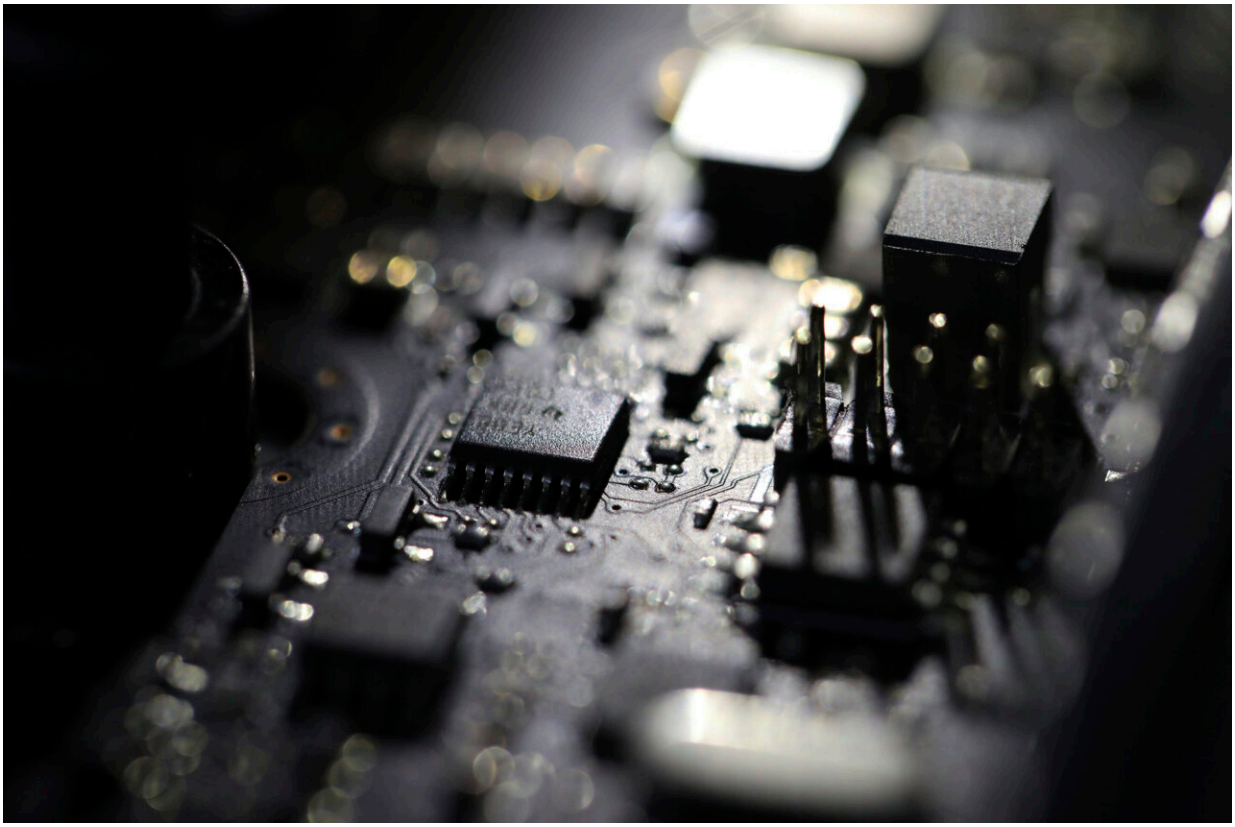
Ransomware attack before holiday leaves companies scrambling

July 3 2021, by Matt O'brien



This Feb 23, 2019, file photo shows the inside of a computer in Jersey City, N.J. A ransomware attack paralyzed the networks of at least 200 U.S. companies on Friday, July 2, 2021, according to a cybersecurity researcher whose company was responding to the incident. Credit: AP Photo/Jenny Kane, File

Businesses around the world rushed Saturday to contain a ransomware

attack that has paralyzed their computer networks, a situation complicated in the U.S. by offices lightly staffed at the start of the Fourth of July holiday weekend.

It's not yet known how many organizations have been hit by demands that they pay a ransom in order to get their systems working again. But some cybersecurity researchers predict the attack targeting customers of software supplier Kaseya could be one of the broadest ransomware attacks on record.

It follows a scourge of headline-grabbing attacks over recent months that have been a source of diplomatic tension between U.S. President Joe Biden and Russian President Vladimir Putin over whether Russia has become a safe haven for cybercriminal gangs.

Biden said Saturday he didn't yet know for certain who was responsible but suggested that the U.S. would respond if Russia was found to have anything to do with it.

"If it is either with the knowledge of and or a consequence of Russia then I told Putin we will respond," Biden said. "We're not certain. The initial thinking was it was not the Russian government."

