KINETICS GROUP

making IT work for you

CRYPTOLOCKER WHITE PAPER

Author	Bill Lunam
Date	November 2016
Document Reference	CryptoLocker white paper
Version	2.4

Contents

1 What is CryptoLocker?

Throughout this document I will use the generic name “CryptoLocker”. The original CryptoLocker hasn’t actually been around for several years. It was a specific type of ransomware which was shut down in May 2014. So pervasive was CryptoLocker, (at least 500,000 victims) that we now refer to almost all ransomware as CryptoLocker.

CryptoLocker is online extortion. It encrypts your files and then demands a fee to unencrypt them. Paying the fee is no guarantee you will get your files unlocked or that they will not get encrypted again. Like traditional extortion, paying the fee only encourages the perpetrators.

Money changes everything and security is no exception.

Originally we had viruses, the writers of which earned nothing from their work. Essentially, virus writing was an amateur pursuit. Then Adware came along. It would earn the writer a very small fee for each ad clicked on. Even when adding in vast numbers of PC’s, adware still earned the writer insignificant income. Ransomware on the other hand can demand bitcoins worth $300 - $500 a time. It’s thought the original GameOver Zeus CryptoLocker earned $4.5m. That sort of money gets serious attention from serious criminals.

Now that money is involved, things evolve quickly. New versions of the software, new hooks to draw in the unwary and new web sites for delivery can come and go in a matter of hours.

2 How does CryptoLocker spread?

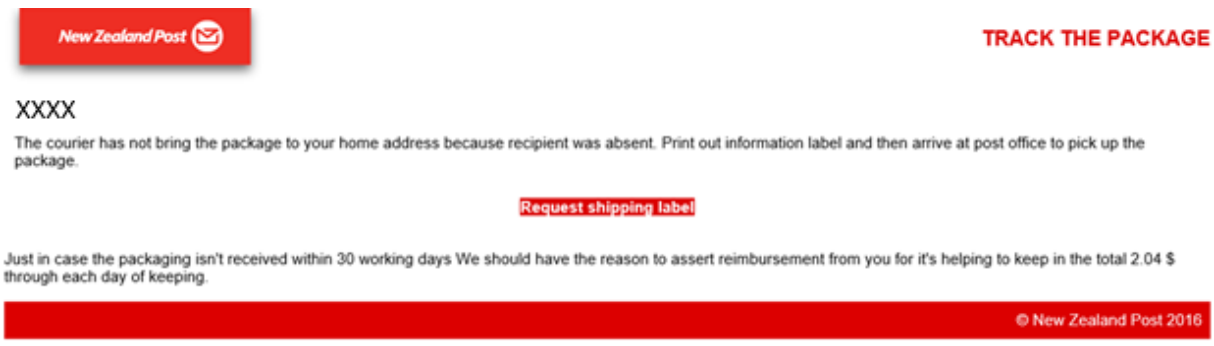
CryptoLockers typically don’t spread themselves or contain a payload that infects new hosts. It is happy to run on just one device and set about encrypting files, locally and on the any networks/devices it has access to. Typically, it does not encrypt all files, it’s more likely to target documents and photos. Sometimes it has it’s own encryption software, sometimes it uses the encryption features built into existing applications.

It’s important to remember that when talking about ransomware things change so quickly, there are no norms.

You are most likely to get CryptoLocker from a website, but you will have been lured into visiting the website via an email.

The most common trick is a link inside an email. You may think you are following a link to:

- Shared files (drop box file sharing notification)
- An official document (notification of a fine, tax refund)
- Check your social media (a Facebook or LinkedIn request)
- Track an order (FedEx, Amazon, Post).



NZ Post Phishing Email

Instead you are connecting to a website that has been set up to deliver a payload onto your PC. When a new version of CryptoLocker comes out. It's not uncommon for hundreds of infected websites to be run up in a just a few hours.

