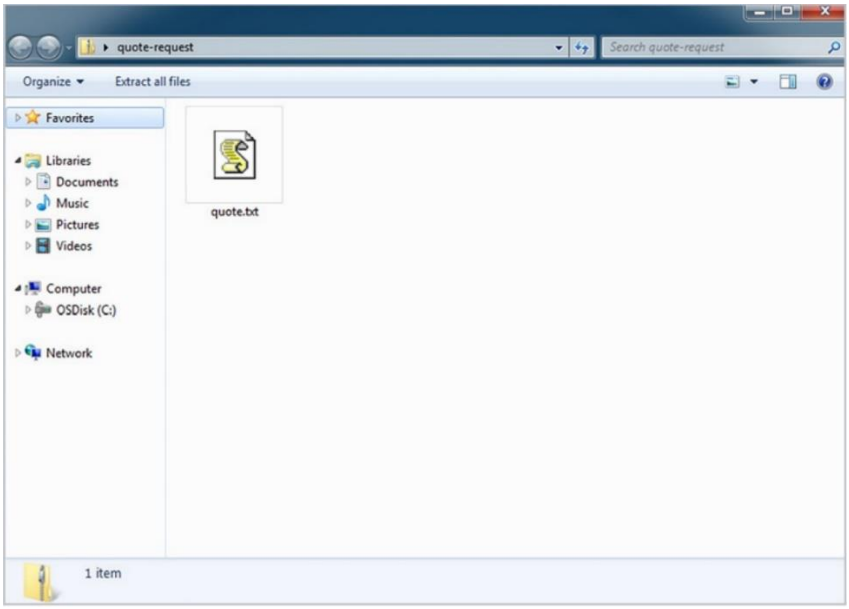
Solutions need to be designed specifically to combat ransomware techniques. There is no single, silver bullet offering the best prevention against threats. Businesses require a layered approach capable of addressing not only today's threats, but tomorrow's as well. And when things fail - and remember, nothing is 100% - businesses need the ability to quickly and effectively remediate those threats.

How does a ransomware attack happen?

Today's cybercriminals are now crafting clever 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. For example:



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.

Another common way businesses are being infected is by visiting a legitimate website that has been infected with an exploit kit. Exploit kits are black market tools that hackers use to exploit known or unknown vulnerabilities (known as 'zero-day exploits').

An unsuspecting user clicks on an innocent-looking link, hover over an ad or in many cases just look at the page. This is often enough to download the ransomware file onto your computer and run it, often with no visible sign until after the damage is done.

Firstly, the ransomware 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 then appears on the desktop explaining how the ransom can be paid (typically in Bitcoins) within a specific time frame.

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

9 Security Practices to Apply Now

Staying secure against ransomware isn't just about installing the latest security solutions or services. Other practices, such as regular awareness training for employees, are just as important.

Make sure you're following as many of these recommendations as possible:

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

Other than ransomware, there are many ways that files can suddenly vanish: 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. We recommend keeping the external backup drive connected to the hardware device as little as possible. Once a day, plug it in, run your backup program and then safely remove it straight away. Take it home or keep it somewhere off site.

2. 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. The Wanna and Petya outbreaks has shown that patching, no matter how mundane, should be placed at the core of our security infrastructure. For 3C Technology customers that have a Support Contract, this is a task we can assist with if required.

3. 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.

4. 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.

5. 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. Many infections rely on persuading you to enable macros - **don't do it!**

6. 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.

7. Don't give yourself or employees more login power than is needed

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.

8. Consider installing the Microsoft Office viewers

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

9. Upgrade and stay up-to-date with new security features in your business apps

For example, Office 2019 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.

Our recommendations

To prevent ransomware and other malicious malware, businesses require effective and advanced protection at every stage of a potential attack.

Malware and spam protection with content filtering, application control and web filtering, is a good start when protecting your business from cybersecurity threats.

Investing in a WatchGuard UTM device, which incorporate a traditional firewall with Intrusion Protection, provides a pre-emptive approach to network security that adds an essential layer of threat detection and prevention. IPS protects your network from a wide range of malicious activities, including SQL injections, cross-site scripting, and buffer overflows.

1. Secure your endpoints and stop email threats

Although traditional antivirus is no longer enough to protect your business against cyber threats, it can still act as your first line of defence. Anti-spam technologies can help to stop some ransomware emails, while antivirus scans for and blocks email-borne threats.

Ensure your antivirus is installed correctly and is up to date across all endpoints within your business. Keep in mind, some AV is based on signatures so new variants may and will slip through the net.

- Sophos Intercept X Advanced with Endpoint Protection & Response (EDR) utilises the unique CryptoGuard technology to stop ransomware attacks in their tracks. It uses behavioural analysis to stop never-before-seen ransomware and boot-record attacks, making it the most advanced anti-ransomware technology available.
- Malwarebytes provide signature-less, heuristic, and behavioural technologies which can fight ransomware at every stage of the attack chain. Their Endpoint Protection and Incident Response product and cloud management console provides easy, direct and centralised security policy management.

2. Stop web threats

Web threats are neutralised at the firewall and web gateway. URL filtering blocks websites hosting ransomware, as well as their command and control servers. Enforcing stricter controls can help stop ransomware-related files from being downloaded.

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 behaviour.

3. Protect your servers

Keep your servers secure by whitelisting authorised applications and identifying what can be changed and updated and by whom. All other attempts to make changes are then automatically blocked, helping to stop hackers from taking hold of your network.

4. Use the 3-2-1 rule for your Backup

It's a good idea to store at least three different copies of your data on two different media, with at least one copy stored offsite. It's critical that your backup strategy features redundancies and leverages storage options not vulnerable to attack - like tape, offline disk, and cloud.

Veeam Availability Suite combines the backup, restore and replication capabilities of Veeam Backup and Replication with the advanced monitoring, reporting and capacity planning functionality found in Veeam ONE. Availability Suite delivers everything you need to reliably secure and manage your VMware vSphere and Microsoft Hyper-V environments**,** providing you with true High Availability (HA).

Veritas Backup Exec 20 also offers fast, efficient and versatile recovery - for cloud, on premise and hybrid environments. The current version features automated disaster recovery testing for virtual machines along with additional private cloud storage. Unlike other solutions, Backup Exec provides deduplication to the cloud, enabling you to reduce the amount of data to be stored and the amount of data traveling over the network while reducing storage costs.

Staying ahead of cybercriminals is a continuous uphill battle. Investing in a multi-layered security approach and DR strategy *before* the occurrence of a cyberattack instead of focusing on after-attack remedial action will not only save you time and money, but could save your reputation too.

3C Technology Ltd
Registered in England 2604836
Network House
Hawkins Road
Colchester
Essex
CO2 8LA

Let 3C Technology help your business reduce downtime, improve efficiency and keep your network running at peak performance.

We are committed to providing complete security solutions tailored to your business to deliver the lowest total cost of ownership.

We provide encryption, endpoint security, web, email, mobile, server and network security. You can wrap up all these services with a flexible IT support contract.

Please visit www.3ctech.co.uk for more details