YOUR MONEY OR YOUR DATA!

The Issue of Ransomware

Ransomware has become the modus operandi of cybercriminals in the last five years. Names like CryptoLocker, WannaCry and Petya have become synonymous with cyberattack, being at the heart of the most devastating and high-profile recent cases of cybercrime. It's basically a bully's game and it's become the hottest game in the cyberspace playground.

Put simply, **ransomware (or ransom malware) is a type of malware which blocks you from operating your system, accessing your files, or reading them until you pay a fee. Mostly, it doesn't involve any actual theft of data**, but rather just holding that data 'functionally' to ransom.

This article outlines the key types of ransomware, how to deal with an attack, and how best to reduce the risk in the first place.

YOUR MONEY OR YOUR DATA!
The Issue of Ransomware

We will firstly consider only the majority of cases in which no data theft has taken place. However, new up-and-coming variants of ransomware are introducing blackmail into the equation, either through public shaming or data theft. So, we will later consider the practical and ethical conundrum presented in this much tougher situation.

TYPES OF RANSOMWARE

There are three main types of ransomware. In order of increasing severity they are: **fake Ransomware (or 'Scareware'), Screen-locking Ransomware, and Encryption Ransomware.**

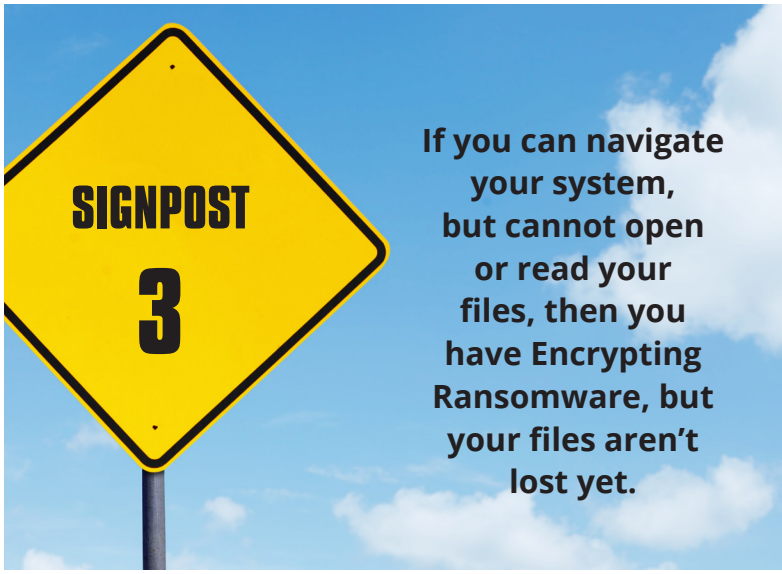
As the name suggests, **Scareware is a charade to make a user believe their system is infected**. The most common symptom is a ransom note which the user is unable to remove, and sometimes bombardment by software claiming to be an anti-malware program and demanding a pay-out to remove an 'infection'. It's all an elaborate ruse, designed to scare the user into making a pay-out for absolutely nothing. This gives us our first signpost.

This is as good a reason as any to follow the advice: Don't panic!

The second type of ransomware is the screen-locking type. This is characterised by an inability to get past the ransom note. Essentially you can't do anything at all. Often, these ransom notes will pretend to be from an authority (such as a federal agency or Revenue and Customs) and will demand you to pay a fine, normally for something illegal they claim you have done. Of course, you will know if this is untrue. But either way, **if it's a screen-lock, your files aren't lost – or even locked – it's just that you can't get to them.**

Again, don't panic!

It's the third type where we can start worrying: **Encryption Ransomware is the real thing**. In this case, you will likely be able to navigate your system, browse through apps and see all your files as normal, but nothing will be openable or readable. You will still get a ransom note, normally specifying a time limit before either radio silence (meaning you cannot get the decryption key) or file deletion – either way, your files are irreversibly gone. **This is the most serious situation, but it still doesn't warrant panic just yet, and you need to keep a level head to enter into negotiation with your attacker.**



HOW TO DEAL WITH RANSOMWARE

So, with the different types now clear, let's walk through what you should do in the event of an attack.

