JUMPSEC

THE IMPORTANCE OF TRUST IN THE BUSINESS OF – AND DEFENCE AGAINST – RANSOMWARE ATTACKS

Our address
Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

Give us a call
0333 939 8080

Send us a message
hello@jumpsec.com

Find out more
www.jumpsec.com

Arguably the greatest threat to organisations in 2021 is ransomware.

At JUMPSEC, we partner with organisations for whom ransomware is a top concern, helping them to build real resilience to these threats without relying on cyber insurance alone.

This article is the second in a series exploring the risks posed by ransomware attacks, and how organisations can undertake targeted activities to protect against attackers leveraging ransomware as the means of achieving their objectives.

Introduction

As discussed in our previous article, ransomware attacks are one of the greatest security threats faced by organisations today, with a host of consequences for the victims and their customers.

At the time of writing, 2021 has seen approx. $42 million of ransomware payments made according to the fantastic ransomwhe.re site (not accounting for untraceable payments such as those made via Monero). **When I started writing this article a week ago, it stood at $37 million.**

> **The ransomewhe.re site was created by Jack Cable, a security architect at Krebs Stamos Group, in response to a tweet from Red Canary Director of Intel Katie Nickels, who stated that it was impossible to gauge the real impact of losses tied to the notorious TrickBot malware. As a result, it was difficult to know whether specific victim actions - like paying or refusing to pay ransoms - makes a real difference.**

Taking a step back for a moment, it's interesting to ponder the fact that we need to track payments directly to have a trustworthy record of which organisations have been ransomed, and which ones have actually paid. Because the disclosure of a ransomware attack has a reputational impact on the victim, there is a clear incentive to keep quiet. Similarly, security professionals who discover such breaches are discouraged from divulging attacks which are not yet in the public domain, no doubt dissuaded by confidentiality agreements and the threat of legal action.

The lack of transparency fuels an environment where victim organisations can be motivated to disguise and downplay a breach. **As this article will explore, this creates a situation where the lines between the good guys and the bad become blurred. This, for me, is the most fundamental problem to be tackled in the fight against ransomware.**

Kaseya: a post-mortem

Consider the recent controversy with Kaseya, for example, who have **denied paying a ransom for a universal decryptor from REvil after days of lingering questions about how the tool was obtained** vaguely announcing that it had been provided by **'a third-party'.**

Even though approximately **50 direct customers, and between 800 and 1,500 businesses down the chain** were affected, Kaseya began to downplay the attack shortly after engaging third-party incident management and response support. In a **press release on July 6th**, Kaseya stated that the **'sophisticated'** attack affected less than 0.1% of its customers, claiming it 'was never a threat nor had any impact to critical infrastructure' – stressing effective containment and a return to business-as-usual. **This is despite the fact that many organisations were severely impacted.** For example, Coop, one of the primary food suppliers in Scandinavia, saw 800 stores in Sweden unable to transact for a number of days.

The situation is made worse by allegations that software engineering and development employees at Kaseya's U.S. offices had brought up a laundry list of "wide-ranging cybersecurity concerns" to company leaders multiple times from 2017 to 2020, with Kaseya allegedly dismissing a 40-page security memo detailing these concerns as 'speculation'.

The Kaseya situation is a case study in how NOT to build trust. Anyone experienced in enterprise crisis management can recognise the signs of denying accountability and downplaying the impact of an incident to save face and dodge criticism. It's disheartening to see this type of strategy in action time and again and contributes to the atmosphere of distrust and scepticism following a cyber breach.

Isn't it strange how cyber attacks are always reported as being sophisticated? Whilst the magnitude and scale of the Kaseya breach points to it having a reasonable level of sophistication, in our experience the majority of ransomware breaches are far from sophisticated. It is obviously always in the interests of a victim to claim that the attack was sophisticated – nobody is going to blame you if the attack was so advanced that you couldn't hope to do anything about it.

To the uninitiated, most cyber attacks seem 'highly sophisticated' because they are not well understood. Greater transparency (and consensus) from the cyber security community on the definition of a sophisticated or unsophisticated attack would reduce the scope for organisations to influence the public relations narrative post-incident if they could have done more to protect their customers.

