Digital Asset Redemption

Breaking Through the Extortion Crisis:

How The DAR Team's 3-Day Operation Outperformed Two Weeks of Traditional IR

Just the Basics

CUSTOMER INDUSTRY

Telecommunications infrastructure

CUSTOMER SIZE

Enterprise (International, 500+ employees)

THE BREACH

Advanced threat actors breached the network, stolen data, and were extorting the company

RESPONSE CHALLENGES

The company engaged a well-known incident response firm but were unable to find details about the breach causes or impacts

THE DAR TEAM RESULTS

Within 72 hours, The DAR Team engaged the threat actors on the dark web, gained information, found the root causes, and helped law enforcement apprehend the threat actors

Executive Summary

After two weeks enduring an attack from multiple unidentified threat actors, a telecommunications company called in The DAR Team.

The DAR Team's Human Intelligence capabilities turned the tide.

By identifying and socially engineering the threat actors into giving away their position, The DAR Team helped the company avoid paying a ransom and enabled law enforcement to apprehend the criminals responsible for the attack.

The company was able to identify and remediate a key weakness in its supply chain, potentially avoiding a cascade of future data breaches.

THREAT ACTORS ATTACKED THE COMPANY ON THEIR HOME TURF.

THE DAR TEAM RETURNED THE FAVOR.

Setting the Stage

THE CUSTOMER

A large Silicon Valley-based telecommunications infrastructure provider.

THE BREACH

The company was breached by a targeted attack by unidentified threat actor(s). This wasn't ransomware; it was something potentially worse – **the threat actor(s) seemed to have continuous access to the company's data supply chain.**

THE RESPONSE

Neither internal nor third-party incident response teams **weren't able to identify the source, velocity, or impact of the breach**, leaving them at the mercy of the threat actors. Outside help from conventional incident response – and a name-brand threat intelligence provider – proved toothless and, worse, **wasted two weeks while the crisis spiraled**.

During this time, news of the breach broke publicly in the media. Customers and investors were as anxious for answers about the breach as the company was to find and provide them. The longer the company went without providing any details around the attack the more damage the company's reputation around their security and diligence programs endured. **Finding answers about the attack was becoming more and more critical by the hour.**

THE DAR TEAM'S ENTRANCE

The company engaged outside legal counsel early in their ordeal. When containment efforts and attempts to identify root causes failed, their "breach coach" suggested a new resource: **deep human intelligence capabilities to go behind enemy lines.**

THE MISSION

The company wasn't willing to negotiate with a threat actor or pay a ransom. The DAR Team empowered an alternative: **break the standstill in their investigation by infiltrating the attacker's organization**. This meant DAR's operatives would leverage their dark web personas to socially engineer an opportunity to collect new information about the cause and scope of the breach.

Phase 1: Aligning Goals

ENGAGEMENT

As with all DAR Team engagements, the engagement started with a crash course on the situation and the company's objectives. Where other providers begin with a script, **The DAR Team worked to match specific outcomes to their capabilities.**

Engaging threat actors in their spaces allowed The DAR Team to find crucial information about the breach IR firms couldn't uncover.

OPTIONS

After understanding the company's intelligence needs and goals, The DAR Team provided some options:

1. **Harness open source intelligence** (OSINT) and other intelligence for threat actor attribution
2. **Investigate and make contact with the threat actor(s)** using established, trusted personas to elicit information
3. **Engage with the threat actor/s on a dark web marketplace**, acting as a potential buyer of the exfiltrated data.

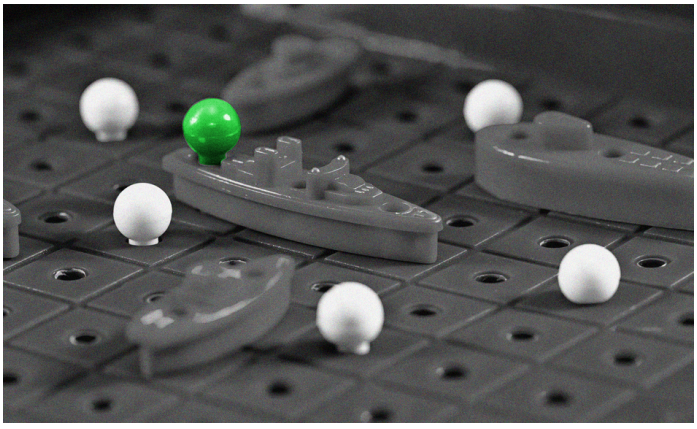
The company opted for all three options in order to gather as much intelligence as possible.

GIVE A LITTLE, GAIN A LOT

Many threat hunters and incident response firms draw the line at making payments on the dark web, because they won't – or can't – operate so far outside their traditional territory. **The DAR Team's "hunt forward" plan offered several new possibilities:**

- Did they want to buy the data set so it wouldn't spread further across cybercriminal networks?
- Or, could they first conduct separate transactions with the threat actor/s, as a ruse to gain attribution intelligence from:
- Where any of the threat actor wallets are hosted;
- Where the threat actor/s might be located;
- Who else could be involved in the attack – access brokers, money launderers, or infrastructure providers.

Without a clear picture of the threat actor(s) hoping to cash in from the attack, a single purchase might not achieve the desired outcome as it could prematurely cut the investigation short. The company chose instead to start with small payments to the threat actors, hoping for more detailed attribution.



Phase 2: Operative Deployment

Just hours after kickoff, The DAR Team engaged the threat actors to find more information, deploying years-old personas with track records of "trustworthiness" in threat actor marketplaces.