Initial Response

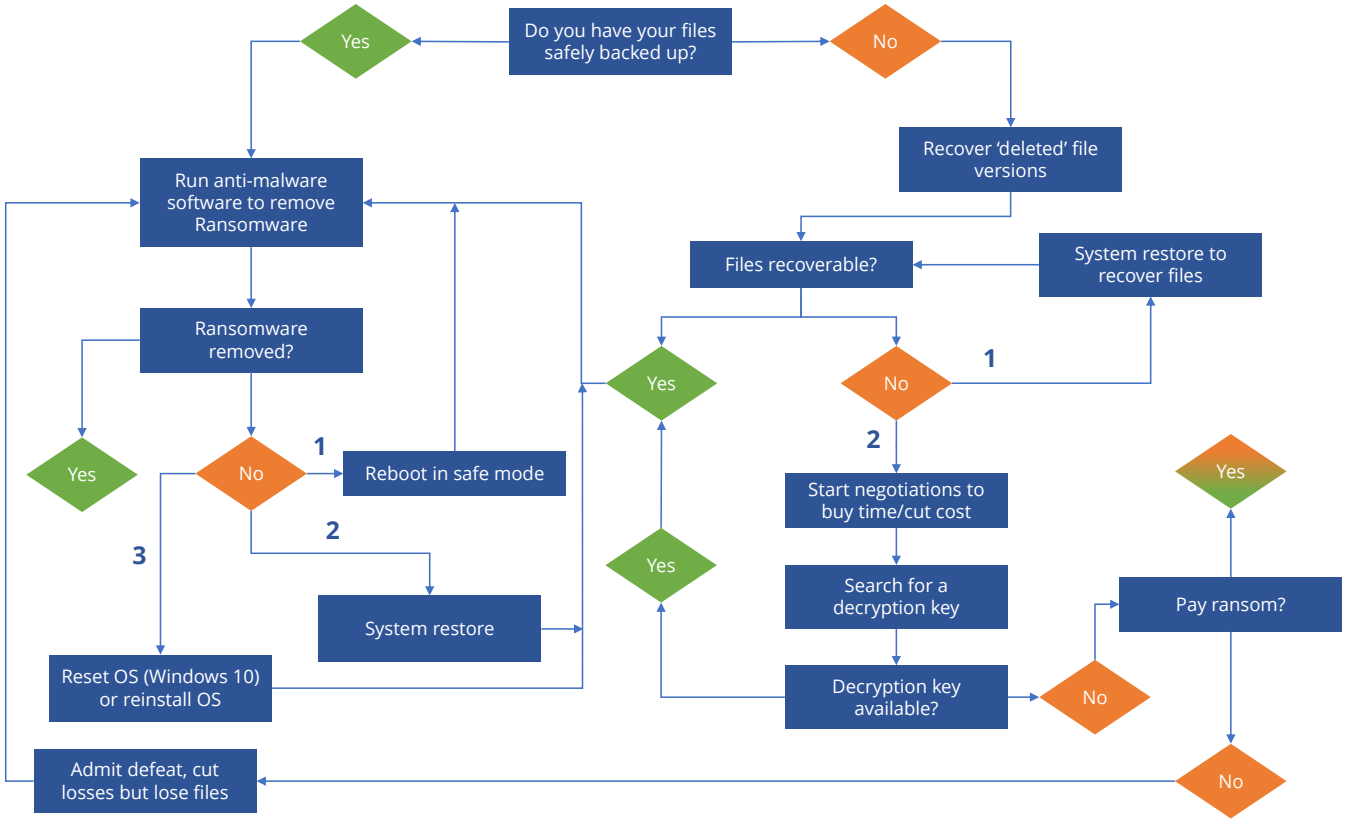
Before you do anything else, isolate the case! Any machine infected will likely be connected to a network and infection spreading must be stopped. Networks with well-designed security infrastructure will have 'compartments', such that there is segregation between different parts of the network and any infection can only spread so far.