JUMPSEC's experience

JUMPSEC recently came across an organisation's compromised details online. An investigation of the data dump found that more than 16,000 card details, addresses and private correspondence, including details of fees paid, were freely accessible by potential fraudsters, and were viewed thousands of times between October 2020 and January 2021.

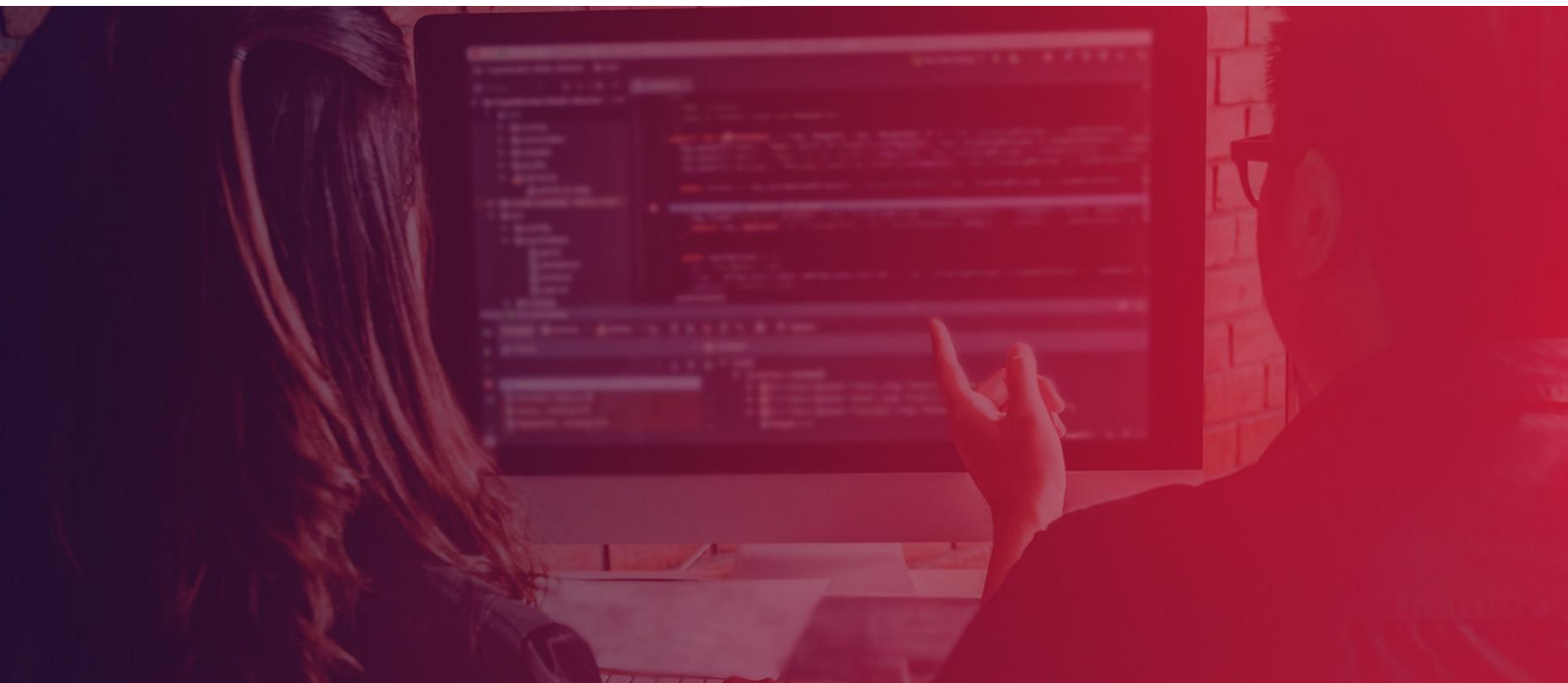
The company in question reported that no 'sensitive data' was stolen – presumably under the proviso that the data leaked publicly was from 2010 and before. We at JUMPSEC were intrigued by this claim. On testing a sample of the data we found that 20% of the cards are still active and vulnerable to fraud, since PAN numbers can exist for the lifetime of an account, and other details (such as expiry dates) can be easily predicted by fraudsters. Furthermore, the absence of data beyond 2010 indicated that the free-to-view information is not the entirety of the breach, and that the more recent data has likely been intentionally withheld for private auction. This has not been acknowledged in any official communications by the breached company.

