The Bottom Line

OCTOBER 2021 | VOL. 108

ONE-TWO PUNCH: RANSOMWARE ATTACKS AND OFAC VIOLATIONS

Summary

Demand for ransomware payments has increased during the COOVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. Victims of these attacks and companies that facilitate ransomware payments on behalf of victims risk encouraging future ransomware payment demands and may also risk violating OFAC regulations.

Background

Ransomware is a form of malicious software ("malware") designed to block access to a computer system or data, often by encrypting data or programs on information technology systems to extort ransom payments. Victims pay ransom in exchange for decrypting the information and restoring access to their systems or data. In some cases, in addition to the attack, cyber actors threaten to publicly disclose victims' sensitive files. The cyber actors then demand a ransomware payment in exchange for a key to decrypt the files and restore victims' access to systems or data. In recent years, ransomware attacks have become more focused, sophisticated, costly, and numerous. According to the Federal Bureau of Investigation (FBI), there was a nearly 21 percent increase in reported ransomware cases and a 225 percent increase in associated losses from 2019 to 2020. Ransomware attacks are carried out against private and governmental entities of all sizes and in all sectors.

Danish shipping giant Maersk has revealed that a 2017 ransomware attack on its systems may have cost the company as much as $300m. The ransomware caused "significant business impact especially within the container business," according to the firm. Chinese COSCO Shipping was idled for weeks in July 2018. Mediterranean Shipping Company was hit in April 2020 by an unnamed malware strain that brought down its data center for days. And French CMA-CGM was victimized in September of 2020.

Trucking company ForwardAir was targeted on December 15 last year with an attack of the Hades ransomware. The company was forced to take all its I.T. systems offline to deal with the intrusion. According to a Freight Waves report, the incident led to massive disruptions to ForwardAir's operations as drivers and employees couldn't access the necessary documents to clear transports through customs. Although Forward Air said it successfully recovered from the attack, a report to the Securities and Exchange Commission (SEC) and the hefty price the company had to pay for it shows once again why most security researchers have been preaching prevention rather than a cure for the ransomware problem.

Current Status

Victims of ransomware attacks often choose to pay the ransom. However, because ransomware attackers rarely, if ever, identify themselves and often demand payment in cryptocurrency, victims making such payments are generally forced to do so without a clear understanding of the recipient. Such conduct potentially exposes the victim, and third-party service providers (including financial institutions and incident response consultants, among others), to violations of and obligations under U.S. sanctions and/or AML laws, in addition to other sanction regimes around the world, such as those recently deployed by the European Union. The Office of Foreign Assets Control (OFAC), the financial intelligence and enforcement agency of the U.S. Treasury Department, has stated that facilitating a ransomware payment that is demanded of malicious cyber activities may enable criminals and adversaries with a sanctions nexus to profit and advance their illicit aims. For example, ransomware payments made to sanctioned persons or comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Such payments not only encourage and enrich malicious actors but also perpetuate and incentivize additional attacks. Moreover, there is no guarantee that companies will regain access to their data or be free from further attacks themselves. For these reasons, the U.S. government strongly discourages the payment of cyber ransom or extortion demands. Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA), U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities on OFAC's Specially

The Bottom Line

OCTOBER 2021 | VOL. 108

ONE-TWO PUNCH: RANSOMWARE ATTACKS AND OFAC VIOLATIONS

Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria). Additionally, any transaction that causes a violation under IEEPA, including a transaction by a non-U.S. person that drives a U.S. person to violate any IEEPA-based sanctions prohibitions, is also prohibited. OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC.

Impact

As a general matter, OFAC encourages financial institutions and other companies to implement a risk-based compliance program to mitigate exposure to sanctions-related violations.

This advice also applies to companies that engage with victims of ransomware attacks, such as those involved in providing cyber insurance, digital forensics and incident response, and financial services, which may include the processing of ransom payments (including depository institutions and money services businesses). In particular, the sanctions compliance programs of these companies should account for the risk that a ransomware payment may involve an SDN or blocked person or a comprehensively embargoed jurisdiction.

Meaningful steps taken to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, such as those highlighted in the Cybersecurity and Infrastructure Security Agency's (CISA) September 2020 Ransomware Guide, will be considered a significant mitigating factor in any OFAC enforcement response. Such steps could include maintaining offline data backups, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols.

RESOURCES

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (U.S. Department of the Treasury)

Maersk Admits NotPetya Might Cost It $300m (InfoSecurity Magazine)

All Four of the World's Largest Shipping Companies Have Now Been Hit by Cyber-Attacks (ZDNet)

Trucking Company Forward Air Said Its Ransomware Incident Cost It $7.5 Million (ZDNet)

Five Key Takeaways from OFAC and FinCEN's Ransomware Advisories (Steptoe & Johnson)