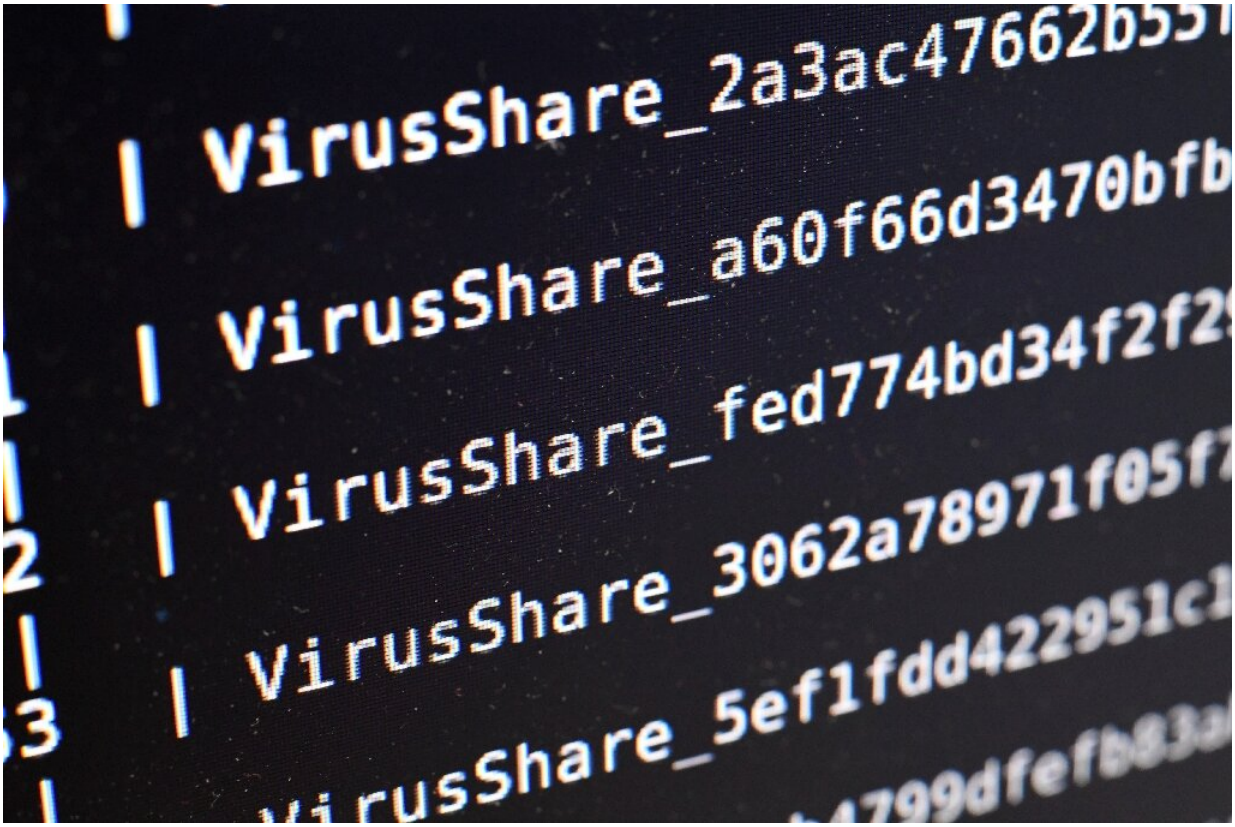
Rising cyberattacks in West highlight vulnerabilities

May 25 2021, by Didier Lauras



Firms and experts have been warning for years about the rising tide of online attacks—some state-orchestrated, some criminally motivated.

A series of high-profile cyberattacks on targets in the West have highlighted the vulnerability of companies and institutions, making the

issue a higher public priority but with no easy solution.

The latest incident to underline the capacity of cybercriminals to disrupt daily life came in early May when Colonial Pipeline, a US-based operator of a key fuel pipeline, became a victim of ransomware.

The attack saw its computer systems encrypted, putting its operations offline and causing fuel shortages for American drivers.