The next most common trick we are aware of is to use a Word document or PDF as the delivery mechanism. When you open the document, a macro embedded inside will connect to the infected site and download the payload. With this method, you may never see a web site at all. The download will happen in the back ground.

Often criminals are targeting individual people or organisations. We have noted that the links inside the email can record the name of the business being targeted. When you click on the link, there is a noticeable increase in phishing emails to that business.

3 Can my Anti-Virus software protect me?

The answer to this is a yes and no. CryptoLocker is not a virus, it does not behave like a virus. But like being in pain, you don't care if it's a disease or an injury. You just need someone (preferably a medical professional) to help you out. Many Anti-virus companies have taken this on-board and introduced features to help combat CryptoLocker.

Because CryptoLocker is not a virus and carries out actions which are legitimate, it is hard for software vendors to produce a single 100% effective tool. Once a variant has been around for a few days and is understood, traditional pattern matching detection works well. But CryptoLocker can change very fast, so many vendors have now introduced or improved *Behavioural Analysis* in their products, increasing the opportunity of blocking new variants.

Running a good Anti-virus, with specific features turned on and detection levels turned up can help. But it is not on its own fully effective or a 100% guarantee against new variants. Activating these settings will also come at price. Typically, you will experience some loss of performance or increased disruption associated with it. Later in this document we list out the suite of changes needed to further increase the effectiveness of Anti-virus.

At this point you may well ask "why is it so hard for a PC to detect CryptoLocker?". The answer is that the action of encrypting a file is not a suspicious one.

Many everyday applications installed on your PC are encrypting sensitive data. Banking, payroll and accounting applications all encrypt. When you log on to your PC, your password is encrypted. If you protect your laptop with Bitlocker, your whole hard drive is encrypted. Word, Excel and PDF all have encryption built into them. To your PC, the actions the CryptoLocker is doing can look legitimate.

4 What do my staff need to know about CryptoLocker?

Almost every CryptoLocker incident starts with someone clicking on a link from an email or opening an attached document.

Ensuring your staff are aware of the risks and take a sensible level of precaution with emails is the starting point with protection. You will receive a CryptoLocker email at some point, most likely you already have and staff have not been fooled. Without awareness, sooner or later someone will click.

Before opening an attachment or clicking on a link, staff need to ask the question "Is this email legitimate?"

- Are you expecting an email from this person/organisation?

  - Example: if they normally send an invoice in the first week of the month, and one arrived in the last week.
- Does the language in the email reflect the norm from that person/organisation?
  - Example: Normally the email starts with a greeting and has an explanation of the contents. Then one arrives with only the words “Invoice attached”.
- Does the email look like it normally does?
  - Many companies have signatures with pictures or may add some advertising to the email. An email without that would be suspect.

Warning: It’s not uncommon for a company that has had a CryptoLocker incident to have another one with in a fortnight. When this happens, it’s surprisingly common for both incidents to be triggered by the same employee.

5 How do I prepare for and recover from CryptoLocker?

This is vital. The odds of your business being hit by CryptoLocker are far higher than the odds of staff embezzling money, a fire, a flood, a power surge blowing up your servers. The odds are higher of you getting CryptoLocker than all four of the others combined.

When you get CryptoLocker you need to restore data, so backups are vital. If you have an image based backup, then backing up locations that hold documents several times a day is a good idea.

5.1 Backup regime

Use disk backups (restores are faster than tapes) with a software product that can do frequent incremental backups. This will allow the setting up of small low impact backups several times a day.

Note: Backups are only effective if they are working. You must have a system of monitoring and testing backups.

5.2 Infection procedure

Have an infection procedure ready to roll. Like a fire drill, staff should know what to do. Delays will result in more files being encrypted and needing to be restored.

- If you use Citrix or Remote Desktop (Terminal Servers) log out of the server.
- Shut down the device, PC, laptop, tablet, thin client.
- Do not let the user logon somewhere else. They are very likely to reopen the same email and start a second infection.
- Contact your IT support immediately. Citrix/Remote desktop users should also immediately alert support that they are Citrix/Remote desktop users.

