
GT GreenbergTraurig
BIGLAW
REDEFINED:
Ransomware Attacks and Sanctions in the Time of War
GTLAW.COM
APRIL 6, 2022

GT GreenbergTraurig

Today's Speakers

Kara Bombach
WASHINGTON D.C.
bombachk@gtlaw.com

Kyle Freeny
WASHINGTON D.C.
freenyk@gtlaw.com

Jena Valdetero
CHICAGO
valdeteroj@gtlaw.com

GT GreenbergTraurig

Agenda

- Ransomware Trends
- Sanctions Update
- U.S. Enforcement Considerations

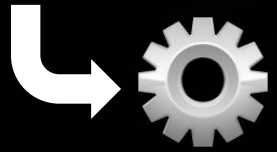
GT GreenbergTraurig

Ransomware Trends

GT GreenbergTraurig

Anatomy of an Attack

1 Initial Entry



2 Lateral Movement and Recon/Backup Destruction

3 Data Exfiltration

4 Ransomware Deployment

****Initial Entry****

- **Malware Infection**
- **Scan-and-Exploit**
- **Credential Abuse**

GT GreenbergTraurig

Are Ransomware Attacks Preventable?

Malware Infection

Endpoint and Network Detection

Scan-and-Exploit

Patch

Credential Abuse

Multi-Factor Authentication

Ransomware "Trends"

- Increase in number of threat actors
- Franchising ransomware
- Increase in monetary demands
- Increase in data access/exfiltration
- Name and Shame sites
- Contacting victims
- DDOS attacks

GT GreenbergTraurig

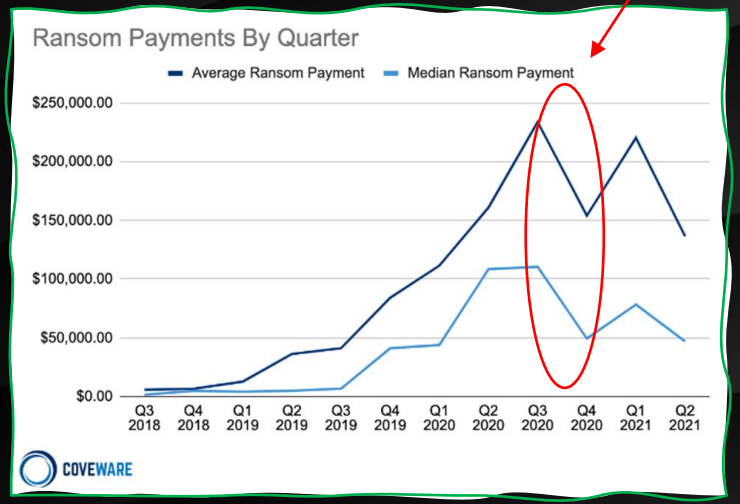
Government Wakeup Call!

- **DOJ gives ransomware attacks similar priority as terrorism**
- **Cyber Incident Reporting for Critical Infrastructure Act**
- **Increased funding for Cybersecurity and Critical Infrastructure Agency (CISA)**
- **Increasing regulations around reporting ransomware attacks**

GT GreenbergTraurig

Ransom: To Pay or Not To Pay?

- Pros v. Cons
- Back-ups
- How do you feel about paying a criminal?
- Will you get your data back?
- Time = Money
- Sanctions



GT GreenbergTraurig

Office of Foreign Assets Control (OFAC) Guidance

- OFAC issued updated advisory in September 2021 in response to increase in attacks due to COVID-19.
- Ransom payments not only encourage the behavior and threaten U.S. national security and foreign policy objectives.
  - Payments **do not** guarantee restored access (Eh…)
- Payments May Violate OFAC Regulations = Civil Penalties based on strict liability
- Implementation of risk-based compliance program is encouraged
  - Banks, cyber insurers, forensic investigators/incident response – may have obligations under FinCEN
- Notifying law enforcement before making a payment is considered a "significant mitigating factor"

GT GreenbergTraurig

How Does Russia Fit In Here?

