Digital Asset Redemption

The Anatomy of Ransomware Negotiations

An inside peek into threat actor engagements from professional negotiators

Executive Summary

One of the loudest drums in security is “assumed breach.” It’s a way to frame our security postures and recovery strategies, but also acknowledges the reality of our situation we’re in. It’s not a matter of if we’ll get hit, but when. Negotiating with – and potentially paying – threat actors is one of the more niche areas in security, which is also why it can feel like a black box of information.

At their core, ransomware negotiations are the art of separating noise from signal, and a negotiator’s job is to consistently assess and piece together many pieces of intelligence, deescalate, evaluate, communicate, and aim toward a resolution as quickly as possible in a crisis situation. But what are those signals in the noise?

The aim of this paper is to provide a glimpse of what goes into these engagements,, what makes an engagement successful, and what’s changing in this environment so you can not just prepare for the before and after of a breach, but during one, too.

> RANSOMWARE NEGOTIATIONS ARE THE ART OF **SEPARATING NOISE** FROM **SIGNAL.**

Ransomware Demands

RANSOM DEMANDS ARE NOT RANDOM

Right now we are still seeing the **average initial ransom demand come in around 1-5% of the victim company's annual revenue**. This has been a sort of "Goldilocks zone" for threat actors for a few years now, where they can score a payment big enough to be worth their time and effort, but not too big where the company cannot survive the financial hit, zeroing out their chances of any payment at all.

However, annual revenue is not the only factor that goes into a threat actor's calculations. Like all of us, they are seeing costs of services rise and are adjusting their business models accordingly. Often a **ransomware payment to a threat actor then will be further dispersed to their network of dark web service providers, ransomware software developers, and others who contributed to the attack** in exchange for a share of the take.

Some factors that play into a threat actor's ransomware demand pricing might include:

- Victim company's annual revenue
- Number of partners on the team
- Ransomware-as-a-Service (RaaS) affiliate fees, typically 10-20% of the payout
- Access broker costs
- Money laundering costs
- Infrastructure, hosting, and security costs for data exfiltration
- Any other services they might utilize for the attack

Like any successful business owner, threat actors need to maintain viable margins in order to remain operational. One shift we've seen recently has been toward threat actors matter-of-factly listing their costs of doing business in the negotiation as a way to indicate to the negotiators how firm their demands are.

RECENT RANSOM TRENDS

Threat actors pushed demands much higher than in previous years in 2024. Our team saw more multimillion-dollar demands than ever before, with multiple $15 million demands and a peak demand of $25 million. This surge coincides with **more Western actors entering the digital extortion space** more than before, often bringing with them a deeper understanding of their targets' background information than their counterparts around the world and a more aggressive approach. This knowledge and market understanding has driven demands upward, as threat actors better comprehend the value of the data.

Threat Actor Intelligence

THREAT ACTOR INTELLIGENCE SOURCES

When building out victim profiles ahead of the attack, threat actors need intelligence to find pertinent information about their victims, such as:

- Financial information
- Technologies used at the company, including security toolsets
- Search and browsing data/patterns
- Employee/staffing information
- Work/education histories
- Recent news/press
- Organizational structures
- Leadership details
- ...and more

All these data points can be used against companies in an attack. And while it might be easy to assume that in order to gather all this information there are tools on the dark web to amass all this information, the reality is **many attackers have premium subscriptions to legitimate sites such as ZoomInfo and LinkedIn**, where this intelligence is readily accessible, sorted, and in a user-friendly interface. Threat actors are the embodiment of "work smarter, not harder," and it turns out that people willing to extort businesses, hospitals, schools, and critical infrastructure don't tend to care about abusing a SaaS application's acceptable terms of use.

This data can also give valuable clues for threat actors for attack vectors. Looking at the profiles of their security teams, threat actors can often see employees' security certifications, past employers and gather a good idea of what's in a company's stack, which could allow them to exploit an already-known vulnerability.