This left us with several unanswered questions. Are the company lying about the extent of the breach? Have they misunderstood the potential impact? Or do they simply not know, and lack the capability to verify whether the data in the breach poses a real risk to customers?

The only way to know for sure would be for the organisation to publish their investigation report. But the reality is that their conclusion is likely based on a lack of evidence. If only limited telemetry is available due to insufficient logging and monitoring, it is possible to conclude that no harm was posed to customers **from the evidence available. But we know that a lack of evidence doesn't really mean that no sensitive data was taken.**

The bottom line is that organisations like this one are incentivised to reduce the amount of information that is exposed. They benefit from their limited network visibility because it gives them plausible deniability.

The lack of transparency in both this case and the Kaseya breach doesn't help the case for ransomware victims. Ransomware gangs know this and exploit the moral grey area to paint themselves as operating with integrity and a code of ethics.



What keeps a ransomware gang "honest"?

I use the oxymoron of the "honest thief" tongue-in-cheek – there is obviously nothing virtuous about ransomware gangs. But it is true that ransomware gangs operate with, and rely upon, a degree of reliability and trust. Reliability that they will release stolen information unless a ransom is paid, and trust that they will free the victim and not leak stolen data if a ransom is paid.

This is perhaps one of the reasons why attackers have not been known to falsify breach data to-date. They certainly could; most organisations who are victims of data theft and leakage are often unable to identify whether a leak even occurred in the first place. **And even if the victim claimed it not to be genuine – who would believe them?**

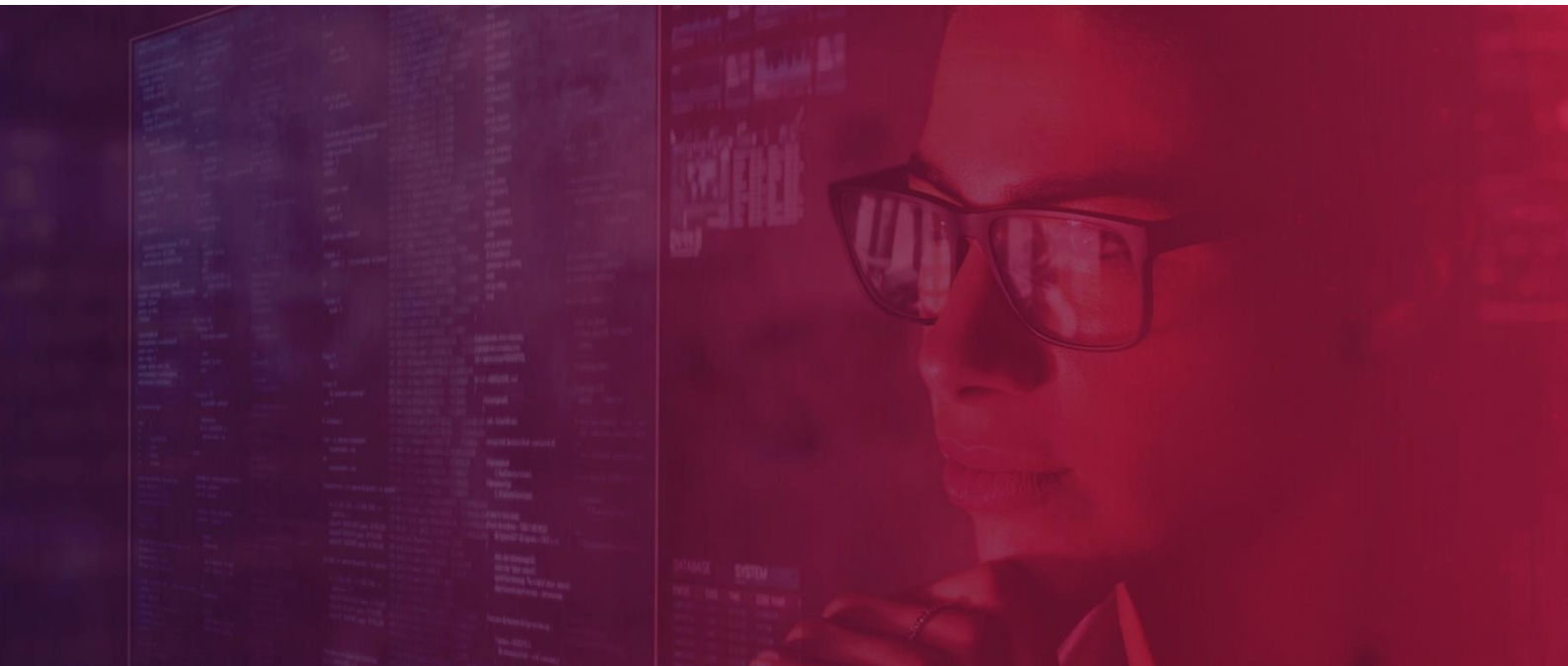
The 'code' for most ransomware groups centres on not targeting critical national infrastructure (CNI). We know that this is more due to self-preservation than any altruistic notion of only targeting 'big bad corporations' and limiting the damage to wider society. For example, in the wake of the alleged DarkSide takedown following the attack which crippled the US East Coast Colonial Pipeline, fellow ransomware-as-a-service operator REvil felt obliged to announce its own restrictions to partners leveraging their tooling and services, stating that:

