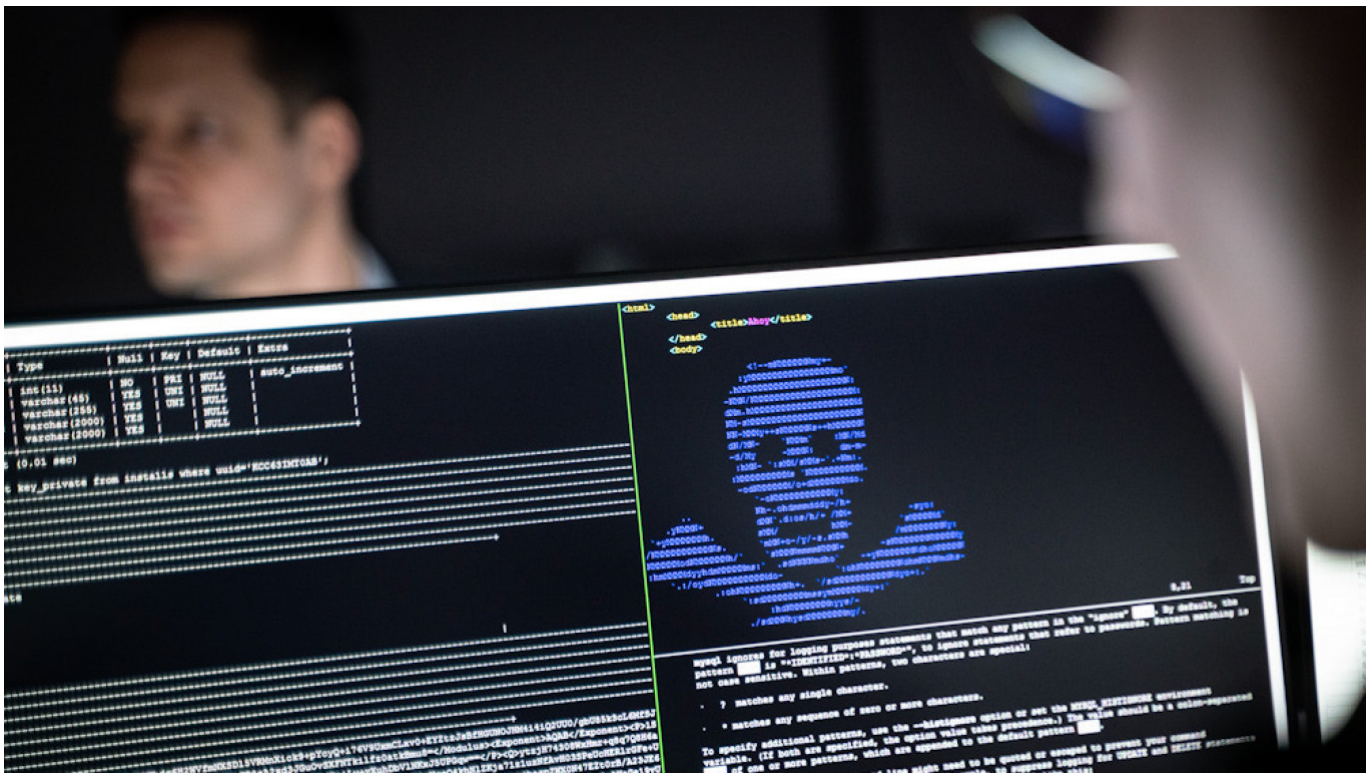
The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

U.S. Software Firm Moves to Restart After Huge Ransomware Attack Linked to Russia-Based Group

By AFP

July 07, 2021



Frank Rumpenhorst / DPA / TASS

A U.S. software firm hit by a major ransomware attack that crippled hundreds of companies worldwide was working to restart its servers late Tuesday to bring customers back online.

Kaseya, the Miami-based IT company at the center of the hack, pushed back its forecast for restarting its cloud-based systems, promising hourly updates.

It told customers to keep their systems shut down until it assures them that it is safe.

"We have been advised by our outside experts that customers who experienced ransomware and receive communication from the hackers should not click on any links — they may be weaponized," Kaseya warned.

The unprecedented attack affected an estimated 1,500 businesses and prompted a ransom demand of $70 million.

Kaseya said its systems were being brought back online with "enhanced security measures" and "the ability to quarantine and isolate files and entire ... servers" in case of infection.

While Kaseya is little known to the public, analysts say it was a ripe target as its software is used by thousands of companies, allowing the hackers to paralyze a huge number of businesses with a single blow.

Related article: Russia Points Finger Back at U.S. Over Latest Cyberattack Accusations

Kaseya provides IT services to some 40,000 businesses globally, some of whom in turn manage the computer systems of other businesses.

The hack affected users of its signature VSA software, which is used to manage networks of computers and printers.

Experts believe this could be the biggest "ransomware" attack on record — an increasingly lucrative form of digital hostage-taking in which hackers encrypt victims' data and then demand money for restored access.

The Kaseya attack has ricocheted around the world, affecting businesses from pharmacies to gas stations in at least 17 countries, as well as dozens of New Zealand kindergartens.

Most of Sweden's 800 Coop supermarkets were shut for a third day running after the hack paralyzed its cash registers.

Kaseya said Monday that while less than 60 of its own customers were "directly compromised," it estimated that up to "1,500 downstream businesses" had been affected.

White House spokeswoman Jen Psaki said the administration was monitoring the situation amid reports that the attacks came from a Russia-based cyber gang. But she noted that "the intelligence community has not yet attributed the attack... we will continue to allow that assessment to continue."

Psaki reiterated the warning President Joe Biden gave to his counterpart Vladimir Putin about Russia harboring cybercriminals, stating that "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."

Biden, asked about the incident Tuesday, said that so far there appeared to be "minimal damage to U.S. businesses" but that "we are still gathering information to the full extent of the attack."

Going out with a bang?

REvil, a group of Russian-speaking hackers who are prolific perpetrators of ransomware attacks, are widely believed to be behind Friday's assault.

A post on Happy Blog, a site on the dark web associated with the group, claimed responsibility for the attack, saying it had infected "more than a million systems."

The hackers demanded $70 million in bitcoin in exchange for the publication of an online tool that would decrypt the stolen data.

While the hackers are thought to have been reaching out to individual victims requesting smaller payments, the unprecedented demand for $70 million has surprised analysts.

French cybersecurity expert Robinson Delaugerre suggested that REvil could be treating the Kaseya attack as a final spectacular act before going out of business.

The group was responsible for around 29% of ransomware attacks in 2020, according to IBM's Security X-Force unit, looting an estimated $123 million.

"Our hypothesis is that REvil is going to disappear and this is its final big act," he told AFP, predicting that the group — which also goes by the name Sodinokibi — could re-emerge under a new name.

The FBI believes REvil was also behind a ransomware attack last month on global meat-processing giant JBS, which ended up paying $11 million to the hackers.

The United States has been a particular target of high-profile cyber attacks in recent months blamed on Russia-based hackers, with the Colonial oil pipeline and IT firm SolarWinds among the targets.

Original url:
https://www.themoscowtimes.com/2021/07/07/us-software-firm-moves-to-restart-after-huge-ransomware-attack-linked-to-russia-based-group-a74449