InfoTrust

netskope CROWDSTRIKE mimecast

EXECUTIVE SUMMARY

RANSOMWARE RESILIENCE

While ransomware has been around for years, it is by no means an old-fashioned form of attack. In fact, cyberattacks using ransomware have experienced somewhat of a resurgence over the past 18 months, particularly in Australia. According to **CrowdStrike's 2020 Global Security Attitude Survey**, over two-thirds of Australian businesses suffered a ransomware attack in 2020, a third of which paid the ransom, costing an average of AU$1.25 million each. Despite its popularity amongst cyber threat actors, businesses are remarkably underprepared.

According to CrowdStrike's 2020 Global Security Attitude Survey, over two-thirds of Australian businesses suffered a ransomware attack in 2020, a third of which paid the ransom, costing an average of AU$1.25 million each.

Most organisations are aware of how ransomware works. The malicious software, often originating from email attachments or links, aims to infiltrate devices, software, and systems in order to render files unusable. Once access is denied, ransoms are then demanded. However, ransomware has evolved over the years to become increasingly sophisticated. Encrypting ransomware uses robust encryption algorithms, and fear-based strategies playing on human emotion to illicit a desired response. The result being, unsecured and unprepared businesses paying up in fear of losing everything.

When it comes to ransomware, there are no guarantees. If organisations pay the requested ransoms, their files aren't always unlocked as promised. Secondary ransoms are sometimes demanded, or businesses are left to suffer regardless. What's more, by paying, organisations reveal themselves to be susceptible and are often targeted again. Ultimately, as long as organisations continue to pay, digital extortion remains a hugely profitable industry, and ransomware is only going to evolve in complexity as well as frequency.

RANSOMWARE IN 2021 AND BEYOND

80% of Australian cybersecurity experts are concerned about ransomwareattacks due to COVID-19 which is higher than the global average according to CrowdStrike's Global Attitude Survey.

New-age ransomware uses a combination of advanced distribution efforts and development techniques. This ensures that not only is it easily and widely distributed, but reverse engineering is extremely difficult. However, today's threats are more than just technological; they take advantage of all vulnerabilities, including urgency, fear, and uncertainty. The COVID-19 pandemic is a prime example where organisational change made it harder for ransomware attacks to be prevented and indeed recovered from.

One of the biggest developments in today's ransomware threats is in the way in which it is delivered. While email is still an important attack vector, **Netskope's 2021 Cloud and Threat Report** has revealed that the majority (61%) of malware is now delivered via cloud applications. This gives attackers the opportunity to evade legacy security systems and put enterprise data at risk. Additionally, the surge in attacks has also seen a rise in the level of payment being demanded. It has been estimated that the total cost of the 11 largest ransomware attacks in the first six months of 2020 was **over $144 million**. This is almost as much as the whole year for 2019.

Although the global pandemic has slowed down detection time and exposed the vulnerabilities of many businesses and industries, it has also shone a light on the threat that ransomware poses. **CrowdStrike's Global Attitude Survey** found that 80% of Australian cybersecurity experts are concerned about ransomware attacks due to COVID-19 which is higher than the global average. As such, the pandemic could pave the way to increased digital transformation and importantly, the increased security transformation that is needed to build resilience against ransomware attacks.

THE BUSINESS RISK OF RANSOMWARE

92% of organisations have reported that their organisation has seen ransomware delivered via email attachments in the past year.

Where individuals used to be the prime target of ransomware attacks, businesses are now in the firing line. In the past year, a colossal **92% of organisations** have reported that their organisation has seen ransomware delivered via email attachments.

Businesses are more likely to give in to the demands in fear of a lack of access to critical systems, regulatory fines and more. Moreover, companies are more likely to pay substantial amounts, making them extremely valuable targets.

The threat of ransomware will continue to target all businesses, large or small, especially those that expose any level of vulnerability. And without the capability to not only defend but to respond and recover in the event of an attack, these businesses risk severe financial and reputational damage.

BREAKDOWN OF A TYPICAL RANSOMWARE ATTACK

Ransomware can infiltrate organisations through a variety of attack vectors. Traditionally, email was the primary point of entry, with malicious email attachments and links to malicious websites being commonplace. However, now the focus has shifted to the cloud. Cloud applications, such as file sharing and social networks, is frequently being leveraged to host malicious files and links. Whatever the route to entry, a ransomware attack typically follows six key stages:

1. **Distribution** - cybercriminals use techniques such as phishing and social engineering to trick users into downloading malicious files or clicking malicious links.

2. **Infection** - the malicious files pass the web gateway and download an executable file, which installs the ransomware onto the user's machine.

3. **Staging** - the ransomware's payload embeds itself in the system and establishes the ability to survive beyond a reboot.

