VerticalStructure

JUNE 2021

RANSOMWARE

A guide to prevent and survive

Prepared by: Gillian Colan-O'Leary
Vertical Structure Ltd

WHAT IS RANSOMWARE?

Ransomware is a form of malicious software that encrypts a victim's files.

THE IMPACT OF AN ATTACK

The attacker will demand a ransom to restore access to the data upon payment. What could happen:

- Loss of earnings
- ICO / GDPR fine
- Loss of reputation

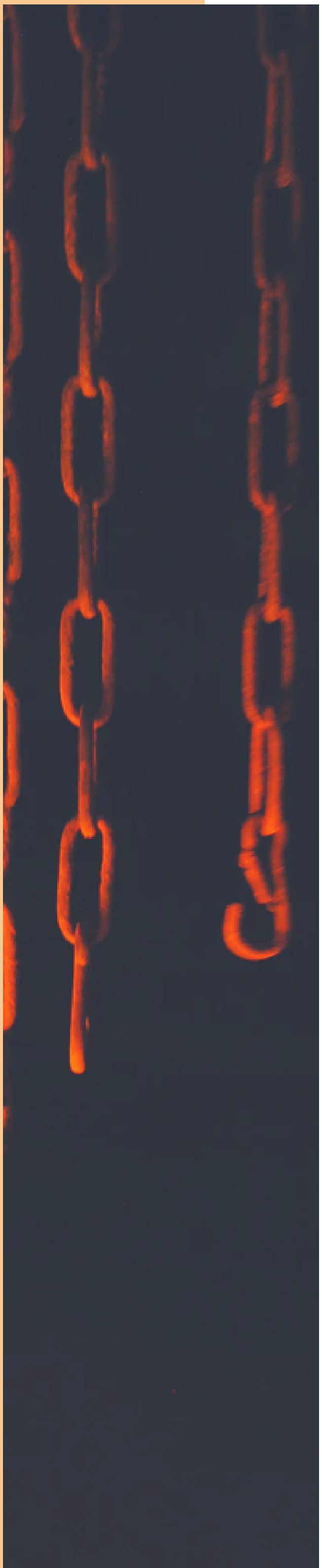
BE PREPARED

Any organisation can be a victim

- Appoint someone with a clear responsibility for the data, for e.g., a data controller
- Make sure you know what a breach looks like
  - ICO definition: "a breach is more than just about losing personal data"
- Understand your own data and the risks related
  - Carry out a data audit - this is a requirement for data protection. It should be done by everyone!
- Have an understanding of what your suppliers are contracted to provide as a service
  - Who are they?
  - What do they provide?
  - How do they provide it?
  - Joint controller/processor?
- Investigate and take out cyber insurance
- Practice what you would do if something was to go wrong with your Disaster Recover and Business Continuity Plan.

A backup isn't a backup until it's tested

HOW WE CAN HELP: **Our team can guide you through creating effective processes to meet requirements of ISO27001 certification (international standard on how to manage information security).**



HOW TO PREVENT #1

Empower your people to be the first line of defence

- PASSWORDS! Have a password policy and make sure **all** staff are adhering to it
- Multi factor authentication for all devices and applications (where appropriate)
- Social engineering awareness - phishing emails are one of the main ways ransomware makes it ways on to servers.

HOW WE CAN HELP: **We can ensure your team is cyber aware, whatever their role. We run Security & Social Engineering Awareness training for non technical staff.**

HOW TO PREVENT #2

KEEP YOUR NETWORK SAFE

3 technology tools to keep you secure:

- **Patches** (or updates) for software close vulnerabilities before attackers can exploit them. Don't ignore prompts to update!
- Love your **firewalls**! Unpatched firewalls are easily compromised
- Install **anti virus** to prevent, scan, detect and delete viruses from a machines.

HOW WE CAN HELP: **We can carry out testing to make sure systems are properly patched. We can run phishing simulations to make sure your staff are aware of this threat.**

HOW TO PREVENT #3

SERVERS

Using managed service providers

If you engage a managed service provider check exactly what service is being provided and whether it is reactive or proactive. For instance is anti virus being installed? They are one of your key suppliers. Make sure you

- Speak to them regularly - be on first name terms!
- Audit them if you want to
- Check your agreements - it's best to be aware of each other's responsibilities.

