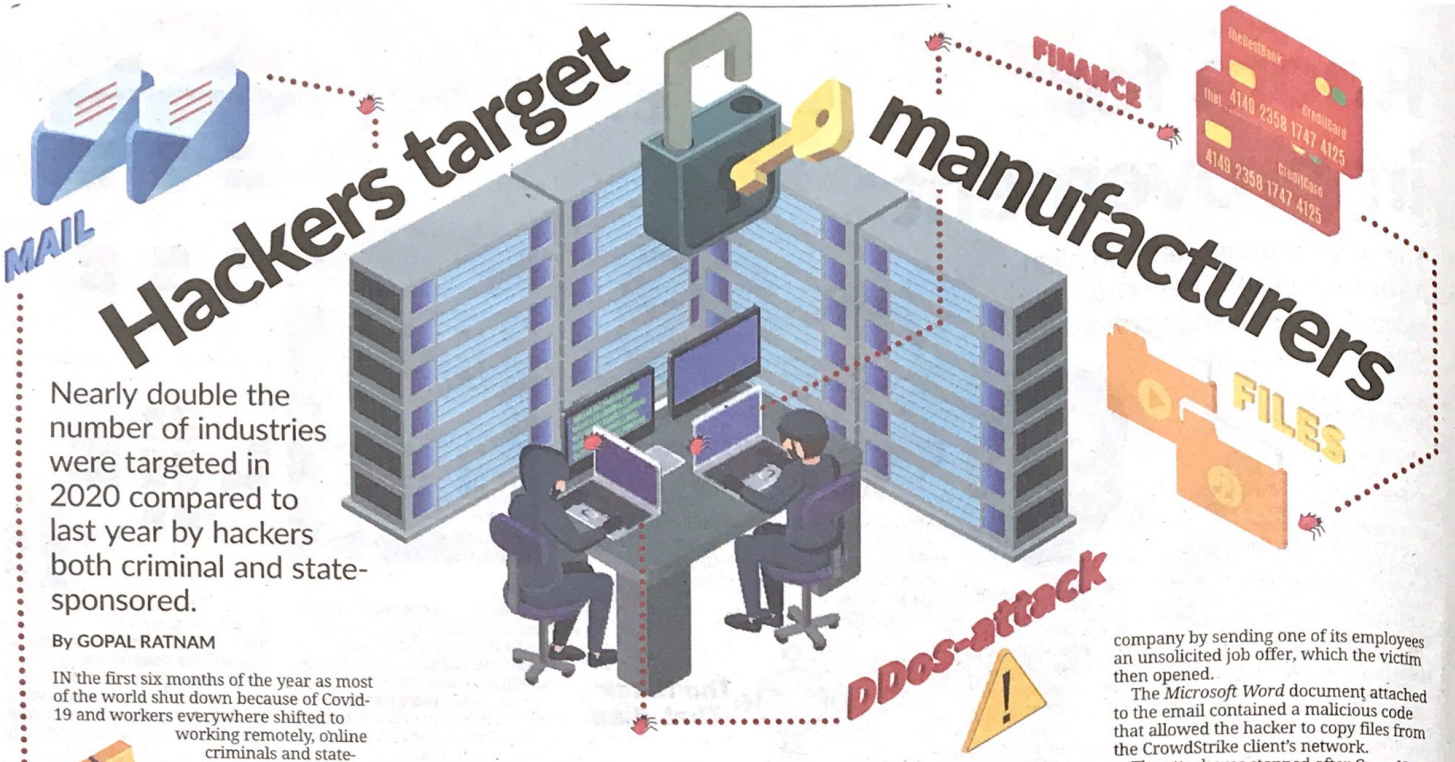
Hackers target manufacturers



Nearly double the number of industries were targeted in 2020 compared to last year by hackers both criminal and state-sponsored.

By GOPAL RATNAM

IN the first six months of the year as most of the world shut down because of Covid-19 and workers everywhere shifted to working remotely, online criminals and state-backed hackers got busy breaking into computer networks, especially those of manufacturing, technology and telecom companies.

Indeed, hackers worked at a greater pace than they did all of last year, according to cybersecurity research firm CrowdStrike.