- Many threat actor groups are associated with Russia
- Russian government, at minimum, looks the other way
- February 25th statement by Conti threatens to "strike back" at Russia's enemies – unwise patriotism?
- However, leaked chat logs don't reveal direct link with Russian government

GT GreenbergTraurig

Where Are We Today?

- FBI's official position is still "do not pay"
- Cyber Insurance rate increases, potential coverage issues
- Mandatory federal reporting of ransom payment for certain industries
- Proposed laws against making ransom payments (unlikely to pass)
- OFAC sanctions issues are real

GT GreenbergTraurig

Sanctions Update

GT GreenbergTraurig

Introduction to OFAC: Overview

- The Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign:
  - Governments
  - Individuals
  - Entities
  - Vessels
  - Practices

GT GreenbergTraurig

Introduction to OFAC: What are OFAC Sanctions

Targeted Party-Specific Sanctions

- Transactions by U.S. persons with listed companies/people are prohibited
  - Sanctioned parties are included on various U.S. government lists
  - Specially Designated Nationals (SDN) list
- To avoid violations:
  - Know who you are doing business with;
  - Screen to make sure transactions with the company/individual are not prohibited.

Comprehensive Sanctions

- No U.S. Person involvement in direct or indirect transactions involving the following:
  - Cuba
  - Iran
  - North Korea
  - Syria
  - Covered Regions of Ukraine
  - The full list of sanctioned countries can be found below: https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information

GT GreenbergTraurig

Who must comply with OFAC sanctions?

- Individuals:
  - U.S. citizens and lawful permanent residents, wherever located
  - Any individual in the United States
- Entities: Any entity organized under U.S. law
  - Any entity organized under the laws of the United States or any jurisdiction therein, including its foreign branches
  - Any entity in the U.S. regardless of whether organized in the U.S.
  - With respect to certain sanctions programs (Cuba and Iran), entities owned or controlled by a U.S. person and established or maintained outside of the United States
- Non-US person liability under primary sanctions
  - Fact specific and case-by-case analysis to determine whether a transaction or activity has an enforceable nexus to the United States
  - Some circumstances that might establish such a nexus include:
    - The goods, services, or technology involved in the transaction are U.S.-origin
    - The transaction involves U.S. persons, including individuals with U.S. citizenship or permanent residency and U.S. financial institutions
    - Activities that take place in the United States

GT GreenbergTraurig

Introduction to OFAC: Fines and Penalties

A company and its employees can be held responsible for violations (even inadvertent)

- Company:
  - Civil fines up to $311,562 per violation, or twice the value of the transaction
  - Criminal fines up to $1,000,000 per violation
  - Debarment from USG contracts
  - Loss of customers
- Employees:
  - Potential civil and criminal fines (up to $1,000,000 per violation) or prison sentence for knowing violations

GT GreenbergTraurig

OFAC Requirements and Procedures

- **U.S. Persons are required to reject or block (and report) certain types of prohibited transactions. EVEN VIRTUAL CURRENCY TRANSACTIONS**

- **Initial Blocked Property Reports:**
  - Must be filed within 10 business days following the date that property is blocked.
- **Annual Blocked Property Reports:**
  - On all blocked property held as of June 30 of the current year must be filed annually no later.
- **Rejected Transaction Reports:**
  - Must be filed within 10 business days of the date the transaction was rejected due to sanctions requirements.

GT GreenbergTraurig

OFAC Compliance: Best Practices

- Risk-Based Compliance Programs for 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.
    - Ex. Sanctions list and geographic screening and other appropriate measures as determined by the company's unique risk profile.

GT GreenbergTraurig

OFAC Compliance: Best Practices

Remediating the Root Causes of Violations

Virtual currency industry remedial actions to suspected OFAC violations, (to halt violations, to identify internal controls weaknesses, and to prevent future violations).

