Cybersecurity Law Report

cslawreport.com

May 25, 2022

RANSOMWARE

Ransomware and Sanctions in the Time of War

By Jena Valdetero, Kara Bombach and Kyle Freeny, *Greenberg Traurig*

Russia's attack on Ukraine has resulted in historic and escalating U.S. sanctions, impacting companies who do business with Russia or Russian affiliates and creating risks even for companies who do not. Since 2020, the number and sophistication of ransomware attacks has spiked, largely perpetuated by organized criminal groups in Russia and Eastern Europe. Against this backdrop lies the U.S. government's position on economic sanctions, which prohibits U.S. persons from making payments directly or indirectly to any individual, entity, group or country that is the target of economic sanctions implemented by the U.S. Department of the Treasury (Treasury).

In this article, we discuss today's most prevalent types of ransomware attacks, considerations for whether to make the ransom payment, the Financial Crimes Enforcement Network (FinCEN) and Treasury's Office of Foreign Asset Control's (OFAC) ransomware guidance, and the U.S. government's efforts in connection with these attacks.

See "Ten Tips to Prepare for and Navigate Ransomware Decisions" (Jan. 12, 2022).

Increase in Number and Types of Attacks

Although ransomware attacks have been around for the past decade, they have increased considerably since the sudden shift to remote work caused by COVID-19 in March 2020. Threat actors, recognizing that companies may not have had sufficient time to put in place best in class security measures, began exploiting security vulnerabilities at a rate like never before. At the same time, because well-prepared companies were increasingly protecting their back-up data through offline or air-gapped storage, threat actors began stealing a victim company's data before launching the attack. That way, if a company did not need the decryption key to restore their data, they were faced with the tough choice of letting the threat actors post their sensitive stolen information – often personal data stolen from HR or customer files – on the dark web. One company that tracks ransomware attacks found that 84 percent of attacks in Q4 2021 involved exfiltrated data.

Other less frequent tactics include conducting a distributed-denial-of-service (DDOS) attack against companies who are refusing to make a ransom payment. A DDoS attack floods a company's online services with web traffic, effectively taking it offline, similar to a telephone line generating a busy signal because multiple calls are coming in at the same time. In addition, threat actors will sometimes call company executives to try to convince them to make a payment. In rarer instances, threat actors will call B2B customers to advise that their partner had a breach and is refusing to pay to prevent the release of stolen data

belonging to the customer and offering to sell the customer's stolen data back to the customer.

To add to this bizarre world, the more sophisticated groups often act like legitimate companies. A recent leak of 60,000 chat messages and files among members of one large ransomware group makes for a fascinating read – it turns out even threat actors complain about their bosses and just want to take a vacation while threat actor groups also have a hard time recruiting and retaining talent.

See CSLR's two-part interview with the Ransomware Task Force co-leader: "Task Force Leader Discusses How to Beat Ransomware in a Year" (May 19, 2021); and "Task Force Leader Addresses Proposed Mandatory Reporting of Ransomware Payments" (May 26, 2021).

Whether to Pay: Three Considerations

Ever since hackers figured out that they could earn a quick payday through ransomware attacks, companies and law enforcement alike have been struggling with how to respond to an impossible dilemma – pay millions to a threat actor or risk never recovering your data and ruining your business. Put this way, it is easy to see why so many companies pay and why ransomware has become big business. Why rob a bank when you can steal millions from the comfort of your living room?

At best, ransom payments fund a lawbreaker's lifestyle; at worst, they support terrorism and threats to democracy and national security. But, whether to pay is often a business decision, generally driven by at least three considerations: (1) the inability to recover data or systems access through back-ups; (2) the threat to release sensitive information stolen by the threat actors; or (3) the cost of business interruption from each day of being unable to operate greatly exceeding the payment demand.

According to one source, the average ransom payment in Q4 2021 was $322,168. This figure is skewed by the fact that victim companies come in all sizes and industries. For larger companies employing between 1,000-10,000 individuals, the average ransom payment exceeded $1 million.

Although companies should always be prepared for the possibility that the threat actor will not make good on his promise to provide a decryption key and destroy any stolen data, in reality, there seems to be some honor among thieves. A ransomware attacker's business model depends on the public believing that paying a ransom will result in getting the data back quickly, and threat actors generally fulfill their end of the bargain.

