Reliance acsn

# Board Briefing Paper: The Rise and Continued Rise of Ransomware

## Executive Summary:

We are all aware that ransomware poses an operational, financial and reputational threat for organisations. At a time when the pandemic has meant that we are all far more digitally dependent, there has been a dramatic increase in the number of ransomware attacks and the range of sectors targeted. In short, your organisation is now much more likely to become a victim of a ransomware attack. At the same time, the latest tactics employed by the attackers are resulting in an even greater impact on victims, who are being left with little option but to pay. This paper explains the new ransomware business model, the tactics that the threat actors employ and provides concrete advice about how to prepare for, and mitigate against the ever-increasing threat of ransomware.

## A New Business Model - Ransomware-as-a-Service

For many years, we have seen the crime groups who utilise ransomware growing in sophistication and capability. The growth in capability is a result of these groups becoming increasingly specialised and the evolution of a new, more secure and effective ransomware eco system. The groups who develop ransomware – products like RYUK and REvil – now make it available to other criminal groups to employ. This is Ransomware-as-a-Service and it has allowed many more cyber actors, in exchange for a percentage of the eventual profits, to deploy ransomware.

The other element in this ecosystem is those groups who achieve the initial compromise of the victims. At Reliance acsn, we see this initial compromise often achieved through the employment of a trojan. This is malware that pretends to be something useful while causing harm or stealing data. Two of the best known trojans are Emotet or Trickbot and they are often delivered in bulk through spam emails controlled by automated programmes or bots. These trojans, utilising automated phishing emails, have resulted in the covert compromise of thousands of UK SME's. Once the initial breach has been achieved and persistent two-way, undetected communication is established, the access is sold on to another group.

In a rare piece of good news, the group that controlled the Emotet bot was disrupted by law enforcement action at the beginning of 2021. However, this is an immensely profitable business and the gap left behind has been filled by Trickbot and other malware types.

## New Tactics

Whilst much of the initial stage may be automated, the second covert stage of a ransomware attack is now likely to be 'human operated'. The actors will use privilege escalation (gaining access to IT administrator accounts) and lateral movement (moving from domain to domain) to covertly move around your network. They are seeking to maximise the power (and value) of the initial breach by identifying what kind of files you have, the data they contain, and potential value. That helps them set the terms of the ransom: how much, how long you must pay, and what the consequences of not paying might be.

A key objective is to gain access to any backups so that they can encrypt them as well. That means you can't recover the files from backups which are constantly connected to your systems. They also disable backup functions. The strategy is simple: when the ransomware is deployed, the attackers want to have blocked off all escape routes and nullified all the recovery options so that you have no choice but to pay.

# The Attack

The next stage is to deploy the ransomware. Reliance and other cyber security companies have observed that 2020's dominant ransomware variant was Ryuk which, when it is executed within the victim's network, sweeps through encrypting the file systems and all attached drives. Once each file is encrypted, Ryuk literally throws away the key. The malicious code is injected into all processes and services, anti-virus protection, databases, backups, and other software are all wiped out.

It is not just criminal groups who use ransomware. The North Korean Intelligence services and the closely related Lazarus hacking group, are known to have a long history of developing ransomware to support their fundraising for the North Korean state. Indeed, it is believed that they created the WannaCry attack which in May 2017 affected 300,000 computers in 150 countries. The Lazarus Group are reportedly exploiting this criminal ransomware eco system to buy access to compromised organisations and employ commercial ransomware. This has helped them to significantly increase the number of attacks that they are able to carry out and to conceal their involvement.

# Data

Crucially, these actors are not just looking to encrypt data, they will also be stealing it. During the covert stage of the attack, they may have exfiltrated key sensitive data. The ransom demands may therefore include the threat of exposure of this stolen data, with the resulting damage to your organisation's reputation and the threat of regulatory fines. A recent development by groups who deploy REvil (or as it is sometimes known, Sodinokibi) ransomware is calling journalists and business partners to expose their victims' loss of data.  For victims, this creates a whole new dynamic in terms of having to manage public disclosure.