- Implementing IP address blocking and email-related restrictions for sanctioned jurisdictions
- Implementing an OFAC-related training program for employees
- Creating a keywords list of a sanctioned jurisdiction's cities and regions to be used when screening customer information
- Conducting additional sanctions compliance training for all relevant personnel
- Reviewing and updating end-user agreements to include information about U.S. sanctions requirements
- Hiring additional compliance staff and a dedicated chief or sanctions compliance officer
- Conducting retroactive batch screening of all users

Red Flags

Virtual currency companies should also consider monitoring transactions and users for risk indicators or "red flags" that may indicate a sanctions nexus. Examples of risk indicators may be individuals or entities who:

- Provide inaccurate or incomplete customer identification when attempting to open an account
- Attempt to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction
- Are non-responsive or refuse to provide updated customer identification
- Are non-responsive or refuse to provide additional transaction information in response to a virtual currency company's request
- Attempt to transact with a virtual currency address associated with a blocked person or sanctioned jurisdiction

GT GreenbergTraurig

Russia Sanctions Developments 2022:

- Direct Blocking/Targeted Sanctions
- Financial Sector and Banking Sanctions
- Expanded Export Controls
- Energy Sector Sanctions
- New Investment Restrictions
- Exceptions and General Licenses

GT GreenbergTraurig

Russia Targeted Sanctions Designations

- Prohibition on dealings with President Putin and designated Russian officials across all jurisdictions
- Covered Regions in Ukraine
  - U.S., EU and UK establish comprehensive embargo against areas of Donetsk and Luhansk ("Covered Regions")
  - Targeted sanctions against individuals and entities involved in all three jurisdictions
- Restrictions on Individuals and Entities in Belarus

GT GreenbergTraurig

Targeted Sanctions

- Other targeted individuals and entities include Russian banks, sovereign wealth fund, influential individuals from Russia and Russian and Belarussian defense companies
- OFAC 50% Rule
- Risks of dealing with someone working for or on behalf of sanctioned person
- Asset freezes typically takes effect immediately; all dealings are prohibited
  - Freezes of bank accounts, yachts and villas
  - Certain U.S. bank sanctions are more limited; and wind-down general licenses may be available for certain sanctioned entities in the U.S.

GT GreenbergTraurig

Sanctions Impact and Reach

In addition to direct impact measures:

- Private firms pausing activities and investments in and supplies to Russia
- Banks implement severe compliance measures; reluctant to process payments linked to Russia
- Supply chain disruptions
- Business partners requesting “no ties with Russia confirmation”

GT GreenbergTraurig

Sanctions in Ransomware Context

- Watch for even indirect dealings with sanctioned person
- Challenges with insurance policies/claims
- Visibility with various U.S. Government agencies
- Potential for export control issues/trade secret releases by malign actors with highjacked data
- Potential multi-agency disclosures appropriate

GT GreenbergTraurig

CLE CODE

For participants seeking CLE credit, today's CLE code is 2237.

Again, the code is 2237.