See "To Pay or Not to Pay? Empirical Studies Show Keys to Ransomware Decisions" (Dec. 15, 2021).

Liability for Payments to Targets of Economic Sanctions

Against the backdrop of the increase in number and types of attacks and issues around whether to make the ransom payment lies the U.S. government's position on economic sanctions, which prohibits U.S. persons from making payments directly or indirectly to any individual, entity, group, or country that is the target of economic sanctions implemented by the Treasury. Apart from comprehensive

country sanctions prohibiting U.S. persons dealings with Iran, Cuba, Syria, North Korea and covered regions of Ukraine, targeted sanctions are imposed by OFAC, primarily through designations on its list of Specially Designated Nationals (SDN).

Risk of Indirect Engagement

The SDN sanctions also prohibit U.S. persons from engaging in activities involving entities 50 percent or more owned by SDNs (even if they are not expressly named on OFAC's SDN List). People are often surprised to learn that, in most cases, cyber threat actor groups are not specifically identified on OFAC's sanctions list (though a few are). Because OFAC prohibits engaging in transactions – directly or *indirectly* – with sanctioned individuals or entities, the risk of paying a threat actor who is not specifically identified but who may have a nexus to a sanctioned person is very real. Notably, in addition to entities and individuals identified on the SDN List, even certain virtual currency wallet addresses are sanctioned by OFAC on the SDN List.

Strict Liability and Material Support

Because the standard for OFAC sanctions violations is strict liability, U.S. persons can be held liable for violations even without knowledge or reason to know that they are engaging in a transaction indirectly involving a sanctioned person. This is particularly relevant in the ransomware context, where U.S. companies making a ransomware payment to an unidentified threat actor run the risk of committing an inadvertent U.S. sanctions violation. And even non-U.S. persons may run the risk of having a payment transaction become subject to U.S. jurisdiction (for example, U.S. dollar denominated or routed through U.S. payment systems),or may become vulnerable to secondary sanctions (itself becoming target of sanctions) for providing "material support or assistance" to a sanctioned person or entity. Depending on the value of a ransomware payment, OFAC could deem such a payment even by a non-U.S. entity or person to be "material support or assistance" to an OFAC-sanctioned person or entity.

OFAC and FinCEN Guidance Discourage Payment

The U.S. government strongly discourages the payment of a ransom, correctly noting that payments encourage future attacks and may harm U.S. national security interests, while also recognizing the economic reality posed by such attacks. Both OFAC and FinCEN have issued guidance on ransom payments highlighting the risk that the challenges of effective diligence in the ransomware space leave payors vulnerable to the additional risk of committing sanctions violations in making a ransomware payment.

See "Steps to Take After OFAC and FinCEN's Warnings on Ransomware Payoffs" (Oct. 21, 2020).

Mitigating Risk of Payment

The OFAC guidance also makes clear that it gives great mitigation credit for potential monetary penalties to payors who disclose the ransomware payment to the FBI, OFAC, and/or the Secret Service. As a practical matter, notifying the FBI and receiving updated indication whether any U.S. government agency considers a particular

threat actor to be sanctioned will go a long way towards minimizing legal exposure for a ransomware payor.

Along with notification to the U.S. government, it is critical for ransomware targets to conduct adequate diligence on the threat actor and payment demand details (including threat actor and payment recipient names, identification, wallet addresses in the case of virtual currency transactions, and geolocation tracking details).

Ransomware demands create risks for anyone involved directly or indirectly in making the payment (including payment processors, insurers, and other intermediaries). So, each should adopt diligence procedures for ascertaining as much as possible about the threat actor and recipient in order to document attempts to identify any known connections with sanctioned countries, regions, entities or individuals. In instances where it is actually known or suspected to be highly likely that a sanctioned person or entity is at the other end of a ransomware demand, the only appropriate way to mitigate the risk of payment – which in many instances may be necessary to prevent complete economic disruption and destruction of the ransomware target or the public release of highly sensitive (in some cases national security sensitive information or technical data) – is to make a voluntary self-disclosure not only to the FBI but also to OFAC of the potential or likely sanctions violation explaining all of the mitigating factors, including the risk to U.S. national security posed by NOT making the ransomware payment.

See "A Look Inside Businesses' Private Disputes Over Ransomware Costs" (Aug. 18, 2021).