- Work in the social sector (healthcare, educational institutions) is prohibited;
- It is forbidden to work on the gov-sector (state) of any country;...

> **DarkSide's history of faux-ethics extends to sending charity donations, and having their own ethics code that prohibited attacks against hospitals, hospices, schools, universities, non-profit organizations and government agencies. However, that didn't stop them from demanding a $4.4 million ransom in the Colonial Pipeline attack, which vitally supplies the US East Coast with ~45 percent of its liquid fuels.**

Clearly, the heat faced by DarkSide was fresh in Conti's mind when they released a free decryptor for HSE, the national healthcare system of Ireland. But they still demanded a ransom of ~$20 million to stop the sale of their stolen data.

Not so ethical after all.



Is ransomware on the ropes? Probably not

The recent disappearance of DarkSide (following the Colonial Pipeline attack) and REvil (following the Kaseya supply compromise), have prompted some to celebrate prematurely that we could be seeing the end of the recent spike in ransomware attacks.

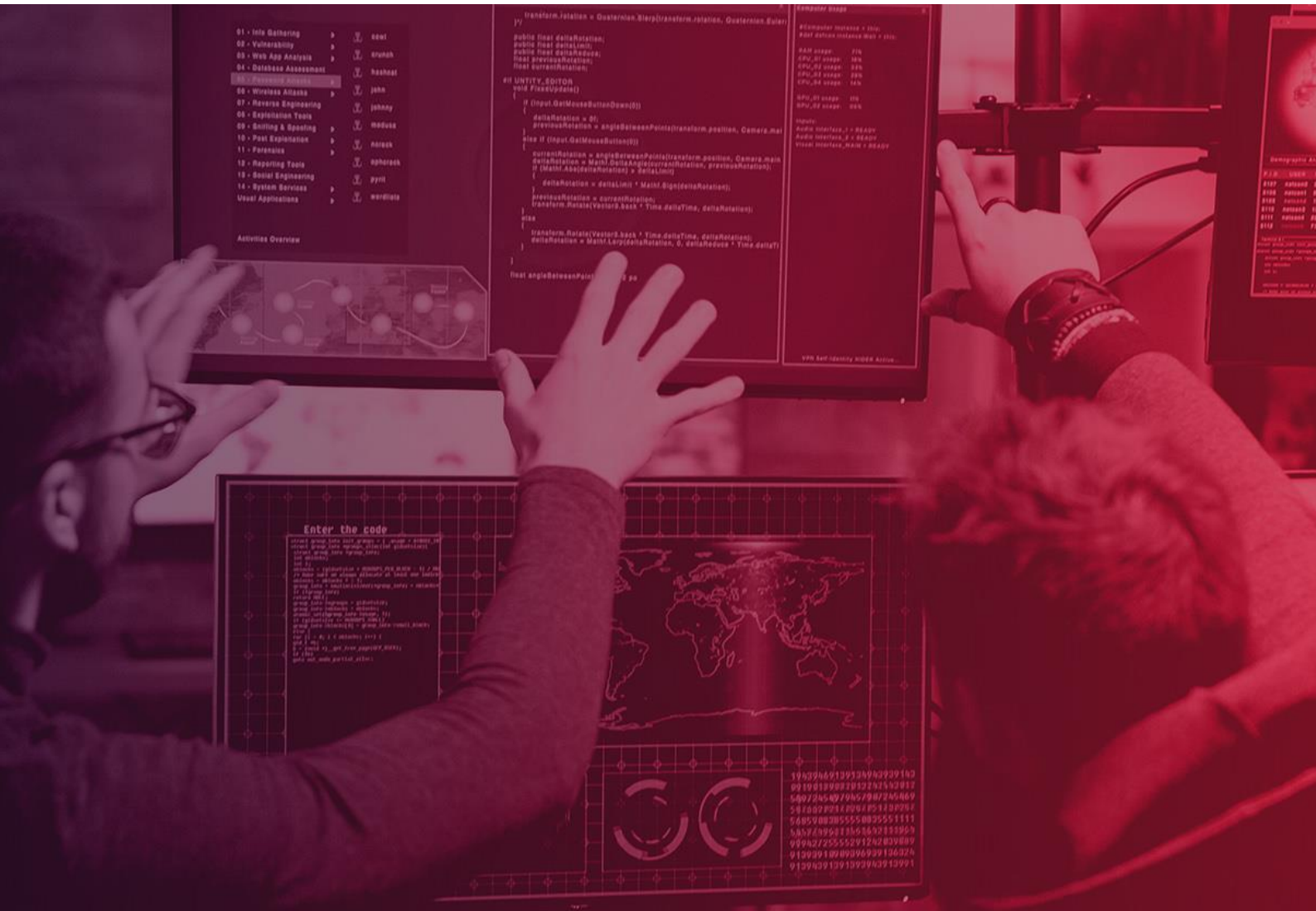
While organisations continue to pay ransoms, ransomware attacks will continue.

BlackMatter – a new ransomware group heavily linked with former DarkSide members – suggested in an interview that as long as cyber insurers continue to cover ransom payments, companies will continue to buy insurance and pay ransoms.

> **BlackMatter also assert that they possess greater control over attacks using their tooling and will vet and exclude targets with potential negative consequences, minimising the chance of partner organisations inviting unwanted attention from counter-offensive cyber operations. They also state that they believe they have the capabilities to "withstand the offensive cyber capabilities of the United States".**

The takeaway here is that the threat of ransomware is not going away quietly. The only way to reliably overcome the threat is to **stop paying ransoms.**

Unfortunately, this isn't as straightforward as it sounds.



