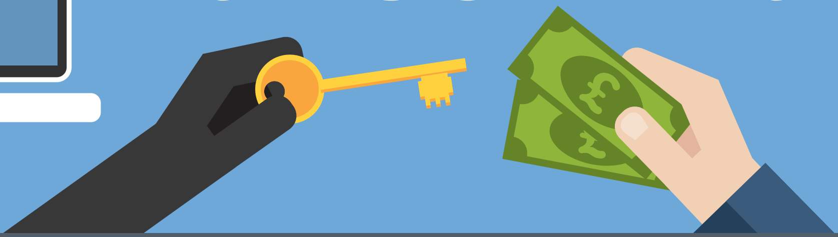
What is ransomware?



Over the last few years' ransomware has gained more and more traction. Throughout 2016 we saw ransomware continue to wreak havoc wherever it managed to get a toe hold. It is the fastest growing malware threat today and is already an epidemic.

What is Ransomware though and why is it becoming so popular with criminal groups as a way to extort money?

Broadly speaking ransomware is malicious software (a virus/malware) designed to encrypt an individual or company's files. If successful ransomware allows criminals to extort their victims and demand payment to restore access to these encrypted files.

Most people have heard of cryptolocker. This was one of the first ransomware to gain widespread notoriety when it came on the scene a few years ago. Due to it being one of the first and gaining a lot of attention people associate any malware that encrypts their data as cryptolocker even though this variant is no longer active. We won't be using the term cryptolocker but discussing ransomware in general.

Why is ransomware becoming so popular?

There are 3 main reasons why it is has grown so popular over the last few years (the first known ransomware was in 1989.)

The release of Android. Android is the most popular mobile operating system around these days and is a popular attack vector. IOS will most likely follow suit in the near future.

Bitcoins. Bitcoin is a form of digital currency, created and held electronically. No one controls it. Bitcoins aren't printed, like pounds or euros. Transactions are made with no middle men – meaning, no banks! Bitcoin enables easy and virtually untraceable payments to anonymous cybercriminals.

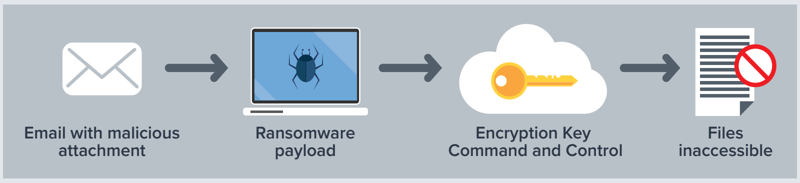
Ransomware as a service.
A ransomware-as-a-service scheme enables even the most technically illiterate cybercriminal to extort payments from victims infected with data-encrypting malware, with the developers of the service taking a significant chunk of the ill-gotten gains.

Locky was 2016's most aggressive ransomware. It is estimated that Locky could have generated around £250 million for its developers. You can see why this type of attack is becoming more and more popular with cyber criminals.

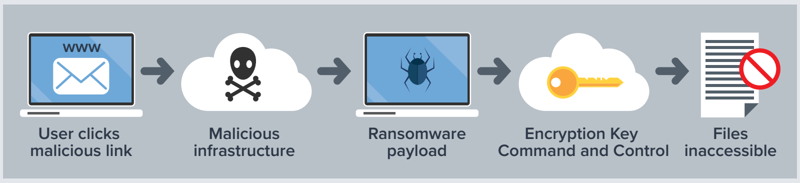
How ransomware infects victims and how it is evolving

Ransomware typically is delivered by two main channels.

Email Phishing campaigns. These emails usually try and trick users in two ways. They either try to get the user to open malicious attachments, usually Office documents with malicious macros. Or they try and get the user to click on a link to a website hosting the ransomware. It is estimated 97% of phishing emails are now delivering ransomware, a frightening number.

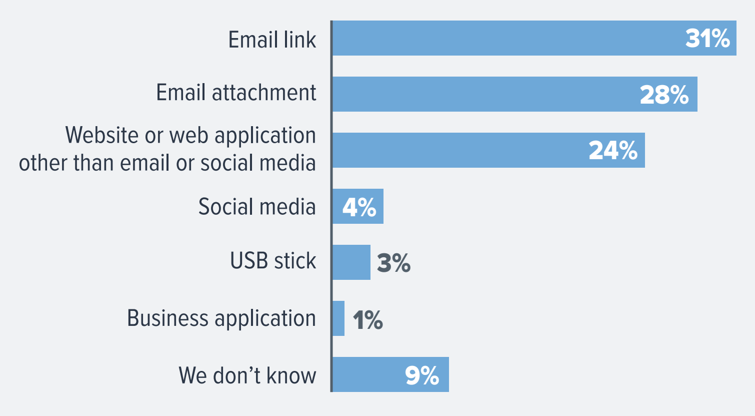

Email with malicious attachment
Ransomware payload
Encryption Key Command and Control
Files inaccessible

Links to malicious or compromised websites. Although the infection comes from a website the majority of times the link to this website comes from a link in a phishing email, other sources which point you to the website are malicious online advertising campaigns. Usually what happens with web based infection is that it uses an exploit kit to infect the user. This is possible due to users having out of date applications or a not fully patched workstation.