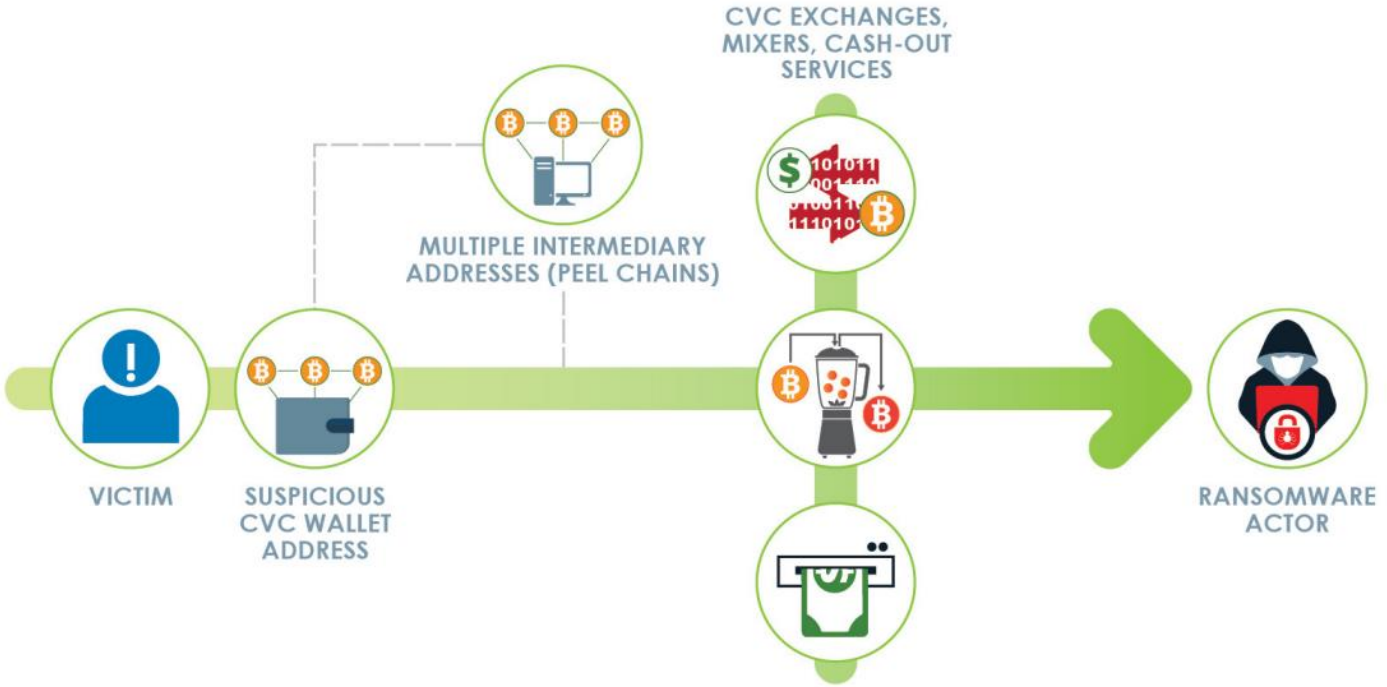
Please enter this code on the attendance affidavit. The link to the affidavit is located in the chat and will also be included in an email after the program.

GT GreenbergTraurig

U.S. Enforcement Considerations

GT GreenbergTraurig

Figure 1. Movement of CVC in Ransomware Attacks



DOJ Enforcement Initiatives

- KleptoCapture Task Force
- National Cryptocurrency Enforcement Team
- Russian Elites, Proxies, and Oligarchs (REPO) multilateral task force

GT GreenbergTraurig

Additional Enforcement Considerations

- U.S. authorities have been taking harder look at what they see as concealment of incidents (vs. mere non-disclosure)
- FinCEN guidance re: companies involved in facilitating ransomware payments
- Considerations for financial institutions (e.g., suspicious activity reporting)

GT GreenbergTraurig

Thank you. Questions?

Kara Bombach
WASHINGTON D.C.
bombachk@gtlaw.com

Kyle Freeny
WASHINGTON D.C.
freenyk@gtlaw.com

Jena Valdetero
CHICAGO
valdeteroj@gtlaw.com

GT GreenbergTraurig

GT Alerts

- United States Continues to Escalate Sanctions Against Russia, Targeting Putin Personally and Cutting off Russia from SWIFT | Insights | Greenberg Traurig LLP (gtlaw.com)
- DOJ Establishes Task Force KleptoCapture to Enforce Sanctions, Export Restrictions in Response to Russia's Invasion of Ukraine | Insights | Greenberg Traurig LLP (gtlaw.com)
- EU Issues Sanctions Against Russia Following Russia's Attacks on Ukraine | Insights | Greenberg Traurig LLP (gtlaw.com)
- UK Introduces Economic Crime Legislation in Wake of Russian Invasion of Ukraine | Insights | Greenberg Traurig LLP (gtlaw.com)
- United States Issues Significant Bank Sanctions and Historic Export Controls Targeting Russia | Insights | Greenberg Traurig LLP (gtlaw.com)
- Preparing for the Possibility of Russian Ransomware Attacks | Insights | Greenberg Traurig LLP (gtlaw.com)
- What Steps Other than Sanctions Might the UK Government Take Against Russian Assets in the UK? | Insights | Greenberg Traurig LLP (gtlaw.com)
- UK Issues Sanctions Against Russia Following President Putin's Attack on Ukraine | Insights | Greenberg Traurig LLP (gtlaw.com)
- US Issues 'First Tranche' of Sanctions Targeting Covered Regions of Ukraine | Insights | Greenberg Traurig LLP (gtlaw.com)