# Fallout continues from biggest global ransomware attack

5 July 2021, by Frank Bajak

This Feb 23, 2019, file photo shows the inside of a computer in Jersey City, N.J. 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. An affiliate of the notorious REvil gang, infected thousands of victims in at least 17 countries on Friday, largely through firms that remotely manage IT infrastructure for multiple customers, cybersecurity researchers said. Credit: AP Photo/Jenny Kane, File

The single biggest ransomware attack yet continued to bite Monday as more details emerged on how a Russia-linked gang breached the exploited software company. The criminals essentially used a tool that helps protect against malware to spread it globally.

Thousands of organizations—largely firms that remotely manage the IT infrastructure of others—were infected in at least 17 countries in Friday's assault. Kaseya, whose product was exploited, said Monday that they include several just returning to work.

Because the attack by the notorious REvil gang came just as a long Fourth of July weekend began, many more victims were expected to learn their fate when they return to the office Tuesday.

REvil is best known for extorting $11 million from the meat processor JBS last month. Security researchers said its ability to evade anti-malware safeguards in this attack and its apparent exploitation of a previous unknown vulnerability on Kaseya servers reflect the growing financial muscle of REvil and a few dozen other top ransomware gangs whose success helps them afford the best digital burglary wares. Such criminals infiltrate networks and paralyze them by scrambling data, extorting their victims.

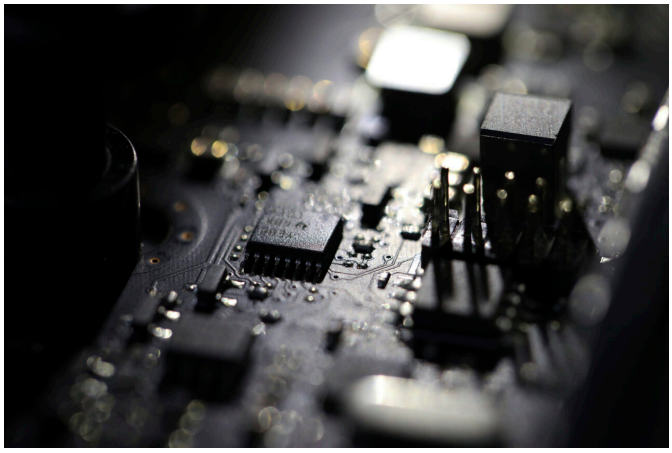
REvil was seeking $5 million payouts from the so-called managed service providers that were its principal downstream targets in this attack, apparently demanding much less—just $45,000—from their afflicted customers.

But late Sunday, it offered on its dark web site to make available a universal decryptor that would unscramble all affected machines if it's paid $70 million in cryptocurrency. Some researchers considered the offer a PR stunt, while others thought it indicates the criminals have more victims than they can manage.

Sweden may be hardest hit—or at least most transparent about the damage. Its defense minister, Peter Hultqvist, bemoaned in a TV interview "how fragile the system is when it comes to IT security." Most of the Swedish grocery chain Coop's 800 stores were closed for a third day, their cash registers crippled. A Swedish pharmacy chain, gas station chain, the state railway and public broadcaster SVT also were hit.

A wide array of businesses and public agencies were affected, including in financial services and travel, but few large companies were hit, the cybersecurity firm Sophos said. The United

Kingdom, South Africa, Canada, Argentina, Mexico, Indonesia, New Zealand and Kenya were among countries affected, researchers said.



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

In a statement Sunday, deputy U.S. national security adviser Anne Neuberger urged all victims to alert the FBI. A day earlier, the FBI said in an alert that the attack's scale "may make it so that we are unable to respond to each victim individually."

The vast majority of ransomware victims are loathe to publicly admit it, and many avoid reporting attacks to law enforcement or disclosing if they pay ransoms unless required by law.

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. In Geneva last month, Biden sought to pressure Russian President Vladimir Putin to end safe haven for REvil and other ransomware gangs that operate with impunity in Russia and allied states as long as they avoid domestic targets. The syndicates' extortionary attacks have worsened in the past year.

On Monday, Putin spokesman Dmitry Peskov was asked if Russia was aware of the attack or had looked into it. He said no but suggested it could be discussed during U.S.-Russian consultations on cybersecurity issues. No date has been set for such consultations, and few analysts expect the Kremlin to crack down on a crime wave that benefits Putin's strategic objectives of destabilizing the West.

Kaseya said Monday that fewer than 70 of its 37,000 customers were affected, though most were managed service providers with multiple downstream customers. Most managed service providers were apt to know by Monday if they were hit but that may not be true for many of the small and medium-sized organizations they serve, said Ross McKerchar, chief information security officer at Sophos. The MSPs are flying blind because the very software tool they use to monitor customer networks was knocked out by the attack.

The hacked Kaseya tool, VSA, remotely maintains customer networks, automating security and other software updates.

In a Monday report on the attack, Sophos said a VSA server was breached with the apparent use of a "zero day," the industry term for a previously unknown software security hole. Like other cybersecurity firms, it faulted Kaseya for aiding the attackers by asking customers not to monitor its on-premise "working" folders for malware. From inside those folders, REvil's code could work undetected to disable the malware- and ransomware-flagging tools of Microsoft's Defender program.

Sophos said REvil made no attempt to steal data in this attack. Ransomware gangs usually do that before activating ransomware so they can threaten to dump it online unless they are paid. This attack was apparently bare bones, only scrambling data.

In a Sunday interview, Kaseya CEO Fred Voccola would not confirm the use of a zero day or offer details of the breach—except to say that it was not phishing and that he was confident that when an investigation by the cybersecurity firm is complete, it would show that not just Kaseya but third-party software were breached by the attackers.

APA citation: Fallout continues from biggest global ransomware attack (2021, July 5) retrieved 22 October 2021 from https://techxplore.com/news/2021-07-scale-massive-kaseya-ransomware-emerge.html