Kaseya gets master decryption key after July 4 global attack

July 22 2021, by Frank Bajak

In this July 3, 2021 photo, 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. The Biden administration will offer rewards up to $10 million for information leading to the identification of foreign state-sanctioned malicious cyber activity against critical U.S. infrastructure, including

ransomware attacks. The administration is launching the website stopransomware.gov to offer the public resources for countering the threat. Credit: Jonas Ekstromer/TT via AP, File

The Florida company whose software was exploited in the devastating Fourth of July weekend ransomware attack, Kaseya, has received a universal key that will decrypt all of the more than 1,000 businesses and public organizations crippled in the global incident.

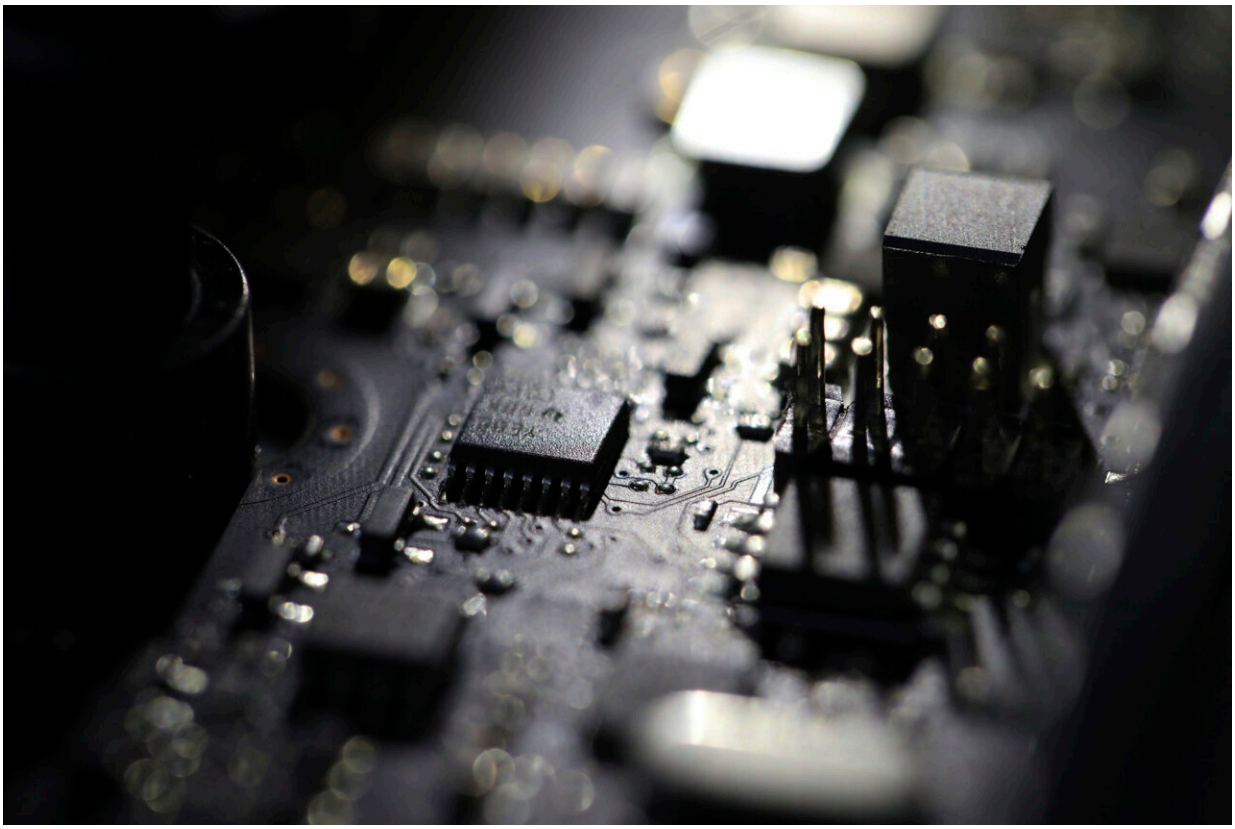
Kaseya spokeswoman Dana Liedholm would not say Thursday how the key was obtained or whether a ransom was paid. She said only that it came from a "trusted third party" and that Kaseya was distributing it to all victims. The cybersecurity firm Emsisoft confirmed that the key worked and was providing support.

Ransomware analysts offered multiple possible explanations for why the master key, which can unlock the scrambled data of all the attack's victims, has now appeared. They include: Kaseya paid; a government paid; a number of victims pooled funds; the Kremlin seized the key from the criminals and handed it over through intermediaries—or perhaps the main attacker didn't get paid by the gang whose ransomware was used.

The Russia-linked criminal syndicate that supplied the malware, REvil, disappeared from the internet on July 13. That likely deprived whoever carried out the attack of income because such affiliates split ransoms with the syndicates that lease them the ransomware. In the Kaseya attack, the syndicate was believed overwhelmed by more ransom negotiations than it could manage, and decided to ask $50 million to $70 million for a master key that would unlock all infections.

In this July 3, 2021 photo, a closed Coop supermarket store in the suburb of Vastberga, Stockholm. 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

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. The Biden administration will offer rewards up to $10 million for information leading to the identification of foreign state-sanctioned malicious cyber activity against critical U.S. infrastructure, including ransomware attacks. The administration is launching the website stopransomware.gov to offer the public resources for countering the threat. Credit: Ali Lorestani/TT via AP, File



This Feb 23, 2019, file photo shows the inside of a computer. The Biden administration will offer rewards up to $10 million for information leading to the identification of foreign state-sanctioned malicious cyber activity against critical U.S. infrastructure, including ransomware attacks. The administration is launching the website stopransomware.gov to offer the public resources for countering the threat. Credit: AP Photo/Jenny Kane, File

This Feb 23, 2019, file photo shows the inside of a computer in Jersey City, N.J. The Biden administration will offer rewards up to $10 million for information leading to the identification of foreign state-sanctioned malicious cyber activity against critical U.S. infrastructure, including ransomware attacks. The administration is launching the website stopransomware.gov to offer the public resources for countering the threat. Credit: AP Photo/Jenny Kane, File

By now, many victims will have rebuilt their networks or restored them from backups.

It's a mixed bag, Liedholm said, because some "have been in complete lockdown." She had no estimate of the cost of the damage and would not comment on whether any lawsuits may have been filed against Kaseya. It is not clear how many victims may have paid ransoms before REvil went

dark.

The so-called supply-chain attack of Kaseya was the worst ransomware attack to date because it spread through software that companies known as managed service providers use to administer multiple customer networks, delivering software updates and security patches.

President Joe Biden called his Russian counterpart, Vladimir Putin, afterward to press him to stop providing safe haven for cybercriminals whose costly attacks the U.S. government deems a national security threat. He has threatened to make Russia pay a price for failing to crack down, but has not specified what measures the U.S. may take.

If the universal decryptor for the Kaseya attack was turned over without payment, it would not be the first time ransomware criminals have done that. It happened after the Conti gang hobbled Ireland's national health care service in May and the Russian Embassy in Dublin offered "to help with the investigation."