THE ART AND SCIENCE OF DATA HOSTAGE NEGOTIATIONS

January 21, 2025

Booz Allen

ANDREW CARR, MS, GCIH, CTCE

Contact me: ***Andrew_Carr2@bah.com***
Linkedin.com/in/andrew-carr-7933b01a

- Senior Director – Incident Response Business Development
- 16-year career in cybersecurity through roles in digital forensics and incident response, cyber governance, and academia
- Expert witness experience including high-profile homicide investigations, civil litigation, corporate acquisitions and mergers, and ransomware negotiations
- Led hundreds of incidents and negotiated multi-million dollar demands with scores of threat actor groups

AGENDA

INSIGHTS FROM THE FIELD

PRIMARY STAKEHOLDERS

COST RELATIONSHIPS

TYPICAL ENGAGEMENT WORKFLOW

NEGOTIATION APPROACH

COMMON PITFALLS

INSIGHTS FROM THE FIELD

RANSOMWARE

Booz Allen

INSIGHTS FROM THE FIELD

Booz Allen's insights are derived from our direct engagement with a variety of criminal and nation-state actors targeting private sector victims in the United States and abroad.

$6,364,773

Average Initial Extortion Demand

$556,751

Average extortion settlement observed (purpose of settlement varies)

> $100,000,000

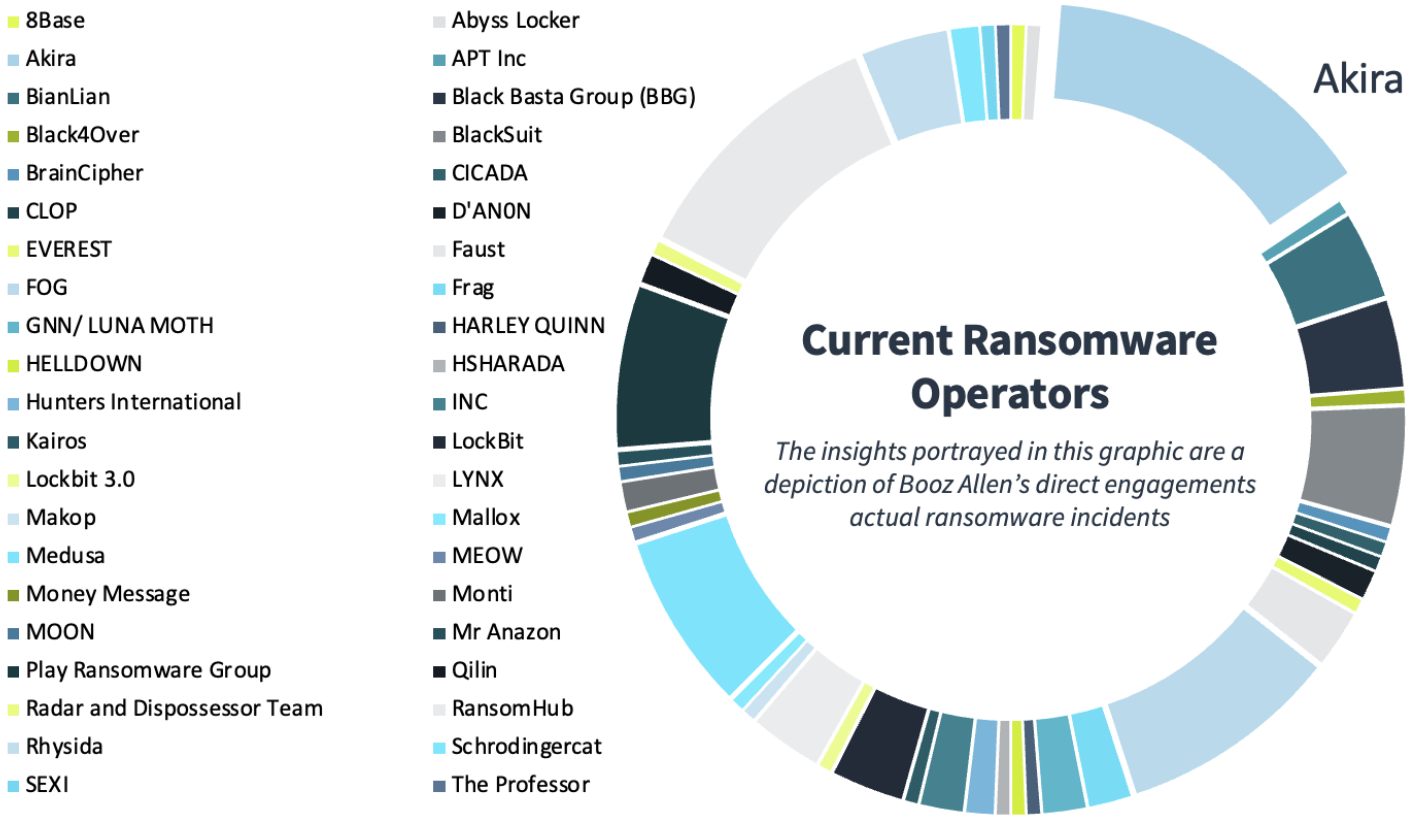
Highest Initial Extortion Demand

80%

Average reduction from initial demand

70%

