CYBERCRIMINALS

Both seasoned cybercriminals and opportunistic individuals spread disinformation in order to benefit from it in different ways. However – not including individuals who derive satisfaction from misleading people – the ultimate aim is always to obtain profit. Some individuals simply seek to obtain direct financial gain through digital advertisements, as engagement with fake news messages about COVID-19 can be very high. The number of new websites related to COVID-19 has soared in recent weeks. Another strategy to profit financially from the COVID-19 crisis is to spread fake news about potential cures for the virus or effective prevention measures. In some cases, these messages are relatively harmless, although they may give individuals a false sense of security. However, such messages can also help criminals seeking to sell items that they claim will help prevent or cure COVID-19. According to the EEAS, state actors also spread disinformation, seeking to sow distrust and destabilise governments. Violent extremists and terrorists are also using the pandemic to spread their message.

RANSOMWARE

Ransomware is a type of malicious software criminals use to take files on a device hostage by encrypting the data and subsequently refusing access to them. To regain access to the files, the victim needs to pay the criminal a ransom. Generally, perpetrators request such a payment in the form of bitcoin or some other virtual currency. The primary focus therefore is on financial gain. In recent years, criminals have focused their attacks on organisations. As many organisations suffer disruption to business when they cannot access their files, criminals have a relatively high likelihood of receiving the payment. Normally, criminals focus their attacks on high-value data or assets within organisations that are especially sensitive to downtime—so the motivation to pay a ransom is consequently very high. Hospitals are such an example, since downtime for a hospital could potentially lead to loss of life. Other examples include government agencies, universities and organisations within the manufacturing sector.

Ransomware is also offered on the dark web as a ransomware-as-a-service product. During the COVID-19 pandemic, most reports to Europol has related to previously known ransomware families, which suggests the involvement of established criminals continuing their business. However, new ransomware families have also continued to frequently appear during the pandemic. To carry out a ransomware attack, criminals need to gain access to the system of their victim. This can be achieved through social engineering techniques such as phishing attacks. When the victim clicks on a link or opens a malicious email, the perpetrator can execute their strategy by infecting the device.

The types of criminals exploiting the COVID-19 pandemic online were also active in the area of cybercrime before. However, some are believed to have intensified their activities and are actively recruiting collaborators to maximise the impact of their attacks or schemes. The period between the initial infection with ransomware and the activation of the ransomware attack is shorter. Criminals do not wait for the ideal moment to launch the attack but try as soon as possible.

DISTRIBUTED DENIAL-OF-SERVICE

Only a slight increase in the number of distributed denial-of-service (DDoS) attacks has been observed following the outbreak of the COVID-19 pandemic. However, it is expected that will be an increase in the number of DDoS campaigns in the short to medium term. Due to a significant increase in the number of people working remotely from home, bandwidth has been pushed to the limit, which allows perpetrators to run ‘extortion campaigns’ against organisations and critical services and functions. DDoS is an accessible type of crime with limited barriers to entry because it is cheap and readily available.