# Questions Boards Should Ask Themselves

As well as inspecting and testing the IT & Security teams that are responsible for delivering the operational security of the organisation, Boards should also be turning the lens on themselves and asking questions about how they as a group manage cyber risk. Below are some suggested questions that will help to shape Board level discussions:

- **Do we have an extortion policy and has it been reviewed for cyber extortion?**

  **WHY?** Critical decisions need to be thought through ahead of time, to take some of the pressure out of the situation, should it happen. For example, many boards haven't discussed and agreed the big ransomware question of 'would we pay?'.  Even if the pre-incident decision is that we would decide based on the specific events of a real attack, the question should then quickly turn to 'if we decide to pay, do we have the means to pay?'. Some organisations have Bitcoin wallets with funds in for exactly this reason.

- **Have the Board attended training on cyber risk?**

  **WHY?** A Board shouldn't need to understand the technical details of cyber security but they should understand the risk that a cyber-attack poses to their business specifically, be comfortable talking about it, and be armed to be able to ask challenging questions of those in operational roles to be assured, or not, that the risk is being managed.

- **Have you appointed a Board member accountable for cyber risk?**

  **WHY?** A single responsible individual at Board level gives the subject the focus it requires but, importantly, demonstrates to both the organisation itself and the outside world the importance that is placed on understanding and managing the cyber risk.

- **Have the Board evaluated and prioritised cyber risks, how frequently do you review the cyber risk, and is the frequency appropriate to the increasing risk?**

  **WHY?** Boards should run exercises to fully understand the cyber risk posed and then prioritise how to approach the risk. This cyber risk register and associated programmes should then be reviewed on an appropriate cadence and adjusted depending on how the risk changes over time. This cannot be a one-off exercise.

- **When were you last briefed on the cyber threat to your business sector?**

  **WHY?** The threat of cyber-attack, in terms of who, why and how, can vary greatly from sector to sector so it's important to understand the specific risk that is being seen within your sector, the types of attack that are most common and the reasons behind them. This will allow you to tune your approach to be more effective.

- **Do you know who manages the cyber risk on a day-to-day basis and when did you last have a discussion with them?**

  **WHY?** It may seem like common sense but in a lot of organisations, we see it's very easy for the board to become disconnected from the operational reality of cyber security and the highly important two-way flow of critical information is often lost.

- **When did you last exercise the business incident response plan and do you understand your role?**

  **WHY?** Time is always critical in a ransomware attack so having key members of the response plan fully understand their individual roles and the overall process is vitally important. Practicing against different scenarios will help you talk through key decisions like 'do we pay?', 'when should we notify the regulator?' or 'when do we involve the PR company?', to name a few.

- **Do you have business continuity plans in the event of a major cyber incident and when were these last reviewed?**

  **WHY?** If the worst happens and you are hit with a ransomware incident, or similar event that causes a major incident, it is vitally important that you have reviewed and tested, as far as possible, your ability to bring the business back online and operational again with minimal disruption.

# Questions to Ask Your IT and Security Teams

At Reliance acsn, we do not believe that there is a single answer to the ransomware threat. What is needed are a range of measures. Many are technical controls that form part of good cyber defence. Others are around the business processes. Here are some of the questions that we believe a Board member should be asking IT and IT security teams:

- **How confident are we that we can spot the early stages of an attack? Has there been a Security Operations (SOC) assessment framework to baseline our capabilities to detect and respond to attacks?**

  **WHY?** Industry standard frameworks have been developed and are continually evolving to include the very latest tactics, techniques and procedures (TTPs) and allow you to evaluate whether your security teams can detect any of these, and importantly, then do anything about it once detected. As we have seen, most ransomware attacks begin with an attacker gaining access to your systems, moving around them and increasing their permissions, before achieving a position by which they can launch a devastating ransomware attack. If your security teams can detect and respond to the early-stage attacker behaviour, you have a much higher chance of removing them from your environment before they launch their attack.