Nevertheless, the first item on the response agenda is to **disconnect the infected machine** from others, and additionally from any local servers, external drives and the internet. **This is especially important if backups are stored on connected platforms** (via external hard drives or online storage places such as Dropbox).

Next, identify the ransomware type and any demands being made and by whom. It is important to **document everything**, including photographing the ransom note with your phone. This will not only help security experts identify solutions, but will also be needed to **file a police report afterwards**, which could be necessary for any insurance claim.

You also need to **plan your move**: you've essentially entered into a delicate game of anonymous chess. You can use our decision flow chart on the next page to help you with this and decide which strategy you are going to take.

Choosing a Strategy



Your first step in choosing a strategy rests on your backup situation. Do you have one? Is it secure? Cybercriminals search for data backups not only as a way in, but if they are looking to ransom data, then also as a target to encrypt. **If you have a safe backup, the attack is futile** and your victory is but a few steps away.

Essentially, if safe backup is confirmed, you can go ahead and remove the ransomware. Some difficulties may still arise; removing ransomware isn't always as easy as running anti-malware software. You may need to reboot your system in safe mode before running any software, and in the worst case you may have to reset or reinstall your operating system (OS). The latter will, of course, result in losing your files, but if you have a safe backup this isn't a problem.

If you don't have a safe backup because it's either out of date or has been compromised, then you have a battle ahead, but all is not lost.

If you are dealing with Screen-locking Ransomware, then your data is fine, you just need to remove the malware without compromising your files. A number of options are available depending on the tenacity of the malware, but **usually running anti-malware software in system safe mode is sufficient**. If not, then a system restore to the last point of normal activity is the next best thing. Before considering resetting or reinstalling an OS, which will remove your files, **contact cybersecurity experts who will almost always be able to remove this type of infection without a problem**.

If you have encrypting ransomware, this is much trickier, because your files are already compromised and you need a key to uncompromise them.

The first avenue to try is recovering 'deleted' files. Often, in the process of encryption, the malware will first copy, then encrypt your files and then delete the originals. It may, therefore, be possible to

recover the deleted versions. If you don't have the available technical expertise on call to do this, then software which can be found online may be of help.

If this doesn't work, then you must enter into negotiations as soon as possible. Details and advice on negotiating will be covered extensively in the next section, but what is important at this stage is to **buy yourself time**. This time will allow you or a technical team to **search for a decryption key** for the encrypted files. Many encryptions are not unique, but rather reused and recycled, so there is a possibility of finding the corresponding key. One such tool for doing this can be found at 'No More Ransom!'[1]. Created by a joint partnership between top cybersecurity specialists, this tool offers a wealth of information on ransomware (and reporting it), in addition to a decryption key searching facility.

It is, however, possible that the key is custom made and so no amount of searching will yield a result. At this point you must engage in negotiations properly and ultimately **decide whether or not your files are worth paying the ransom**. It is important to realise that this is **not just about whether you can afford the ransom** (which, if you have insurance against such things, might sound like a trivial question), but you also have to consider the potential consequences. For example, **paying a ransom might make you vulnerable to repeat attacks** even from other cybercriminals in the 'community', and might result in higher ransom amounts being demanded. Furthermore, **there is no guarantee that your files will be unlocked once you pay** – they are criminals after all. However, if your attacker is a serious cybercriminal, they are actually more likely to release your files to maintain a reputation: if future victims don't think they will have their files returned, why would they even entertain the notion of paying a ransom fee?

There are other things to consider too: the ethics of paying a criminal to avoid a data loss scandal, for example. Will you be encouraging them to continue, putting others (and yourself again) at risk? Is paying the criminal even legal in your jurisdiction? Doing so was illegal in the US until a very recent policy change made by the FBI[2].

Most big cybersecurity firms[3] and government agencies still maintain the stance that ransoms should not be paid, but now admit that paying has to remain an option, especially where such malware is crippling an organisation. They also now recognise that **security professionals are able to verify the functionality of decryption keys and ensure that malware is effectively removed** to prevent immediate reinfection.