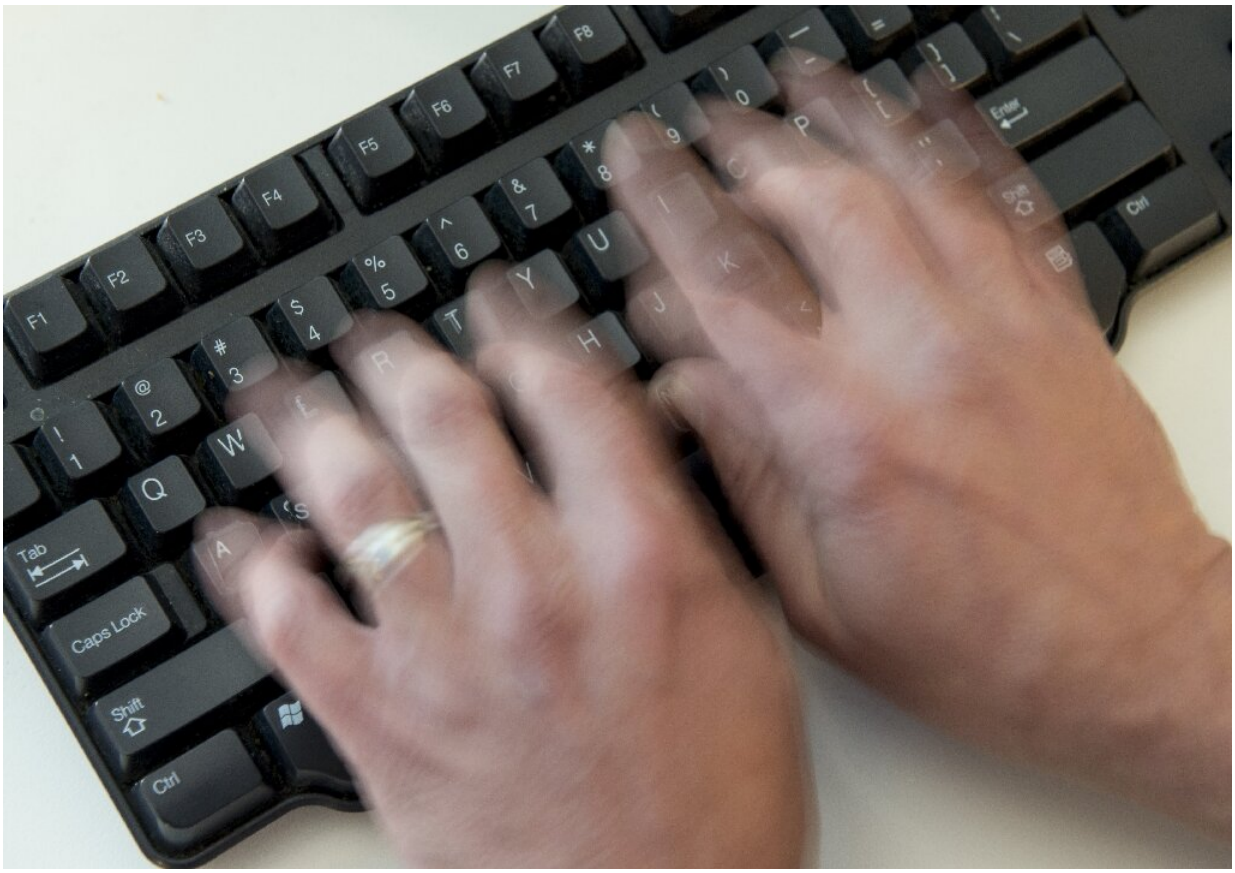
At the end of 2020, US authorities also revealed that hackers had compromised SolarWinds software which was run by large parts of the US government and companies around the country. Russia was blamed.

Other attacks include the hacking of the Democratic Party ahead of the 2016 US election as well as the major global malware outbreaks called WannaCry and NotPetya which paralysed computers all over the world in 2017.

Beyond the major incidents that make the news, cybersecurity firms and experts have been warning for years about the rising tide of online attacks—some state-orchestrated, some criminally motivated.

"It is hard to imagine that we haven't had enough significant cyber incidents for everyone to realise how important it is," said Suzanne Spaulding of the Center for Strategic and International Studies, a Washington-based think-tank.

Despite all of them, the issue "has not been given sufficient priority," she said.



The best defences against cybercrime are simple: deleting suspect emails, updating software regularly, changing passwords, and keeping saved back-ups.

Complacency

The best defences against cybercrime by individuals and small companies are simple and almost free: deleting suspect emails, updating software regularly, changing passwords, and keeping saved back-ups.

Larger organisations can afford specialised IT security teams and the best-equipped employ outside monitoring services to keep an eye on their networks and check for intrusions round-the-clock that foretell a major attack.

