COVID-19: (AUSTRALIA) A PHISHING PANDEMIC – PART I

Date: 25 March 2020

Australia Technology Sourcing and Privacy Alert

By: Cameron Abbott, Rob Pulham, Michelle Aggromito, Rebecca Gill

It's upsetting to report, but should come as no surprise, that scammers are seeking to take advantage of organisations during the COVID-19 pandemic.

The Australian Competition and Consumer Commission's Scamwatch website reports that phishing attacks are on the rise, with scammers impersonating the World Health Organisation and other agencies. Scams include anything from offering victims a vaccine for COVID-19 to investment opportunities created by the pandemic.

FraudWatch International also states that they have monitored various types of cyberattacks over the last few weeks arising in response to the pandemic, which include phishing attacks, state-sponsored attacks, and malware in the form of Trickbot and other trojans. In fact, more than 3,600 new domains containing the phrase "Coronavirus" were created in the past five days, with the vast majority of them destined to host phishing sites and spread malware.

Scammers are also targeting employees and businesses who are working remotely from their homes. Cynet reports that there has been an increase in remote user credential theft and weaponised email attacks, given that working from home often means working on personal, and predominantly unsecure, devices. While the increases in such attacks have primarily arisen in Italy, they are likely to take place in other countries as COVID-19 continues to spread worldwide.

Insurance organisation Beazley also reports that it saw an increase in 2019 and 2020 of its policyholders being victim to cyberattacks. Many business operations came to a standstill during the attacks and ransoms demanded by malicious actors skyrocketed, reaching seven or eight figures! Beazley also notes that scammers have been using ransomware variants alongside banking trojans during the pandemic. This two-pronged approach has the ability to encrypt, access and steal an organisation's data for the purposes of a ransom.

The message from these reports is clear:

- All organisations should be continuously reminding their employees and contractors of their security and data protection protocols, as well as making sure that the security measures are actively working to prevent coronavirus-related scams.
- Organisations should also update and refresh their employee training to provide employees with the tools to mitigate the heightened risks.

We will be providing some tips on how to prevent these risks in Part II.

To keep up-to-date with developments in this area, you can sign up to our CyberWatch: Australia blog at: www.cyberwatchaustralia.com. Simply add your email address under "Subscribe to Blog Updates".

KEY CONTACTS

CAMERON ABBOTT
PARTNER

MELBOURNE
+61.3.9640.4261
CAMERON.ABBOTT@KLGATES.COM

ROB PULHAM
SPECIAL COUNSEL

MELBOURNE
+61.3.9640.4414
ROB.PULHAM@KLGATES.COM