Entering into Negotiation

Negotiating a ransom fee – whether it be data, a physical object of value, or a person – has always been a delicate balancing act. The key questions to ask yourself are:

1. **How much am I willing to pay** (realistically) and what do I think is the lowest fee my attacker is willing to accept?
2. What type of attacker do I have – **what are their motivations?** Are they likely to walk away with the key or do they really just want my money?
3. **Am I willing to walk away** from my data?

There are many similarities to real-life hostage scenarios, including the psychology around negotiating, and much that can be learnt from the wealth of information available on this[4]. The global trends are also mirrored, for example, with the changing stances of insurers, experts and government agencies on paying real-life ransoms[5].

[1] https://www.nomoreransom.org/
[2] https://www.theregister.co.uk/2019/10/03/fbi_softens_stance_on_ransomware/
[3] See, for example, Malwarebytes: https://www.malwarebytes.com/ransomware/
[4] See, for example: https://www.nytimes.com/2015/04/19/magazine/how-to-negotiate-a-ransom.html for general ransoms, and https://www.ft.com/content/1f3917ae-ca59-11e9-af46-b09e8bfe60c0 for data specific
[5] See, for example: https://www.theguardian.com/news/2019/jan/25/business-of-kidnapping-inside-the-secret-world-of-hostage-negotiation-ransom-insurance

The first piece of valuable advice we can take is that **the main negotiator should not be the person who values the 'hostage'** (or in the cyber case, 'the data') the most. In real life, the person best placed to negotiate is a distant relative, or family friend, but with the strategist behind them being a third party – someone with little to no connection to the victim. The parallel then is that **the chief negotiator might be someone in the company, but not the owner of that particular data set** (assuming the ransomware has been isolated to a part of the network) and **the strategist should be a consultant or third-party security expert**.

The financially driven hostage scenario is widely considered to be the simplest of cases (where the motivation isn't politically, personally, or espionage driven) because it is essentially a cost-benefit balance and **everyone wants the hostage kept alive** (or in the cyber case, at least the illusion that the data is safe). This can be used to the advantage of the victim when negotiating, yielding tactic 1:

TACTIC 1

Start by asking your attacker to prove your data is still safe, and not already deleted or irreversibly damaged. Doing this not only proves it's worth your time and money to negotiate a ransom, but is also one way of buying time.

This **evidence could be in the form of a small data sample** – two or three files you provide them with that they will decrypt to prove that they are able to do so. This is the equivalent of what in the real world is called **a 'proof-of-life' question** – a question that can only be answered by the person being held hostage. In the case of data theft (see section 'Ransomware Involving Blackmail') an even more direct comparison can be made: you can **ask the attacker for proof-of-theft**, since they may be bluffing. This might involve them showing you some of your data they have stolen (after first decrypting it) or answering a question which could only be answered by looking at the contents of the files.

Another parallel with real-world hostage scenarios is that **the perpetrator doesn't want to drag out the situation** indefinitely because as time passes, something is more likely to go wrong for them and all the while they are not gaining any money. This needs tact: too long and the attacker may just walk away with your locked data, but they also might settle for a lower fee to cut their own losses. It is, however, important to take your time; the essence of tactic 2:

TACTIC 2

Never settle for a sum too soon, even if you are comfortable with the amount being requested. Doing so makes you vulnerable to repeat attacks and higher fees next time.

