K&L GATES

Guillermo Santiago Christensen
Partner, Washington DC

Ransomware Extortion Payments in the United States

How to Reduce Risks When Paying Criminals

Brief Overview of Ransomware

Criminal and nation-state threat actors compromise a company network

Insert malware that encrypts data and system files

Offers the victim company the decryption keys or a decryptor for a sum of money, almost always cryptocurrency

Typical Ransomware Timeline

1. Attack Detected
2. Forensic Response
3. Determine whether recovery is realistic
4. Initiate contact with threat actor (cyber criminal)
5. Negotiate terms of payment/outcome
6. Proof of life test/commitments to perform deletion
7. Payment
8. Receive decryptor/attempt to verify data leak site is inactive

Are We Allowed to Pay?

No federal laws that prohibit paying ransom/extortion

Federal government highly discourages ransom payments

At least one state law bans *public* entities from paying ransoms

- April 2022 North Carolina banned government entities from paying ransom
- Prohibits **even communicating** with the threat actor
- Mandatory reporting
- New York and Pennsylvania considering other types of bans

But, Prohibitions on *Who* You Can Pay

- Not specific to ransomware/extortion
- U.S. government prohibits “U.S. persons” from being involved in transactions with persons that are blocked or designated
  - Blocks dealing with any property interests
  - Prohibits facilitation
- “Specially Designated Individuals” or SDNs
  - Companies or individuals
- OFAC is the enforcer/regulator for civil, DOJ for criminal

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

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

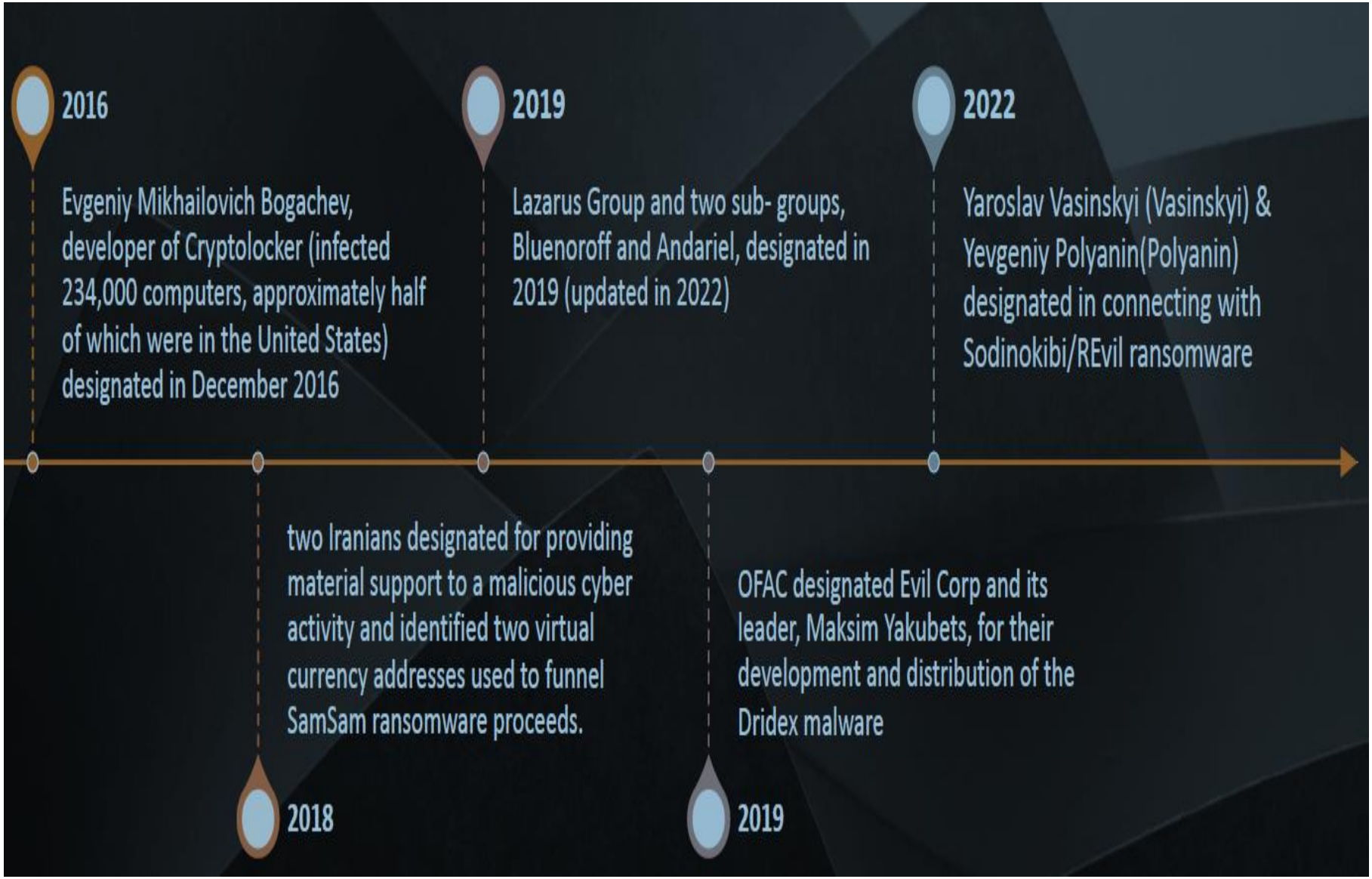
Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