Percent of ransomware cases with observed exfil



RANSOMWARE AS A SERVICE (RAAS) STRUCTURE

Booz Allen's insights are derived from our direct engagement with a variety of criminal and nation-state actors targeting private sector victims in the United States and abroad.

Leadership

Functional Role

Leadership exists at the top of the structure and develop and maintain the ransomware software, chat, payment, and data leak site infrastructure. They have the final say on acceptance of negotiation settlements and are the keeper of the decryption keys.

Affiliates

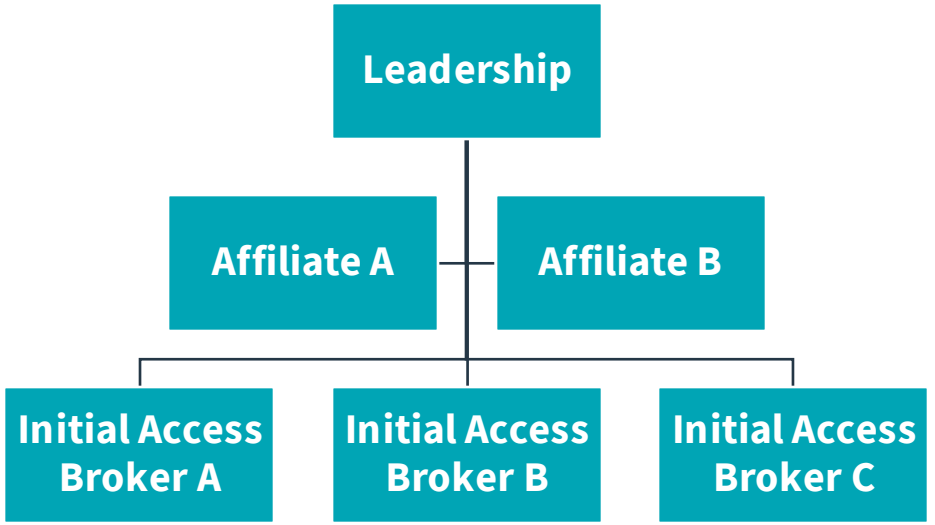
Functional Role

Members that "buy in" to a ransomware group to gain access to the software and functions provided by leadership. These are the individuals carrying out the ransomware attacks against organizations. This is often the individual being communicated with during threat actor outreach and negotiations.

Initial Access Brokers

Functional Role

Gain access to organizations with the intent of selling it to the highest bidder on the dark web. Generic details about the industry, organization size, types of infrastructure systems and method of access will be provided when advertising. Skillsets can range from development and use of zero-day exploits to highly effective social engineering.



