Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Risk Of Breaching Sanctions Adds To Ransomware Headache

By **Ben Kochman**

Law360 (August 5, 2020, 6:43 PM EDT) -- Companies facing extortion demands from cybercriminals have encountered a new form of risk in recent months over whether paying such a ransom could violate sanctions issued by the U.S. Department of the Treasury, industry attorneys say.

The Treasury's Office of Foreign Assets Control, or OFAC, has yet to penalize a U.S. entity for making a payment to a group of cybercriminals under sanction. But last month's cyberattack on wearable technology and GPS device giant Garmin Ltd., which said malicious software **knocked service offline** for users of its fitness tracking and pilot navigation products, highlights the treacherous terrain companies may navigate in this area.

Garmin has not said whether it paid a ransom. But a news report said the company used an intermediary to pay a multimillion-dollar bounty to criminals who had hit its network with a virus known as "WastedLocker," which some cybersecurity experts say was developed by a Russia-based, sanctioned cybercriminal group that calls itself "Evil Corp."

Whether such a payment could lead to a Treasury Department penalty is uncertain, industry lawyers say**.**

"The unclear question of whether a payment will violate sanctions can leave an already desperate company tied in elaborate knots as they struggle to survive a ransomware event," said attorney Michael Phillips, chief claims officer at the cybersecurity analytics company Arceo.ai. "Government sanctions add a new layer of complexity to every ransomware emergency."

Garmin's announcement that the malicious software **"encrypted some of our systems"** suggests that the episode was a ransomware attack, a term used to describe cyberattacks in which criminals demand digital currency in exchange for unlocking frozen networks or giving back stolen data.

According to Sky News, the Switzerland-based company restored access to its systems with the help of a third-party ransomware response firm, which paid off the criminals that had used the WastedLocker malicious software to infiltrate Garmin's systems.

U.S. authorities sanctioned Evil Corp., the alleged developer of WastedLocker, in December along with two Russian nationals accused of leading the group, saying they engaged in a decadelong hacking and fraud scheme that stole **more than $100**

million from banks and financial institutions in more than 40 countries.

Cybercriminals linked to the North Korean government — itself the target of stiff financial sanctions, including from the U.S. and U.N. — have also turned to ransomware attacks on financial companies and other businesses as a way to generate revenue for the regime, the U.S. Departments of State, Treasury and Homeland Security and the FBI **warned in April.**

And the European Union last week issued its **first-ever sanctions** related to cybercrime, imposing financial and travel restrictions on a Russian military intelligence unit and Chinese and North Korean companies accused of supporting a global set of cyberattacks.

The threat that an extortion payment could violate sanctions adds to the growing list of headaches that ransomware victims face, industry lawyers say, including whether targets have the ability or time to restore their networks without paying the hackers.

Despite OFAC having not penalized a company to date for violating sanctions with a ransomware payment, companies would be wise to do an "internal vetting" of any ransomware incident for evidence that the cybercriminals are linked to a sanctioned group, said Guillermo Christensen, a partner in the data security and privacy group at Ice Miller LLP and a former CIA intelligence officer.

But in many incidents, companies that bring in third-party forensics firms to analyze a cyberattack won't have clarity about who the hackers making the demands are within the first crucial hours or days, if ever, Christensen said.

"The most common scenario is that they get in, you have a couple of days to respond to the demand, and by the time forensics gets involved, you've already made the payment," Christensen told Law360.

Ransomware crews have grown more organized and market-savvy in the past couple of years, **finding a sweet spot** of companies and governments willing to pay rising sums to avoid having to rebuild their networks from scratch, industry experts say. Victims often cave to the attackers' payment demands, despite the FBI's advice that doing so will embolden cybercriminals to launch more attacks.

Trying to rush victims into paying up is part of the hackers' strategy. "Their incentive is to move as quickly as possible to get you to make decisions with as little reflection as possible," Christensen said.

The growing notoriety of organized ransomware crews believed to be behind several high-profile attacks may give victims some information about who they are dealing with, even if that information is limited, said Luke Dembosky, co-chair of the data strategy and security practice at Debevoise & Plimpton LLP.

"Although the world of cybercrime is murky generally, the leading ransom groups are quite well known, so in many cases the victim will have at least some details to inform its decision," said Dembosky, who called it "very important to learn what you can about who you'd be paying and whether there is a legal barrier or added reputational risk involved."

Even among ransomware incident response companies, the question of who is truly behind a set of cyberattacks can be up for debate.

In Garmin's case, for example, the company turned to a ransomware response firm called Arete Incident Response after another such outfit refused to negotiate with the

hackers, citing concerns about the connection between the WastedLocker malware and the sanctioned Evil Corp. hackers, Sky News reported.

Arete, which did not respond Wednesday to a request for comment, published research on July 24 that called attribution of the ransomware strain to the sanctioned group a "theory" that is "not conclusive." Some of the tactics used in WastedLocker attacks are also used by other cybercriminal gangs, Arete said, including the Maze group, which has gained attention for trying to **publicly shame** its victims.

But Kivu Consulting Inc., another company that offers ransomware response services, told Law360 that its own investigation concluded "with a reasonable degree of certainty that WastedLocker was developed by Evil Corp."

And even if it was another set of cybercriminals using the sanctioned group's tool, there is a possibility that those cybercriminals would kick back a portion of the proceeds from the attack to Evil Corp., Kivu's investigation found.

"Kivu's official position is that we cannot facilitate a payment for this variant at this time, and we are continuing our investigation by gathering more human intelligence on the variant to confirm how they operate," said Bridget Q. Choi, Kivu's associate director.

Choi suggested that ransomware victims considering paying cybercriminals through an intermediary confirm that the third-party company has a policy of conducting due diligence, including filing a Suspicious Activity Report with Treasury's Financial Crimes Enforcement Network, or FinCEN, which helps the government trace the activities of cybercriminals.

A Treasury Department representative declined to comment Wednesday on under what circumstances an extortion payment to cybercriminals could violate sanctions.

The most challenging scenario for a ransomware victim to face, Christensen said, would be if the FBI or U.S. Secret Service has told victims that they suspect that an attack has been carried out by hackers linked to a sanctioned entity like the North Korean government.

"In that, rare instance, your option to pay is going to be very tough," the attorney said.

--Editing by Jill Coffey.