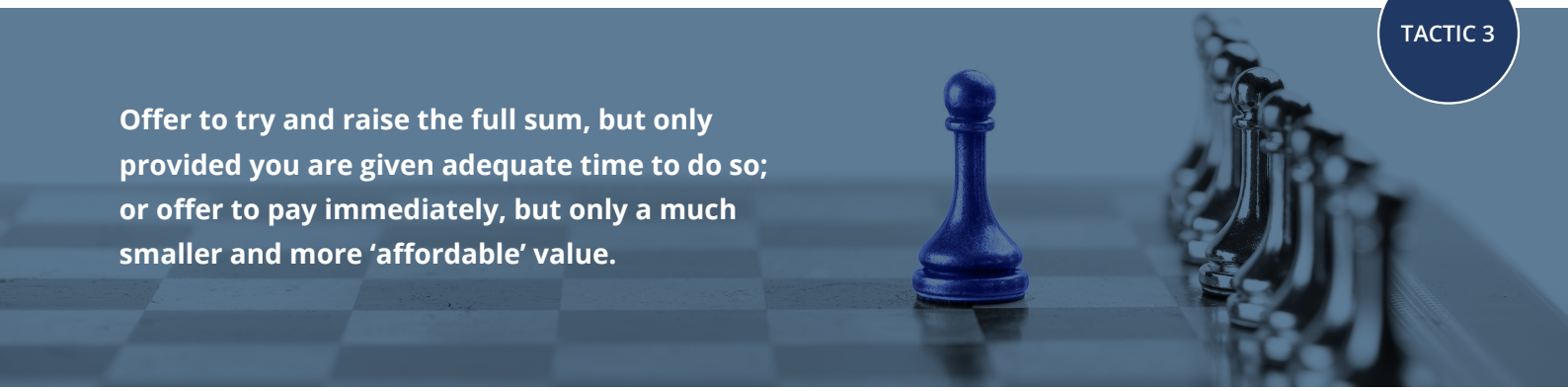
To ascertain an appropriate counteroffer, **research should be done on similar scenarios** (similar types of attacker, similar types of data) to see what others have eventually paid or been asked for. **Your adversary will have done this.** They will have researched your business and the type of data you have; they will have a good idea of its value, sensitivity and worth in terms of your reputation. They will also know if a breach is likely to attract fines from legislation such as GDPR.

These are, of course, all things you should think about as well: there's no point in offering an amount lower than the fine imposed by data protection legislation for example. **You must avoid making a poorly judged counteroffer** – whether it be too high or too low. Once your first counteroffer is made, the rest are far easier, as in any bartering scenario.

An alternative strategy here is to provide a 'double offer': that is, an immediate offer and a delayed offer. Known as the 'time-wedge', this can be an excellent way to buy time and is explicated by tactic 3:

TACTIC 3

Offer to try and raise the full sum, but only provided you are given adequate time to do so; or offer to pay immediately, but only a much smaller and more 'affordable' value.