Email is the number one delivery vehicle for ransomware

Now, the only way a phishing attack can be successful is to convince the end user that the email is legitimate. No one is going to think the email is legit if it doesn't look the part. So, attackers go to great lengths to make sure end users will be fooled. This means creating customised, relevant messages and making it look like it is coming from a sender the victim is likely to know (spear phishing) or a company who the victim uses for services or products.



Why anti-virus alone is no longer enough

People think that if they have an up to date anti-virus then they are protected and safe and unsurprisingly they are very upset when this turns out to not be the case.

The reason anti-virus is no longer enough to ensure an optimal level of protection is because hackers know how anti-virus works and are constantly battling with the security vendors to find a way around them. Malware is now using multiple evasive techniques (500+) to evade detection, they can even tell when sandboxing is being used and will not deliver the payload until they reach their desired target. Four types of evasive techniques are most prevalent and successful for ransomware: 1) environmental awareness, 2) confusing automated tools, 3) timing-based evasion, and 4) obfuscating internal data.

Traditional anti-virus works by performing routine file scans and looking up file signatures in a database of known malware signatures. This approach is very effective for blocking known malware, but it doesn't stop brand new malware or old malware that has been repackaged with a new signature. Some malware is repackaged every day/week or coded to change the malware's domain on a daily basis and employ a domain generation algorithm (DGA), which computes where the C&C servers will be at any given time. **All to ensure it can keep evading traditional anti-virus.**

So what's next: how is ransomware evolving?

With the amount of money being made via ransomware more and more criminals are flocking to exploit it as a cheap and easy way to make money.

More and more variants are being created each month putting a strain on security vendors to keep up. If you ask a bank robber why he robbed a bank he will tell you because that's where the money is. Now ransomware is where the money is and it is a hell of a lot less risky than robbing a bank and way more profitable.

Executables in email attachments are being replaced with javascript files as these are not under the same scrutiny as executables and can be made to look like simple text files.

Encrypting your files was a good start for cyber criminals but they are now raising the stakes. They are finding way to encrypt your databases too, your line of business application will soon no longer be safe from ransomware.

Brute force attacks on remote servers are also becoming more and more popular with hackers scanning the internet for unsecured RDS servers and then trying to brute force accounts, once in they run their software and wait for the ransom.

Some malware is delivering more than one payload, not only are they encrypting files but some are dropping key loggers to try and gain access to financial systems.

Most worryingly, what seems to be emerging is attackers releasing your data publicly if you do not pay. That threat is especially damaging for companies who deal with their customers' personal data such as law firms, financial services, travel agents to name a few.

Implementing best practices to reduce ransomware exposure

There is no way to 100% protect yourself from a ransomware attack, it just is not possible right now so we look at ways to reduce your exposure and mitigate damage from an attack through the following:

- Being pro-active about ransomware defence.
- To detect, block and defend an attack that does get through by automating responses.
- Finally, how to recover from an attack.

Before an attack

Prevention is king. Like most people a hacker would rather have an easy job than a hard one so don't give them one. Most attacks, unless you are specifically targeted, are opportunistic and the attackers' motive most often is profit with as little risk and effort as possible.

So preventing an attacker from gaining entry with an architectural approach is the most effective way to kill the ransomware attack before it begins.

The following best practises should be implemented:

End users. This may seem very simplistic but ransomware doesn't install itself, right now most ransomware needs some level of end user intervention to install itself.

- Strong password policies to mitigate brute force attacks
- Encourage using only company sanctioned programs
- Disable macros for all users unless expressly required
- Educate users on the dangers of phishing attacks

Threat exposure. You should be performing ongoing risk assessments to identify security weaknesses and address any weaknesses.

- Conduct periodic penetration testing
- Ensure patch management for operating systems and application is rolled out and reported on
- Disable unnecessary services
- Enforce the principle of least privilege
- Up to date, active, next gen anti-virus on all end points
- Gateway defences such as firewall, UTM, email and spam filtering
- FSRM file screening
- DNS layer protection
- Regularly backup systems and data and replicate offsite
- Run time malware protection

Educating users on how to spot malicious emails can help transform them from a major liability to a solid first line of defence.

