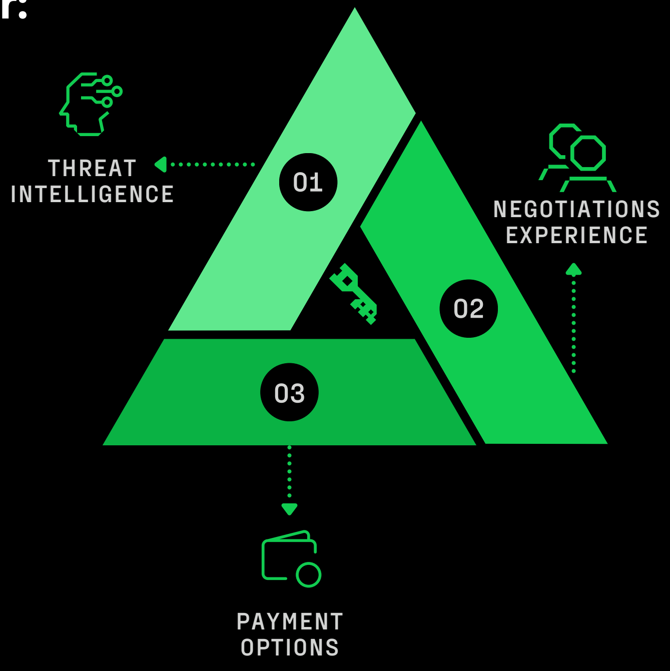
Who is Digital Asset Redemption ?

When you're hit by ransomware, we're the ones who make sure you don't leave home without your:

- Forward deployed intelligence.
- Negotiations experience.
- Compliant payment options.



ASSUMING A BREACH MEANS ASSUMING RECOVERY.

Planning for recovery means you need to know who you'll have on your side to **engage threat actors**, understand **who the threat actors are**, and, when necessary, **provide compliant payments**, all ready to deploy at a moment's notice in a crisis.

INTELLIGENCE + NEGOTIATIONS + PAYMENT OPTIONS, ALL WORKING TOGETHER FOR YOU.

Successful ransomware recovery requires three things working together in tandem. Without **forward deployed intelligence**, negotiations are limited and payments could wind up as sanctions violations. Without **expert negotiations**, ransom demands stay high and recovery teams might be limited. Without **compliant payment options**, your negotiation options are limited, and your threat intelligence isn't actionable.

Forward deployed dark web intelligence

Operatives **embedded in the deepest corners of the dark web**, watching and acting on your behalf and can mobilize and deliver actionable intelligence about threat actors, including their identities, activities, associations, IOCs, TTPs, and more.

Compliant Payment Options

You need a payment provider who can perform **threat actor attribution, assess your sanctions risks, and keep your payments compliant**. We manage your crypto wallet and hold crypto reserves to facilitate immediate payments to recover your stolen assets.

Experienced Negotiators

Our negotiators mobilize at a moment's notice to **combine forward-deployed intelligence with years of negotiations experience** to provide expert services during your ransomware event. With over 1000 successful engagements, we know how to get results for you.

Digital
Asset
Redemption

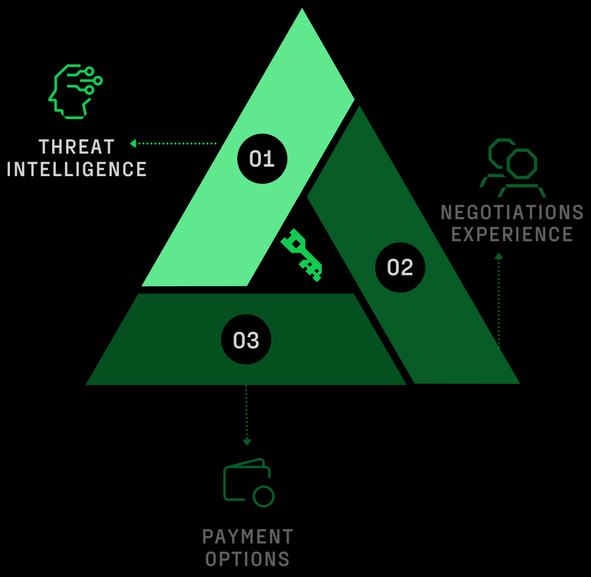
Intelligence Services

FRIENDS IN DARK PLACES

Do you know what threat actors are saying about your organization? If not, then you need **someone embedded in the deepest corners of the dark web**, watching and acting on your behalf.

