Companies Facilitating Ransomware Payments Could Face Penalties

Bloomberg Law News 2020-10-12T12:46:52542-04:00

Companies Facilitating Ransomware Payments Could Face Penalties

By William Turton2020-10-01T18:04:15417-04:00

- Advisory limits U.S. firms paying ransoms to sanctioned groups
- Payments to hackers has long existed within legal gray area

Companies that assist victims of ransomware attacks in making payments to criminal hackers could face penalties, according to a new advisory from the U.S. Department of the Treasury.

The civil penalties would apply to those who assist in making ransom payments on behalf of victim companies or governments hacked by criminal groups that have been sanctioned by the Treasury Department. The new advisory, from the department's Office of Foreign Assets Control, could fundamentally change the calculus for companies -- and their advisers -- after they've been infected with ransomware.

"Companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands but also may risk violating OFAC regulations," the Treasury Department said in its new advisory.

Treasury officials didn't respond to messages seeking comment.

Victims of ransomware attacks that make the payments aren't specifically mentioned in the advisory as being subject to civil penalties for paying ransom. However, Treasury Department rules prohibit victims from paying ransom to sanctions entities. These rules haven't changed. What's changed in that the U.S. government threatened to start enforcing these rules, said Joshua Motte, chief executive officer of Coalition Inc., the cyber insurance company.

Ransomware is a type of malware that locks computers and blocks access to files in lieu of a payment. Companies targeted with ransomware must decide whether to pay the ransom, using via cryptocurrency, or find some other way to restore its files and rebuild its computer network. The attacks can be devastating, with the potential to bring company operations to a stop.

From 2018 to 2019, there was a 37% increase in reported ransomware cases and a 147% annual increase in associated losses, according to the FBI.

"The ransomware problem has blown up exponentially over the past two months," said Charles Carmakal, senior vice president and chief technology officer at the cybersecurity company Mandiant. "Mandiant is aware of over 100 organizations in which ransomware operators had network access to in September alone, more than double what we were aware of in September of the previous year."

Paying ransom to criminal groups has long existed within a legal gray area. The ransom, which can sometimes be in the millions, are often paid to organized criminal groups in Eastern Europe or Russia. While the FBI discourages paying ransom, the U.S. government hasn't previously punished victims who pay the hackers' demands.

The Treasury Department has issued sanctions on criminal ransomware groups, including last December against Russia-based Evil Corp. That group is suspected of being behind a ransomware attack on smartwatch maker Garmin Ltd. Sky News reported that the cybersecurity company Arete Incident Response, which is based in the U.S., allegedly paid a ransom to Evil Corp. on behalf of Garmin.

Arete didn't respond to a request for comment.

The new advisory could create another headache for companies struck by ransomware -- figuring out if the attackers have been sanctioned by the U.S. It is often difficult to conclusively prove who is behind a ransomware attack, thanks to the obfuscation provided by the internet and the fact that criminal ransomware groups are sometimes skilled hackers who can cover their tracks.

"The intention of the OFAC advisory is positive, but it will certainly add more pressure and complexity to victim organizations already challenged with protecting the confidentiality of their stolen customer data and recovering their business operations after a security incident," Carmakal said. "The true identity of the cyber criminals extorting victims is usually not known, so it's difficult for organizations to determine if they are unintentionally violating U.S. Treasury sanctions."

According to the Treasury advisory, companies that notify law enforcement of ransomware attacks may decrease its risk in the event it ends up paying a sanctioned entity.

--With assistance from **Kartikay Mehrotra**.

To contact the reporter on this story:
William Turton in New York at wturton1@bloomberg.net

To contact the editor responsible for this story:
Andrew Martin at amartin146@bloomberg.net