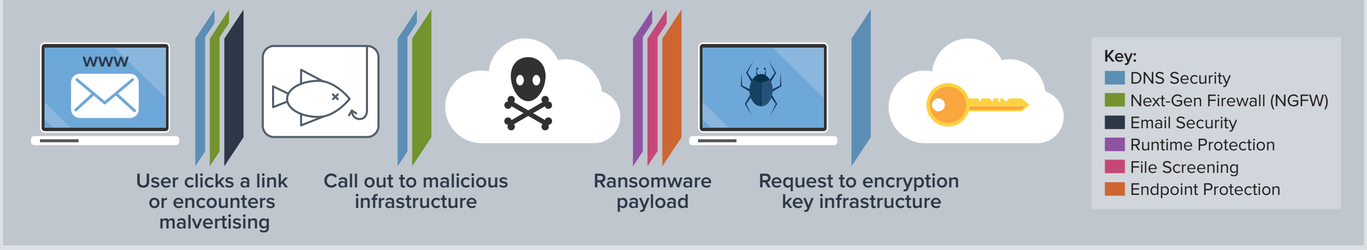
Most of the technological solutions are common sense, mature and well known such as patch management, anti-spam, anti-virus, firewalls and reliable secure backups but it would amaze how often these solutions are not implemented or managed properly leaving a massive hole for ransomware to drop its payload.

New solutions such as runtime protection and DNS layer protection are specifically geared to stopping ransomware and can be very successful if ransomware actually makes it through to your network, by either stopping the process before it can start encrypting your files or blocking access to the command and control centres so the malware cannot pull down it's encryption keys.

In built tools, such as FSRM file screening can also be extremely cost effective, however take more management time to be truly effective.

Despite your best efforts, and even if you strictly stick to the best practises outlined for preventing an attack, an attacker may still succeed in infiltrating your network.

Protection at each threat phase


www
User clicks a link or encounters malvertising
Call out to malicious infrastructure
Ransomware payload
Request to encryption key infrastructure
Key:
🟦 DNS Security
🟩 Next-Gen Firewall (NGFW)
⬛ Email Security
🟪 Runtime Protection
🟥 File Screening
🟧 Endpoint Protection

During an attack

If your organisation is under attack you need to respond quickly and decisively to mitigate any damage caused and have relevant processes and policies in place to return to normal working practise.

The primary issue is the speed at which ransomware encrypts the files. Communication is key and the quicker you identify an attack the less damage will be done. You may find yourself with only one infected device (rare, consider yourself very lucky) or multiple file shares and servers.

This is what your basic response should look like:

Isolate the infection. First thing to do is isolate the infected machines from the network.

Determine the severity. Most ransomware leaves a trace behind so it is easy for you to contact the attackers. Usually they change the file name extensions (ie .wallet, .zepto, .locky) and usually there is an html or text file explaining how to unlock your files. Track down these markers and determine the extent of the infection and the type of ransomware you have. If any machines that have not been isolated have these markers and are infected, isolate them immediately.

Patient Zero. You then need to determine where the initial infection came from then ask the user to retrace their steps to find out how the system was compromised. This is a must for ensuring it cannot happen again as the stats show once you have been infected once you are a target moving forward.

Cleanup. Make sure all traces of the malware are gone before moving on to how to recover.

After an attack

The main focus after an attack is getting back to business as usual with the least amount of disruption. However, lessons need to be learned to minimise the chance of another attack.

- Check if malware researchers have developed decryption tools for your specific ransomware
- Decide on what is the right course of action for recovery of data – pay the ransom, recover from backup or try the decryption tools if available.
- Collect and preserve evidence for law enforcement or auditing purposes.
- Perform root cause analysis.
- Deploy security services or change processes as determined necessary via the root cause analysis
- Educate users

Stats show the majority of companies infected refuse to pay the ransom, but ultimately each company will have to make that decision based on their own specific circumstances and policies.

By far the safest thing to do after an attack is to wipe the infected machines and restore from backup. In a virtual environment, this is much quicker and easier to achieve.

Why prevention is important

Having the ability to recover from an attack is very important so you need robust backup procedures in place. However backups have limitations:

- They aren't always reliable and you could lose more data than you think.
- They don't protect against data theft.
- Time is money. The longer it takes to recover and the amount of data lost is going to affect your staff and your clients potentially causing lost work or missed deadlines and a dent in your professional reputation.

5 key ransomware takeaways

- Ransomware is evolving.
- Ransomware-as-a-service is an emerging threat.
- Paying a ransom doesn't solve your security problems.
- You need best of breed security solutions which are rolled out and managed properly.
- End users can be a liability or an asset – educate them.