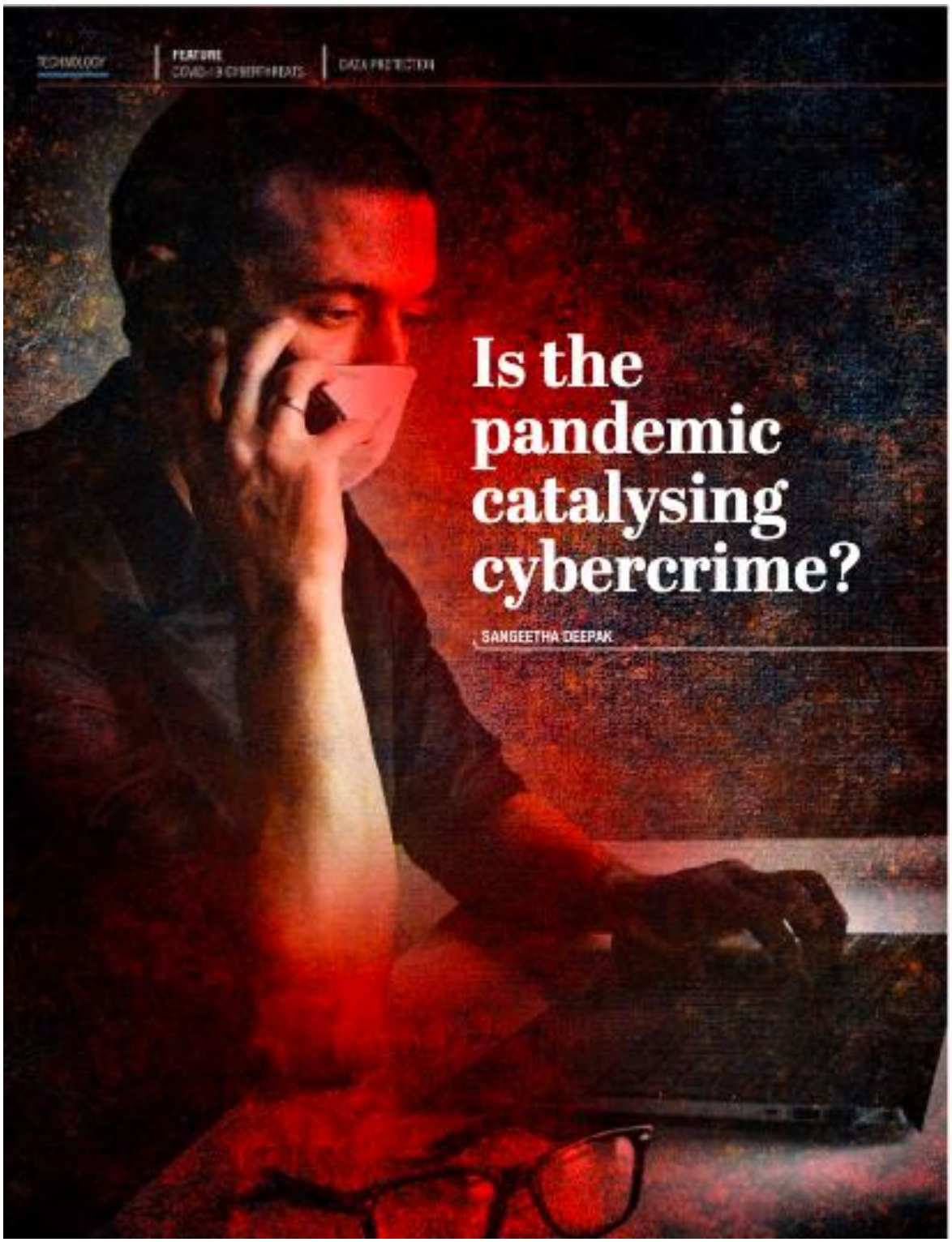
Publication: International Finance Magazine
Date: 25.09.20
URL: https://internationalfinance.com/digital-issue-september-2020/
Title: Is the pandemic catalysing cybercrime?
Author: Jerry Askar, Managing Director of Certes Networks Middle East, Levant and Africa



A 600 percent increase in malicious emails have been recorded this year

The business world is constantly challenged by cybercriminals who often carry out sophisticated cyber attacks to gain access to sensitive data through banks and retail businesses. But this year, cybercrime has seemingly hit a new target: there is a 600 percent increase in malicious emails owing to the coronavirus pandemic, according to the UN disarmament chief Izumi Nakamitsu. It is estimated that one cyber attack takes place every 39 seconds and 90 countries are still in the nascent stages of strengthening their cybersecurity.

