Up to 1,500 firms hit in Kaseya ransomware attack

July 6 2021, by Katy Lee

Sweden's Coop supermarket chain is racing to reopen hundreds of stores closed as a result of the ransomware attack.

Hundreds of Swedish supermarkets remained shut Tuesday after a major cyberattack that has crippled hundreds of companies worldwide for the past four days, with the perpetrators demanding $70 million in bitcoin to undo the damage.

Kaseya, the Miami-based IT company at the centre of the hack, said late Monday that up to 1,500 businesses had been affected by Friday's attack, which has been blamed on Russian-speaking hackers.

Experts believe this could be the biggest "ransomware" attack on record—an increasingly lucrative form of digital hostage-taking in which hackers encrypt victims' data and then demand money for restored access.

The Kaseya attack has ricocheted around the world, affecting businesses from pharmacies to gas stations in at least 17 countries, as well as dozens of New Zealand kindergartens.

Most of Sweden's 800 Coop supermarkets were shut for a third day running after the hack paralysed its cash registers.

"Before the end of the day, the hope is that there will be more open stores than closed ones," Coop press officer Tarik Belqaid told broadcaster SVT.

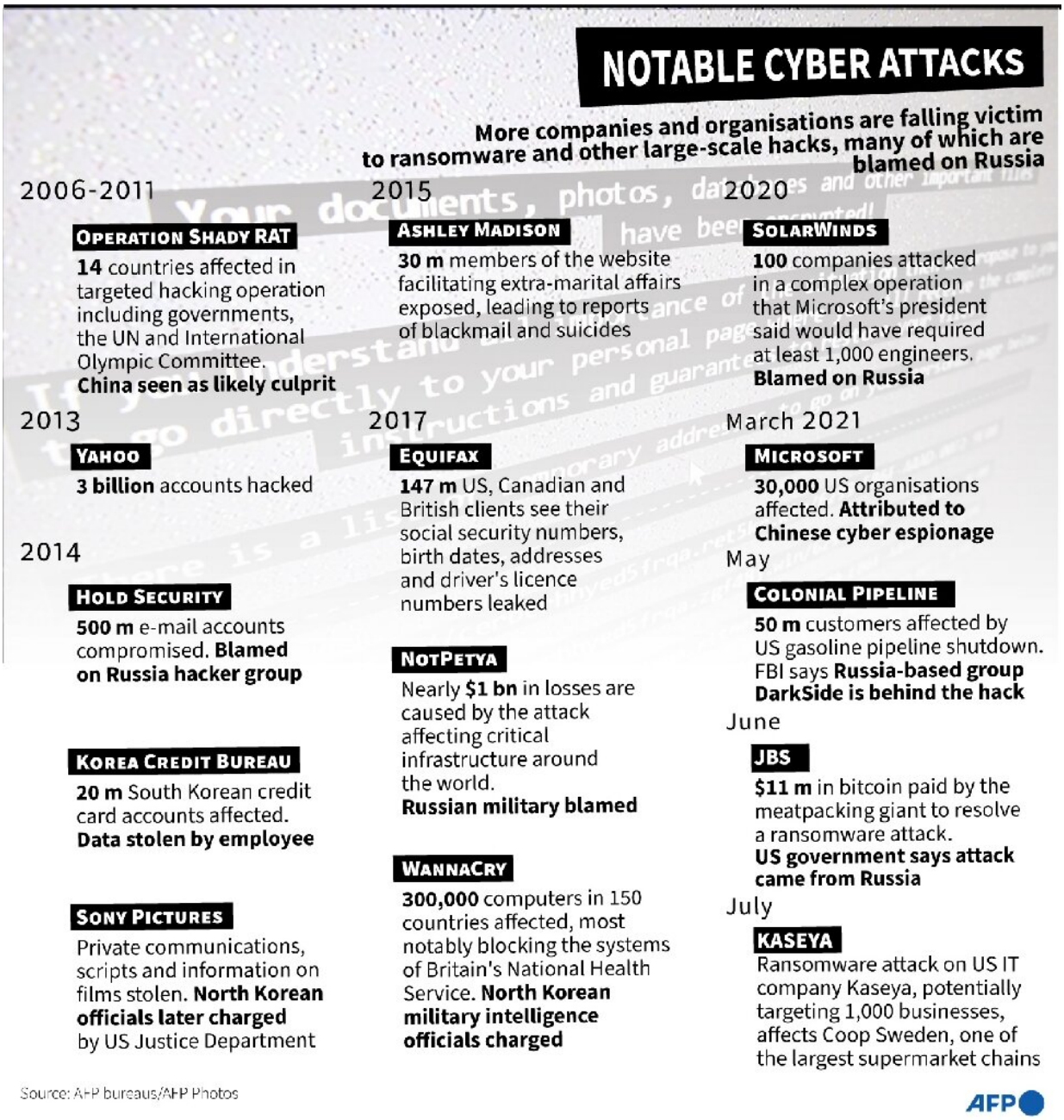
While Kaseya is little known to the public, cybersecurity analysts say it was a ripe target as its software is used by thousands of companies, allowing the hackers to paralyse a huge number of businesses with a single blow.

Kaseya provides IT services to some 40,000 businesses globally, some of whom in turn manage the computer systems of other businesses.

The hack affected users of its signature VSA software, which is used to manage networks of computers and printers.

While Kaseya said Monday that while less than 60 of its own customers were "directly compromised", it estimated that up to "1,500 downstream businesses" had been affected.

Kaseya said it was hoping to bring its own servers back online Tuesday afternoon between 2:00 pm and 5:00 pm Eastern Time, with a software update released within the following 24 hours to allow customers to restore their systems.



Notable cyber attacks since 2006.

Going out with a bang?

REvil, a group of Russian-speaking hackers who are prolific perpetrators of ransomware attacks, are believed to be behind Friday's assault.

A post on Happy Blog, a site on the dark web associated with the group, claimed responsibility for the attack, saying it had infected "more than a million systems".

The hackers demanded $70 million in bitcoin in exchange for the publication of an online tool that would decrypt the stolen data.

While the hackers are thought to have been reaching out to individual victims requesting smaller payments, the unprecedented demand for $70 million has surprised analysts.

French cybersecurity expert Robinson Delaugerre suggested that REvil could be treating the Kaseya attack as a final spectacular act before going out of business.

The group was responsible for around 29 percent of ransomware attacks in 2020, according to IBM's Security X-Force unit, looting an estimated $123 million.

"Our hypothesis is that REvil is going to disappear and this is its final big act," he told AFP, predicting that the group—which also goes by the name Sodinokibi—could re-emerge under a new name.

The FBI believes REvil was also behind a ransomware attack last month on global meat-processing giant JBS, which ended up paying $11 million to the hackers.

The United States has been a particular target of high-profile ransomware attacks in recent months blamed on Russia-based hackers, with the Colonial oil pipeline and IT firm SolarWinds among the targets.