$10 million rewards bolster White House anti-ransomware bid

15 July 2021, by Frank Bajak

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

The State Department will offer rewards up to $10 million for information leading to the identification of anyone engaged in foreign state-sanctioned malicious cyber activity, including ransomware attacks, against critical U.S. infrastructure. A task force set up by the White House will coordinate efforts to stem the ransomware scourge.

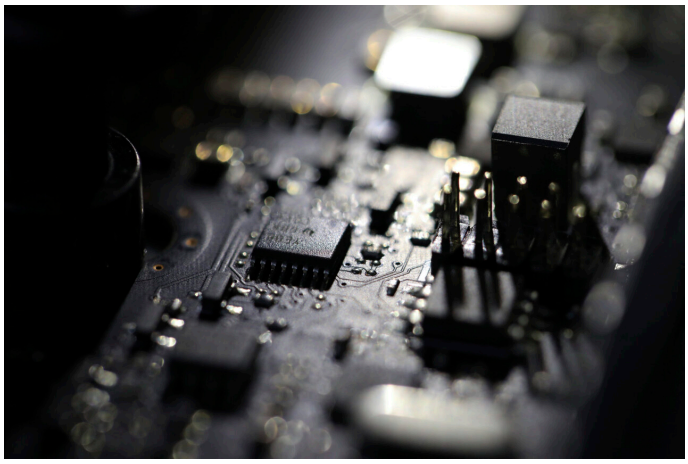
The Biden administration is also out with a website, stopransomware.gov, that offers the public resources for countering the threat and building more resilience into networks, a senior administration official told reporters.

In another move Thursday, the Treasury Department's Financial Crimes Enforcement Network will work with banks, technology companies and others on better anti-money-laundering efforts for cryptocurrency and more rapid tracing of ransomware proceeds, which are paid in virtual currency.

Officials are hoping to seize more extortion payments in ransomware cases, as the FBI did in recouping most of the $4.4 million ransom paid by Colonial Pipeline in May.

The rewards come from the State Department's Rewards for Justice program. It will offer a tips-reporting mechanism on the dark web to protect sources who might identify cyber attackers and/or their locations, and reward payments may include cryptocurrency, the agency said in a statement.

The administration official would not comment on whether the U.S. government had a hand in Tuesday's online disappearance of REvil, the Russian-linked gang responsible for a July 2 supply chain ransomware attack that crippled well over 1,000 organizations globally by targeting Florida-based software provider Kaseya. Ransomware scrambles entire networks of data, which criminals unlock when they get paid.



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

Cybersecurity experts say REvil may have decided to drop out of sight and rebrand under a new name, as it and several other ransomware gangs have done in the past to try to throw off law enforcement.

Another possibility is that Russian President Vladimir Putin actually heeded President Joe Biden's warning of repercussions if he didn't rein in ransomware criminals, who enjoy safe harbor in Russia and allied states.

That seemed improbable, however, given Kremlin spokesman Dmitry Peskov's statement to reporters Wednesday that he was unaware of REvil sites disappearing.

"I don't know which group disappeared where," he said. He said the Kremlin deems cybercrimes "unacceptable" and meriting of punishment, but analysts say they have seen no evidence of a crackdown by Putin.

The White House updated lawmakers Wednesday on the administration's response to the recent rash of high-profile ransomware attacks, a threat it has deemed a national security priority.

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

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

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

Sen. Angus King, an independent from Maine, said he was impressed with the "thoroughness with which they are confronting this issue," particularly with outreach to the private sector.