On premise - do you have servers in your office?

If your servers are on premise make sure:

- You have the right resource to manage them (usually in the form of a dedicated systems administrator). If not consider if "on prem" is the best option!
- Practice what you would do if something went wrong.

HOW WE CAN HELP: **We can facilitate workshops such as Exercise in a Box and Digital Decisions & Disruptions.**

HOW TO PREVENT #4

WORKING FROM HOME - REMOTE DESKTOPS (RDP) & VIRTUAL PRIVATE NETWORKS (VPN)

Never, ever allow RDP directly from the internet.
Like ever.
Seriously - never.

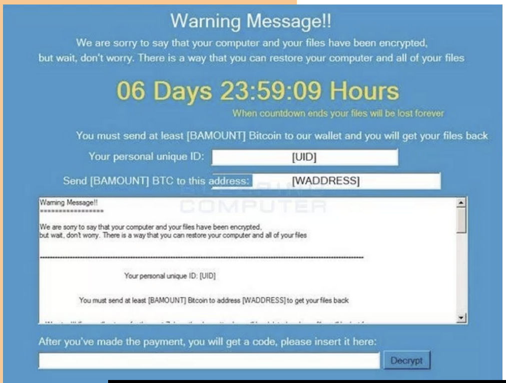
Accessing your servers' or workstations' desktops remotely is a great way to manage them. Unfortunately it's also a huge target for bad actors.

Rather, set up a VPN to establish a secure connection between you and the internet. All your data traffic is routed through an encrypted virtual tunnel, securing against external attacks.

HOW WE CAN HELP: We can test your cloud infrastructure. We can then advise you on what actions are needed to make it more secure.

IF YOU'RE A VICTIM

WHAT TO DO.... AND WHAT NOT TO DO



Warning Message!!

We are sorry to say that your computer and your files have been encrypted,
but wait, don't worry. There is a way that you can restore your computer and all of your files

06 Days 23:59:09 Hours

When countdown ends your files will be lost forever

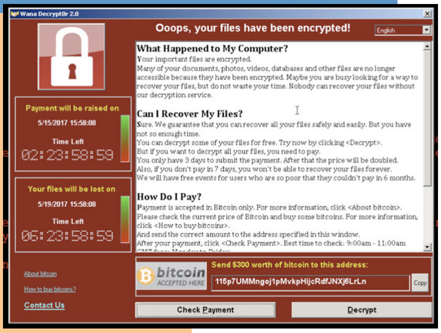
You must send at least [BAMOUNT] Bitcoin to our wallet and you will get your files back

Your personal unique ID: [UID]

Send [BAMOUNT] BTC to this address: [WADDRESS]

```
Warning Message!!
*****************

We are sorry to say that your computer and your files have been encrypted.
but wait, dont worry. There is a way that you can restore your computer and all of your files

-----------------------------------------------------------------------------

                    Your personal unique ID: [UID]

          You must send at least [BAMOUNT] Bitcoin to address [WADDRESS] to get your files back
```

After you've made the payment, you will get a code, please insert it here:



Ooops, your files have been encrypted!

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

You should speak to:

- Your insurance provider straight away – they can help
- The ICO (within 72 hours of becoming aware of the breach) if appropriate
- The PSNI / Action Fraud – this is a crime and needs to be reported
- **The Vertical Structure team - we have experience of dealing with ransomware attacks.**

Do not

- **Do not delete evidence of attack in process of restoring!** The evidence might help with the investigation into how and when you were compromised
- Don’t go back too early - it’s vital to discover when the compromise happened, if you restore too early you could be bringing the attacker back into the network.

HOW WE CAN HELP: **We provide guidance and support on what to do and who to speak to.**

SUMMARY

WE CAN HELP

Ransomware attacks are on the rise. But we can:

- Help you prevent attacks (cyber awareness and social engineering training)
- Advise on processes, technologies and tools to keep you safe
- Make sure you're prepared to handle an attack
- Support your organisation if it is the unfortunate victim of an attack.

Please get in touch:
hello@verticalstructure.com