Designing Compliance Programs With Diligence Procedures

OFAC also expects that anyone operating internationally, and frankly, anyone poised to make a ransomware payment, have in place a risk-based economic sanctions compliance program including diligence procedures, internal review and approval protocols for minimizing the risk of activities with sanctioned persons entities, or countries.

The design and structure of risk-based compliance programs for those in the virtual currency industry will depend on a variety of factors, including the type of business involved, size and sophistication, products and services offered, customers and counterparties, and geographic locations served. Companies in the virtual currency industry, including technology companies, exchangers, administrators, miners and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers, should develop, implement and routinely update a tailored, risk-based sanctions compliance program. It is very much a best practice to implement sanctions list and geographic screening and other appropriate measures tailored to the company's unique risk profile.

Conti Ransomware Group

On February 25, 2022, a perhaps overzealous member of ransomware group Conti decided to issue a statement expressing their "full support" of the Russian government, threatening to "strike back at the critical infrastructures of an enemy." Likely recognizing the optics and potential sanctions impact on the willingness of ransomware targets to make ransomware payments to Conti, hours later, Conti issued a second statement walking back

its support for Russia, clarifying that it "does not ally with any government and we condemn the ongoing war."

But the damage was already done. Cyber insurers and vendors began shutting down approvals for payment to Conti, even though, as of press time, Conti still has not been identified by OFAC as an SDN. This has been challenging for companies hit by Conti since the announcement, who have struggled to find support in making a payment and recovering the payment under their cyber insurance policies.

What the U.S. Government Is Doing

And where is the U.S. government in all of this? Since early 2021, likely in response to the ransomware attack on Colonial Pipeline, which resulted in the shutting down of a key gas pipeline and subsequent gasoline supply disruption, we have seen more activity and funding to fight cyber attacks than ever before.

See "How Colonial Pipeline Changed Advice on Ransomware Preparation and Response" (Apr. 6, 2022).

Critical Infrastructure Bill

Most recently, Congress passed a bill requiring critical infrastructure to report cyber attacks, including ransomware, within 72 hours to the federal Cybersecurity and Infrastructure Security Agency, although this requirement will not take effect until after regulations are finalized to flesh out a number of issues, including which entities are considered "critical infrastructure." Those regulations could take as long as 36 months to be finalized.

Focus on Disruption

Prosecutions of those involved, however, can be very challenging for U.S. authorities, not least because the actors often operate from countries – including Russia – that do not cooperate with, or extradite to, the United States. That explains, at least in part, the U.S. government's focus on *disruption* of the activity, rather than solely on prosecution, including by seizing ransomware proceeds, as we saw to spectacular effect in the Colonial Pipeline attack.