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. The U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands and recommends focusing on strengthening defensive and resilience measures to prevent and protect against ransomware attacks.

This advisory describes the potential sanctions risks associated with making and facilitating ransomware payments and provides information for contacting relevant U.S. government agencies, including OFAC if there is any reason to suspect the cyber actor demanding ransomware payment may be sanctioned or otherwise have a sanctions nexus.[3]

Ransomware-related SDNs



Pivot to Exchanges

- 2021
  - OFAC designated SUEX OTC, S.R.O. a virtual currency exchange, for facilitating financial transactions for ransomware actors
- 2022
  - Added Chatex to the SDN list along with IZIBITS OU, Chatextech SIA, and Hightrade Finance Ltd for providing material support and assistance to Chatex

OFAC Advisories on Ransomware

- U.S. persons are generally prohibited from engaging in transactions, **directly or indirectly**, with persons on the SDN List and those covered by country or region embargoes (Cuba, Crimea, Iran, North Korea, and Syria)

- Any transaction that causes a violation … including a transaction by a non-U.S. person that causes a U.S. person to violate any … sanctions prohibitions, is also prohibited

- U.S. persons, wherever located, are also generally prohibited from facilitating actions of non-U.S. persons that could not be directly performed by U.S. persons due to U.S. sanctions regulations

OFAC & Strict Liability

- OFAC may assess civil penalties for sanctions violations on strict liability basis

=

May be held civilly liable even if they
did not know

or

have reason to know
that they were engaging in
a prohibited transaction

Mitigating Factor in Any OFAC Enforcement Response

- Maintaining offline backups of data
- Developing incident response plans
- Instituting cybersecurity training
- Regularly updating antivirus and anti-malware software
- Employing authentication protocols, among others

Law Enforcement Cooperation = OFAC Credit?

- Victim reports ransomware attacks to U.S. government agencies
- Nature and extent of cooperation with OFAC, law enforcement, including whether an apparent violation is voluntarily self-disclosed
- Voluntary self-disclosure could be a significant mitigating factor in determining appropriate enforcement response
- Will also consider a company's full and ongoing cooperation with law enforcement both during and after a ransomware attack to be a significant mitigating factor
  - Meaning – providing all relevant information such as technical details, ransom payment demand, and ransom payment instructions as soon as possible

Typical Information Sharing Request for FBI

- Date the incident began and when it was noticed
- General information about what was impacted
- Intrusion set or malware/ransomware variant
- Tactical intelligence
  - Wallet information, logs, attacking IPs, etc.
- Was anything exfiltrated?
- What about evidence?

