
Microsoft
DCU: Ransomware
Kemba Walden
Assistant General Counsel, Microsoft Digital Crimes Unit

Ransomware adversaries are evolving strategies

Commodity Ransomware

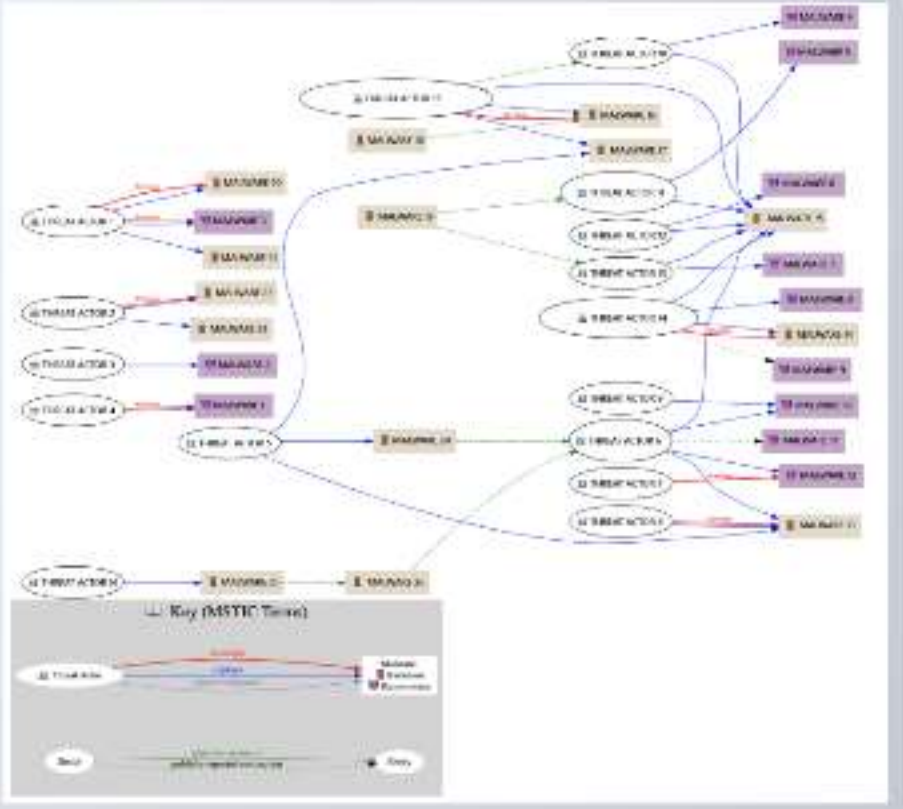
Human Operated Ransomware

Microsoft

Proposed Taxonomy Mapping

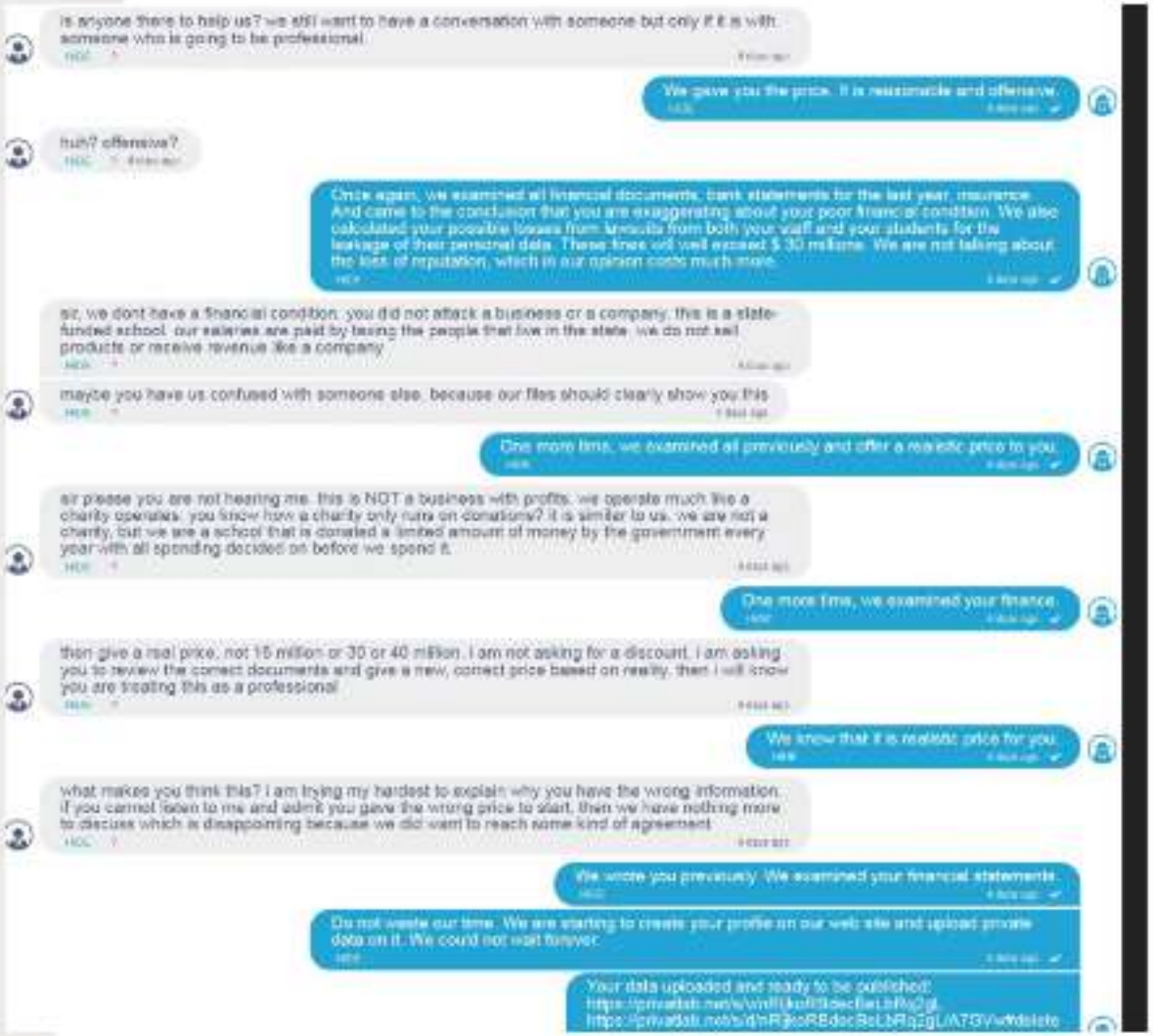
Clarifying how we describe ransomware activities