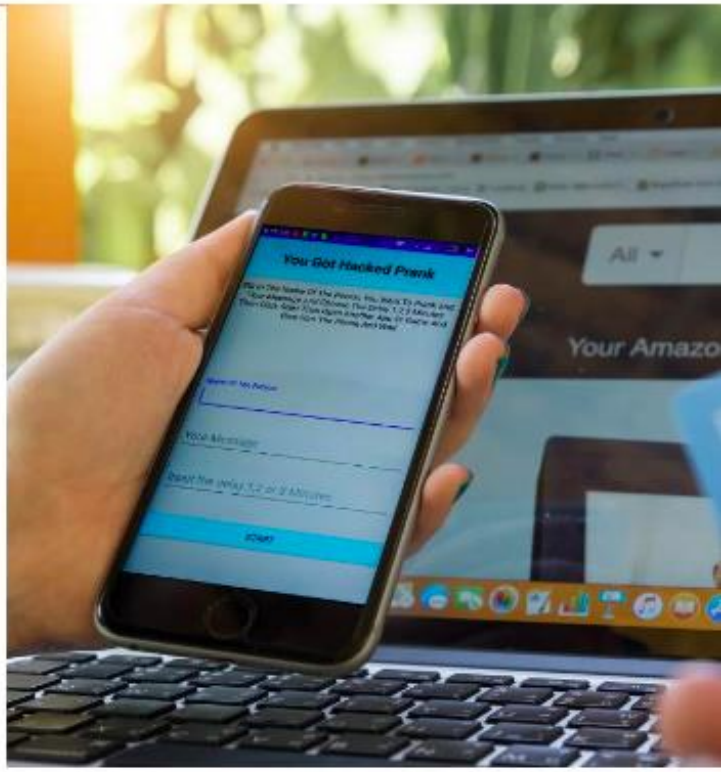
In May, the International Criminal Police Organisation (Interpol) in cooperation with the law enforcement agencies worldwide launched an awareness campaign on cyberthreats during the pandemic. Data analysts firmly believe that hackers are thriving on the distress caused by the pandemic through tools such as data-harvesting malware, ransomware, online scams and phishing. Even so, as David Emm, the principal security researcher at Kaspersky, puts it, "cybercriminals are always on the lookout for topical issues that they can exploit to trick the unwary into installing malware or disclosing personal information that can be used to access their online accounts — and the pandemic provides them with the perfect storm".

For the campaign, Interpol is using Purple Notices to alert member countries to become more aware of the high-risk cybercrimes and victim organisations with technical guidance and conduct global cybercrime surveys to understand the severity of the situation.

"Cybercrime is a topic of interest to everyone around the world and one that is persistent. Cybercriminals are exploiting the disruption caused by the pandemic through a range of phishing and malware attacks. These include messages purporting to come from the World Health Organisation, HMRC, delivery companies, governments and much more. With the coronavirus outbreak making the headlines daily, scams are only becoming more credible and convincing," Emm told **International Finance.**

A statistical analysis shows that an increase in the coronavirus messaging is used to trick people into opening malicious links or attachments and downloading malware, with a 43 percent growth recorded between January and March. Additionally, there has been a surge in brute-force attacks on database servers that were up 23 percent in April. Malicious files planted on websites climbed 8 percent during the same month while network attacks and phishing emails have also risen.

Roberto Bassig, who is the lead partner for technology and risk consulting at PwC, told **International Finance**, that the pandemic has disrupted businesses in many ways, including the immediate shift to digital means in order to maintain business as usual. "Such knee-jerk reactions have opened up risks for people leading to low appreciation of digital technologies, immediate transition from manual to electronic approval of transaction, quick deployment and overnight adoption of untested collaboration tools," he said. "Clearly, these examples create opportunities for



malicious actors to exploit the situation. Therefore, it requires immediate risk assessment to determine the actions needed to align with the risk appetite of the organisation." In short, the pandemic is forcing companies across industries to rethink data security.

One of the more serious challenges faced by companies was the need to enable a full remote workforce. This move has left many of them exposed to high-risk cyberthreats. Roberto points out that most companies have "moved to uncharted waters through adoption of digital technologies for collaboration, transaction processing and work from home arrangements for employees." These efforts are needed to keep businesses afloat and running during unplanned lockdowns—but what are the repercussions of implementing those changes?

