INTERPOL

GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT

#WashYourCyberHands

Prolific and opportunistic criminals are taking advantage of the COVID-19 coronavirus pandemic to launch a variety of cyberattacks. In particular, known malware which had been relatively dormant were re-detected since the outbreak began, taking new forms or using COVID-19 to boost their social engineering tactics. Although these cyberthreats are constantly evolving, some of the latest threat identified include:

GLOBAL LANDSCAPE ON COVID-19 CYBERTHREAT

Malicious domains

There has been an increase of domains registered with the key words 'COVID' or 'corona' , to take advantage of the growing number of people searching for information about COVID-19. Many of these are considered to be developed with malicious intent – as of the end of March, 2,022 malicious and 40,261 high-risk newly registered domains were discovered, according to Palo Alto Networks.

Online scams and phishing

Cybercriminals are creating fake websites related to COVID-19 to entice victims into opening malicious attachments or clicking phishing links, resulting in identity impersonation or illegal access to personal accounts. Also, Trend Micro reported that nearly one million spam messages have linked to COVID-19 since January 2020.

Business Email Compromise (BEC) has become the scheme of choice, involving the spoofing of supplier and client email addresses – or use of nearly identical email addresses – to conduct attacks. The extreme need for key supplies provides an ideal scenario for criminals to harvest details or to divert millions of dollars of procurement funds into criminal accounts.

Data-harvesting malware

Data-harvesting malware such as Remote Access Trojan, info stealers, spyware and banking Trojans infiltrate systems, using COVID-19 related information as a lure to compromise networks, steal data, divert money and build botnets.

Disruptive malware (ransomware and DDoS)

Cybercriminals are deploying disruptive malware like ransomware against critical infrastructure and response institutions such as hospitals and medical centres, which are overwhelmed with the health crisis. Such ransomware or DDoS attacks do not typically aim to steal information, but prevent it from accessing critical data or disrupt the system, exacerbating an already dire situation in the physical world.

Vulnerability of working from home

Threat actors are exploiting vulnerabilities of systems, networks, and applications used by businesses, governments and schools to support staff who are now working remotely. As the growing number of people relying on online tools overburdens the security measures put in place prior to the virus outbreak, offenders search for more chances of exposure to steal data, make a profit or cause disruption.

Expected future developments

The cyberthreats facing individuals, businesses and critical infrastructure will continue to evolve causing harm globally, following the rapidly changing social and economic circumstances. Further increases in cybercrime will occur as criminals look for other revenue streams by leveraging the cyber elements of other types of crime. We expect to see:

- Online scams, phishing and BEC will surge due to the economic downturn and shift in business landscape, generating new criminal activities.
- Criminals will take advantage of the underground market to look for 'cybercrime-as-a-service' given the ease of access, low cost and potential high returns that such platforms can offer.
- Threat actors will target individuals' personal information through the spoofing and exploitation of digital content providers.
- Governments, businesses and schools will come to rely on online connectivity and virtual communications tools as employees continue to work from home, increasing their vulnerabilities and presenting more opportunities for cybercriminals to exploit.

INTERPOL's response

INTERPOL's Global Cybercrime Programme is developing and leading the global law enforcement response against cyberthreats which are leveraging the coronavirus outbreak. We use Purple Notices to alert member countries to emerging and high-risk cyberthreats, provide technical guidance to victim organizations for their recovery efforts and conducted a global cybercrime survey to better understand the rapidly evolving global situation. We are also working with online cybersecurity communities and holding emergency virtual meetings with a variety of stakeholders to provide tailored services to member countries for prevention, detection and investigation of cybercrime, including the Heads of national and regional cybercrime units, the INTERPOL Global Cybercrime Expert Group, and our private sector partners.

INTERPOL

INTERPOL General Secretariat
Tel: +33 4 72 44 70 00
www.interpol.int