- Deploys
- Provides Access To
- Develops
- Manages
- Publicly Reported Connection



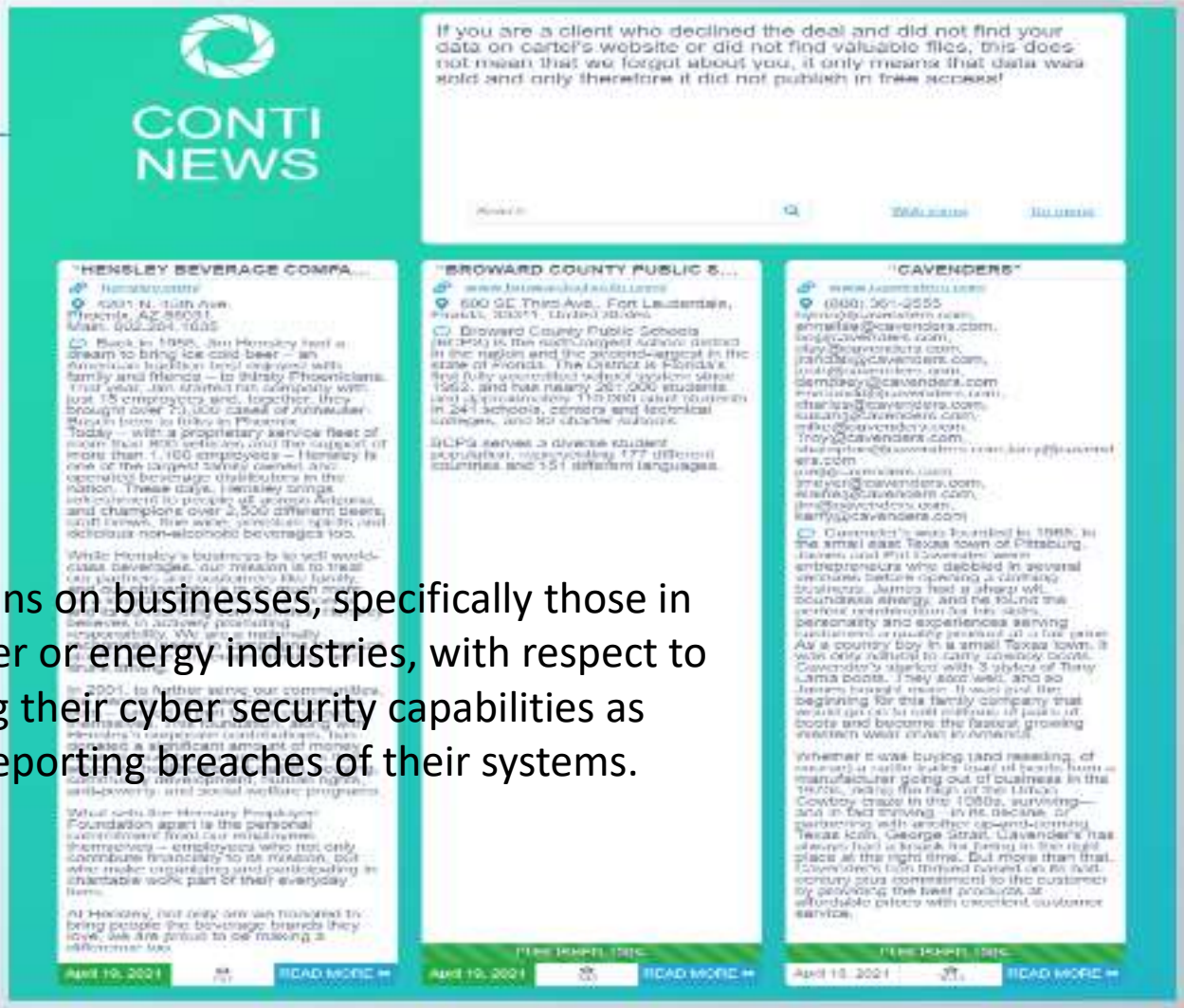
CONTI

- Ransom Negotiations
- Contirecovery.icu



CONTI

- Data Dump – Continews.icu



regulations on businesses, specifically those in the power or energy industries, with respect to reporting their cyber security capabilities as well as reporting breaches of their systems.