Should ransom payments be banned?

As long as ransom payments are seen as an effective solution they will persist. In response, discussion groups have considered whether they should be banned altogether.

One of the primary arguments against paying the ransom is that it is **not a guaranteed method of recovery.** We know from our own investigations that ransomware actors often fail to include all stolen data within the ransom efforts, siphoning off the most valuable information for private auction on the black market.

In both the Colonial Pipeline and HSE attacks mentioned previously, the decryptor used (paid for in the former example, frantically volunteered in the latter) failed to be of much use. The Colonial Pipeline company allegedly ended up restoring from backups anyway after paying due to problems with the decryptor, while HSE worked with a third-party to use their supposedly faster decryptor.

The failure of ransomware gangs to deliver on their word is, all things considered, a good thing. The more that victims recognise that paying a ransom is not a guaranteed resolution plan, the more that organisations will start trying to do the right thing – investing in their cyber security defences and recovery plans, and not fuelling criminal enterprise because it is 'the easy way out'.

Ransom payment also fails to undo the loss of data during an incident. We reached out to the ICO for clarification, who stated:

"a requirement of the GDPR (Article 32) is that the organisation has measures in place to be able to restore personal data in the event of an incident. When we are assessing if the organisation had appropriate measures in place to meet this requirement, we would not consider the payment of the ransom as an effective measure to restore the data... If an organisation chooses to pay the ransom, we would still consider the individual has lost many of the data subjects rights granted to them by the GDPR. This is because whilst we may accept that the attacker will not publish the data, we can not put any trust in a criminal actor that they will actually delete it."

