Biden: US damage appears minimal in big ransomware attack

July 7 2021, by Frank Bajak and Zeke Miller

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

President Joe Biden said Tuesday that damage to U.S. businesses in the biggest ransomware attack on record appears minimal, though information remained incomplete. The company whose software was exploited said fewer than 1,500 businesses worldwide appeared compromised but cybersecurity experts caution that the incident isn't over.

Also Tuesday, a security researcher who chatted online with representatives of the Russia-linked REvil gang behind the attack said they claimed to have stolen data from hundreds of companies, but offered no evidence.

Answering a reporter's question at a vaccine-related White House event, Biden said his national security team had updated him Tuesday morning on the attack, which exploited a powerful remote-management tool run by Miami-based software company Kaseya in what is known as a supply-chain attack.

"It appears to have caused minimal damage to U.S. businesses but we're still gathering information," Biden said. "And I'm going to have more to say about this in the next several days." An official at the Cybersecurity and Infrastructure Security Agency, speaking on condition they not be further identified, said no federal agencies or critical infrastructure appear to have been impacted.

On Wednesday, Biden and Vice President Kamala Harris will lead an

interagency meeting to discuss the administration's efforts to counter ransomware.

White House spokeswoman Jen Psaki held out the prospect of retaliatory action. What Biden told President Vladimir Putin in Geneva last month still holds, she said: "If the Russian government cannot or will not take action against criminal actors residing in Russia, we will take action or reserve the right to take action on our own."

What sort of action that would be is unclear.

Biden has said repeatedly that the Kremlin bears responsibility for giving ransomware criminals safe harbor, even if it is not directly involved. There is no indication that Putin has moved against the gangs. Psaki said Russian and U.S. representatives were meeting next week and would discuss the matter.

Further underscoring the geopolitical stakes in cyberspace, the Republican National Committee said Tuesday that it had been informed over the weekend that one of its contractors had been breached, though it was not immediately clear by whom. The RNC said no data was accessed.

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

The contractor, Synnex, initially said that the action "could potentially be in connection with the recent cybersecurity attacks of Managed Service Providers," a likely reference to the breaches last week. But it backed away from that claim in a second statement late Tuesday.

Friday's attack hobbled businesses in at least 17 countries. It shuttered most of the 800 supermarkets in the Swedish Coop chain over the weekend because cash registers stopped working, and reportedly knocked more than 100 New Zealand kindergartens offline.

Kaseya said 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.

Cybersecurity experts said, however, it is too early for Kaseya to know the true impact given its launch on the eve of the Fourth of July holiday weekend in the U.S. They said many targets might only discover 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.

Security researchers said that in this attack, the criminals did not appear to have had time to steal data before locking up networks. That raised the question whether the motivation behind the attack was profit alone, because extortion through threatening to expose sensitive pilfered data betters the odds of big payoffs.

But Ryan Sherstobitoff, threat intelligence chief of the cybersecurity firm Security Scorecard, said REvil representatives claimed Saturday to have stolen data from hundreds of companies and were threatening to

sell it if ransom demands of up to $5 million for bigger victims—they were seeking $45,000 per infected computer—were not met.

"The operators are claiming that, though there is not necessarily direct evidence," added Sherstobitoff, who said he masqueraded as a victim to engage the criminals. He said the criminals claimed banks were among victims.

REvil offered a universal software decoder to free all victims in exchange for a lump sum payment of $50 million, he added. On Sunday, that sum rose to $70 million in a post on the criminals' dark web site.

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

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.

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. Others researchers also questioned Kaseya's visibility into crippled managed service providers.

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.

In an interview on Sunday, Kaseya CEO Fred Voccola estimated the number of victims in "the low thousands." The German news agency dpa had reported that an unnamed German IT services company told

authorities that 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, apparently on all continents, including in financial services, travel and leisure and the public sector—though few large companies, the cybersecurity firm Sophos said.

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

REvil, previously best known for extorting $11 million from the meat-processing giant JBS after hobbling it on Memorial Day, broke into at least one Kaseya server after identifying a "zero day" vulnerability, cybersecurity researchers said.

Dutch researchers said they alerted Kaseya to the zero day and a number of "severe vulnerabilities" ahead of the attack. Neither they nor Kaseya would say how far in advance.