THREAT ACTOR COMMUNICATIONS
RANSOMWARE

Booz Allen

PRIMARY STAKEHOLDERS

A brief, non-exhaustive outline of the functional roles and responsibilities of interested parties in threat actor communications / negotiations engagements to provide general insights into the level of involvement of each of those indicated below.

Victim Organization

Functional Role

The victim of a ransomware incident should have intimate knowledge of their environment, have initially identified some semblance of business impact at the time of the attack and have determined the appropriate stakeholders involved in approving messages sent to the threat actor as proposed by Booz Allen and evaluated by the Client's chosen Outside Counsel.

Responsibilities

- Identify personnel involved in communications review and approval
- Establish "burner" email accounts for threat actor communications efforts
- Ensure Counsel is included on all communications

Outside Counsel

Functional Role

The involvement of outside counsel cloaks the investigation and threat actor communications engagement under attorney-client privilege, with Booz Allen's engagement then being subject to the work product doctrine which would include all communications and deliverables. Simultaneously, outside counsel may also assist with internal and external messaging if an outside Public Relations firm is not also engaged.

Responsibilities

- Assist with the filing of IC3 report and act as conduit to any law enforcement comms
- Oversee and opine on messaging distributed to threat actor

Cyber Insurance Carrier

Functional Role

Cyber insurance carriers have largely taken an increased role in their involvement in threat actor communications engagements. As a party which is primarily responsible for the payment of an insurance claim and requires express-written approval when doing so, they may be involved directly and attempt to opine on the messages sent to the threat actor. This varies from carrier to carrier, as not all insurers are intensively involved in this process.

Responsibilities

- If required, approval of messaging to threat actor
- Approval of any monetary amounts agreed to with a threat actor prior to distribution

PRIMARY STAKEHOLDERS

A brief, non-exhaustive outline of the functional roles and responsibilities of interested parties in threat actor communications / negotiations engagements to provide general insights into the level of involvement of each of those indicated below.

Booz Allen Hamilton

Functional Role

Booz Allen's Threat Actor Communications and Intelligence team will handle all communications with threat actor, providing transparency in messaging and including historical insights into the threat actor/group, common methods of extortion leveraged and any other operational insights.

Responsibilities

- Initiate and continue communications with threat actor
- Monitor leak site for any publication
- Oversee cryptocurrency settlement
- Download leaked data provided by threat actor
- Sanctions compliance / due diligence attestation

Law Enforcement

Functional Role

The involvement of law enforcement in these engagements is not always as direct as many might initially anticipate. The investigation may involve close coordination with law enforcement or other government agencies (DHS, FBI, CISA, etc.) but threat actor communications engagements commonly does not.

Responsibilities

- Provide historical intelligence on threat actor/group involved
- Intake IC3 reporting for information gathering purposes
- Indicate availability of any functioning decryptor(s) not already known

COST RELATIONSHIPS

Ransom vs. Business Interruption Costs and the Impact of Time

Ransom

A direct relationship exists between the length of time a negotiation continues prior to settlement, and the size of the ransom paid.

- Typically, the longer the negotiation the smaller the ransom paid
  - Extending negotiations can create additional risks for the organization including secondary extortion and disruption techniques (e.g. DDoS, harassment campaigns, data publication)
  - Protracted negotiations can also result in increased downtime for the organization if a decryption utility is required to resume operations
- The inverse is also true

Business Interruption

Downtime, recovery, staff hours, and other costs can quickly accumulate relative to the severity of the ransomware attack's impact

- These costs are felt most severely by sectors like manufacturing and healthcare
  - Maximum tolerable downtime for these sectors is typically shorter than other industries
  - Health and human safety risks can present significant costs

Steps 1-4

TYPICAL ENGAGEMENT WORKFLOW

Common workflow of threat actor communications/negotiations engagements for organizations impacted by ransomware.