Companies in as many as 27 different industries fell victim to the hackers, nearly double the number of industries that were targeted in all of 2019, CrowdStrike said in a report made public this month.

While technology, telecom and financial companies are routinely targeted, "the manufacturing industry has experienced a dramatic increase in interactive intrusion activity compared to past years", CrowdStrike said.

Manufacturing companies saw an 11% increase in attacks and intrusions on their networks compared with all of 2019, the company said.

The attacks on manufacturing companies observed by CrowdStrike affected the business systems or front-office networks rather than computers involved in factory control systems, Jennifer Ayers, vice president at CrowdStrike, wrote in an email to CQ Roll Call.

The report is based on CrowdStrike's analysis of attacks on its clients' networks around the globe.

Both online criminals and state-sponsored hackers may have chosen to target industries already left vulnerable because of large-scale disruption in their global supply chain of materials, CrowdStrike said.

Businesses experiencing trouble getting materials and supplies led attackers to believe that the companies may be "more inclined to pay a ransom to prevent further disruption", CrowdStrike said.

Criminal groups "are focused on monetary gain through ransom and extortion by theft of data, whereas state-sponsored attackers are focused on a different agenda which can range from espionage to (intellectual property) theft as examples", Ayers said.

For nation-state hackers, "international trade tensions, increased competition for essential goods, and efforts by some firms to decrease their reliance on offshore suppliers could all have contributed to increased foreign interest in the operations of firms in these sectors", CrowdStrike said in the report.

But in some cases the difference in tactics used by the two kinds of attackers is blurred, with criminal groups willing to play the long game in search of greater profits, the report said.

Working from home

The increase in attacks was also likely driven by the sudden shift to remote working, and the "accelerated set up of new infrastructure by many companies", which may have led to more security gaps and vulnerabilities being exploited, the report said.

Some companies made sure to take the security of their corporate networks into account as they made the transition to remote work, "while some have had to invest heavily or change their security strategy to survive", Ayers said.

"If you had to move the majority of your business to an online presence rapidly but did not employ basic security, that is a ripe target for a criminal actor who could deploy ransomware and request several million dollars to recover," Ayers said.

"That can decimate a business not just operationally but financially as well," Ayers added.

"This year, at this time, it is not an 'if' there will be an attack, it is a 'when' and that statement applies to all companies regardless of size."

Although some industries saw a spike in attacks directed at them, others such as airlines, hospitality and retail businesses saw a drop in hackers targeting them, mostly because the industries were the hardest hit by the Covid-19 pandemic and likely offered little potential for extracting ransoms, CrowdStrike said.

For state-backed hackers, companies in agriculture, healthcare, media, tech and telecom appeared to be the most attractive, with more than one hostile country targeting these sectors, CrowdStrike found.

Key sectors

North Korea and China are both targeting agriculture companies, the report said.

In one case, a North Korean government-backed group code-named Labyrinth Chollima targeted an unnamed agricultural company by sending one of its employees an unsolicited job offer, which the victim then opened.

The *Microsoft Word* document attached to the email contained a malicious code that allowed the hacker to copy files from the CrowdStrike client's network.

The attack was stopped after CrowdStrike identified the attack and took steps to prevent any data loss, the report said.

The attack could be a case of economic espionage targeting a sector that North Korean leader Kim Jong-un has identified as key to the country's economic development, CrowdStrike said.

Six separate Chinese hacking groups are targeting telecom companies, a popular target for state-backed hackers, CrowdStrike said.

An Iran-based hacking group code-named Tracer Kitten used a custom-designed backdoor to break into a telecom company that had operations in Europe, the Middle East and Africa, CrowdStrike said.

The telecom "industry still remains firmly within the crosshairs for targeted attacks, the motivations of which are likely associated with espionage and data theft objectives", CrowdStrike said.

In another case involving an attack on a healthcare company in Asia, CrowdStrike found that Chinese hackers had penetrated the company's network using a remote-access tool that masqueraded as a genuine Microsoft Windows process available on GitHub, an online platform that hosts open-source software code used by programmers.

Companies across the globe need to step up investment and attention on defending their computer networks, CrowdStrike said.

"In my opinion, defence can be less expensive" than trying to recover from an attack, Ayers said. – CQ-Roll Call/Tribune News Service