Application of U.S. Sanction Laws and Ransomware Payments

Trinity Woodbury
Old Dominion University

Application of U.S. Sanction Laws and Ransomware Payments

Trinity Woodbury

Old Dominion University

Table of Contents

I. Introduction

II. Overview of Ransomware

III. U.S. Sanctions Laws

IV. Sanction Violation Consequences under Ransomware Payment Context

V. Cybersecurity Resilience

VI. Conclusion

I. Introduction

Ransomware is a major threat that widely affects individuals and organizations, including businesses. Ransomware victims face the situation of potentially paying ransom payments to threat actors, some of whom might be foreign-based criminals. Ransomware affects victims from all sectors and industries.

There are government regulations that affect cryptocurrencies, including banning certain types of ransomware payments. Government regulations that prohibit such ransom payments disrupt the ransomware criminal enterprise, which may discourage threat actors from focusing on profiting from their cybercrimes. Lately, cybercriminals have shifted their focus to critical infrastructure IT systems, including those supporting hospitals, energy providers, and educational institutions. Threat actors know that these critical infrastructure systems are least likely able to tolerate downtime, and they may potentially face enormous amounts of pressure to quickly restore their operations by paying the ransom.

Sanction regulations of the U.S. government require U.S. citizens not to transact with certain identified entities or face civil action by the government. If a ransomware threat actor happens to be designated as a sanctioned entity, such as a sanctioned Russian government agency, then U.S. citizens are not allowed to transmit ransom payments to those actors, even if there is no way to quickly remedy the effects of the ransomware. This is a massive dilemma for ransomware victims because, on the one hand, U.S. citizens face civil liabilities, such as fines, for paying ransom to unlock encrypted files; on the other hand, U.S. citizens will likely have the means to unlock their encrypted files by not paying the ransom, unless law enforcement seizes appropriate decryption tools from threat actors.

Sanction laws have unanticipated effects in the cybersecurity arena. Concerning ransomware, IT professionals and organization leaders should be aware of the legal dilemma surrounding ransom payments in this field. This paper explores the dilemma.

II. Overview of Ransomware

Ransomware incidents can severely disrupt business processes and leave organizations without operating IT infrastructure to support mission-critical services. Paying ransom encourages perpetrators to target more victims and incentivizes others to get involved in cybercrime activity. Ransom payments don't guarantee the victim that threat actors will help to restore encrypted data.[1]

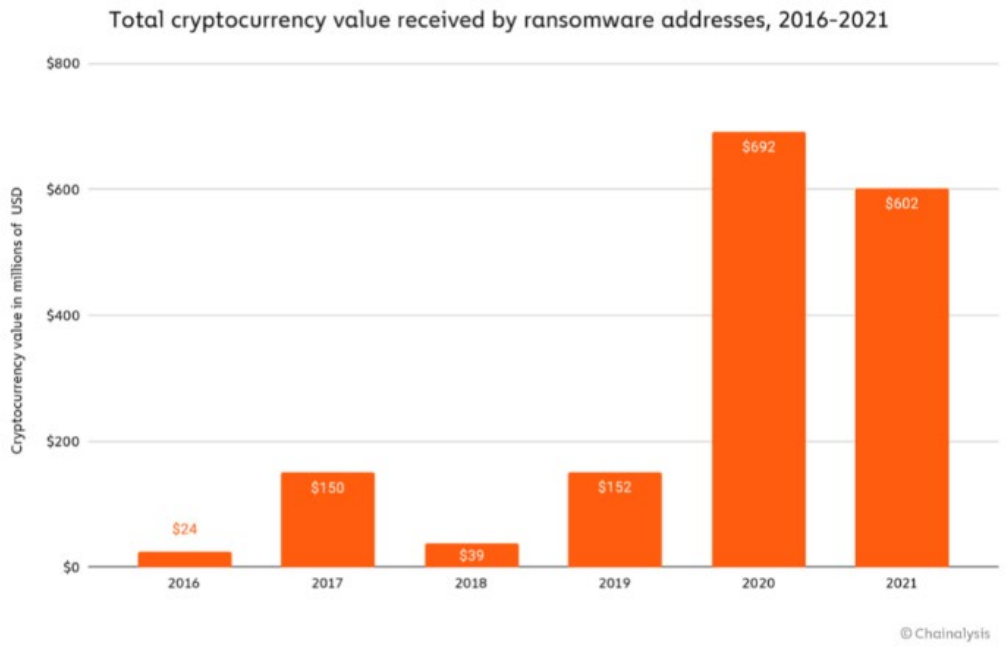

Figure 1: Data from Chainalysis indicating the rise of cryptocurrency ransoms paid to threat actors.[2]

[1] *Scams and Safety,* Federal Bureau of Investigations (February 2021), (https://www.fbi.gov/scams-and-safety).

[2] *As Ransomware Payments Continue to Grow, So Too Does Ransomware's Role in Geopolitical Conflict*, Chainalysis (February 10, 2022), (https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/).

Over the years, the monetary value of ransom demands has also increased, with some demands exceeding $1 million.[3] To help reduce ransomware harm, the NIST Cybersecurity Framework helps to identify, assess, and manage cybersecurity risks for potential victim organizations.[4] Meanwhile, the FBI does not support paying ransom in response to ransomware attacks.[5]

III. U.S. Sanctions Laws

In general, it is unlawful for any U.S. Person, including U.S. citizens, to transact with certain identified entities and individuals that are sanctioned by the U.S. Department of the Treasury's Office of Foreign Asset Control (OFAC).[6] OFAC has established regulations that prohibit U.S. Persons from providing services and facilitating transactions to individuals and entities listed under Specially Designated Nationals And Blocked Persons List, unless a general or specific license is obtained by OFAC.[7]

Sanction laws often target hostile countries to the U.S., such as Iran and North Korea. In general, U.S. companies have to implement certain procedures to ensure compliance with U.S. sanction laws, which impact U.S. companies on a day-to-day basis. Due to the severe civil and

---

[3] *Ransomware Guide,* Cybersecurity and Infrastructure Security Agency (April, 2020), (https://www.cisa.gov/stopransomware/ransomware-guide).

