

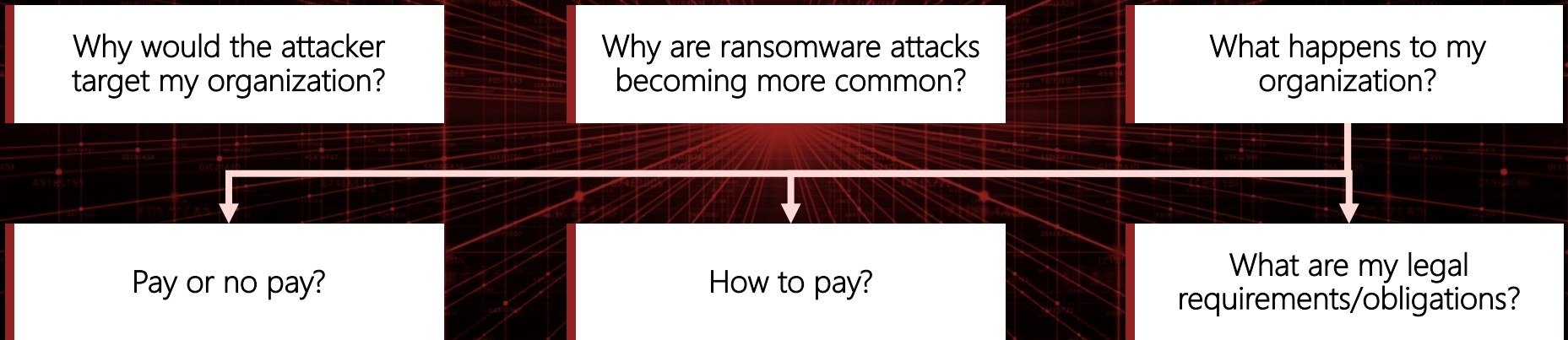
June 6, 2022 | Michigan State University –  
Interdisciplinary Conference on Cybercrime



HERJAVEC  
GROUP

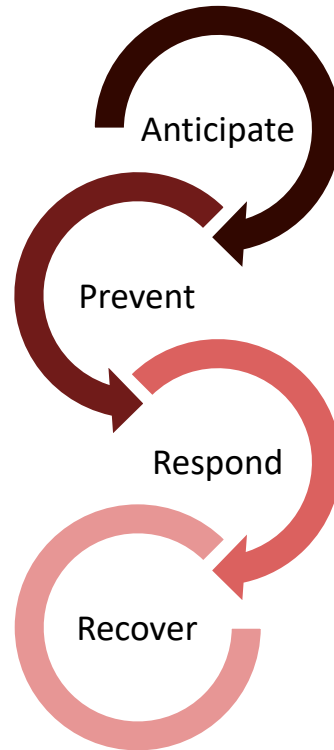
# What is Ransomware?

Many details do not matter; here is what does:

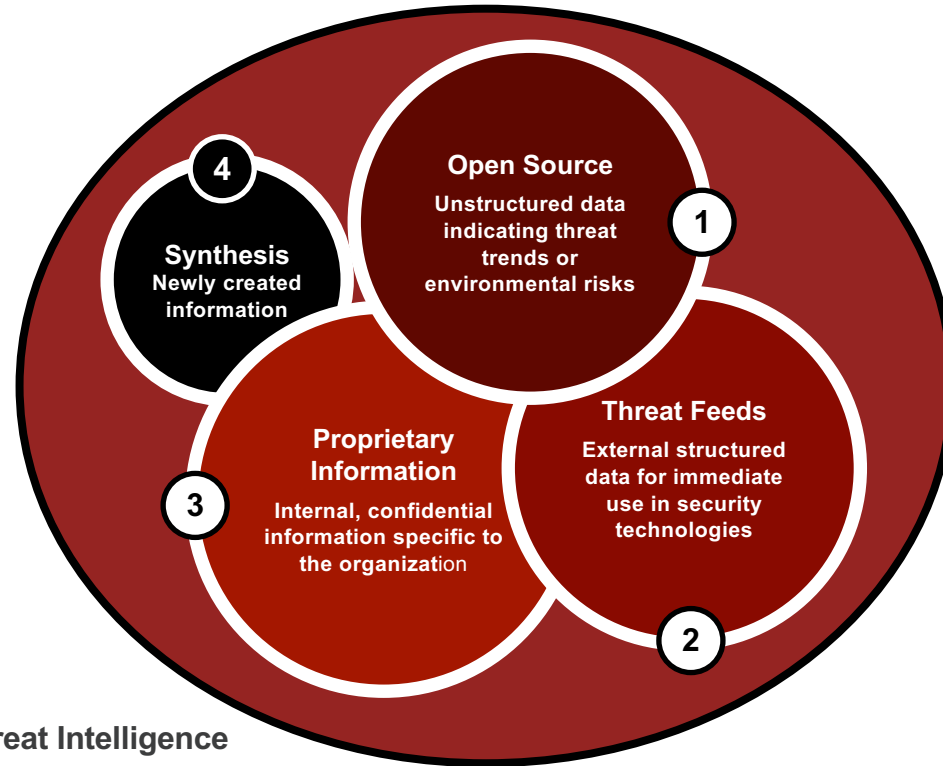


# Cyderes Cyber Security Model

"Actionable intelligence" needs context



# Cyber Threat Intelligence



Actionable Threat Intelligence

## Analysis Framework: Economic Rationality

- Financial attacks are among the most common cyber attackers. The two most common attacks are ransomware and business email compromise.
- Attacks evolve to defeat cyber security.
- Attackers .



# Attackers Monetize Your Data

Path to monetization your data

Ransom

Extortion

Theft

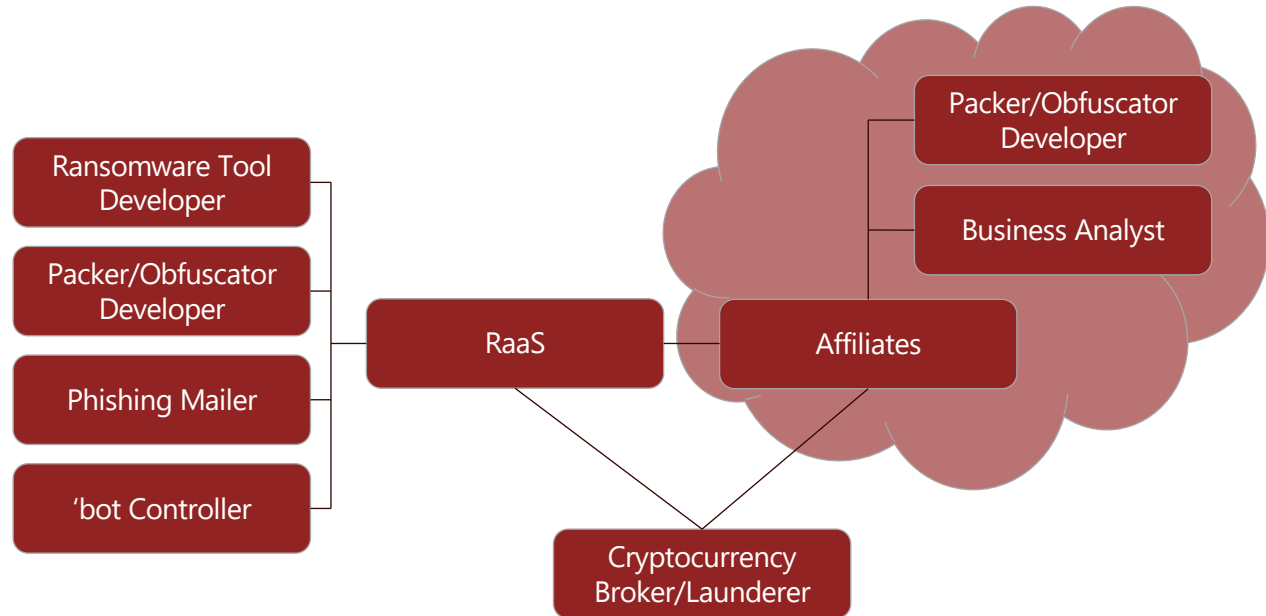
## Analysis Framework: Economic Rationality

- Economic relationships are enabled and controlled by the Dark Web and cryptocurrency.
- Reputation and ability to monetize attract affiliates.
- Breakdown of an affiliate relationship yielded the CONTI playbook suggesting vulnerabilities to exploit, password templates, and server IP's.



