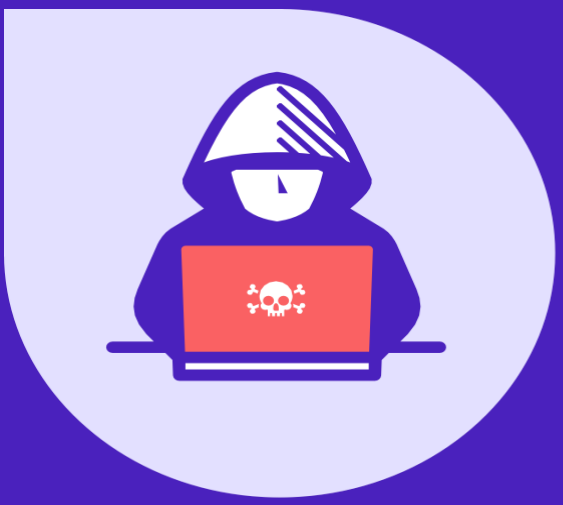
COVID-19 PROFITEERING - CYBERCRIME



KEY FINDINGS

The global pandemic of COVID-19 is not only a serious health issue but also a cybersecurity risk. Criminals swiftly took advantage of the virus proliferation and are abusing the demand people have for information and supplies.

Criminals have used the COVID-19 crisis to carry out social engineering attacks, namely phishing emails through spam campaigns and more targeted attempts such as business email compromise (BEC).

There is a long list of cyber-attacks against organisations and individuals, including phishing campaigns that distribute malware via malicious links and **attachments, and execute malware and ransomware attacks that aim to profit** from the global health concern.

Information received from law enforcement partners strongly indicates increased online activity by those seeking child abuse material. This is consistent with postings in dedicated forums and boards by offenders welcoming opportunities to engage with children whom they expect to be more vulnerable due to isolation, less supervision and greater online exposure.

The pandemic has an impact on Darkweb operations. Certain illicit goods will become more expensive, as source materials become unavailable. Vendors on the Darkweb offer special corona goods (scam material) at discounts.

Source: Europol Report, March 2020

OUTLOOK

The number of cyber-attacks is significant and expected to increase further. Cybercriminals will continue to innovate in the deployment of various malware and ransomware packages themed around the COVID-19 pandemic. They may expand their activities to include other types of online attacks.

Cybercriminals are likely to seek to exploit an increasing number of attack vectors as a greater number of employers adopt telework and allow connections to their organisations' systems.

Source: Europol Report, March 2020