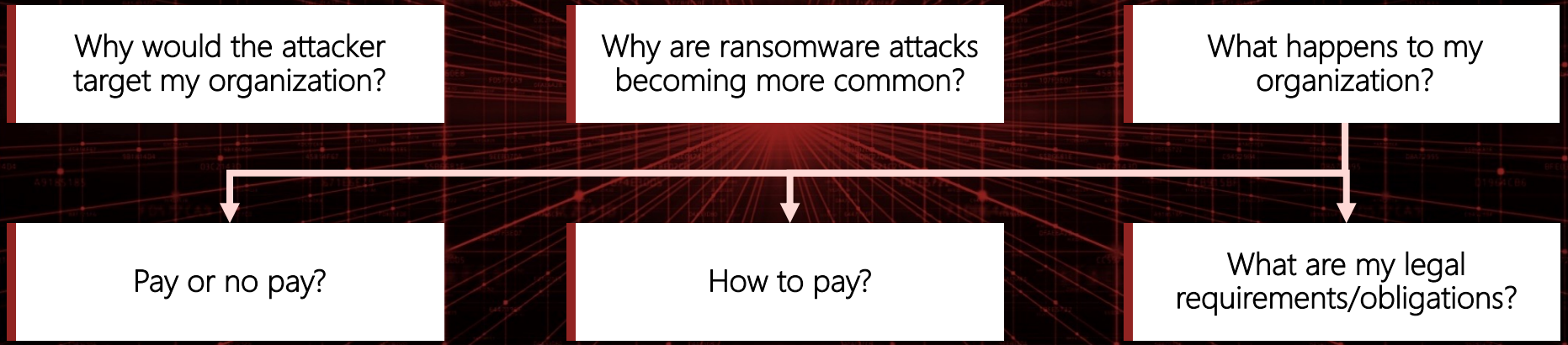
June 6, 2022 | Michigan State University – Interdisciplinary Conference on Cybercrime

HERJAVEC GROUP

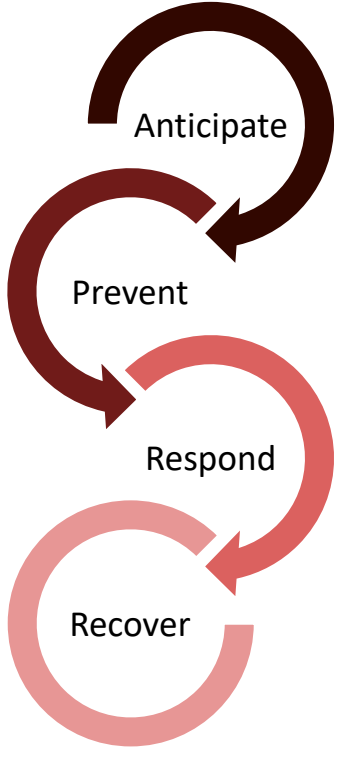
What is Ransomware?

Many details do not matter; here is what does:

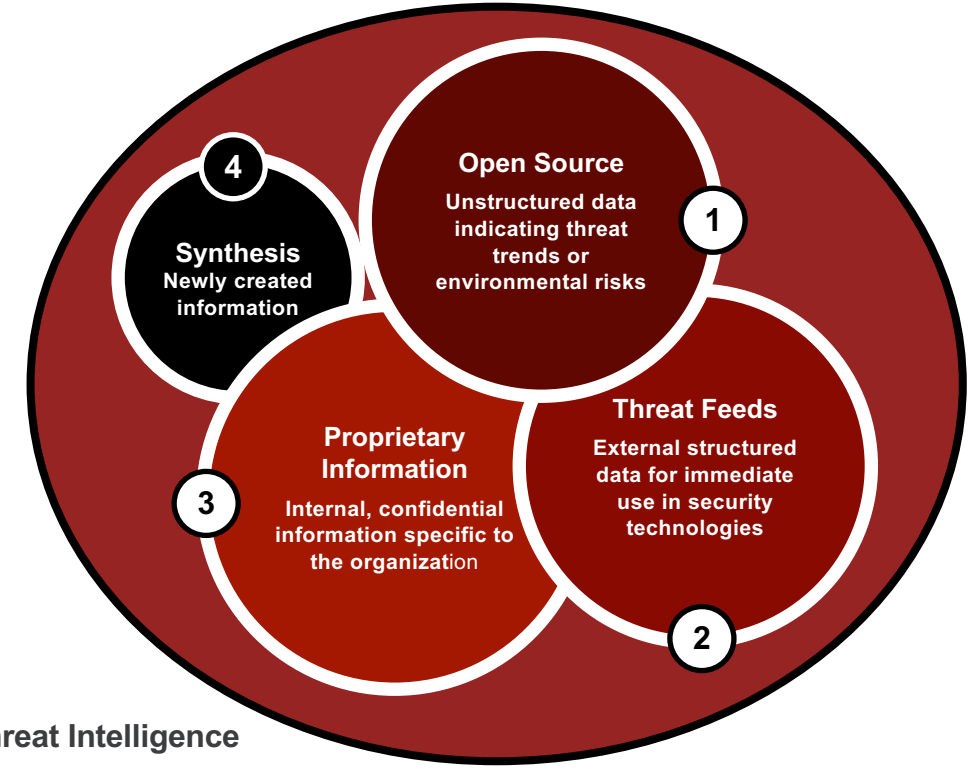


Cyderes Cyber Security Model

"Actionable intelligence" needs context



Cyber Threat Intelligence



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

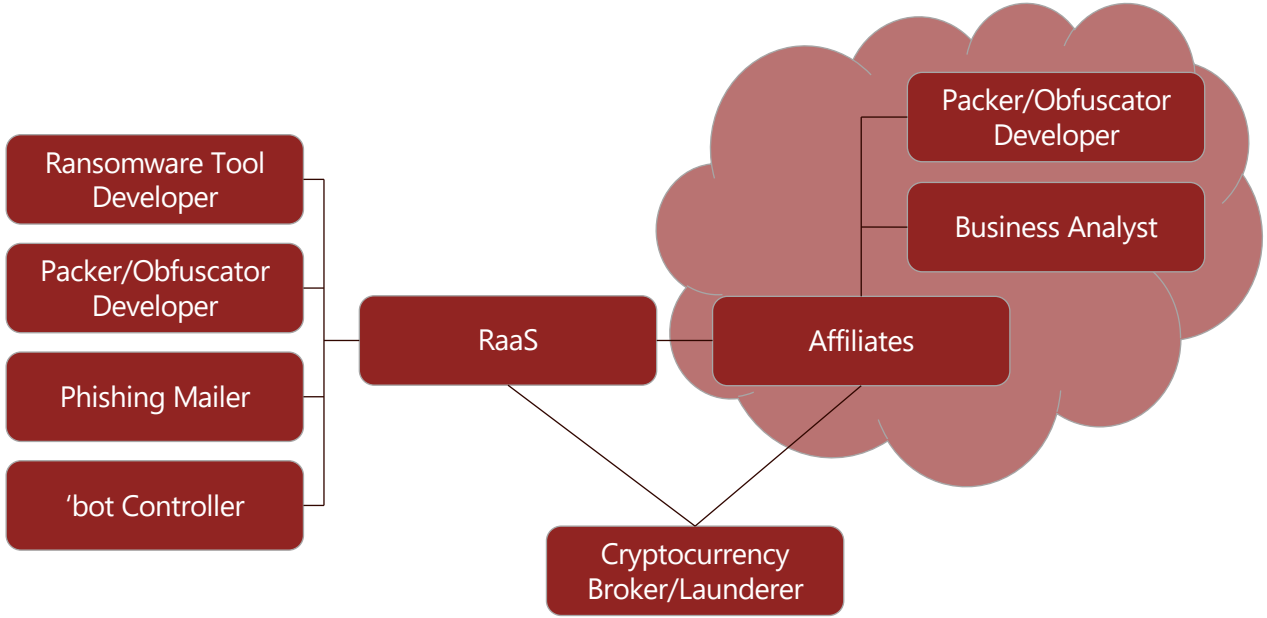
Theft

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

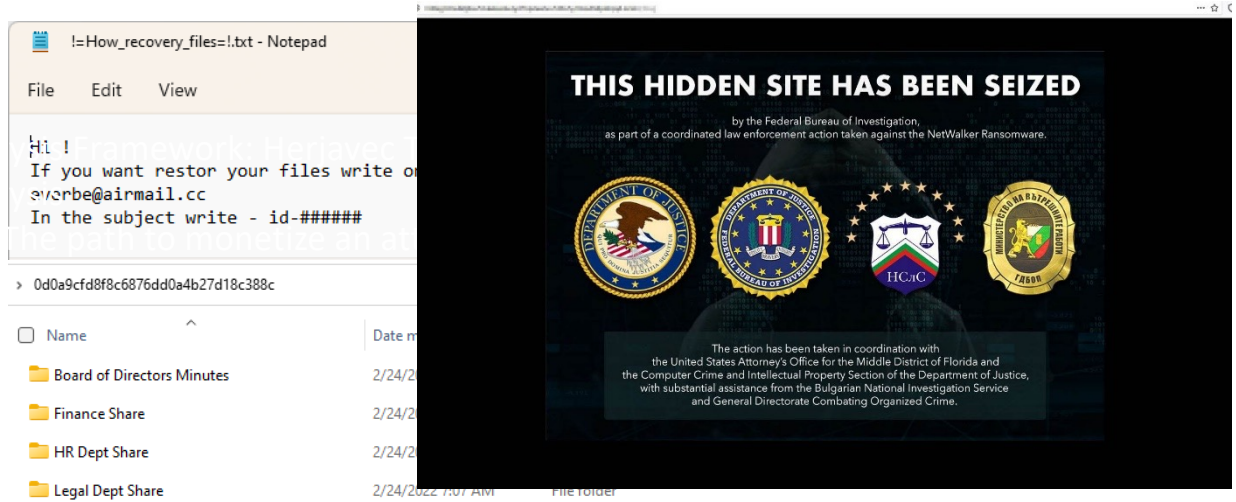
Within 1 hour	Estimated 4-12 hours	Estimated 4-12 hours		Variable (~8-48 hours)
GC typically contacts external counsel Counsel engages negotiator	Attacker typically uses throw-away address or anonymous chat Attacker seeks short negotiation and lump sum Smaller