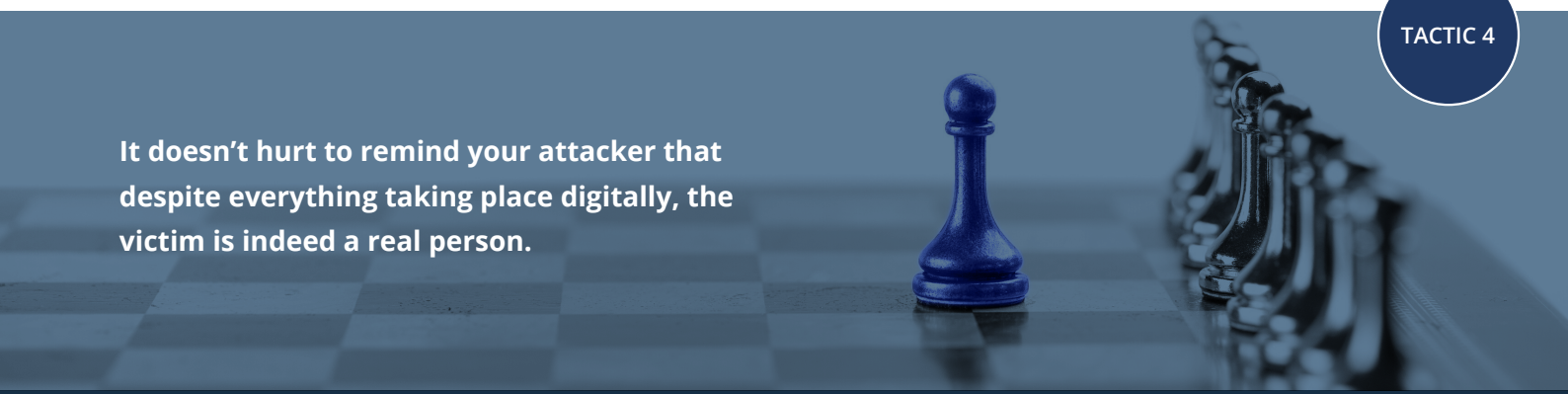


Cybercriminals always demand payment via cryptocurrency, one example being Bitcoin. This can make it difficult to do anything with any speed when it comes to ransom transactions, not only because few businesses hold such currencies, but also because the transactions are not instant. It is, therefore, a good idea to **have your IT security provider hold some funds in cryptocurrency** for this very purpose. You should also **use a 'Burner Wallet'**: essentially a throwaway wallet with set funds where the transactions can be made digitally via QR codes. This method can improve transaction times and also increase security and anonymity.

One of the biggest differences between real-world and cyber hostage scenarios is that it is very easy for the attacker to de-humanise the victim because they make no real-world connection with them. There is, therefore, a much **lower chance of any empathy for the victim**. However, this can be improved by an ongoing negotiation process, and by tactic 4:

TACTIC 4

It doesn't hurt to remind your attacker that despite everything taking place digitally, the victim is indeed a real person.



This should be subtle and definitely not overbearing (the empathetic capacity of criminals is, at the end of the day, limited). And remember, **this communication should still not be made by the victim**, because they are more susceptible to emotionally driven, impulsive decisions which might compromise the negotiation.

This brings us to tactic 5:

Irritating your attacker will get you nowhere and may cause them to act irrationally, even if it's not in their own best interests. **This professionalism should also carry over to delivery.** If you decide to pay the ransom, **be prepared to act quickly and efficiently**. If you don't have funds in cryptocurrency and don't have a planned response for obtaining and transferring funds, this delay will be exacerbated by the fact that your systems may be offline for days or weeks while negotiations are ongoing.

In real life, the logistics often involve cash drops, or handovers, depending on the scale of the situation. Similarly, **you will need a competent financial and IT security team, alongside cybersecurity professionals**, to assist with anonymous online payments using cryptocurrencies in a timely and accurate fashion. If anything goes wrong, it could all have been for nothing.

PREPARING FOR AN ATTACK

Be prepared. It might be the motto of Boy Scouts, but this is the best advice that can be offered.

Proactivity is Paramount

Prepare for an attack. After all, there is no getting away from the fact that their frequency is increasing. As made clear earlier, the single most critical way to prepare for an attack is to **create a safe backup of all your data**. Then make a backup of this backup. Then make a backup of that and put it in a shoebox in your wardrobe.

The last point is in fact half serious: a completely offline, physical hard drive (or disconnected server) stored in a safe place is the ultimate form of backup.

Other advice for backup safekeeping includes:

- **Do not leave external hard drive backups connected to machines**, especially those with network connections
- **Use a variety of backup methods**, such as external hard drives, local servers, and cloud-based platforms
- **Use backups with available encryption services and multi-factor authentication** (particularly important for cloud storage)

- **Do not rely on cloud storage**, because they often have auto-synchronising features; after infection, encrypted files may be copied onto your cloud backup resulting in backup file loss

In addition to backing up, try to **restrict lateral movement of an infection**. As mentioned before, **try to compartmentalise your network so that different areas are segregated**. This will reduce the chance of a 'global' infection across your network. This is becoming increasingly important, since **attackers are now penetrating networks more deeply prior to activating ransomware**, spending on average a minimum of three days compromising different machines and systems[6], This 'dwell time' also allows the intruders to explore their victim's network and organisation, gathering critical intelligence on their capacity to negotiate a ransom fee. **Knowledge is certainly power in this situation.**

This organisation exploration can also inform attackers of high-privilege users, so it can be useful for organisations to restrict the number of these – **adopt a 'Principle of Least Privilege' approach**. Those who do have high privileges should be mindful not to use administrative accounts for internet browsing or email access, and instead have a separate account for all such 'normal' activities.

