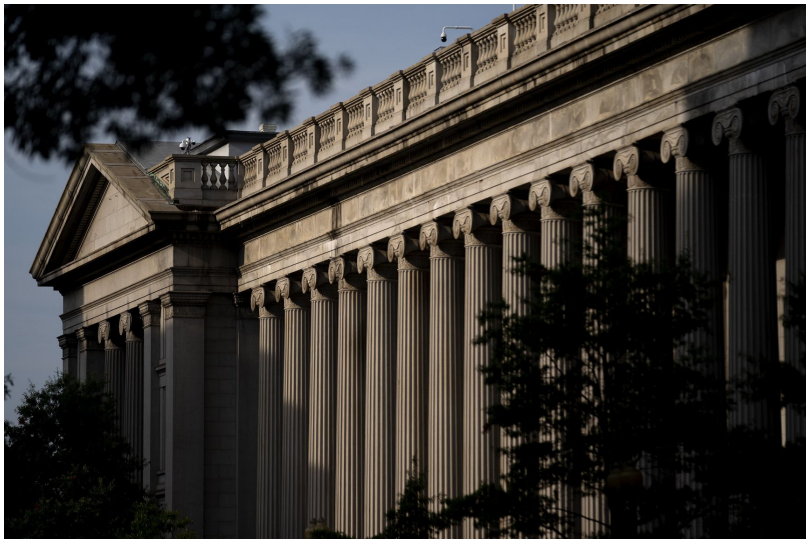
https://www.wsj.com/articles/u-s-to-target-crypto-ransomware-payments-with-sanctions-11631885336

◆ WSJ NEWS EXCLUSIVE | FINANCIAL REGULATION

U.S. to Target Crypto Ransomware Payments With Sanctions

Biden administration hopes to disrupt digital finance infrastructure that facilitates ransomware cyberattacks, a threat traced to Russia



The U.S. Treasury Department hopes to choke off access to a form of payment that has supported a booming criminal industry.

PHOTO: STEFANI REYNOLDS/BLOOMBERG NEWS

By Ian Talley and Dustin Volz

Sept. 17, 2021 9:28 am ET

The Biden administration is preparing an array of actions, including sanctions, to make it harder for hackers to use digital currency to profit from ransomware attacks, according to people familiar with the matter.

The government hopes to choke off access to a form of payment that has supported a booming criminal industry and a rising national security threat.

The Treasury Department plans to impose the sanctions as soon as next week, the people said, and will issue fresh guidance to businesses on the risks associated with facilitating ransomware payments, including fines and other penalties. Later this year, expected new anti-money-laundering and terror-finance rules will seek to limit the use of

cryptocurrency as a payment mechanism in ransomware attacks and other illicit activities.

The actions collectively would represent the most significant attempt yet by the Biden administration to undercut the digital finance ecosystem of traders, exchanges and other elements that cybersecurity experts say has allowed debilitating ransomware attacks to flourish in recent years.

Senior officials have said ransomware attacks this year have grown more severe than ever and represent a serious threat to critical infrastructure, including power operators, hospitals and banks.

The Treasury Department declined to comment and the people familiar with the matter declined to specify the targets of sanctions. But to effectively disrupt illicit crypto transactions, Treasury would need to target the digital wallets that receive ransom transactions, the crypto platforms that help exchange one set of blockchain coins for another to obscure the culprits and the people that own or manage those operations, according to analysts who specialize in such transactions.

The sanctions are expected to single out specific targets, rather than blacklist the entire crypto infrastructure where ransomware transactions are suspected of taking place. Nonetheless, the action will be intended to deter others from continuing their activities.

The administration scrambled to tackle the issue after high-profile attacks in the spring, all traced back to criminal groups believed to reside in Russia. Those attacks prompted the shutdown of a major U.S. fuel pipeline, disrupted a top meat supplier and infected scores of smaller and midsize organizations. Hacker payment demands have grown steadily larger and now routinely can reach into the millions or tens of millions of dollars.

With hackers demanding payments largely denominated in cryptocurrencies, the attacks have sparked debate between fintech proponents and policy makers over how to protect the market against criminals, terrorists and other bad actors without smothering its growth or creating long-term national security problems.