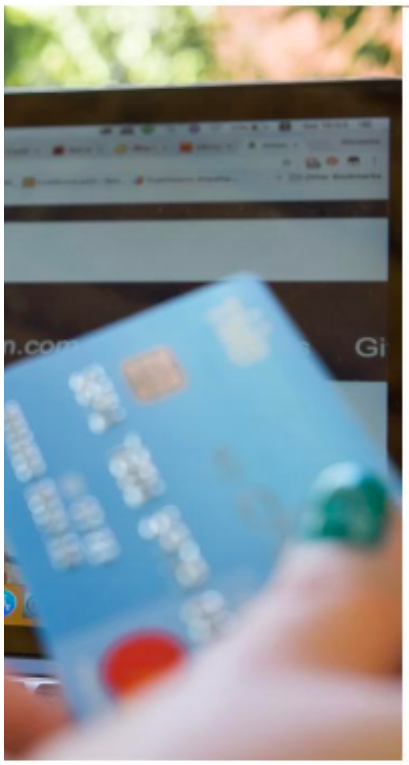
Remote work shows depths of cyber vulnerability

The industry-wide shift to remote working has surfaced new challenges related to physical infrastructure such as wireless networks and secure printing at employees homes. Subsequently, it has uncovered other threats such as employees' connecting to established infrastructure using personal devices that do not carry robust security parameters. Such examples have led to the emergence of new cyber risks. A new research found that mobile phishing is dramatically increasing as cybercriminals target unprotected mobile devices used by employees. With remote working, companies have encountered 31.7 percent rise in mobile phishing, up from 15.8 percent in the last quarter of 2019 to 21.6 percent in the first quarter of 2020.

"The necessary changes needed to be implemented by organisations would be how to ensure that all remote employees working from home can still do their day to day business while ensuring high levels of security for data traveling outside of the internal perimeter," Jerry Askar, the managing director of Certes Networks Middle East, Levant and Africa, told **International Finance**. "The most important element is to maintain maximum data security for employees with remote access and now, suddenly, they have all been moved from inside the "secured" internal perimeter to the outside world connecting to various collaborative tools and cloud applications."

Is the pandemic to be blamed?

The pandemic is creating new opportunities for cybercriminals to capitalise on in the near future. But could it really lead to phishing and business email compromise attacks on a large scale? It is reported that highly targeted business email compromise attacks are growing due to remote work environments this year. In practice, senior executives emails are compromised through fraudulent requests for payments. Typically, cybercriminals leverage a myriad of techniques using social engineering to acquire their targets' trust. This process usually involves months of research as criminals continue to access emails and grasp their targets' language patterns — often tracking their movements such as travel times and off work. Now that the pandemic has made business leaders more available, cybercriminals end up making multiple attempts on their targets' emails, which in turn has limited their power to exploit. So these attacks are increasing in number but resulting in low success rates.



With remote working, companies have encountered

31.7 percent

rise in mobile phishing, up from

15.8 percent

in the last quarter of 2019 to 21.6 percent in the first quarter of 2020

These estimates stoke anxiety and strain credulity, especially since cyber-related hype is constant. On the downside, it has forced companies that historically demonstrated slower adoption of cyber security practices to quickly respond to threats. This means many of them are deploying technologies without testing for a greater purpose. But on the bright side, the fear is also encouraging them to take cybersecurity seriously for the future.

Approaches to fortify cybersecurity

For now, companies will have to explore alternative approaches to data security. According to Aska, this is now more crucial than ever that technology and data security measures are in place to prevent any potential breaches during this transition. "Companies want a data security solution that can be achieved without interruption to their business or network operations with simplicity and ease of deployment," he said. Roberto further explained that companies must revisit their existing information security and protection policies as remote work or virtual arrangements embraced during the pandemic might continue in the foreseeable future. Unfortunately, not many of them have their existing policies and procedures in line with the current shift of work environment. So it is important that companies carry out proper assessment and testing of tools before deployment to fortify their cybersecurity.

In Aska's view, the current situation necessitates companies to adopt cybersecurity alternatives, specifically in areas related to data security and network security posture.. In fact, many cybersecurity companies are addressing these complexities with sophisticated technologies. For example, the Certes Networks' patented Layer 4 technology is aimed to support multiple deployments across a multi-vendor environment on any network or transport. The technology enables companies to be sure that their security posture will scale to support the depth and breadth of their environment, whether deployed top-of-rack, in a virtual environment, between data centres and applications or simply across the WAN or SD-WAN.

In April, HFS Research conducted a study which found that 55 percent of major companies are likely to increase their investments in automation solutions, while 53 percent of them in smart analytics. In addition, 49 percent of them seek to boost their investments in hybrid or multi-cloud, while 46 percent in artificial intelligence. Against this background, only a limited percentage of companies are planning to increase spending on augmented and virtual reality technologies, blockchain and edge computing this year.

The contagion effects of cybercrime is concerning because companies cannot afford to have their work schedules interrupted, lose sensitive business data or be held ransom. "This can be devastating to an organisation or industry which is critical to national infrastructure," Aska said. The impact of the pandemic on global cybersecurity is deep. "Businesses must remember that network security is not data security, so it is crucial that different technology can sufficiently secure the data regardless of the network infrastructure," he concluded. ■

editor@ifinancemag.com