15% of 2020 ransomware payments carried a sanctions violations risk

therecord.media/15-of-2020-ransomware-payments-carried-a-sanctions-violations-risk/

May 11, 2021

Around one in six ransomware payments in 2020 were made to ransomware gangs that had some sort of connection to a US-sanctioned entity.

Payments to ransomware gangs such as **Bitpaymer**, **DopplePaymer**, **WastedLocker**, and **Clop** carried a sanction violations risk in 2020, said Chainalysis, a company specialized in analyzing blockchain transactions.

Security researchers believe these four ransomware strains have been created or have worked together with a cybercrime cartel known as EvilCorp, sanctioned by the US Treasury Department in December 2019.

In addition, Chainalysis said that payments to ransomware groups such as **Pay2Key**, **Sorena**, and **VoidCrypt (Hydra)** also carried a risk of a sanctions violation.

The three ransomware strains, which were active and made victims throughout 2020, are believed to have been developed by cybercrime gangs operating out of Iran, a country under heavy US economic sanctions, and with which US entities are forbidden to engage in financial transactions or render any services.

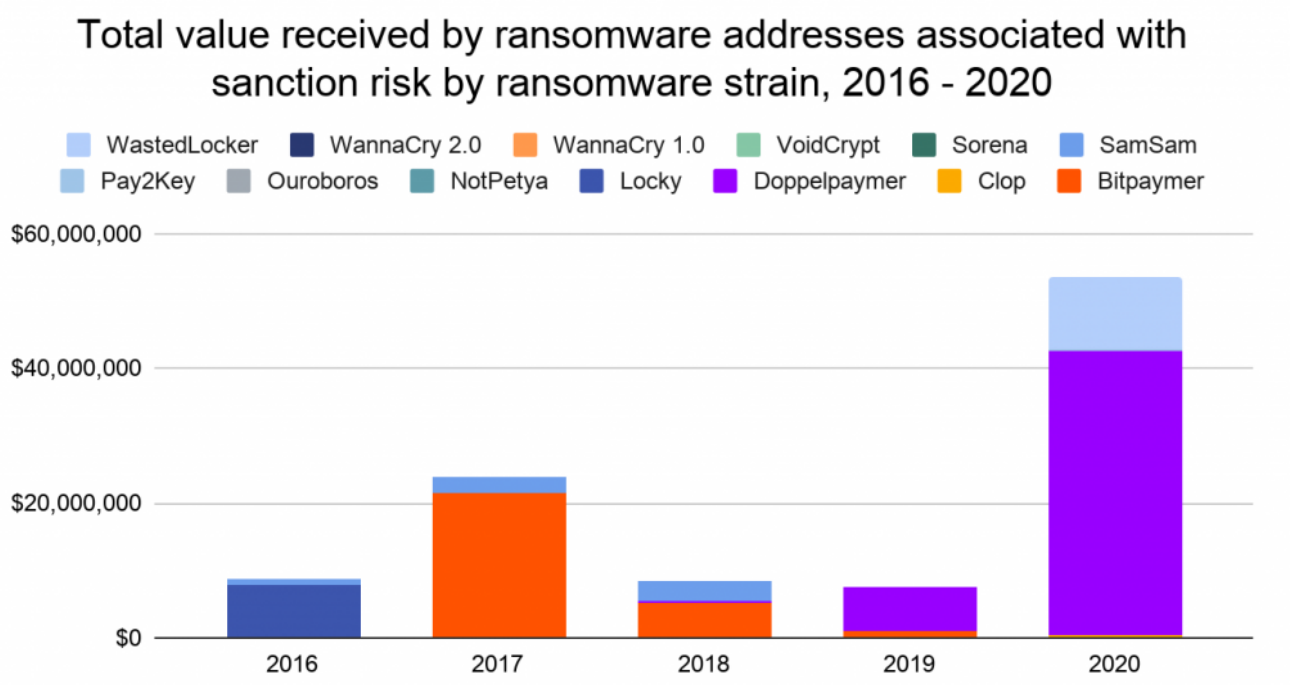

Image: Chainalysis

The Chainalysis report, published last month, comes after the US Treasury Department warned US entities in October 2020 that some ransomware payments can trigger a sanctions violation investigation, which could end up with big fines.

At the time, the US Treasury urged ransomware victims, companies that handle incident response and ransom negotiations, and financial institutions to reach out to the Treasury's Office of Foreign Assets Control (OFAC) and seek approval in advance for any ransom payment to a gang they believe might be working together with a sanctioned entity.

US Treasury guideline hard to enforce on SMBs

But in an interview with *The Record* last month, Christina M. Gagnier, a technology and privacy lawyer with law firm Carlton Fields and a former member of the Federal Communications Commission's Consumer Advisory Committee and the California Attorney General's Cyber Exploitation Task Force, said the US Treasury measures are disconnected from what some ransomware victims have to deal with during an attack.

"This ignores the reality of small to medium-sized businesses who are increasing falling victim to these types of attacks. For smaller businesses who are subject to these attacks, and may not have the systems in place, for better or worse, to restore backups of data, they may be forced to pay the ransom to get their critical data back," Gagnier told us.

"The mitigating factors suggested by Treasury presume that smaller businesses, who probably have no knowledge of OFAC and its guidelines since it likely never implicates their day-to-day operations, are supposed to know to contact OFAC to report ransomware."

"**This ascribes a level of resources and sophistication that simply may not be present in a business**," Gagnier said.

"It also seems to suggest that businesses have an obligation to check OFAC resources for updated ransomware strains, but if you are not expecting an attack in the first instance, this is likely not top of mind when a breach occurs."

"Finally, how many U.S-based small businesses, who generally do not deal with OFAC and its rules, have a sanctions compliance program? While Treasury's intent may be to crack down on the emergence of a new form of terrorist activity, it does ignore the reality of the diversity of the types of businesses who find themselves victims to these attacks today," Gagnier told *The Record*.

But while the Treasury's guideline didn't list all the ransomware strains that may incur a sanctions violation, the Chainalysis team has compiled this list instead. Entries in grayed-out italics are for ransomware groups that have ceased operations. The rest is for ransomware groups still active today and for which there's a risk of a sanctions violation, at least for US entities.

- ***SamSam:*** *OFAC designated cryptocurrency address.*
- ***Ouroboros:*** *Linked to Iranian actors.*
- **VoidCrypt:** Linked to Iranian actors.
- **Sorena:** Linked to Iranian actors.
- **Pay2Key:** Linked to Iranian actors.
- ***WannaCry 1.0, WannaCry 2.0:*** *Linked to North Korean actors.*
- ***NotPetya:*** *Associated with sanctioned actors in Russia.*
- ***CryptoLocker:*** *Associated with sanctioned actors in Russia.*
- **Bitpaymer:** Speculated to be associated with sanctioned group Evil Corp.
- ***Locky:*** *Speculated to be associated with Evil Corp.*
- **Doppelpaymer:** Speculated to be associated with sanctioned group Evil Corp.
- **WastedLocker:** Speculated to be associated with sanctioned group Evil Corp.
- **Clop:** Disputed but speculated to be associated with Evil Corp.

Tags

- BitPaymer
- Clop
- DopplePaymer
- EvilCorp
- OFAC
- Ransomware
- Russia
- sanction list

- sanction violation
- sanctions
- US government
- US Treasury
- WastedLocker

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.