To help shape the market, lawmakers and regulators are crafting new rules, including new Treasury Department reporting requirements for international cryptocurrency transactions and for transactions that are conducted outside of central exchanges. The

rules are aimed at enhancing transparency, which some security officials argue will deter transactions by individuals who want their illicit activities to stay hidden.

Treasury and other regulating agencies also have been levying penalties and sanctions against individuals and companies facilitating illicit finance through the crypto markets as a warning to others. A warning in October 2020 by Treasury's Office of Foreign Assets Control cautioned victims of attacks and those acting on behalf of victims against making ransomware payments, saying they could violate U.S. laws.

More recently, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency issued similar warnings. "Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities," CISA said in an advisory in late August.

Sanctioning a cryptocurrency exchange that handled ransomware payments, for example, couldn't only disrupt that firm's ability to do business, but also spook other cryptocurrency platforms into avoiding such transactions or bolstering their compliance programs.

Ari Redbord, a former senior Treasury security official, said the Biden administration has so far worked with the private sector to harden cyber defenses as bad actors have taken advantage of the speed and cross-border reach of cryptocurrency. "An action of this kind would be an aggressive, proactive approach to going after those who facilitate ransomware payments," he said, referring to the expected sanctions.

Any sanctions levied by the administration would "most likely be designed to go after those illicit actors themselves, not cryptocurrency or the technology itself, which is simply the payment mechanism," said Mr. Redbord, now head of legal and government affairs at the blockchain intelligence firm, TRM Labs.

The administration has focused enforcement efforts on the primary sources of the attacks, which both private sector and government analysts say are in Russia and former Soviet satellite nations where Moscow exerts strong political influence.

Crypto analytics firm Chainalysis said the digital paper trail of blockchain transactions associated with ransomware payments shows most were paid into accounts in the former Soviet Union states of Eastern Europe.

The Biden administration also has been seeking to internationalize the struggle against ransomware. That collaboration follows from a vow late last year by the leaders from the Group of Seven wealthiest democracies to collectively act against ransomware, citing the crypto payments in particular.

Though many U.S. officials, including President Biden, have said the Kremlin may not be directly involved in ransomware campaigns, they blame Russian President Vladimir Putin for allowing those groups to permissively operate within his country.

> **"There is no indication that the Russian government has taken action to crack down on ransomware actors."**
>
> — Paul Abbate, FBI deputy director

At a meeting between the two leaders in July, Mr. Biden warned that he would take "any action necessary" to defend the U.S. against ransomware emanating from within Russia's borders.

The summit was followed by bilateral talks between senior U.S. and Russian officials, But those negotiations have yielded little progress, senior administration officials say.

"There is no indication that the Russian government has taken action to crack down on ransomware actors that are operating in the permissive environment they have created there," FBI Deputy Director Paul Abbate said Tuesday at an intelligence conference.

Treasury in late 2019 tied Russian intelligence to a company, Evil Corp., that private-sector analysts have since tagged as the creator of two major ransomware programs. Treasury officials said Evil Corp.'s leader, Maksim Yakubets, worked for Russia's premier intelligence service, the Federal Security Bureau. Mr. Yakubets couldn't be reached to comment.

The cybersecurity firm CrowdStrike Inc. in March said a wealth of digital evidence suggests the Evil Corp group, now known as Indrick Spider, is responsible for developing the WastedLocker and Hades ransomware programs.

Former U.S. security officials say one of the pieces of evidence suggesting Russian government involvement is code within the programs that prevents them being used on operating systems located in Russia and the former Soviet Union states.

Analysts say that by blacklisting key financial interlocutors in the region, the administration wouldn't only lock targets out of the Western financial system, but also be signaling its frustration at Moscow and warning others face the same fate if they continue to handle such transactions.

—Gerald F. Seib
contributed to this article.

Write to Ian Talley at ian.talley@wsj.com and Dustin Volz at dustin.volz@wsj.com

Appeared in the September 18, 2021, print edition as 'U.S. to Target Crypto Use In Ransom Cyberattacks.'