- **How vulnerable are we to an attack? Have we got the security basics right? How quickly do we patch to ensure that our systems are not vulnerable? Are our systems administrators protected? Have we deployed multi-factor authentication to minimise the impact of a password compromise? Are legacy systems treated as untrustworthy and suitably protected?**

  **WHY?** Most ransomware attacks are successful because the network defenders have struggled to address these issues.

- **How have we identified our critical assets and what have we done to assess our ability to protect and recover them, if needed, from a Ransomware attack?**

  **WHY?** Your critical assets, whether it be a payment system, Operational Technology environment or client database, enable your business to operate. If your business is processing card payments and your core payment platform is taken offline by a ransomware attack, the damage to your organisation will be significant on several fronts. By focusing budget and effort on your critical assets first you can protect, or at least plan to quickly recover, the core parts of the business.

- **Are our end points as difficult to attack as we can make them and can we spot attackers who are on these devices?**

  **WHY?** The first step in the vast majority of attacks is for a user to interact with an attacker's 'bait', enabling the attacker to then get access to their endpoint (e.g. laptop). From there, the attacker will perform various activities to make sure they can get back in without, for example, the user clicking on another link and will then try to gain more permissions from the system to give them more and more access to the environment. There are methods that make an endpoint much more difficult for an attacker to exploit and, when applied, may not fully prevent an attack but can certainly slow attackers down, and make the activities they need to perform to overcome these methods much easier to detect. These methods are commonly known as 'endpoint hardening'. As well as applying endpoint hardening, combining this with appropriate endpoint detection can allow security teams to catch attackers as they enter your environment, before they are able to perform widespread damage.

- **When was the last time we had a simulated cyber-attack performed against us, how successful were they and what were the recommendations?**

  **WHY?** Once an organisation has covered the questions above, it's useful to get an independent, friendly red team attack to understand how much an advanced attacker, with a reasonable amount of resource, could achieve against your organisation within a defined period. There are a few different ways to do this but essentially, a red team attack is asking a competent cyber security organisation, with the right credentials and track record, to perform a safe attack against you to evaluate and improve your detection and response capability in as close to a real situation as possible.

- **Have we got a secure offline backup? Has it been independently tested and evaluated from a ransomware perspective and if so, what were the conclusions and recommendations? Have we exercised recovery from the backup?**

  **WHY?** Organisations that are hit by ransomware but can recover from backups quickly, suffer significantly less damage than the organisations that can't. As we have shown, ransomware attackers will attempt to encrypt backup storage, as well as the live environment, to ensure the likelihood of paying the ransom is much higher. Your approach to backing up critical data should be reviewed from the perspective of a ransomware attack, to understand how and if attackers could access and encrypt even your backup data, and what you could do differently to give yourselves a much higher chance of recovering your organisation's data and becoming operational again as quickly as possible.

- **When was the last time we ran an operational level crisis management exercise with a ransomware scenario, what was the outcome and what were the recommendations?**

  **WHY?** Critical decisions need to be thought through ahead of time to take some of the pressure out of the situation, should it happen. Putting your IT operational security teams through their paces in a simulated environment ensures that your people, as well as their operating manuals, are tested, evaluated and importantly, improved. You don't want to find out in a real ransomware incident that your people don't have access to the critical information they need to make decisions, or a poorly thought through policy stops them from acting, which could mitigate the impact significantly.

# Conclusion

The chances of becoming a victim (or repeat victim) have increased significantly over the last 12 months. Given our greater digital dependency, with more staff working remotely and the increased sophistication of attacks, the impact of a ransomware attack could be much greater. However, a successful attack is not inevitable and there are a range of measures that could, and indeed should, be taken to reduce both the likelihood of your organisation becoming a victim and/or the impact, should your defences fail. As a Board member, you should be seeking assurance that those measures are being taken.

**If you have any further questions on the ransomware threat or what measures you should be taking, please contact us via contact@relianceacsn.co.uk**

**Or click the link below:**

**Contact Reliance acsn**