Cybersecurity experts say the REvil gang, a major Russian-speaking ransomware syndicate, appears to be behind the attack that targeted the software company Kaseya, using its network-management package as a conduit to spread the ransomware through cloud-service providers.

"The number of victims here is already over a thousand and will likely reach into the tens of thousands," said cybersecurity expert Dmitri Alperovitch of the Silverado Policy Accelerator think tank. "No other ransomware campaign comes even close in terms of impact."

The cybersecurity firm ESET says there are victims in least 17 countries, including the United Kingdom, South Africa, Canada, Argentina, Mexico, Kenya and Germany.

In Sweden, most of the grocery chain Coop's 800 stores were unable to open because their cash registers weren't working, according to SVT, the country's public broadcaster. The Swedish State Railways and a major local pharmacy chain were also affected.

Kaseya CEO Fred Voccola said in a statement that the company believes it has identified the source of the vulnerability and will "release that patch as quickly as possible to get our customers back up and running."

Voccola said fewer than 40 of Kaseya's customers were known to be affected, but experts said the ransomware could still be affecting hundreds more companies that rely on Kaseya's clients that provide broader IT services.

John Hammond of the security firm Huntress Labs said he was aware of a number of managed-services providers—companies that host IT infrastructure for multiple customers—being hit by the ransomware, which encrypts networks until the victims pay off attackers.

"It's reasonable to think this could potentially be impacting thousands of small businesses," said Hammond, basing his estimate on the service providers reaching out to his company for assistance and comments on Reddit showing how others are responding.

At least some victims appeared to be getting ransoms set at $45,000, considered a small demand but one that could quickly add up when sought from thousands of victims, said Brett Callow, a ransomware expert at the cybersecurity firm Emsisoft.

Callow said it's not uncommon for sophisticated ransomware gangs to perform an audit after stealing a victim's financial records to see what they can really pay, but that won't be possible when there are so many victims to negotiate with.

"They just pitched the demand amount at a level most companies will be willing to pay," he said.

Voccola said the problem is only affecting its "on-premise" customers, which means organizations running their own data centers. It's not affecting its cloud-based services running software for customers, though Kaseya also shut down those servers as a precaution, he said.

The company added in a statement Saturday that "customers who experienced ransomware and receive a communication from the attackers should not click on any links—they may be weaponized."

Gartner analyst Katell Thielemann said it's clear that Kaseya quickly sprang to action, but it's less clear whether their affected clients had the same level of preparedness.

"They reacted with an abundance of caution," she said. "But the reality of this event is it was architected for maximum impact, combining a supply chain attack with a ransomware attack."

Supply chain attacks are those that typically infiltrate widely used software and spread malware as it updates automatically.

Complicating the response is that it happened at the start of a major holiday weekend in the U.S., when most corporate IT teams aren't fully staffed.

That could also leave those organizations unable to address other security

vulnerabilities, such a dangerous Microsoft bug affecting software for print jobs, said James Shank, of threat intelligence firm Team Cymru.

"Customers of Kaseya are in the worst possible situation," he said. "They're racing against time to get the updates out on other critical bugs."

Shank said "it's reasonable to think that the timing was planned" by hackers for the holiday.

The U.S. Chamber of Commerce said it was affecting hundreds of businesses and was "another reminder that the U.S. government must take the fight to these foreign cybercriminal syndicates" by investigating, disrupting and prosecuting them.

The federal Cybersecurity and Infrastructure Security Agency said in a statement that it is closely monitoring the situation and working with the FBI to collect more information about its impact.

CISA urged anyone who might be affected to "follow Kaseya's guidance to shut down VSA servers immediately." Kaseya runs what's called a virtual system administrator, or VSA, that's used to remotely manage and monitor a customer's network.

The privately held Kaseya is based in Dublin, Ireland, with a U.S. headquarters in Miami.

REvil, the group most experts have tied to the attack, was the same ransomware provider that the FBI linked to an attack on JBS SA, a major global meat processor forced to pay a $11 million ransom, amid the Memorial Day holiday weekend in May.

Active since April 2019, the group provides ransomware-as-a-service,

meaning it develops the network-paralyzing software and leases it to so-called affiliates who infect targets and earn the lion's share of ransoms.

U.S. officials have said the most potent ransomware gangs are based in Russia and allied states and operate with Kremlin tolerance and sometimes collude with Russian security services.

Alperovitch said he believes the latest attack is financially motivated and not Kremlin-directed.

However, he said it shows that Putin "has not yet moved" on shutting down cybercriminals within Russia after Biden pressed him to do so at their June summit in Switzerland.

Asked about the attack during a trip to Michigan on Saturday, Biden said he had asked the intelligence community for a "deep dive" on what happened. He said he expected to know more by Sunday.