Of course, **all normal guidance for reducing data breaches applies**, such as keeping operating systems up to date, implementing permission for application execution, filtering incoming mail, and so on. Ransomware attacks search for system vulnerabilities to execute code, so **organisations would certainly benefit from Vulnerability Assessments and Penetration Tests** offered by cybersecurity providers. One such example of this is the Compromise Assessment[7] offered by Cyber Citadel. This assessment provides a comprehensive evaluation of environmental risks, security incidents and ongoing threat activity in a network environment.

Reactivity is Also Important

Having a **strong incident response process** is also crucial to dealing efficiently with a ransomware attack. This will involve quickly and effectively implementing the initial response measures previously discussed, and will also engage with the ransom response strategy, enlisting all necessary internal and third-party personnel required to deal with the incident.

If paying the ransom is an option your company keeps on the negotiating table, then **a payment team should immediately be established** to set up an appropriate fund in a cryptocurrency and a line through which that payment can be made (such as a 'Burner Wallet').

Preparing in advance will reduce stress throughout the response process and help keep everyone involved calm and level-headed.

[6] FireEye (March 2020): https://www.fireeye.com/blog/threat-research/2020/03/they-come-in-the-night-ransomware-deployment-trends.html
[7] https://www.cybercitadel.com/d/Cyber-Citadel-Compromise-Assessment-Datasheet.pdf

RANSOMWARE INVOLVING BLACKMAIL

Recent developments in the ransomware community have sought to counter the effective defence strategy of creating multiple backups. This development is to actually steal your data, in addition to encrypting your copy of it. The result is that **attackers are now able to blackmail organisations into paying ransom** by threatening to either 'name and shame' them publicly and, if that still doesn't force a pay-out, by threatening to publish or sell data online.

This isn't strictly new. In the past, cyber criminals had threatened organisations with this, but never followed through with it. That all changed with **Maze, a new type of ransomware which implemented these threats** in late 2019. And it used both tactics: publishing data as well as 'naming and shaming'. The latter can be more dangerous than it sounds, especially if the data is sensitive or personal, because such a data breach has potentially huge legal implications.

Others have followed suit. A ransomware named Sodinokibi (also known as REvil) was used to attack Travelex in early 2020, who at the time masked the event as a 'planned maintenance' issue. This left them extremely vulnerable to 'name and shame' blackmail, made worse by the fact that the nature of their data is sensitive financial information.

Though it was not admitted publicly by Travelex, the *Wall Street Journal* reported that a payout of USD 2.3 million was made to REvil in order to prevent release of sensitive data online[8]. This confirms one thing: **ransomware has elevated itself from a low-level money-grabbing business to an international multi-million-dollar extortion enterprise**.

In this case, many ethical questions were raised.

Should Travelex have hidden the breach in the first place? Revealing the breach may have allowed customers to respond by changing passwords and security details to protect accounts, and in addition provided the attackers with less blackmail material.

Should Travelex have paid the ransom? This may have flagged them for future attacks, since it seems they were unable to mitigate it and were susceptible to such blackmail tactics. Nevertheless, their options were limited, because the fallout from publication of such personal financial data would have been catastrophic. There is no one 'right' answer to this.

If this teaches organisations one thing, it's that if they didn't think so before, **cybersecurity is now definitely worth the investment**. Although immediate benefits may not be seen, as with insurance, the alternative is the potential for millions of dollars in losses. It certainly is worth the time and (considerably less) money investing upfront in cybersecurity and all statistics suggest, the sooner the better.

[8] https://www.wsj.com/articles/travelex-paid-hackers-multimillion-dollar-ransom-before-hitting-new-obstacles-11586440800?mod=business_major_pos7

Cyber Citadel

Get in touch:
info@cybercitadel.com

www.cybercitadel.com