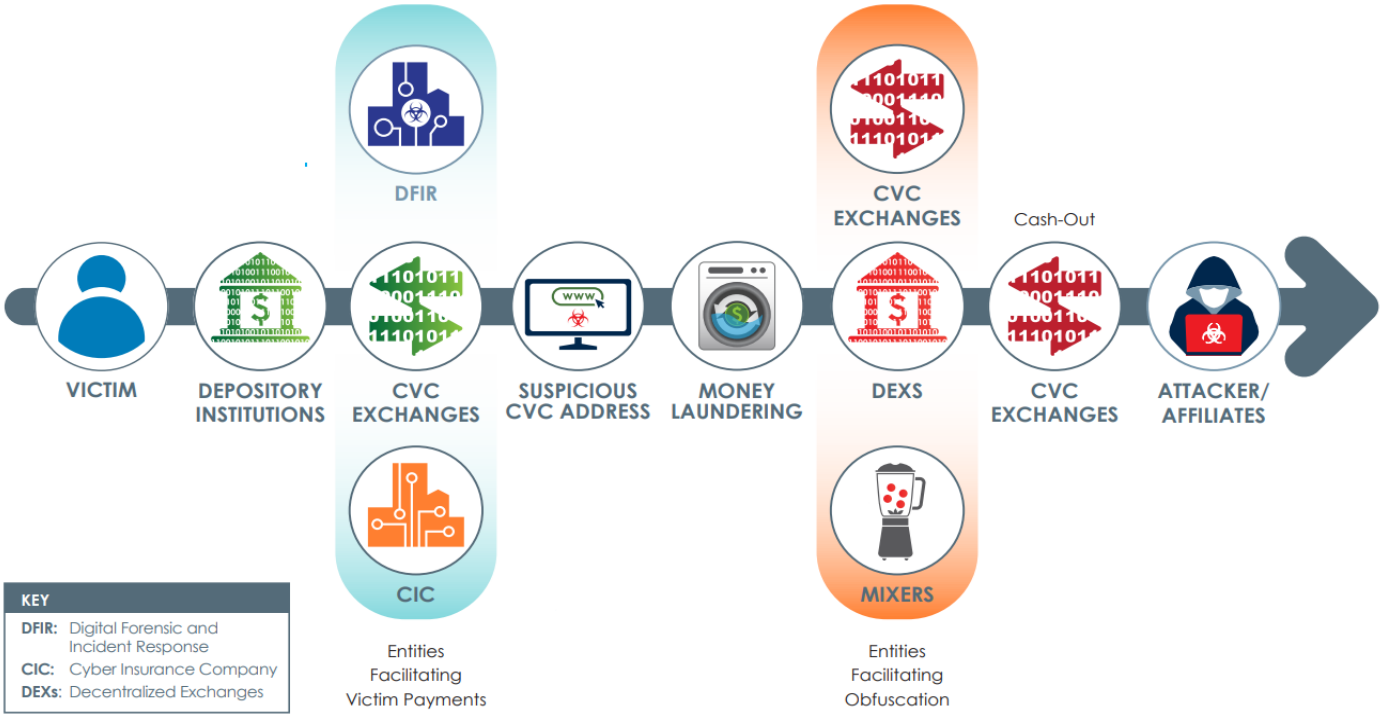
KleptoCapture Task Force and Cryptocurrency Enforcement Team

Law enforcement's focus on disrupting ransomware attacks dovetails with several other U.S. law enforcement initiatives likely to affect the ransomware space. First, shortly after Russia's invasion of Ukraine, the Department of Justice announced the creation of a special KleptoCapture Task Force dedicated to enforcing sanctions against Russia and prosecuting those who would evade them. Second, the DOJ also recently announced the creation of a National Cryptocurrency Enforcement Team, focused on the criminal uses of cryptocurrency, including ransomware attacks.

Harder Look at Payment Chain

In light of the U.S. government's concerted focus on ransomware payments, especially where those payments might implicate Russian sanctions, we can expect to see the U.S. government taking a harder look at the entire process of ransomware payments. FinCEN recently published the figure below to illustrate the flow of funds in a ransomware payment:

Figure 1. Movement of CVC in Ransomware Incidents



We may expect to see FinCEN and other U.S. regulators and enforcement agencies take a harder look at legitimate companies operating along this chain to facilitate ransomware payment, including to ensure that those companies are complying with the Bank Secrecy Act, which imposes certain anti-money laundering and know-your-customer requirements on covered businesses.

Jena Valdetero is an attorney and shareholder in the Chicago office of Greenberg Traurig, LLP. She is co-chair of the firm's U.S. data, privacy and cybersecurity practice. She has led more than 1,000 data breach investigations and has designed and conducted dozens of data breach tabletop exercises to empower clients to respond effectively to a data security incident. Valdetero also counsels companies on data privacy and security compliance programs and advises on cyber risks associated with mergers and transactions.

Kara Bombach is an attorney and shareholder in the Washington, D.C., office of Greenberg Traurig, LLP. She is chair of the firm's Washington, D.C. international trade practice. She counsels companies and organizations on best practices in economic sanctions, trade, and anti-corruption compliance issues that arise in their global operations. Bombach regularly represents clients in matters before U.S. government agencies and has significant experience representing individuals and entities before OFAC in compliance and enforcement matters as well as delisting matters and challenges to OFAC sanctions designations.

Kyle Freeny is an attorney and shareholder in the Washington, D.C., office of Greenberg Traurig, LLP and co-chair of the firm's

cryptocurrency enforcement team. She focuses her practice on government and internal investigations and anti-money laundering and international corruption matters. Freeny is a former prosecutor with the Department of Justice and the Special Counsel's Office, where she investigated Russian cyber interference in the 2016 presidential election, and she has considerable experience handling complex transnational enforcement matters.