BIZCOMMUNITY

Ransomware predictions for 2020

Ransomware has become big business, generating estimated annual revenues of $1bn a year for malicious threat actors. The victims of ransomware continue to stack up as criminals develop new, more creative ways to infiltrate IT environments, seize data and hold organisations to ransom.

Image supplied

As we reach a new decade, Simon Jelley, VP of product management at Veritas, explores how ransomware is likely to continue evolving in the year ahead.

Public sector, healthcare providers and manufacturers to be singled out by ransomware attackers

We haven't yet seen ransomware reach its peak, but we will see it become more niche and target specific sectors in the year ahead.

Until recently, ransomware attackers took a scattergun approach to their crimes. The Ryuk attacks and 2017's WannaCry typified an approach that focused on large attack volumes designed to net enough victims to make the effort worthwhile. Now, we're about to see attackers get more selective and focus on those industries where they can get the highest return on investment.

The public sector, healthcare and manufacturing industries are all emerging as some of the most likely targets. It's not necessarily because these sectors have a traditionally soft security posture or are particularly cash-rich, it's because they rely so heavily on mission-critical information for their day-to-day operations.

Cybercriminals know that if their attacks halt essential services, organisations will have less time to make a decision and will be more willing to pay the ransom. The stakes of a successful attack are much higher, so the chances of a victim paying up are so much greater.

As attackers grow more selective over their targets, organisations in healthcare, manufacturing and the public sector need to be aware that the threats they are facing from savvy ransomware criminals will only get more severe. To keep pace and prepare for a worst-case scenario, it will be imperative to improve visibility over all their data assets and leverage greater automation to ensure their data is backed up and recoverable across a rapidly expanding number of locations and IT environments.

Ransomware attackers to target intellectual property

What do successful businesses do once they have established themselves in a market? They diversify. Ransomware is no different. Just as businesses today are seeking new revenue streams, ransomware attackers are looking to boost their profits with new data exfiltration techniques.

In 2020, ransomware variants will emerge that combines the usual data lock-out with data exfiltration capabilities. What makes this type of attack so devastating is that it is aimed at the most lucrative data - intellectual property (IP).

Where once the goal was mainly to bypass defences and encrypt as much data as possible, we will soon see examples of ransomware attacks going after incredibly high-value information, such as product prototypes, schematics and designs.

If a ransomware attack can deny an organisation access to the prototypes of a new car or phone, they could also take this information outside the walls of an organisation and sell it to competitors on the black market. Ransomware will no longer be a matter of data denied, it will be a case of data compromised.

With businesses needing to remain agile to stay ahead of the competition, losing access to critical IP slams the brakes on product development and other crucial projects that feed into the revenue stream. We can expect attackers to tune their ransomware to seek out and capture this information specifically. That's why it's so important for businesses to have the right data protection measures in place for their most business-critical data.

Social engineering attack methods will evolve to target the wider supply chain

Cybercriminals have long relied on social engineering as one of their most successful modes of attack. By fooling employees to share information or download their malware, ransomware attackers acquire the credentials they need to

capture a company's most important digital assets. However, in response to improved, more rigorous company policies, their techniques will evolve.

We're already seeing the beginnings of a secondary illegal market for stolen credentials. On the dark web, ransomware is fuelling the rise of a burgeoning market that makes it quick and easy for cybercriminals to gain remote access to corporate systems.

This boom is being supported by a shifting attack strategy that will only become more embedded in 2020. Ransomware attackers will increasingly target their efforts, not on existing employees, but on adjacent targets and other accounts with access to the systems of their intended victim. This includes outside contractors, freelancers, partners and approved vendors.

Thankfully, there's a solution. In response to adjacent attacks, we are likely to see IT and cybersecurity teams given a larger role in the procurement process to ensure supplier integrity. Before onboarding a new supplier, an organisation must be confident they have comparable data protection measures and policies. Very soon, data responsibility won't just be for internal consumption, it will be how organisations do business and choose who they work with.

Always have a backup plan

To defend your organisation from ransomware in 2020, it's crucial to take a proactive approach to prevention, supported by a system of layered data protection solutions and policies. This must include ransomware resiliency solutions that offer enhanced protection of business-critical data against ransomware attacks, coupled with a data protection education programme for employees at all levels of the business. Any gap in your defences is a weakness cybercriminals will exploit, so comprehensive protection is a must.

However, the only thing that can assure protection in the long term is a sound backup strategy. No ransomware defence is perfect, so a successful attack becomes a matter of when rather than if. Organisations need to create isolated, offline backup copies of their data to keep it out of reach of any successful attack. Organisations then need to proactivity monitor and restrict backup credentials, while running backups frequently to shrink the risk of potential data loss.

Last but by no means least, businesses should then test and retest their ransomware defences regularly. The coming years will be a period of great innovation and evolution in ransomware variants and attack methods, so stress testing will be critical to ensuring your backup strategy keeps pace and can deliver when it counts.