transactions provide protection	Single transaction 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



Search | Everest ransom team | Menu

U.S. GOV

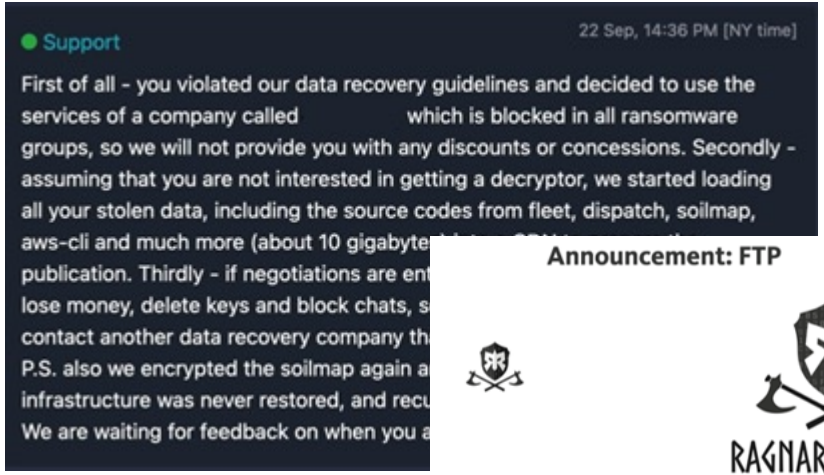
Government access in sale. A huge number of passports, tax, court cases and other documentation. Domain admin

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



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, ir
and insurer subroga
the Security Incident
review of customer
customers of the Se
Incident. In addition,
consolidated under

Q&A

Dr. Kall Loper, Vice President of DFIR,
kloper@herjavecgroup.com