DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: October 1, 2020

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this advisory to highlight the sanctions risks associated with ransomware payments related to malicious cyber-enabled activities. Demand for ransomware payments has increased during the COVID-19 pandemic as cyber actors target online systems that U.S. persons rely on to continue conducting business. 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. This advisory describes these sanctions risks and provides information for contacting relevant U.S. government agencies, including OFAC, if there is a reason to believe the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[2]

Background on Ransomware Attacks

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 from victims in exchange for decrypting the information and restoring victims' 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, usually through digital currency, 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's 2018 and 2019 Internet Crime Reports, there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.[3] While ransomware attacks are carried out against large corporations, many ransomware attacks also target small- and medium-sized

[1] This advisory is explanatory only and does not have the force of law. It does not modify statutory authorities, Executive Orders, or regulations. It is not intended to be, nor should it be interpreted as, comprehensive or as imposing requirements under U.S. law, or otherwise addressing any particular requirements under applicable law. Please see the legally binding provisions cited for relevant legal authorities.

[2] This advisory is limited to sanctions risks related to ransomware and is not intended to address issues related to information security practitioners' cyber threat intelligence-gathering efforts more broadly. For guidance related to those activities, see guidance from the U.S. Department of Justice, Criminal Division, Computer Crime and Intellectual Property Section, Cybersecurity Unit, *Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources* (February 2020), available at https://www.justice.gov/criminal-ccips/page/file/1252341/download.

[3] *Compare* Federal Bureau of Investigation, Internet Crime Complaint Center, *2018 Internet Crime Report*, at 19, 20, available at https://pdf.ic3.gov/2018_IC3Report.pdf, *with* Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, available at https://pdf.ic3.gov/2019_IC3Report.pdf.

businesses, local government agencies, hospitals, and school districts, which may be more vulnerable as they may have fewer resources to invest in cyber protection.

OFAC Designations of Malicious Cyber Actors

OFAC has designated numerous malicious cyber actors under its cyber-related sanctions program and other sanctions programs, including perpetrators of ransomware attacks and those who facilitate ransomware transactions. For example, starting in 2013, a ransomware variant known as Cryptolocker was used to infect more than 234,000 computers, approximately half of which were in the United States.[4] OFAC designated the developer of Cryptolocker, Evgeniy Mikhailovich Bogachev, in December 2016.[5]

Starting in late 2015 and lasting approximately 34 months, SamSam ransomware was used to target mostly U.S. government institutions and companies, including the City of Atlanta, the Colorado Department of Transportation, and a large healthcare company. In November 2018, OFAC designated two Iranians for providing material support to a malicious cyber activity and identified two digital currency addresses used to funnel SamSam ransomware proceeds.[6]

In May 2017, a ransomware known as WannaCry 2.0 infected approximately 300,000 computers in at least 150 countries. This attack was linked to the Lazarus Group, a cybercriminal organization sponsored by North Korea. OFAC designated the Lazarus Group and two sub-groups, Bluenoroff and Andariel, in September 2019.[7]

Beginning in 2015, Evil Corp, a Russia-based cybercriminal organization, used the Dridex malware to infect computers and harvest login credentials from hundreds of banks and financial institutions in over 40 countries, causing more than $100 million in theft. In December 2019, OFAC designated Evil Corp and its leader, Maksim Yakubets, for their development and distribution of the Dridex malware.[8]

OFAC has imposed, and will continue to impose, sanctions on these actors and others who materially assist, sponsor, or provide financial, material, or technological support for these activities.

---

[4] Press Release, U.S. Dept. of Justice, U.S. Leads Multi-National Action Against "Gameover Zeus" Botnet and "Cryptolocker" Ransomware, Charges Botnet Administrator (June 2, 2014), available at https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware.

[5] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016), available at https://www.treasury.gov/press-center/press-releases/Pages/jl0693.aspx.

[6] Press Release, U.S. Dept. of the Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), available at https://home.treasury.gov/news/press-releases/sm556.

[7] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), available at https://home.treasury.gov/news/press-releases/sm774.

[8] Press Release, U.S. Dept. of the Treasury, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware (Dec. 5, 2019), available at https://home.treasury.gov/news/press-releases/sm845.

Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests

Facilitating a ransomware payment that is demanded as a result 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 to comprehensively sanctioned jurisdictions could be used to fund activities adverse to the national security and foreign policy objectives of the United States. Ransomware payments may also embolden cyber actors to engage in future attacks. In addition, paying a ransom to cyber actors does not guarantee that the victim will regain access to its stolen data.

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[9] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially 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 transactions by a non-U.S. person which causes a U.S. person to violate any IEEPA-based sanctions, is also prohibited. U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons, which could not be directly performed by U.S. persons due to U.S. sanctions regulations. 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 it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under sanctions laws and regulations administered by OFAC.

OFAC's Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)[10] provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Under the Enforcement Guidelines, in the event of an apparent violation of U.S. sanctions laws or regulations, the existence, nature, and adequacy of a sanctions compliance program is a factor that OFAC may consider when determining an appropriate enforcement response (including the amount of civil monetary penalty, if any).

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.[11] This 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 that may involve processing ransom payments (including depository institutions and money services

[9] 50 U.S.C. §§ 4301–41; 50 U.S.C. §§ 1701–06.
[10] 31 C.F.R. part 501, appx. A.
[11] To assist the public in developing an effective sanctions compliance program, in 2019, OFAC published *A Framework for OFAC Compliance Commitments*, intended to provide organizations with a framework for the five essential components of a risk-based sanctions compliance program. The *Framework* is available at https://home.treasury.gov/system/files/126/framework_ofac_cc.pdf.

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. Companies involved in facilitating ransomware payments on behalf of victims should also consider whether they have regulatory obligations under Financial Crimes Enforcement Network (FinCEN) regulations.[12]

Under OFAC's Enforcement Guidelines, OFAC will also consider a company's self-initiated, timely, and complete report of a ransomware attack to law enforcement to be a significant mitigating factor in determining an appropriate enforcement outcome if the situation is later determined to have a sanctions nexus. OFAC will also consider a company's full and timely cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor when evaluating a possible enforcement outcome.

OFAC Licensing Policy

Ransomware payments benefit illicit actors and can undermine the national security and foreign policy objectives of the United States. For this reason, license applications involving ransomware payments demanded as a result of malicious cyber-enabled activities will be reviewed by OFAC on a case-by-case basis with a presumption of denial.

Victims of Ransomware Attacks Should Contact Relevant Government Agencies

OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

- U.S. Department of the Treasury's Office of Foreign Assets Control
  - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
  - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
- U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
  - OCCIP-Coord@treasury.gov; (202) 622-3000
- Financial Crimes Enforcement Network (FinCEN)
  - FinCEN Regulatory Support Section: frc@fincen.gov

[12] *See* FinCEN Guidance, FIN-2020-A00X, "Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments," October 1, 2020, for applicable anti-money laundering obligations related to financial institutions in the ransomware context.

Contact Information for Other Relevant U.S. Government Agencies:

- Federal Bureau of Investigation Cyber Task Force
  - https://www.ic3.gov/default.aspx; www.fbi.gov/contact-us/field
- U.S. Secret Service Cyber Fraud Task Force
  - www.secretservice.gov/investigation/#field
- Cybersecurity and Infrastructure Security Agency
  - https://us-cert.cisa.gov/forms/report
- Homeland Security Investigations Field Office
  - https://www.ice.gov/contact/hsi

If you have any questions regarding the scope of any sanctions requirements described in this advisory, please contact OFAC's Sanctions Compliance and Evaluation Division at (800) 540-6322 or (202) 622-2490.