WITHIN 72 HOURS, THE DAR TEAM HAD DISCOVERED:

- The attack was perpetrated by two threat actors, not one;
- The threat actors' point of entry into the company's environment, **down to the exact computer system infected** with the malware;
- **Where the attackers** were located;
- The **initial compromise was not in the victim's network, but rather a third-party vendor** – which had dangerous levels of access and permissions into the company's environment.

THE IR TEAM HAD A NEW, FOCUSED DIRECTION:

- An internal audit confirmed the intelligence and information The DAR Team operatives had elicited from the threat actors as **100% accurate**.
- The incident response team received **a clear scope the velocity of the attack and its impacts** – answering critical questions, such as:
  - **Where did the attack go?**
  - **What did it hit?**
  - **How much data did the threat actors exfiltrate?**

Phase 3: Threat Actor Takedown

CRACKING THE CASE THROUGH CRYPTO TRANSACTIONS

The DAR Team cracked the case by tracing out-of-band cryptocurrency transactions.

DAR operatives posed as potential buyers of stolen data. Despite the company's refusal to pay a ransom demand, they recognized the value of keeping the threat actors engaged. The DAR Team engineered a scenario where the data sellers agreed to a small initial transaction.

Though the amount was only enough for a stiff drink or two, this action **provided The DAR Team with critical intelligence:**

1. **The threat actors were working together.**
   Both threat actors provided crypto wallet addresses and after receiving the small transactions, the two addresses made deposits into a single, different wallet. This indicated they were working in tandem for the same threat actor group.

2. **The threat actors' locations.**
   DAR traced the destination of the cryptocurrency to an exchange, giving the threat actor a specific, unique geographic profile.

3. THE BEST ONE!
   Information to identify and apprehend the individuals responsible for the attack.
   The wallet addresses were attributed to a KYC exchange, meaning the threat actors had submitted their identity and passport information to open the accounts where they received the cryptocurrency!

A WIN FOR THE GOOD GUYS

Once The DAR Team uncovered this information, they **engaged local law enforcement officials** in those countries about this operation.

While most ransomware operators are located in countries without extradition treaties such as Russia or other CIS nations, the two unmasked threat actors were not as careful. The information The DAR Team provided to law enforcement **ultimately led to their arrests**, a rare but welcome triumph.

The DAR Team found intelligence that led to the arrest of the threat actors in their local jurisdictions.

Why the DAR Team Was Successful

Why couldn't one of the biggest incident response firms gather the necessary intelligence in two weeks that took The DAR Team 72 hours to discover?

Undercover, forward-deployed intelligence.

Established personas

The places where threat actors communicate aren't accessible to just anyone. It takes years of establishing personas, engaging threat actors in the ways they engage each other, and building trust in the communities.

Building this type of intelligence capability out in-house takes years. And companies typically can't risk allowing their employees to engage in these types of dark web spaces and criminal communications – for obvious legal and liability reasons.

Trained operatives

Understanding where to engage with threat actors is just the beginning. Forward-deployed intelligence operations also require specific skills such as offensive security backgrounds and social engineering experience. This experience helps the operatives frame engagements to elicit valuable responses and intelligence without arousing suspicion.

Operational security

Threat actors are quick to recognize “security researchers” who won’t engage in their business dealings. The intelligence gathered from the small cryptocurrency transaction provided a boon of intelligence to the victim, incident response team, and law enforcement. With payment options at the ready, The DAR Team is able to keep intelligence-gathering operations going while maintaining the threat actors’ trust and confidence.

Payment options

Because undercover operations can put organizations at risk if not performed properly, The DAR Team follows a strict operational security code. Combined with a deep understanding of adversaries, these operational guardrails allow The DAR Team to operate without putting victims at further risk.

Outcomes

FROM CRISIS TO VICTORY

The tide turned from crisis to victory when the company found The DAR Team.

After two full weeks of their incident response team spinning wheels, expending countless billable hours, and still coming up short, within 72 hours The DAR Team was able to engage the threat actor, gather critical information about the attacks down to the exact location of the access point, identify the threat actors, identify the third party vendor, and provide international law enforcement officials enough information to make arrests and take these threat actors off the market.

The company told The DAR Team that their services were **the least expensive part of their incident response bill with the most amount of positive impact.**

3RD-PARTY VENDOR CLEANUP

The DAR team also provided crucial information about this attack to the third party vendor to help them secure their products. The third party received the information, took it seriously, and worked to clean up their product so it could no longer be used as an attack vector.

CONCLUSION

The DAR team's forward-deployed intelligence capabilities were on full display during this engagement. **This entire operation took place on the dark web** and was able to unblock a weeks-long jammed incident response effort, provide details to a third party vendor so more companies didn't fall victim to this particular threat vector, and provided enough intelligence to law enforcement that led to the takedown of two advanced threat actors – all within 72 hours.

This type of intelligence cannot be found with automated scans or by the layperson. These specialized skills and toolsets are what makes The DAR Team uniquely positioned to act as any company's eyes into what threat actors are actually saying.

MOST SECURITY TOOLS SHOW YOU WHAT THREAT ACTORS WANT YOU TO SEE.

THE DAR TEAM CAN FIND WHAT THEY'RE HIDING.

DARK_MDR is the world's first service that monitors, detects, and responds entirely on the dark web. If you'd like to learn more about how DRK_MDR can help your company, The DAR Team can help.