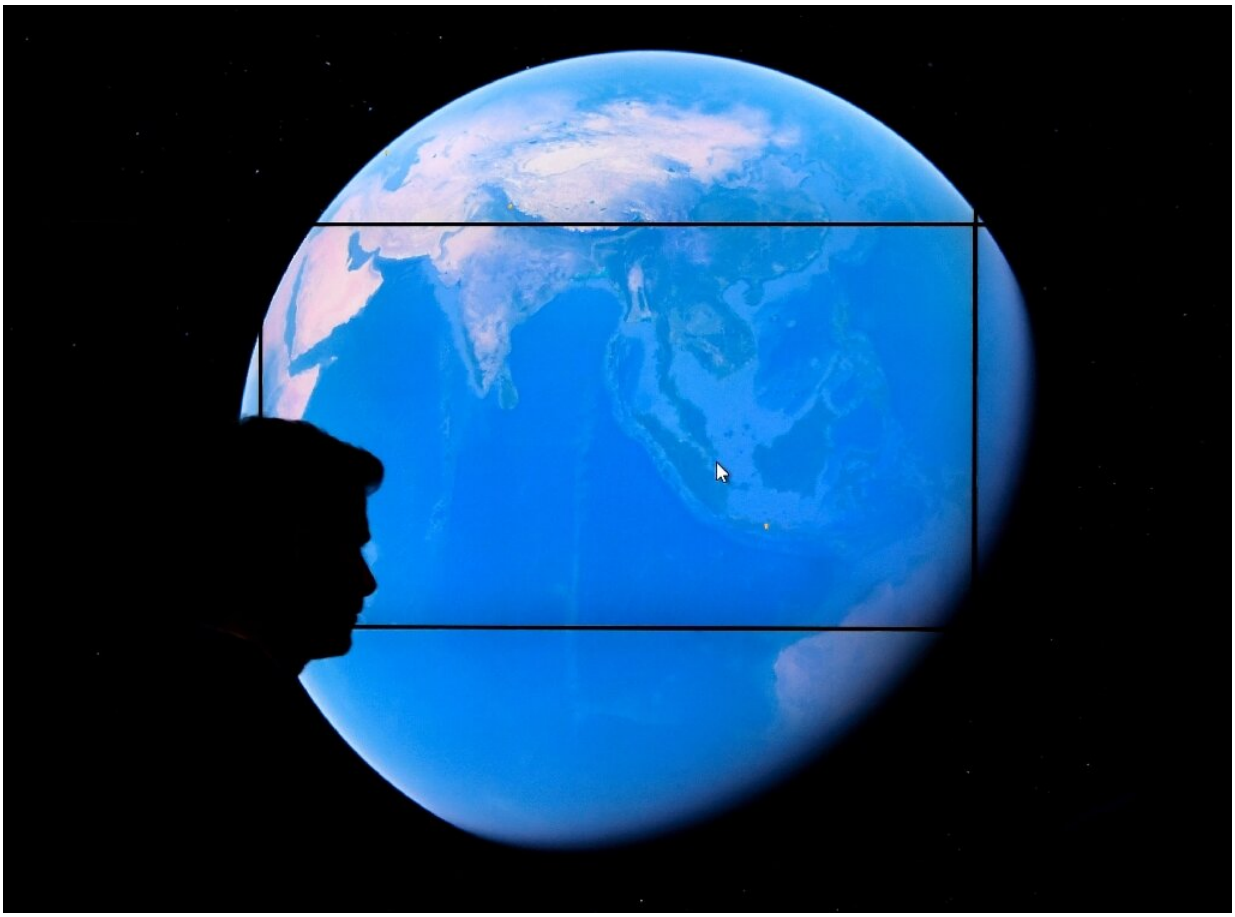
But many organisations are complacent, said Spaulding.

"There are two kinds of companies in the world, those who have been hacked and those who haven't detected it yet," she told AFP.

Another problem is that many countries are not producing enough trained IT technicians, which drives up wages for the most sought-after skills, putting them beyond the reach of many organisations, particularly in the public sector.

Adam Meyers from cybersecurity firm CrowdStrike says the key to safety is often simply being better protected than the weakest targets.

"There's an old adage that you don't have to run faster than the bear to get away. You have to run faster than the person next to you," he said.



Western governments have been building up their own cyber-military powers, which enable them to investigate and deflect attacks.

State capabilities

One area that has been prioritised by Western governments is building up their own cyber-military powers, which enable states to investigate and deflect attacks, as well as carry out their own spying and operations.

"For the last decade, it's been in the toolbox of armies and intelligence services as part of a conflict that is not necessarily open, but is latent," said Julien Nocetti, a researcher at the Geode institute at Paris 8

university.

The National Cyber Power Index by the Belfer Centre at Harvard University puts the United States at the top of 30 countries ranked on their ambitions and cyber-capabilities, with China second, and Britain third.

The reach and power of the US National Security Agency was laid bare in 2013 following leaks by fugitive contractor Edward Snowden.

"Europe and the United States are sometimes shown as being the victims and the nice guys in this domain ... but that's not how it is. There's a general blindness about our own operations," said Nocetti.

And the rules of engagement are still being defined, with a multilateral attempt to create some sort of framework for states failing to make progress.

Some experts worry that one day a state-backed cyberattack will trigger a spiral of reprisals and counter-reprisals that could trigger real-life hostilities.

Countries may have built up enough digital weapons to serve as a deterrent.

"One of the reasons why Russia, the US and China don't turn each other's lights off is because they are afraid of what the reaction would be," said Adam Segal, director of the Digital and Cyberspace Policy program at the Council on Foreign Relations, a US think-tank.