Number of victims in major ransomware attack still unclear

6 July 2021, by Frank Bajak

A sign that reads: "Coop Forum supermarket in Vastberga is closed due to IT disturbances, no prognosis as to when we will open again", on a closed Coop supermarket store in the suburb of Vastberga, Stockholm, Sweden, Saturday July 3, 2021. Cybersecurity teams worked feverishly Sunday July 4, 2021, to stem the impact of the single biggest global ransomware attack on record, with some details emerging about how the Russia-linked gang responsible breached the company whose software was the conduit. The Swedish grocery chain Coop said most of its 800 stores would be closed for a second day Sunday because their cash register software supplier was crippled. Credit: Jonas Ekstromer/TT via AP, File

The company whose software was exploited in the biggest ransomware attack on record said Tuesday that so far it appears fewer than 1,500 businesses were compromised. But cybersecurity experts suspect the estimate is low and note that victims are still being identified.

A couple examples of the impact the attack has had in the at least 17 countries affected: the weekend shuttering most of the 800 supermarkets in the Swedish Coop chain because the malware crippled their cash registers, and the reported knocking offline o f more than 100 New Zealand kindergartens.

Miami-based Kaseya said that it believes only about 800 to 1,500 of the estimated 800,000 to 1,000,000 mostly small business end-users of its software were affected. They are customers of companies that use Kaseya's virtual system administrator, or VSA, product to fully manage their IT infrastructure.

The statement was widely reported after the White House shared it with media outlets.

Cybersecurity experts said, however, it is too early for Kaseya to know the true impact of Friday's attack. They note that because it was launched by the Russia-linked REvil gang on the eve of the Fourth of July holiday weekend in the U.S., many targets may only be discovering it upon returning to work Tuesday.

Ransomware criminals infiltrate networks and sow malware that cripples them by scrambling all their data. Victims get a decoder key when they pay up. Most ransomware victims don't publicly report attacks or disclose if they've paid ransoms. In the U.S, disclosure of a breach is required by state laws when personal data that can be used in identity theft is stolen. Federal law mandates it when healthcare records are exposed.

Unlike many ransomware attacks, the criminals in this one apparently had no time to steal data before locking up networks. They are demanding up to $5 million for bigger victims, and $45,000 for small ones.

And in what many researchers considered a PR stunt, REvil is offering on its site on the dark web to release a universal software decoder to free all victims in exchange for a lump sum payment of $70 million. It did not say who it expected to pay. The

criminals claim to have infected a million systems.

In this July 3, 2021 file photo, a sign reads: " Temporarily Closed. We have an IT-disturbance and our systems are not functioning", posted in the window of a closed Coop supermarket store in Stockholm, Sweden. Cybersecurity teams worked feverishly Sunday July 4, 2021, to stem the impact of the single biggest global ransomware attack on record, with some details emerging about how the Russia-linked gang responsible breached the company whose software was the conduit. The Swedish grocery chain Coop said most of its 800 stores would be closed for a second day Sunday because their cash register software supplier was crippled. Credit: Ali Lorestani/TT via AP, File

Most of the more than 60 Kaseya customers that company spokeswoman Dana Liedholm said were affected are managed service providers (MSPs), with multiple customers downstream.

"Given the relationship between Kaseya and MSPs, it's not clear how Kaseya would know the number of victims impacted. There is no way the numbers are as low as Kaseya is claiming though," said Jake Williams, chief technical officer of the cybersecurity firm BreachQuest.

The hacked VSA tool remotely maintains customer networks, automating security and other software updates. Essentially, a product designed to protect networks from malware was cleverly used to distribute it.

"It's too soon to tell, since this entire incident is still under investigation," said the cybersecurity firm Sophos, which has been tracking the incident closely. It and other cybersecurity outfits questioned whether Kaseya had visibility into the crippled managed service providers.

In an interview with The Associated Press on Sunday, Kaseya CEO Fred Voccola estimated the number of victims in "the low thousands." The German news agency dpa reported earlier Sunday an unnamed German IT services company told authorities several thousand of its customers were compromised. Also among reported victims were two Dutch IT services companies.

A broad array of businesses and public agencies were hit by the latest attack, apparently on all continents, including in financial services, travel and leisure and the public sector—though few large companies, Sophos said.

Liedholm, the Kaseya spokeswoman, said the vast majority of the company's 37,000 customers were unaffected and said the company expects to release a patch Wednesday.

The attackers, previously best known for extorting $11 million from the meat-processing giant JBS after crippling its Australian and New Zealand plants on Memorial Day, broke into at least one Kaseya server after identifying a "zero day" vulnerability, cybersecurity researchers said.

In this July 3, 2021 file photo, a sign reads: " Temporarily

Closed. We have an IT-disturbance and our systems are not functioning", posted in the window of a closed Coop supermarket store in Stockholm, Sweden. Cybersecurity teams worked feverishly Sunday July 4, 2021, to stem the impact of the single biggest global ransomware attack on record, with some details emerging about how the Russia-linked gang responsible breached the company whose software was the conduit. The Swedish grocery chain Coop said most of its 800 stores would be closed for a second day Sunday because their cash register software supplier was crippled. Credit: Ali Lorestani/TT via AP, File

Dutch vulnerability researchers said they alerted Kaseya to a number of "severe vulnerabilities" ahead of the attack.

"We think they have been responsible in the way they responded to our disclosure and we actually have seen them reacting diligently," said Frank Breedijk of the Dutch Institute for Vulnerability Disclosure. "Unfortunately, too late. The malware gang beat us in the end sprint."

Neither Breedijk nor Kaseya would say when the Dutch researchers alerted the company to exploited vulnerabilities.

President Joe Biden said Saturday that he ordered a "deep dive" by U.S. intelligence into the attack and that the U.S. would respond if it determines the Kremlin is involved. Moscow gives REvil and other ransomware gangs safe haven as long as they refrain from domestic attacks. Biden asked Vladimir Putin in Geneva last month to put and end to that but there is no indication the Russian president has moved to do so.

Analysts say the chaos ransomware criminals have wrought in the past year—hitting hospitals, schools, local governments and other targets at the rate of about one every eight minutes—serves Putin's strategic agenda of destabilizing the West.

The cybersecurity company Mandiant was leading the response to the Kaseya crisis, coordinating with the Cybsecurity and Infrastructure Security Agency, Kaseya said.

On Saturday, the FBI said in a statement that the attack's scale "may make it so that we are unable to respond to each victim individually." The next day, the White House urged all victims to notify the FBI.

Federal lawmakers are working on bipartisan legislation to make the reporting of ransomware attacks mandatory in the case of critical infrastructure, with government officials deciding whether to make details public.