5.3 Review File access permissions

Review what network resources staff have access to. Often permissions are set only because someone “should not see” something. It is better to ask, do they need to see this, if the answer is “no” remove the permissions.

5.4 Be open and accepting

Sooner or later someone will get fooled into enabling an encryption attack. The sooner you know the sooner you can react. Staff will need to feel they can put their hand up when something goes wrong.

5.5 Know the signs

There are two key signs of an encryption attack.

- One is the notification to pay a ransom.
- Two is that you can't open documents.

No one should ever ignore either of these signs. The sooner you realise there is a problem, the sooner the damage can be limited.

6 What can I do to stop CryptoLocker?

6.1 Awareness

The first line of defence will always be awareness.

- Have a documented policy on opening and dealing with suspect emails.
- Just like OHS, make sure you have a program of awareness. Regularly remind company email users about the policy, arm them with details about identifying suspect emails.

6.2 Use a Cloud Based Mail Scrubber

Cloud based mail scrubbers scan and disinfect or block email before reaching your network. The advantages of using an external scrubber are:

- Dedicated team monitoring, managing and reacting to new varieties.
- Often use early release versions of updates.

Likely impact:

- Some false positives will require whitelisting.

Protection improvement:

- Moderate to high.
- Best effectiveness is against known threats.

6.3 Increase Anti-Virus settings

All good anti-virus products will include a feature that scans the behaviour of applications. Behavioural Analysis is an important tool in detecting and blocking new variants.

Note:

Feature names and settings will vary between products. These settings are not always the highest available. They have been chosen to give a high level of protection without necessarily over burdening the device. The introduction of these setting will most likely result in some disruption. Applications and websites will need to be whitelisted and in some cases, some features may need to be reduced or removed. Network (Traffic) scanning and Firewalling may need to be disabled in some situations. Laptop users will need to test Wi-Fi and remote access. Behavioural Analysis should not be disabled or have its levels reduced. It is highly likely that exclusions will be needed.

The following settings are recommended:

On Access settings:

- On detection: disinfect, quarantine or deny access.
- File types: All types
- Maximum size: 100 mbps.
- Archive scanning: Maximum size 100 mbps, maximum depth 4.
- Scan Boot sectors.
- Scan for key loggers.
- Do not scan mapped drives
- Scan USB drives.
  - Do not scan attached devices larger than 250GB
  - Prompt before scanning attached drives.

Behavioural Analysis:

- Set to highest available levels.

Content Control/Internet access:

- Block File Sharing
- Block Scams
- Block Web Proxy

Network scanning (note this is traffic, not mapped drives):

- Scan HTTP and SSL Traffic
- Scan SMTP and POP
- Enable browser search advisor and plugin

Anti-Phishing:

- Enabled and set to highest.

Firewalling:

- Disabled: Unless it integrates with Behavioural Analysis. If it integrates, enable and monitor wireless.

Updates:

- Check every hour
- Use an update server
- Allow internet updates if update server unavailable for 2 hours

Likely Impact:

- Most applications will still run. But some white lists will be required.
- Will require some planning and testing.
- Low specification or aging devices will run slower.

Protection improvement:

- High to Very High depending on the software. Highly recommended.
- Behavioural Analysis is useful for new (zero hour) threats.

6.4 Enable UAC (User Access Control)

UAC (User Access Control) prompts the user for permission when certain settings are being changed. With UAC enabled the user has an increased opportunity to be aware that changes are taking place without their knowledge.

- Set UAC to “Always notify”

Likely Impact:

- All most all applications will still run.
- User will likely be interrupted by some updates and when starting some applications.

Protection improvement:

- Moderate to High.
  - Some ransomware can still run without making changes.
  - Users can still approve the software to run. This does not protect against poor decisions.

6.5 Remove Local Administrator Rights

It’s common for users to have local administrator rights on their PC though Domain Users group. These rights empower the user to customise the machine more to their work habits. However, the user’s rights are also available to any applications they run. Effectively making any ransomware an administrator.

