UnderCover
Insurance and legal news from the VL desk
vero liability insurance limited

April 2020 | Issue 02

The COVID-19 Storm and Remote Working Presents Opportunities for Cyber Criminals

Following the New Zealand Government's unprecedented decision to implement the COVID-19 Level 4 lockdown, businesses of all sizes are now facing increased vulnerability to their systems being attacked by cyber criminals.

We feel it is important to keep our broker customers informed about some of the risk scenarios being experienced by businesses at present, due to significant numbers of people working from home, so they can advise their customers accordingly.

Level 4 lockdown meant many organisations faced a scramble to transition their employees to remote working capabilities. A transition which would usually be months in the making needed to happen in a matter of days. This put pressure on some IT departments to provide remote working solutions and build up network capacity at speed, creating the risk of security gaps. In some cases, security controls like access management systems or Virtual Private Network (VPN) gateways may be hastily bypassed and thus decreasing the organisation's security level (i.e. authentication security or remote access restrictions).

Even with enough lead in time to set up secure remote access, employees working outside of their organisation's network are operating in less secure environments for many reasons, including:

- Organisations may allow employees to use personal devices for remote working purposes as providing all staff with corporate devices might be too costly. However, these personal devices may not have the latest anti-virus or security patches installed and/or could already be infected with malicious software. Essentially, you are trusting your employees to undertake best security practices on their devices. Strong Bring Your Own Device (BYOD) policies can go some way to assisting (e.g. organisations can implement inventory and security checks of personal devices accessing their network). However, IT teams won't be able to force security updates or have visibility over personal devices the way they do on corporate devices, increasing the complexity of patch management;

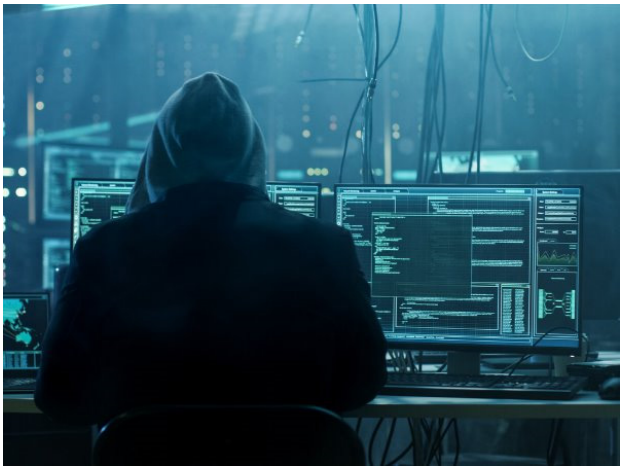
- Organisations may not have control over what applications and software can be downloaded on personal devices (known as application whitelisting);

- Less secure network connections from home Wi-Fi (i.e. default router passwords and/or router firewalls disabled) or public Wi-Fi (i.e. attackers snooping unencrypted network communications);

- The increased use of mobile devices or remote access to business systems increases an organisations attack surface, thereby increasing the possible entry points or vulnerabilities being exploited, making cyber security more challenging;

- Remote access can increase the difficulty of access authentication controls (i.e. knowing if the person accessing the system is who they say they are).

Employees should be considered part of an organisation's IT security department; they are often the weakest link in the chain, as well as being the first line of defence. Employees working from home are an even weaker link and an attractive target for cyber attacks.



Attackers are implementing new techniques and tactics specifically designed to take advantage of the opportunities that COVID-19 disruption presents. It is important to note malicious actors are not taking time off during the lockdown – instead their business model is thriving. COVID-19 for cyber criminals is like the holiday period for burglaries. Criminals know over the holidays many people will be away and homes become easier targets. With COVID-19, cyber criminals know employees are working from home and they can use the pandemic to invoke fear through their scams – cyber criminals see this as an ideal time to strike.

The information security and insurance markets are seeing increased cyber-crime activity arising from a series of attack vectors taking advantage of COVID-19, including:

- Rising online fraud with COVID-19 as a catalyst. For example, fraudulent offers of medication or protective masks recently emerged as a business model. Additionally, scammers often ask for charity donations for studies, doctors, or victims that have been affected;

- Phishing and social engineering messages are being circulated by cyber criminals via e-mail or social platforms allegedly offering help for dealing with the pandemic. These messages contain malicious links or attachments (e.g. ransomware or key-loggers). For example, COVID-19 provides the perfect storm for attackers to create new strategies for business email compromise scams. Mass confusion and panic can lead to fraudulent emails requesting urgent calls to action to be acted upon, leading to malicious links or attachments being clicked;

  Additional information on COVID-19 themed scams can be found on the CERT NZ website.

- Watering hole attacks through COVID-19 related websites. Just like a lion knows large numbers of prey congregate around watering holes, cyber criminals look to infect websites where groups of people are known to visit. Visiting these malicious sites, especially with outdated web browsers (i.e. without the latest security patch), could lead to the visitor's system being infected;

- Live COVID-19 maps that spread malware;

- With the increase in virtual meetings attackers are targeting video conferencing software to eavesdrop on sensitive business conference calls.

In the end, an organisation can reduce their risk through good hygiene practices. For instance, both CERT NZ and NCSC highlight key security controls for remote working that organisations can implement.

If you wish to discuss any aspect of this issue, please contact Dan Lowe - VL's Cyber Specialist.