Develop Initial Negotiation Strategy 1

Strategy may fluctuate based on situational aspects of the engagement throughout negotiation

- Settlement Not Required = obtain proof of exfiltration and buy time for the affected organization
- Decryptor(s) Not Needed, Data Suppression Potential = gather intelligence via TA provided proof of data access/exfiltration to buy time to delay public exposure via leak site posting
- Decryptor(s) Needed = gather intelligence via TA provided proof of data access/exfiltration and attempted to delay public exposure via leak site posting, ensure deliverables are established and decryptors function as intended

Initiate Contact with Threat Actor 2

- Establish authority and approval chain of command
- Assume the persona of middle management

Site and Chat Monitoring 3

- Monitor site throughout negotiation
- Monitor chat window - various threat actors/groups may have the ability to delete posted messages and replace with modified messages in the chat window

Set the Tone 4

- Approach threat actor communications as a “business deal”, assuming the faux role of middle-management

Steps 5-8

TYPICAL ENGAGEMENT WORKFLOW

Common workflow of threat actor communications/negotiations engagements for organizations impacted by ransomware.

Understand Threat Actor Motivations 5

- Most ransomware groups are criminally motivated, other extortion-only related operations may have ulterior motives

Push Back 6

- Know when and how to move actor back when out of line with strategy during the engagement

TA Communications Transparency 7

- Updates are provided throughout the course of the engagement with the threat actor and approvals are required prior to distributing messages to the threat actor

Closeout 8

Deliverables may vary by threat group, but the following has been observed if settlement is achieved with the victim organization

- Proof of data deletion
- Indication of the method of initial access (may not be necessary given the current status of the vulnerability referenced)
- Ceasing of any harassment campaigns derived from the incident
- Promise not to publish victim's name on any leak site
- Functioning decryptor
- Ceasing of any threat of or ongoing DDoS campaign against victim organization

Psychology at every stage

HOW WE APPROACH NEGOTIATIONS

INTEL GATHERING & RAPPORT BUILDING

Establish a credible persona by balancing non-urgency with sincerity

BE KIND AND COURTEOUS *(AT LEAST AT FIRST)*

Start by attempting to catch flies with honey, knowing that the TA might post the entire transcript

MIRROR THEIR TONE

Increase the likelihood that the TA will respect your position/requests

FEED THEIR EGO TO YOUR ADVANTAGE

Ask questions about their tools and their work and avoid disparaging their product

COMMON PITFALLS

Typical mistakes which can lead to further escalations in threat actor communications / negotiations engagements which have directly been observed by Booz Allen in its threat actor communications engagements.

Client handling negotiations internally

Inexperienced negotiators can allow their emotional state to impact the negotiations effort and lead to increasingly hostile circumstances involving the threat actor / group, leading to early leak site publication and/or additional extortion tactics leveraged by the threat actor / group.

Inexperienced vendor or internal employee engaging with threat actor

Many ransomware groups (whether operating within the confines of a RaaS platform or as an independent group) incorporate a timer into their chat sites and / or leak sites which is triggered by the entry into the chat site. We have observed other incident response vendors or a client's internal employees visiting the TOR site hosting communications unknowingly trigger the timer, leading to increasingly disruptive extortion tactics such as harassment campaigns, DDoS, etc.

Overcommunication to Customers

Victim organizations have a propensity to overcommunicate the current status of their operations during the course of an ongoing investigation, creating future difficulties

Dismissing Sanctions Compliance Requirements

These processes are created for the protection of the victim, the definition of facilitation is overly broad

Not Communicating with the Threat Actor

Only 23% of our TA comms engagements lead to settlement, not communicating with TA invites more disruptive tactics

THANK YOU

WE ARE AVAILABLE TO ANSWER OUTSTANDING QUESTIONS.

Questions? Find us at boozallen.com

Contact me: ANDREW_CARR2@BAH.COM
Linkedin.com/in/andrew-carr-7933b01a/

Booz Allen