- Remove local Administrator rights from domain users.
- If needed make explicit users local administrators.

Likely Impact:

- All most all applications will still run.
- Some changes users make maybe lost at the next boot.

Protection improvement:

- Moderate to high: Highly recommended.
- Some ransomware can still run without user permissions.

6.6 Remove Domain Administrator Rights

Some staff that undertake network tasks such as resetting passwords or checking backups will have Domain Administrator rights assigned to their login accounts. The majority of work undertaken by internal IT support staff does not require Domain administrator privileges. These privileges give any ransomware access to a larger pool of data for encryption.

- All IT staff should have two accounts. Their personal login on account (associated with email etc) which has standard network rights and a separate administer account used only when undertaking Domain administrative tasks.

Likely Impact:

- Very low. IT staff will complain, but the inconvenience is extremely low.

Protection improvement.

- High.

Rule of thumb. If the account has a mailbox associated with it, it should not have Domain admin rights

6.7 Apply Software Restriction Policies

Software Restriction Policies utilise AppLocker to control what and how applications run. An example is blocking an application which tries to run from the internet temp folder. To be effective AppLocker

needs to block everything and then create rules to allow. Setup will result in some false positives and require testing.

- Enable AppLocker and block applications form running from Internet and Temp folders.

Likely Impact:

- Will likely result in false positives requiring rule changes.
- Will require planning and testing during deployment.

Protection Improvement:

- High to Very High.

6.8 Ensure patch status are current

Application vendors are constantly releasing updates. Keeping your devices up to date is a key component in protection.

- Regular patching and reporting on devices.

Likely Impact:

- Low. PC's can be patched after hours. Laptop user will experience occasional slowdowns.

Protection improvement:

- High. Highly recommended.

6.9 Enforce Macro policies

A common delivery method is malicious Macros embedded inside of Word and Excel documents. Group Policies can be used to disable the automated executions of Macros unless the document is in a trusted location.

- Use trusted Locations and disabled macros settings.

Likely impact:

- Low for most users. Some sectors that make extensive use of macros (legal for example) will require more planning and testing.

Protection Improvement:

- Moderate to High. Effective only against embedded macros. Users can still choose to activate the macro.

Instruction inserted into an email on how to activate the macro inside the attachment.

6.10 Restrict File access

CryptoLocker can only encrypt data it has access to. Reviewing network share rights to remove unnecessary access, reduces the target area.

- Review and restrict network file access.

Likely impact:

- Low. But the process may take some time to complete.

Protection improvement:

- Moderate. It does not stop infection but does control the damage.

6.11 Web Protection Solutions

There are software solutions which scan your internet browsing and will block infected sites. Some antivirus applications include a slimmed down version of this.

- Install Web scanning solution.

Likely impact:

- Low. Some sites may require white listing.

Protection improvement.

- Moderate. Effective against known threats.

6.12 Hide Shares

Some CryptoLockers are reported to seek out and attack shares. Hiding all network shares reduces the impact area.

Likely impact:

- Low. IT staff may resist as it may introduce small conveniences for them.

Protection improvement

- Moderate to High.

6.13 Protect backup Locations

When you are hit by CryptoLocker, you will be restoring. Currently, CryptoLockers do not appear to encrypt backup files. It is however sensible to check that access to the backup location is restricted.

6.14 Turn on Shadow Copies

The effectiveness of this is open to debate. But we have heard that in some case documents can be salvaged form the shadow copy. As shadow copy location should always have a size limit the effectiveness maybe restricted.

Volumes holding documents should have shadow copy enabled.

6.15 Advanced Persistent Threat Detection

If your Firewall supports Advanced Persistent Threat (ATP) detection or can be upgraded to do so. This is highly recommended. APT features will vary between manufactures. WatchGuard's for example include a feature that will send attachments with unknown code to a cloud sandbox. The attachment is then activated and its actions tracked. If its starts scanning drives or encrypting files, the mail is blocked.