Covid-19: Cyber criminals exploit changes brought by pandemic

Cyber criminals have sought to capitalise on changes to companies’ and governments’ working practices as a result of the Covid-19 pandemic. James Blake and Eli Polanco outline the effect of the pandemic on cyber crime

Key Points

• Cyber criminals have used the Covid-19 pandemic to increase phishing and malware attacks.
• The rise in remote working and changing financial practices have led to increased points of vulnerabilities for both private companies and governments.
• However, it is likely that this will drive increased willingness to adopt more advanced encryption and information security technology.

The World Health Organization (WHO) stated on 21 March that cyber criminals who had disguised themselves as WHO employees had attempted to steal money and proprietary information from organisations and individuals. In some instances, these criminals designed fake websites or links to appeals from the WHO – or similar organisations – claiming to be related to the Covid-19 response. This is one of many schemes that organised criminals have adopted to profit from the Covid-19 pandemic.

The increase in cyber crime during the Covid-19 pandemic coincided with organised criminal groups continuing to reach higher levels of sophistication and capability. For instance, on 10 March 2020, a combination of state actors and large companies, including Microsoft, disrupted the Necurs botnet, allegedly linked to criminals from Russia. According to a Microsoft blog post on 10 March, Necurs was used for a range of crimes that infected nine million computers globally. Microsoft said that the crimes included “pump-and-dump stock scams, stealing confidential data”, and also for distributing “financially-targeted malware and ransomware and cryptomining”.

According to data from research company Cybersecurity Ventures, by 2021 cyber crime is likely to cost the world USD6 trillion a year. However, in the short term the risk of cyber criminals stealing sensitive data from companies and governments is likely to be heightened by the Covid-19 pandemic.

Coronavirus and cyber threat landscape

According to the cyber-security firm SecDev, there was a 475% increase in ransomware cases between January and March, which correlates largely to the spread of Covid-19. Cyber criminals exploited vulnerabilities presented by significant increases in individuals working remotely through...
phishing and malware attacks. The attacks were largely focused in locations that were already experiencing a significant impact from Covid-19.

G20 leaders attend a video conference to discuss the Covid-19 pandemic on 26 March. Cyber criminals are exploiting the opportunities provided by the greater use of online services as more people work from home. (Gary Ramage/POOL/AFP via Getty Images)

For instance, in the United States, the spike in activity was, at the time of writing, largely focused on the states of New York, California, and Washington, where the highest number of cases of Covid-19 in the US was recorded. According to public statements to the media by the FBI, the majority of attacks were scams, including criminals attempting to steal government aid cheques, attempts on the dark web to sell fake ‘vaccines’ for Covid-19, and fake websites mimicking charities’ appeals to fundraise in response to the disaster.

However, Robert Muggah, co-founder of the Igarapé Institute and The SecDev Foundation, told Jane’s on 26 March that many of the cyber attacks were “targeting cities, utilities, and of course healthcare facilities”. It is likely that these targets will be attacked by those with a political or a criminal motivation. Juliette Kayyem, a former senior adviser in the Homeland Security Advisory Council (HSAC) under President Barack Obama, told Jane’s on 26 March that the most likely beneficiaries of this would be groups affiliated to the Chinese government.

One trend since around 2017 is the growing capabilities and tactical ability of Chinese organised criminal groups. This has made them prominent actors within the pandemic crisis. According to a
2020 report from McAfee’s Advanced Programs Group, Chinese criminal groups have developed their capabilities and attack patterns, which are increasingly internationally focused.

The Covid-19 pandemic is likely to incentivise the transition of even low-capability, or opportunistic, criminals into cyberspace. A rudimentary skillset in sending malware or in basic phishing attacks would enable them to make a profit.

The use of encrypted chat platforms such as Telegram and WhatsApp offers space for cyber criminals to trade skills, join new groups, and offer their skills-for-hire to conduct specific attacks. Encryption in these chat rooms makes it exceptionally difficult for the authorities to monitor them and therefore to mitigate attacks. Along with more established organised cyber groups, it is also likely that these groups will share skillsets, tactics, and resources, and hire ‘consultants’ for specific tasks.

In certain regions across the world, greater use of the dark web may be more common, particularly in Latin and Central America, where it is less well-policed than across Europe and in the West.

[Continued in full version…]

(652 of 2281 words)

For the full version and more content:

Jane’s Military and Security Assessments Intelligence Centre

With structured ORBATs data for more than 17,700 units and 8,900 bases; plus inventories for more than 190 countries, Jane’s Military and Security Assessments allows you to quickly understand and assess capabilities and threats. By connecting this data to the 40,000 structured equipment profiles contained in Jane’s Defence Equipment and Technology Intelligence Centre, Jane’s is uniquely positioned to provide timely, accurate, validated intelligence that delivers unique insights.

To learn more visit http://janes.com/products