FinCEN ADVISORY

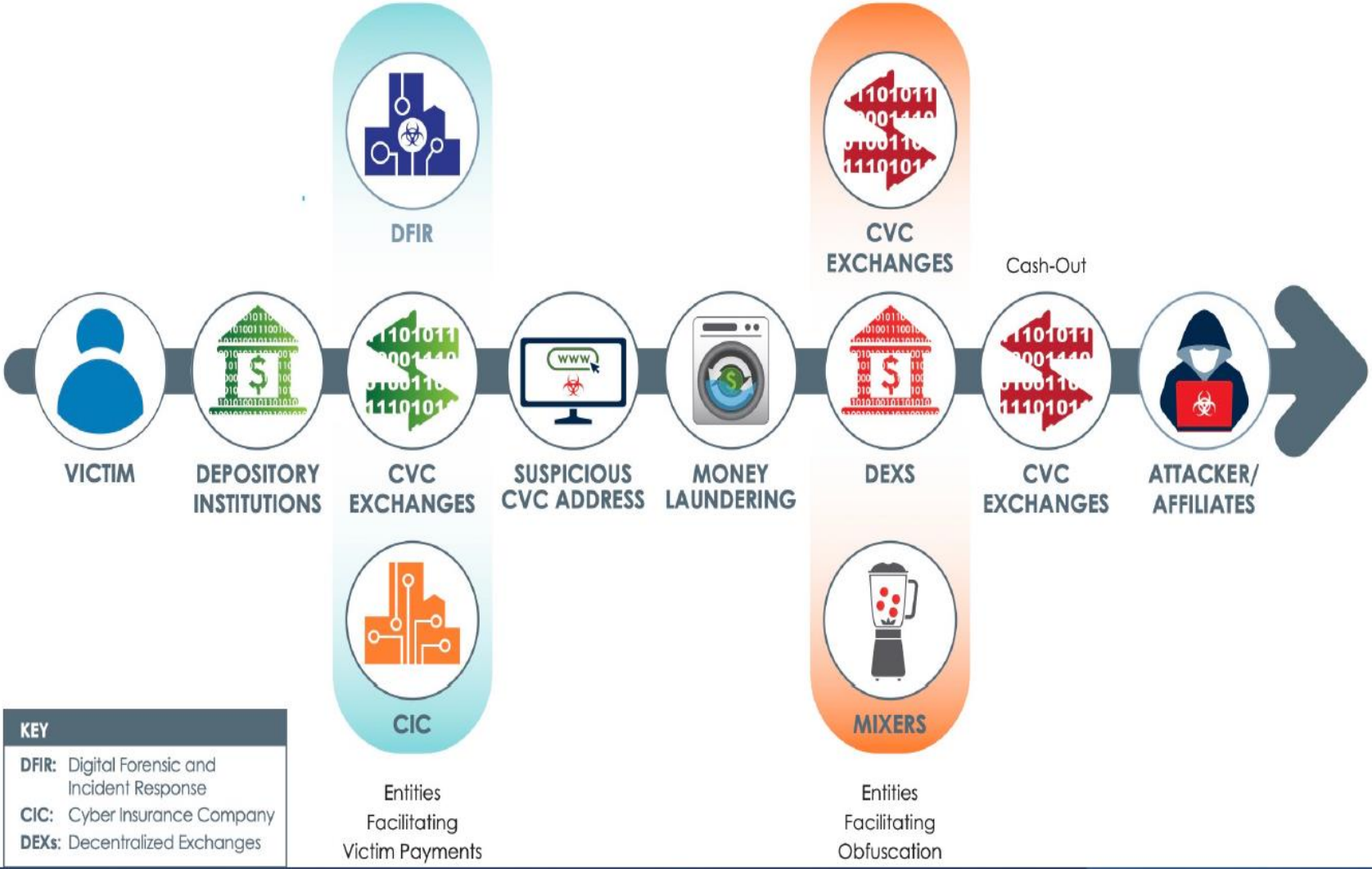
FIN-2021-A004 **November 8, 2021**

Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments

Detecting and reporting ransomware payments are vital to holding ransomware attackers accountable for their crimes and preventing the laundering of ransomware proceeds.

https://www.fincen.gov/sites/default/files/advisory/2021-11-08/FinCEN%20Ransomware%20Advisory_FINAL_508_.pdf

Figure 1. Movement of CVC in Ransomware Incidents



FinCEN and Suspicious Activity Reporting

Report to FinCEN through a SAR when dealing with an incident of ransomware conducted *by, at, or through* financial institution (incl ransom payments made by financial institutions that are victims of ransomware)

SAR obligations apply to *attempted and successful* transactions, including both attempted and successful initiated extortion transactions

Deciding Whether to Pay

- Complex process that mixes intelligence analysis, forensics and legal counsel
  - Typically done under expedited circumstances (days, maybe weeks)
- Forensics = What kind of ransomware?
- Threat Intelligence = who is the attacker and where are they?
- Legal counsel = assessing OFAC risk (high, medium, low)

Factors Going into Decision

- Type of ransomware?
- Type of victim?
- Type of attack?
- RaaS?
- Extortion demand?
- Wallet info?
- Law Enforcement input?
- Threat Intelligence?

Guillermo Christensen

Cybersecurity + National Security + CFIUS + Investigations + OFAC + FC...

Guillermo.Christensen@klgates.com

K&L GATES