History and Operational Factors

OLDER, COLDER, AND BOLDER

During an attack, negotiators are constantly formulating expectations on how the engagement will land. Information is power during this dynamic, and each piece gives a clearer picture of their flexibility and risks involved in future steps in the negotiation. Some of these indicators about threat actors include:

- Acting independently/solo or part of a larger ransomware/RaaS group
- Size of the affiliate team
- Nation state sponsorship
- Attack history and record of actions after previous attacks
- Associations
- International sanctions

For instance, knowing a threat actor is operating in a team of 5 as an affiliate of a particular ransomware group can give negotiators an **understanding of that group's typical tactics, techniques, and procedures (TTPs), payment split structure, and more**. When negotiators have access to advanced dark web intelligence, this knowledge gives negotiators a wider view of the situation and which outcomes are possible for the victim.

Generally speaking, **as threat actors get older, they also get bolder and colder**. Competing ransomware groups will try to lure threat actors known for big takes with the promise of a higher share of the ransom split when their reputation gains notice. Since the operators would rather have a smaller share of a more guaranteed take on organizations with deeper pockets, having "big" names in the community might influence others to join that group as well.

These more established threat actors are much less likely to negotiate down on their ransom, hit bigger targets, and will often resort to more aggressive tactics much faster such as publishing exfiltrated data or using dark web services that automate harassment and increase chaos in order to pressure the victim to pay. (In fact, one of these services is appropriately named "harassyou".)

Additional Intelligence Indicators

GEOPOLITICAL, CULTURAL, AND LINGUISTIC CONSIDERATIONS

Nothing exists in a vacuum, and threat actors are no exception to this. Fitting threat actors into a larger context can, and often does, impact negotiations. Threat actor attribution involves trying to determine what external forces could influence both the attacker and the negotiation at large.

As an example, during a negotiation for an incident in late December 2024, a negotiator determined the threat actor was Russian based on linguistic patterns, response times mapped to a Russian time zone, known associations, past history, and other intelligence indicators. As the negotiation progressed, the negotiator knew there were a series of upcoming national holidays in Russia around Orthodox Christmas, with the New Year's holiday acting as one of the largest national holidays in the country. The negotiator was then able to land the resolution in a more favorable position, offering a much lower figure than the threat actor was hoping to gain, but knowing the threat actor would want to finish this negotiation before their holiday season began. The threat actor took that deal, saving the victim hundreds of thousands of dollars in the process and getting their business back online.

SCRIPTED NEGOTIATIONS ARE A LIABILITY

Unfortunately, there isn't a script for negotiating with extortionists. Scripts simply cannot take into account the myriad of factors that will play into the outcome of the ransomware attack, triage them, and adjust in real time. Arguably more importantly than that, threat actors will use a script as an advantage, knowing the negotiator's tactics and how to throw a wrench in a scripted negotiation.

WHY MOST NEGOTIATIONS DON'T END IN PAYMENT

While most organizations enter negotiations during a ransom event, only about 10% proceed to payment. The primary driver behind payment decisions is operational impact. If an organization can recover systems and data within a reasonable timeframe, they typically won't pay, regardless of the data stolen or threats made. This is why negotiations are very often a strategic tool to buy time for incident response to investigate, perform backup validations, resolve vulnerabilities, etc.

Notably, data exfiltration/extortion alone rarely drives payment decisions. Organizations face the same reporting and breach obligations whether they pay or not. This approach often reveals that payment isn't necessary for recovery, allowing organizations to make decisions based on actual impact rather than initial panic.

Conclusion

PUTTING THE PIECES TOGETHER

Ransomware negotiations are dynamic, high stakes endeavors. Each negotiation requires negotiators to quickly piece together intelligence such as:

- Technical clues about the attackers' capabilities and tools
- Cultural, geopolitical, and linguistic insights
- Business intelligence
- Ransomware groups, dynamics, and operations

Piecing together technical, psychological, linguistic, cultural intelligence dynamically under high pressure in order to gain leverage in a ransomware negotiation will most often buy time for the victim and gain intelligence on the attack's TTPs from the negotiations themselves. This is why most organizations in a ransomware event enter into negotiations, but only 10% end up resolving the negotiation with a payment to a threat actor.

About Digital Asset Redemption

DAR infiltrates ransomware groups to respond to threats behind enemy lines on the dark web. During a ransomware attack, **DAR negotiates with threat actors and provides compliant crypto payments** when needed. By combining threat intelligence, negotiations, and payment options, and **over 4,000 threat actor engagements**, our **DRK_MDR** offering allows DAR customers to gain protection on their dark web threat surface and confidently confront cybercrime.

Learn more: **digitalassetredemption.com**