So, there are valid arguments against paying the ransom. But for many organisations it can also sometimes be the only choice; to pay, or face insolvency without the resources to recover. It's also worth considering that:

- **The banning of ransom payments could have more severe consequences**. For example, by increasing the scale and lethality of attacks to make recovery impossible and leave victims with no choice but to pay.
- **Paying the ransom can sometimes be the most ethical choice.** Many organisations end up paying the ransom in the best interests of their customers. Regardless of whether ransomware gangs can really be trusted, making the payment in the hope that sensitive personal data is not exposed.

It's clear that the answer to the ransomware problem isn't black and white, and that organisations who choose to pay are not always in the wrong. However, the lack of public visibility into the decision-making factors that led to a ransom payment will always lead to speculation. Blame culture is rife and leads spectators to assume that if you're paying the ransom, it means you have something to hide, or you didn't do enough.

Building trust through transparency

A less heavy-handed alternative to banning ransom payments is to encourage, guide, and reward good behaviours (i.e. refusing to pay) rather than prohibiting bad. But to do this effectively, there needs to be a supporting infrastructure that guides and incentivises organisations to make this choice.

The negative stigma associated with the victims of ransomware attack is partly responsible for some of the less commendable behaviours exhibited following an incident. **But self-preservation is a natural response in a crisis.** It's important to remember the strain that the victim is under, and the situation they find themselves in. Managing and responding to the incident itself is only one component of the issue; most victims quickly find themselves surrounded by third-party representatives – including incident responders, risk managers, insurers, regulators, and public relations. **Many of these parties will have more than one agenda and do not always put the victim's interests first** – for example, working on behalf of the insurer to scrutinise whether conditions of the insurance pay-out have been met.

To encourage greater transparency, there should be an infrastructure which addresses problems and supports victims rather than punishes them. This could be achieved through:

- **Increased support from insurers to victims who undertake cyber improvement programmes.** As mentioned in our previous article, mechanisms like cyber insurance often encourage the wrong behaviours for organisations when the cost of recovery can often exceed the cost of paying the ransom. Were cyber insurance instead leveraged to address the root cause of the breach rather than paying the ransom, both the victim and insurer would reap long-term benefits by discouraging future attacks. **To this point, cyber insurance is not inherently bad, so long as the funds are put to good use – namely, by investing in securing the organisation to prevent further harm to customers.**
- **Increased regulatory oversight and technical scrutiny of recovery and improvement plans.** Regulators have a key role to play in ensuring that organisations undertake structured and measured cyber improvement programmes to enhance their resilience to subsequent attacks. Especially when choosing to pay the ransom, organisations regularly fail to address the underlying security weaknesses that led to the compromise.

While as a customer the last thing you want to hear is that your data has been recently stolen, being unexpectedly defrauded because the company 'found insufficient evidence' to report the leak is infinitely worse. Being open and honest with customers does not have to destroy a victim's reputation if handled in the correct way. To this point, investing in having the technical visibility of the extent of an attack can guide organisations to making an informed, ethical choice. This can still be the payment of a ransom if an unacceptable type and volume of sensitive data is exposed.

Today, ransomware groups masquerade as legitimate businesses, operate successful marketing and outreach campaigns, and trade on the trust placed in them. The uncomfortable moral balance grants criminals leverage, and without greater public transparency the pendulum is likely to swing ever further in their favour. **While technical-focused improvements are vital, the battle against ransomware is clearly more than just a technical one.** An environment and infrastructure that drives good behaviours is vital to increasing transparency, restoring trust, and building a cyber-resilient society.

In our next article, we will highlight some of the most effective projects that JUMPSEC clients have undertaken to build cyber resilience and reduce their susceptibility to, and the impact of, ransomware attacks.

Unit 3E-3F, 33-34 Westpoint,
Warple Way, Acton, W3 0RG

0333 939 8080

hello@jumpsec.com

www.jumpsec.com