JUMPSEC

RANSOMWARE RESILIENCE SERIES:

Evaluating the risk posed by ransomware threats

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 first in a series exploring the risks posed by ransomware attacks, and how organisations can undertake targeted activities to build genuine resilience against attackers leveraging ransomware as the means of achieving their objectives.

Understanding the risk (and cost) of a ransomware attack

Ransomware proliferated in 2020, increasing by 435% compared to 2019[1]. The number of ransoms paid has also increased from 39% in 2018 to 58% in 2020[2] (the figure is likely to be even higher when factoring in those organisations that have not disclosed whether a ransom has been paid).

Clearly, ransomware is becoming increasingly viable for attackers as a reliable method of attack with a high degree of success and a strong chance of financial reward. The potential impact of a successful ransomware attack upon a victim organisation includes:

- Disruption of operations for the duration of the incident
- Cost of payment or cost of incident management, recovery and IT rebuild
- Loss of customer confidence and potential legality issues when paying a ransom
- Scrutiny and sanctions from industry regulators
- Data theft and loss, and associated fines (e.g. under GDPR)

Ransomware attacks today have evolved. They are no longer limited to the encryption of victim systems. Ransomware 2.0 now involves extortion under the threat of information leakage. Under a ransomware 2.0 attack, not only are the victim's systems encrypted but any data extracted will be made public if payment is withheld, opening the victim up to further damages due to the mishandling of sensitive data.

Perhaps the most dangerous thing about ransomware attacks is that they are indiscriminate. Historically, ransomware attacks have been perceived as highly opportunistic, with the potential to afflict any and every organisation with exposed and unsecured internet-facing assets, susceptible users, and/or credentials that have been leaked in previous and often unrelated data breaches.

The reality today is that ransomware attacks are becoming more targeted – although not in the conventional sense. Any organisation with a strong reason to pay is vulnerable. This means that organisations who rely on digital products and services to deliver their core business services (and are therefore exposed to the greatest risk), who also have the resources to pay a ransom, are most likely to be targeted.

This contrasts with many other types of attack, which have historically focused on organisations with the most valuable resources to steal, or the most abusable operations. These attacks seek to, for example:

- Access and exfiltrate sensitive payment and cardholder information
- Steal valuable intellectual property
- Disrupt or destroy critical national infrastructure
- Issue fraudulent high-value payments

[1] https://www.helpnetsecurity.com/2021/02/17/malware-2020/
[2] https://securityboulevard.com/2020/04/successful-ransomware-infections-surge-to-record-in-2020-as-victims-grow-more-willing-to-pay-research-shows/

While ransomware attacks are opportunistic in nature, attackers will refine the targets on their hit list to align their efforts with the greatest chance of reward. **While not quite 'targeted', ransomware attacks are better described as prioritised.** Ransomware 2.0-style extortion attacks in particular entail significant human investment in terms of time and resources. To ensure they maximise the returns on their investment, attackers will research an organisation before committing resources to a full compromise - not only prioritising who they attack, but calculating what ransom sum the organisation is able to pay.

Ultimately, attacker groups (and more specifically criminal fraternities motivated by financial reward) operate like legitimate businesses. If the potential return on investment from targeting an organisation is limited, they will invest their time and resources on other targets more likely to yield results.

The comparison with legitimate business doesn't end there. For example, DarkSide the attacker associated with Sunday's ransomware 2.0 attack on the US colonial pipeline - threatening 45% of the East Coast's supply of diesel, gasoline and jet fuel - has several diverse revenue streams. This includes an 'affiliate' model where their malicious software is shared with would-be attackers in a starter kit including user instructions and a template ransom demand. In return, any attacks carried out using the ransomware results in dividends paid to Darkside.

The group also recently invited journalists to interview them on their newest (more deadly) software version, and documents their successes on their dark web page; listing the companies hacked, what was stolen, and testifying to their 'ethics' - their reliability once a ransom is paid, and the organisations it will not attack for moral or political reasons. These are all tactics designed to encourage victims to pay.[3]

Organisations which operate in industries that have been historically less targeted than others (and therefore are likely to have a lower security baseline) are more likely to be targeted by actors utilising ransomware. **Any successful organisation can be ransomed and/or extorted; organisations operating in sectors with lower cyber-maturity present the optimal target for attackers as they are less difficult to compromise, yet equally profitable.**

[3]https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

Lessons learned from high profile ransom payments in 2020/21

Many of the highest-profile ransomware attacks, resulting in the largest ransom payments being made, are not organisations that would have been seen as a high value target for cyber criminals historically. For example, noteworthy attacks occurring over the last year which have reportedly ended in a payment being made include:

- Garmin (the technology and wearables company) reportedly paid a ransom in the region of $10 million.[4] Hackers deployed the ransomware tool WastedLocker, known to be used by Evil Corp - an APT that was added to the US sanctions list last year for stealing over $100 million from banks and financial institutions.

- CWT Global, the US travel services company, paid $4.5 million to hackers who stole vast amounts of their confidential business files, taking 30,000 computers down using a type of ransomware dubbed RagnarLocker.[5] In the talks with the hacker, which were open to the public in an anonymous chatroom, a CWT official said the organisation was severely affected by the COVID-19 pandemic and agreed to pay the ransom in Bitcoin as a result.