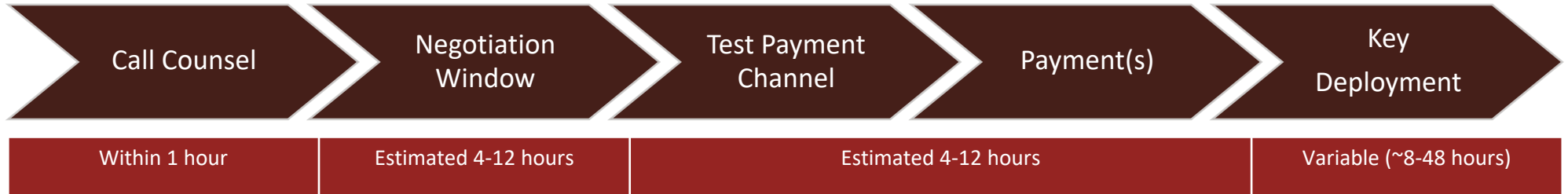
# Economic Relationships

## Ransomware as a Service (RaaS)



# Actionable Experience

Analysis: observations from ransomware responses across industries adds context to intelligence



- ▶ GC typically contacts external counsel
- ▶ Counsel engages negotiator

- ▶ Attacker typically uses throw-away address or anonymous chat
- ▶ Attacker seeks short negotiation and lump sum
- ▶ Smaller transactions provide protection

- ▶ Single transaction for a small/single decryption key
- ▶ Validate payment channel
- ▶ Validates decryption key and process

- ▶ Multiple decryption keys may be used depending on the attacker
- ▶ Additional scope may require additional payments

- ▶ Instructions for key deployment can be minimal
- ▶ Key deployments on production systems and may interfere with other recovery
- ▶ Scanning process is recommended before return to production
- ▶ Restored systems may not be usable
- ▶ Decryption may be slow

## Analysis Framework: Herjavec Threat Analysis

- The path to monetize an attack indicates that even if extortion is paid, data will not be destroyed in its entirety.
- Infrastructure needed for dump sites has increased and become more vulnerable; stolen data volume has been impacted.
- Threat actors now regularly offer such data for sale. Everest even put the data on sale at 54% off. This may be a leading indicator of dissolving trust in the underground or simply a failing threat actor.



# Extortion

Name and shame requires resources and exposure

The image shows a Notepad window with ransomware instructions and a seized website. The Notepad window contains the following text:

```
Hi !  
If you want restore your files write o  
e/erbbe@airmail.cc  
In the subject write - id-#####  
  
> 0d0a9cfd8f8c6876dd0a4b27d18c388c
```

The seized website displays the following information:

**THIS HIDDEN SITE HAS BEEN SEIZED**  
by the Federal Bureau of Investigation,  
as part of a coordinated law enforcement action taken against the NetWalker Ransomware.

The website also features logos for the Department of Justice, Federal Bureau of Investigation, HCoC, and the Ministry of Internal Affairs of Bulgaria.

The action has been taken in coordination with the United States Attorney's Office for the Middle District of Florida and the Computer Crime and Intellectual Property Section of the Department of Justice, with substantial assistance from the Bulgarian National Investigation Service and General Directorate Combating Organized Crime.

Below the seizure notice, there is a search bar and a menu for "Everest ransom team".

**U.S. GOV**

Government access in sale. A huge number of passports, tax, court cases and other documentation. Domain admin



## Analysis Framework: Routine Activities

- Following the Colonial Pipeline recovery in Q3 of 2021, various interventions reduced ransomware attacks.
- Threat actors and affiliates saw a period of reduced activity following government intervention.
- Ragnar Locker had a very public tantrum following the intervention, but others also reacted.
- The U.S. OFAC banned entities list has been a topic for anyone considering paying ransom/extortion.



