Wavelink
Global Technology | Local Knowledge

MEDIA RELEASE

Cyberthreat activities ramping up during COVID-19 crisis

The confusion, fear, and genuine distress caused by the COVID-19 pandemic and its economic fallout means now is a perfect time for malicious actors and cybercriminals to strike. Australia has already seen its share of scammers, from fake emails and text messages to phone calls and fraudulent products. Social engineering scams are most likely to succeed during this time of upheaval and worry, so it's crucial to be aware of coronavirus-related threat activity and act to protect the organisation against it, according to Wavelink, a Fortinet distributor.

Ilan Rubin, managing director, Wavelink, said, "Right now there are so many legitimate pieces of communication regarding COVID-19 that it's very easy to slip in some phishing emails and other fake communications. This has created a significant vulnerability that attackers have been quick to exploit. People are hungry for information while organisations are looking for products that can help protect them against the virus. This has seen a dramatic rise in attacks that put malicious links in legitimate-looking emails purporting to be from government agencies or news outlets, for example."

The attacks related to COVID-19 aren't just limited to fringe actors, although there are plenty of new cybercriminals entering the market during this fruitful time. However, well-known, professional cybercriminal organisations are also taking advantage of the situation to launch attacks.

Some of these attacks include:

- the Emotet trojan, which steals sensitive and private information such as banking details, and can cost upwards of US$1 million per incident to clean up (1)
- BabyShark, a relatively new North Korean malware that persistently exfiltrates system information and receives additional commands
- the Ukrainian Centre for Public Health spoof, which impersonates the World Health Organisation trademark to lure users into opening a malicious Word document
- an Italian phishing attack that warns the recipient that COVID-19 cases in their region have been documented and the recipient should urgently open the attached, malicious Word document
- a FedEx customer advisory email that looks like a PDF document but is, in fact, an executable file that infects the user with the Lokibot infostealer.

These are just a few examples of the more sophisticated attacks that are affecting users around the world. Organisations need to act fast to protect themselves against these known threats as well as unknown and emerging threats. To a large extent, this can be done using smart security solutions.

For example, organisations should update their anti-virus and intrusion protection system definitions constantly, and proactively patch whenever vendor updates are available. Additionally, businesses should consider a secure mail gateway solution to block specific file types that are likely to be malicious. Using a sandbox solution, IT professionals can determine if a file displays malicious behaviour. Furthermore, a firewall with anti-virus can also be configured to detect and block these threats.

However, technology alone isn't a magic bullet. Strong protection requires the full participation of the entire organisation.

Ilan Rubin said, "Technology can only go so far to protect an organisation against attack in such chaotic and challenging times. With more employees working outside the corporate firewall for perhaps the first time, businesses need to be more vigilant than ever in making sure these employees understand the importance of basic security hygiene. This includes never opening attachments from someone they don't know and always treating emails from unrecognised senders with an abundance of caution.

“Employees should be trained to be sceptical of instructions in emails, text messages, or even phone calls that require them to click on a link, open an attachment, provide login details, or transfer funds. If in doubt, users should contact their IT or information security department to verify if an email is legitimate.

“If people stay vigilant and refuse to trust suspicious emails, then, at worst, a business activity may be delayed. At best, an expensive and potentially devastating cyberattack could be averted. Now more than ever, individuals play a crucial role in protecting an organisation against cyberattacks.”

Reference:

(1) https://www.malwarebytes.com/emotet/