- Several US universities and education faculties, including the University of California San Francisco ($1.14 million) affecting their School of Medicine, the University of Utah ($457,000), and Yazoo County School District ($300,000)[6]. This trend has continued in late 2020 and 2021 in the UK with a spate of attacks on higher education institutions.[7]

When considering some of the companies that refused to pay – Cognizant ($50 million cost), Sopra Steria ($50 million cost), and ISS World ($74 million cost)[8] – it is clear that attackers are not only going after bigger targets with the resources to pay higher ransoms, but also smaller targets for whom rebuilding is more difficult due to the cost, meaning there is little option but to pay.

Organisations with cyber insurance are often more likely to pay up given that the cost of recovery can often exceed the cost of paying the ransom. For example, when Lake City, FL was paralysed by a ransomware attack, the council paid the ransom ($460,000) when calculating that the cost of recovery would exceed its $1 million insurance coverage limit.[9]

Organisations which have previously fallen victim to an attack are likely to be re-targeted by attacker groups where easily exploitable weaknesses continue to exist.

---

[4]https://www.cshub.com/attacks/articles/incident-of-the-week-garmin-pays-10-million-to-ransomware-hackers-who-rendered-systems-useless
[5] https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/
[6] https://heimdalsecurity.com/blog/ransomware-payouts-of-2020/
[7]https://www.zdnet.com/article/ransomware-attacks-against-schools-are-rocketing-with-students-coursework-encrypted/
[8] https://www.getsignal.info/blog/12-largest-ransomware-attacks-of-2020
[9]https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

Particularly when the organisation refuses to pay an initial ransom, different malicious parties are likely to repeat an attack – hypothesising that the second time round, the victim is more likely to take the easy way out given the strain on their fiscal and human resources from the first round of recovery. Similarly, if an organisation has a history of paying ransoms, they will be seen as a viable target and more likely result in a positive outcome for the attacker.

On the other hand, IBM reports that the larger a breach, the less likely that the organisation will be targeted in the following two years; this again highlights the pragmatism of attackers – if an organisation no longer has the resources to facilitate extortion, then they hold less value.[10]

[10] https://www.ibm.com/security/data-breach

Paying a ransom makes the problem go away fast - but doesn't equate to real resilience

To build resilience against ransomware threats it is not enough to insure against the problem.

The payment of a ransom demand has always been an ethical grey area for companies, and there is clear evidence that the upward trend in payments made is fuelling more attacks. There are even signs to suggest that attackers will specifically target organisations who are known or likely to hold cyber insurance, as they can be more inclined to pay the ransom (as they aren't footing the bill themselves) - **meaning that holding insurance in itself can make you a target.**

Add to this the fact that the cyber insurance market is structurally fragile due to the comparatively small pool of capital versus significant exposure[11]. It is no surprise that AXA, the global insurance company, recently stated that it will stop writing cyber-insurance policies in France that reimburse customers for extortion payments made to ransomware criminals.[12] This affirms that cyber insurance companies are increasingly unable to meet the demand of direct ransom payments when confronted with rising payout costs that threaten profitability.

Interestingly, the change does not affect coverage for responding and recovering from ransomware attacks - only opposing the direct payment of the ransom itself. While the change is only in effect in France (for now) and does not impact existing premiums, expect more providers around the world to take this stance, which may also lead to a rise in insurers refusing to pay out on their existing policies.

In the future, failure to demonstrate that organisations have taken all reasonable steps to prevent a successful attack is likely to invalidate the terms of cyber insurance, meaning that organisations relying on insurance alone leave themselves exposed.

While the most direct route to restoring business operations may be through paying a ransom, the approach of taking out insurance to facilitate ransom payment does not create real resilience and exposes the organisation to increased indirect costs over time. Organisations who don't invest in building appropriate cyber defences – particularly in terms of retroactive remediation work in the wake of an attack – are signalled as a viable target to the rest of the cybercriminal fraternity.

[11] https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem
[12] https://apnews.com/article/europe-france-technology-business-caabb132033ef2aaee9f58902f3e8fba

JUMPSEC

Building ransomware resilience with layered capabilities and controls

An organisation's ability to defend against a ransomware attack is not limited to preventing malicious technical actions. Current industry best practice recognises that a skilled and motivated attacker will inevitably breach even the most hardened network perimeter.

Once breached, an organisation's ability to limit the extent of a compromise (and the attendant direct and indirect costs) relies on maintaining layered defensive controls that span multiple components – encompassing prevention, detection, response, and recovery.

To build ransomware resilience, organisations must:

- Implement preventative security controls designed to block known ransomware-related tactics, techniques and procedures (TTPs), such as configuring access points to the network (e.g. user mailboxes) to prevent the entry and/or detonation of malicious file types associated with historical ransomware attacks.
- Architect their internal network to limit the blast radius of an attack by segregating environments and tiering user accounts to prevent a full domain compromise in the event of a successful attack, preventing the propagation of ransomware across the network.
- Tailor security monitoring activities to identify successful and failed attempted activities associated with ransomware attacks to accelerate investigation and response activities, decreasing the mean time to respond (MTTR) to limit the extent of a compromise.
- Formalise and simulate the business-wide response to a ransomware attack to facilitate a decisive and effective response, leading to the timely containment and eradication of the threat before systemic damages are incurred.

Taking steps such as these to create a layered, defence-in-depth strategy is fundamental to building resilience against ransomware attacks – and could be the difference to the tone of tens of millions of dollars in terms of the cost of remediation and recovery alone.

Read **Part 2** where we unpick the ransomware operator's psyche and the importance of reputation and trust in the business of ransomware.

Read **Part 3** to learn about how our clients have taken steps to enhance their ransomware resilience.

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

0333 939 8080

hello@jumpsec.com

www.jumpsec.com