# Government Intervention

## Threat re-actor

Support 22 Sep, 14:36 PM [NY time]

First of all - you violated our data recovery guidelines and decided to use the services of a company called [redacted] which is blocked in all ransomware groups, so we will not provide you with any discounts or concessions. Secondly - assuming that you are not interested in getting a decryptor, we started loading all your stolen data, including the source codes from fleet, dispatch, soilmap, aws-cli and much more (about 10 gigabyte [redacted]) to the public [redacted] publication. Thirdly - if negotiations are [redacted] we will [redacted] lose money, delete keys and block chats, so [redacted] contact another data recovery company [redacted] P.S. also we encrypted the soilmap again [redacted] infrastructure was never restored, and recu [redacted] We are waiting for feedback on when you a [redacted]

### Announcement: FTP



In our practice we has facing with the professional negotiators much more often in last

## Russia takes down REvil hacking group at U.S. request - FSB

By Tom Balmforth and Maria Tsvetkova

easier or safer, on the contrary it's  
are usually working in recovery-  
Police/FBI/investigation agency and  
ial success of their clients or in safety of

f you will hire any recovery company for  
Police/FBI/Investigators, we will  
iate the publication of whole  
ease that any negotiators will be able to  
ny ways to recognize such a lie. Dear  
y, don't ask the Police to do this for you.

## Analysis Framework: Context

- Privacy regulations and mandatory reporting impact ransomware and extortion decisions.
- Multi District Litigation (MDL) and class actions lawsuits are strong disincentives.
- OFAC and Treasury advisories increase pressure to avoid paying ransom.



# Reporting

## Data breach reporting and follow-on litigation

### Operational Risks

*The Security Incident could have numerous adverse effects on our business.*

As previously disclosed, on July 16, 2020, we contacted certain customers to inform them about the Security Incident, including that in May 2020 we discovered and stopped a ransomware attack. Prior to our successfully preventing the cybercriminal from blocking our system access and fully encrypting files, and ultimately expelling them from our system with no significant disruption to our operations, the cybercriminal removed a copy of a subset of data from our self-hosted environment. Although the nature of the incident, our research and third party (including law enforcement) investigation have provided no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly, our investigation into the Security Incident remains ongoing and may provide additional information.

To date, we have received approximately 260 specific requests for reimbursement of expenses ("Customer Reimbursement Requests") and approximately 400 reservations of the right to seek expense recovery in the future from customers or their attorneys in the U.S., U.K. and Canada related to the Security Incident (none of which have as yet been filed in court) and are in the process of assessing what liability may exist pursuant to such claims. *Of the Customer Reimbursement Requests received to date, approximately 170 have been fully resolved and closed. In addition, if*

An official website of the United States Government.

Accessibility Languages

and insurer subrogated the Security Incident, review of customer and consolidated under r



U.S. DEPARTMENT OF THE TREASURY

ABOUT TREASURY POLICY ISSUES DATA SERVICES NEWS

HOME > POLICY ISSUES > FINANCIAL SANCTIONS > SANCTIONS PROGRAMS AND COUNTRY INFORMATION > SANCTIONS RELATED TO SIGNIFICANT MALICIOUS CYBER-ENABLED ACTIVITIES

### FINANCIAL SANCTIONS

Specially Designated Nationals List (SDN List)

SDN List - Data Formats & Data Schemas

Consolidated Sanctions List (Non-SDN Lists)

Additional Sanctions Lists

## Sanctions Related to Significant Malicious Cyber-Enabled Activities

Sign up for Cyber-related Sanctions e-mail updates.

### IMPORTANT ADVISORIES AND INFORMATION

- Sanctions Compliance Guidance for the Virtual Currency Industry 📄 (October 15, 2021)
- Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments 📄 (Updated September 21, 2021)
- North Korea Cyber Threat Advisory 📄 (April 15, 2020)
  - Non-English Translations of the North Korea Cyber Threat Advisory



# Q&A

Dr. Kall Loper, Vice President of DFIR,  
[kloper@herjavecgroup.com](mailto:kloper@herjavecgroup.com)