[4] William Barker, *Ransomware Risk Management: A Cybersecurity Framework Profile* (February 2022), (https://csrc.nist.gov/publications/detail/nistir/8374/final).

[5] *Ransomware*, Federal Bureau of Investigations, (https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware).

[6] *Basic Information on OFAC and U.S Sanctions*, U.S. Department of Treasury (August 11, 2020), (https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/1501).

[7] *Overview of US Sanction Laws and regulations,* Norton Rose Fulbright *(*April 12, 2022*)*, (https://www.nortonrosefulbright.com/en-us/knowledge/publications/5522bd68/overview-of-us-sanctions-laws-and-regulations).

criminal penalties involved (including recent penalties of over $1 billion), it is important for companies to stay in compliance with U.S. sanction laws.[8]

U.S. sanction laws have been applied to cryptocurrencies. For example, on September 21, 2021, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) levied its first sanctions against a Russian-operated virtual currency exchange involved in ransomware payments and published an updated advisory on sanctions risks for ransomware payments.[9]

A ransomware payment made to a sanctioned person or sanctioned country would violate U.S. law even if the victim of the ransomware attack was unaware of the sanctions. Therefore, U.S. citizens and companies will be held liable if they pay ransom to sanctioned entities.

The U.S. Department of Homeland Security and the U.S. Department of Justice established the StopRansomware.gov website to help private and public organizations access resources to mitigate their ransomware risk.[10] U.S. industries, such as financial services, are often targeted by ransomware attacks, and the cybersecurity firms that help victims manage attacks sometimes may suggest paying ransom to threat actors, unaware of the unanticipated effects of U.S. government sanction laws prohibiting certain transactions. There needs to be greater public awareness of how U.S. sanction laws create legal liability for ransomware victims when threat actors just happen to be sanctioned entities.

---

[8] *Understanding the OFAC Sanctions Laws: Requirements for U.S. Companies,* JDSupra (December 18, 2020), (https://www.jdsupra.com/legalnews/understanding-the-ofac-sanctions-laws-66379/).

[9] *OFAC Imposes New Sanctions to Thwart Ransomware,* Wilmerhale (September 23, 2021), (https://www.wilmerhale.com/en/insights/client-alerts/20210923-ofac-imposes-new-sanctions-to-thwart-ransomware).

[10] *Ongoing Public U.S. Efforts to Counter Ransomware,* White House (October 13, 2021), (https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/).

IV. Sanction Violation Consequences under Ransomware Payment Context

OFAC imposes civil penalties based on strict liability, where individuals could be held civilly liable even if they did not know or have reason to know that they were engaging in a transaction that was prohibited under sanctions laws and regulations.[11] U.S. sanctions regulations aim to protect national security interests. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands. Instead, it recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.[12] Ransom 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. Therefore, businesses and U.S. citizens have to implement backup and restoration practices in case of a ransomware attack.

V. Cybersecurity Resilience

Having a backup strategy in place is vital for data security in case of a ransomware attack.[13] Data backups are your only guarantee against data loss and having to pay a ransom in the event of a ransomware attack. Storing the copy of the data on a separate medium is critical to

---

[11] Daniel Shin, *Treasury's Office of Foreign Assets Control publishes updated advisory on ransomware payments,* Center for Legal & Court Technology, William & Mary Law School (October 11, 2021), (https://legaltechcenter.net/files/sites/159/2021/11/Cyber-Newsletter-Issue-11.pdf).

[12] *Ransomware Payments with a Sanctions Nexus Threaten U.S. National Security Interests,* U.S. Department of Treasury (September 2021), (https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf).

[13] Victor Congionti, *Keeping your backups safe from Ransomware attacks* (May 11, 2020), (https://www.infosecurity-magazine.com/opinions/keeping-backups-ransomware/).

protect against data loss or corruption.[14] This additional medium can be as simple as an external drive or USB stick, or something more substantial, such as a cloud storage container or tape drive.

Fortunately it is easier than ever to have regular backups done and stored off site in case of a ransomware attack with cloud services. To help mitigate the effects of ransomware attacks, companies and users should back up data regularly and double-check that those backups were completed. Data backups are important to ensure you are protected in the event of hardware failure, natural disaster, and cyberattacks.[15] Data loss can be a huge cost to a company and maybe impossible for the company to recover if facing a ransomware attack.[16] Overall, backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data.

V. Conclusion

To defend against ransom under U.S. sanction laws, U.S. citizens should backup their files in case of a ransomware attack. Backing up their data will grant U.S. citizens a solid defense mechanism against threat actors who hack into U.S. citizens' networks to steal and encrypt information/data for ransom. Therefore, U.S. citizens should backup their information and data in case sanctioned entities target their information and demand ransom.

---

[14] *What is Backup and Recovery?*, NetApp (November 2022), (https://www.netapp.com/data-protection/backup-recovery/what-is-backup-recovery/).

[15] Shimon Brathwaite, *Why are data backups important?*, Security Made Simple (January 22, 2021), (https://www.securitymadesimple.org/cybersecurity-blog/why-are-data-backups-important).

[16] Stu Sjouwerman, *Seven Factors Analyzing Ransomware's Cost To Business?*, Forbes (July 29, 2021), (https://www.forbes.com/sites/forbestechcouncil/2021/07/29/seven-factors-analyzing-ransomwares-cost-to-business/).