EXCLUSIVE Governments turn tables on ransomware gang REvil by pushing it offline

reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/

Joseph Menn, Christopher Bing

1/3
Acting U.S. Attorney for the Northern District of California Stephanie Hinds speaks about the Colonial Pipeline ransomware attack during a news conference with Deputy U.S. Attorney General Lisa Monaco and FBI Deputy Director Paul Abbate at the Justice Department in Washington, U.S., June 7, 2021. REUTERS/Jonathan Ernst/Pool/File Photo

Oct 21 (Reuters) - The ransomware group REvil was itself hacked and forced offline this week by a multi-country operation, according to three private sector cyber experts working with the United States and one former official.

Former partners and associates of the Russian-led criminal gang were responsible for a May cyberattack on the Colonial Pipeline that led to widespread gas shortages on the U.S. East Coast. REvil's direct victims include top meatpacker JBS (JBSS3.SA). The crime group's "Happy Blog" website, which had been used to leak victim data and extort companies, is no longer available.

Officials said the Colonial attack used encryption software called DarkSide, which was developed by REvil associates.

VMWare (VMW.N) head of cybersecurity strategy Tom Kellermann said law enforcement and intelligence personnel stopped the group from victimizing additional companies.

"The FBI, in conjunction with Cyber Command, the Secret Service and like-minded countries, have truly engaged in significant disruptive actions against these groups," said Kellermann, an adviser to the U.S. Secret Service on cybercrime investigations. "REvil was top of the list."

A leadership figure known as "0_neday," who had helped restart the group's operations after an earlier shutdown, said REvil's servers had been hacked by an unnamed party.

"The server was compromised, and they were looking for me," 0_neday wrote on a cybercrime forum last weekend and first spotted by security firm Recorded Future. "Good luck, everyone; I'm off."

U.S. government attempts to stop REvil, one of the worst of dozens of ransomware gangs that work with hackers to penetrate and paralyze companies around the world, accelerated after the group compromised U.S. software management company Kaseya in July.

That breach opened access to hundreds of Kaseya's customers all at once, leading to numerous emergency cyber incident response calls.

DECRYPTION KEY

Following the attack on Kaseya, the FBI obtained a universal decryption key that allowed those infected via Kaseya to recover their files without paying a ransom.

But law enforcement officials initially withheld the key for weeks as it quietly pursued REvil's staff, the FBI later acknowledged.

According to three people familiar with the matter, law enforcement and intelligence cyber specialists were able to hack REvil's computer network infrastructure, obtaining control of at least some of their servers.

After websites that the hacker group used to conduct business went offline in July, the main spokesman for the group, who calls himself "Unknown," vanished from the internet.

When gang member 0_neday and others restored those websites from a backup last month, he unknowingly restarted some internal systems that were already controlled by law enforcement.

"The REvil ransomware gang restored the infrastructure from the backups under the assumption that they had not been compromised," said Oleg Skulkin, deputy head of the forensics lab at the Russian-led security company Group-IB. "Ironically, the gang's own favorite tactic of compromising the backups was turned against them."

Reliable backups are one of the most important defenses against ransomware attacks, but they must be kept unconnected from the main networks or they too can be encrypted by extortionists such as REvil.

A spokesperson for the White House National Security Council declined to comment on the operation specifically.

"Broadly speaking, we are undertaking a whole of government ransomware effort, including disruption of ransomware infrastructure and actors, working with the private sector to modernize our defenses, and building an international coalition to hold countries who harbor ransom actors accountable," the person said.

The FBI declined to comment.

One person familiar with the events said that a foreign partner of the U.S. government carried out the hacking operation that penetrated REvil's computer architecture. A former U.S. official, who spoke on condition of anonymity, said the operation is still active.

The success stems from a determination by U.S. Deputy Attorney General Lisa Monaco that ransomware attacks on critical infrastructure should be treated as a national security issue akin to terrorism, Kellermann said.

In June, Principal Associate Deputy Attorney General John Carlin told Reuters the Justice Department was elevating investigations of ransomware attacks to a similar priority.

Such actions gave the Justice Department and other agencies a legal basis to get help from U.S. intelligence agencies and the Department of Defense, Kellermann said.

"Before, you couldn't hack into these forums, and the military didn't want to have anything to do with it. Since then, the gloves have come off."

Reporting by Joseph Menn and Christopher Bing; Editing by Chris Sanders and Grant McCool