RANSOMWARE TASK FORCE

Report Briefing

Combating Ransomware: A Comprehensive Framework for Action

THE RANSOMWARE TASK FORCE

- 60+ experts from industry, government, law enforcement, civil society, and international organizations worked hand-in-hand
- Met Jan — April to centralize expertise from different sectors, create comprehensive solutions

Notable Sectors Included:

- ➔ Incident Responders, Threat Intelligence
- ➔ Cyber Insurance Providers, Brokers
- ➔ Healthcare Entities
- ➔ Cryptocurrency Analysis Firms / Exchanges
- ➔ International Law Enforcement
- ➔ Financial Regulators
- ➔ Corporations including Microsoft, Amazon
- ➔ CTA, GCA, other civil society organizations

RANSOMWARE TASK FORCE

RTF Framework

1. *Deter Ransomware Attacks*
2. *Disrupt the ransomware business model*
3. *Help organizations prepare*
4. *Respond to ransomware attacks more effectively*

RANSOMWARE TASK FORCE

PRIORITY RECOMMENDATIONS

1. Coordinated, international diplomatic and law enforcement efforts must **proactively prioritize ransomware through a comprehensive, resourced strategy**, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.

RANSOMWARE TASK FORCE

PRIORITY RECOMMENDATIONS

2. The United States should lead by example and **execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign**, coordinated by the White House. This must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.

RANSOMWARE TASK FORCE

PRIORITY RECOMMENDATIONS

3. Governments should establish Cyber Response and Recovery Funds to **support ransomware response** and other cybersecurity activities; **mandate that organizations report ransom payments**; and require organizations to consider alternatives before making payments.

RANSOMWARE TASK FORCE

PRIORITY RECOMMENDATIONS

4. An internationally coordinated effort should **develop a clear, accessible, and broadly adopted framework** to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to **drive adoption**.

RANSOMWARE TASK FORCE

PRIORITY RECOMMENDATIONS

5. **The cryptocurrency sector that enables ransomware crime should be more closely regulated.** Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

LEGISLATIVE OPPORTUNITIES

Action 2.1.1. Develop new levers for voluntary sharing of cryptocurrency payment indicators
Action 2.1.2. Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws
Action 2.2.3: Clarify lawful defensive measures that private-sector actors can take when countering ransomware
Action 3.3.1: Update cyber-hygiene regulations and standards
Action 3.3.2: Require local governments to adopt limited baseline security measures
Action 3.3.3: Require managed service providers to adopt and provide baseline security measures
Action 3.4.2: Expand Homeland Security Preparedness grants to encompass cybersecurity threats
Action 3.4.3: Offer local government/SLTTs/critical NGOs conditional access to grant funding for compliance with the Ransomware Framework (2.1.1)
Action 3.4.4: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework
Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services
Action 4.1.1: Create ransomware emergency response authorities
Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments (incentivize non-payment of ransoms)
Action 4.1.3: Increase government resources available to help the private sector respond to ransomware attacks
Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment
Action 4.3.2: Require organizations to review alternatives before making payments
Action 4.3.3: Require organizations to conduct a cost-benefit assessment prior to making a ransom payment

KEY LEGISLATIVE OPPORTUNITIES

1. Action 1.2.4: Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public
2. Action 3.2.2: Run [state]-wide, government-backed awareness campaigns and tabletop exercises
3. Action 3.3.1: Update cyber hygiene regulations and standards
4. Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments *
5. Objective 4.2: Increase the quality and volume of information about ransomware incidents

RANSOMWARE TASK FORCE

GLOBAL ORGANIZATIONS CAN TAKE THE LEAD

1. Action 1.1.1: Issue **declarative policy** through coordinated international diplomatic declarations that ransomware is an enforcement priority
2. Action 1.2.2: Establish an operationally focused U.S. Government Joint Ransomware Task Force (JRTF) to collaborate with **a private-sector Ransomware Threat Focus Hub**
3. Objective 2.3: **Disrupt the threat actors**, including ransomware developers, criminal affiliates, and ransomware variants (for those with authority to take action, blocking, etc)
4. Action 3.1.1: Develop a clear, actionable **framework for ransomware mitigation**, response, and recovery.
5. Action 3.2.2: Run nation-wide, government-backed **awareness campaigns** and tabletop exercises
6. Action 4.2.1: Establish a **Ransomware Incident Response Network** (RIRN).

RANSOMWARE TASK FORCE