4. **Scanning** - the ransomware searches for all accessible files, both on the local computer and the network.

Cloud applications, such as file sharing and social networks, is frequently being leveraged to host malicious files and links.

5. **Encryption** - the discovered files are locked or encrypted so that the user can no longer gain access.

6. **Ransom** - a ransom note is generated and delivered to the victim demanding payment in order to unlock the files or provide a decryption key.

After these six stages, the pattern the attack will follow will depend on the actions of the organisation in question. If the ransom is paid, the files might be unlocked. However, there is no guarantee that this will happen. The files may remain locked, be deleted, or sensitive data may be published.

DEFENCE IN DEPTH HOW TO MITIGATE EACH RANSOMWARE TACTIC

Phishing simulations can help to test employee knowledge, give valuable insights, and demonstrate what employees should be doing to keep themselves and their data safe.

Once ransomware has infected a device or system, organisations are often left unable to retrieve their data without giving in to cyber-extortion demands. That is why, when it comes to ransomware, it is most certainly a case of prevention being better than cure. While ransomware is constantly evolving, and protection can seem increasingly challenging, there are several security controls that businesses can employ to mitigate each stage of a ransomware attack.

- **Email authentication** - by implementing DMARC (Domain-based Messaging, Authentication, Reporting and Conformance), organisations are able to lock down their domain, take control of their brand's identity and prevent email fraud.
- **Impersonation and sandboxing controls** - using a combination of machine learning and data insights, impersonation controls can identify even unknown attack patterns at an early stage and block compromised assets. Meanwhile, sandboxing controls provide an isolated environment to execute files and URLs before they are opened on the production network.
- **URL click-time protection** - email gateways have changed due to many businesses migrating to cloud-based systems, making them unable to protect against sophisticated attacks. URL click-time protection evaluates links in real-time both before email delivery and again at the time of click so malicious links can be blocked.
- **Security awareness training** - employees are the front line of every organisation's defence and as such, should be trained in good data hygiene practices. This should include implementing strong password protection, using secure Wi-Fi connections, and being on a constant lookout for phishing attempts. Phishing simulations can help to test employee knowledge, give valuable insights, and demonstrate what employees should be doing to keep themselves and their data safe.
- **Web threat isolation** - deploying web threat isolation enables businesses to block file uploads and downloads to uncategorised and security-risk websites as well as block forms associated with phishing attacks.
- **HTTPS traffic inspection** - the full content of web traffic, secure or otherwise, is decrypted and scanned for malware before being delivered to the user.
- **Web proxy solution** - roaming employees who connect to the internet using external networks may not have sufficient security in place. With a web proxy solution, traffic is routed through a cloud proxy when employees are outside the corporate network.
- **Endpoint detection and response (EDR)** - artificial intelligence and machine learning should be leveraged to record, investigate, and analyse endpoint activity and deliver real-time protection and visibility across the enterprise.

WHAT HAPPENS IF YOU DO BECOME A VICTIM OF A RANSOMWARE ATTACK?

When it comes to protecting against ransomware, cybersecurity and cyber resilience aren't the same thing. While it is vital to put advanced security measures in place, there is still a chance that these measures will be infiltrated, and that ransomware will infect and encrypt files. Resilience defines the way an organisation responds in the event of an attack. After all, it is this response that will reduce data loss and downtime and thereby minimise the business impact.

If a business becomes the victim of a ransomware attack, removing the malware and restoring the system to a previous state is a sensible step. Although, files will remain encrypted. At this point, businesses make a choice about whether they are willing to pay to unlock their systems. However, this is not advised as there is no certainty of faster or guaranteed recovery, and payment may only fuel subsequent attacks.

With unified data protection and backup in place, companies can quickly find and restore data, reducing downtime and impact in the event of a breach.

Instead, to ensure business-critical data is always accessible, it is vital that organisations have secure and robust backups in place. Businesses should back up all data both on their network and in the cloud. With unified data protection and backup in place, companies can quickly find and restore data, reducing downtime and impact in the event of a breach. In addition, businesses should have a rehearsed incident response plan in place. This ensures they are prepared for an attack, can rapidly detect incidents, and can work to prevent them from escalating.

PROTECTING YOUR BUSINESS FROM RANSOMWARE

With a stream of high-profile ransomware attacks on Australian businesses in the last 12 months and an evolving working environment in the wake of the global pandemic, now more than ever is the time for organisations to improve their cyber resilience.

InfoTrust can help you to protect your business from ransomware. To find out where you stand or to start your security journey, request a ransomware resilience assessment today.

+612 9221 5555 info@infotrust.com.au www.InfoTrust.com.au

InfoTrust