You need **operatives who can mobilize and deliver immediate, actionable intelligence** about threat actors, including their identities, activities, associations, IOCs, TTPs, and more.

And if your data is at risk on the dark web from exfiltration, stolen credentials, or other threats, you need someone who can **act on your behalf to intercept these threats** before they fall into the wrong hands.



Human in the Loop Intelligence

Our operatives gather high-fidelity intelligence about threat actors from behind enemy lines. Our analysts infiltrate cybercriminal circles, **intercepting stolen data, attack plans, and access credentials** while uncovering emerging threats your teams don't see until it's too late.

Quiet by Design

We deliver only critical, actionable intelligence **without adding to your team's alert fatigue**. Each alert is meticulously vetted, representing a significant threat that demands immediate attention. When DRK_CACHE speaks, it's always worth listening.

Qualified and Contextualized

DAR's intelligence affords you the opportunity to take action. Whether it's proactively disrupting malicious activity, enabling threat hunting teams, or informing incident response teams, you'll have the **information you need about your adversaries** when you need it.

HARNESS FORWARD-DEPLOYED INTELLIGENCE

NEGOTIATIONS

- Who is actually extorting you
- Past activities and outcomes
- Affiliations

THREAT HUNTING & IR

- Threat actor TTPs
- Indicators of Compromise (IOCs)
- Advanced attribution and threat reports

PAYMENT OPTIONS

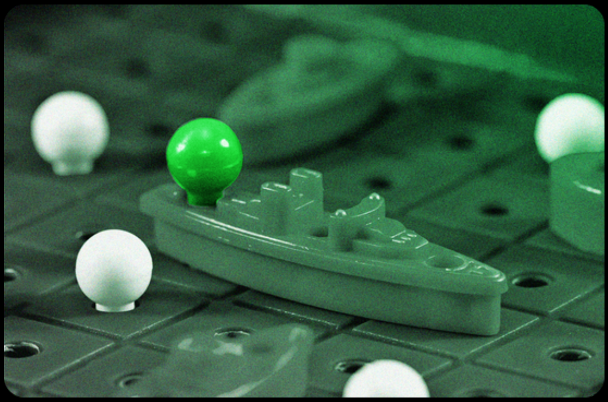
- Sanctions screens
- Interception of stolen access, data, etc.
- Risk evaluations for payment

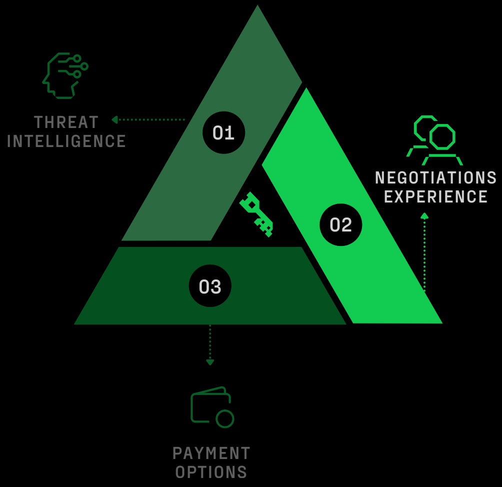
RECOVERY MONITORING

- Post-event monitoring
- Informing security posture improvements
- Reporting and compliance

Digital
Asset
Redemption

Negotiation Services





MEET YOUR THREAT ACTOR NEGOTIATIONS TEAM

"Negotiating with extortionists" probably isn't in your job description. And when your company is in the middle of a ransomware event, you need pros who do this full time.

With over **1000 successful threat actor engagements** under our belt, our team of skilled negotiators guide you through the crisis and back to business – and back to your actual jobs.

CALM IN THE MIDDLE OF THE STORM

Our negotiators **combine forward-deployed intelligence with years of negotiations** experience to help you get to recovery as soon as possible.

Engage threat actors with precision

Provide you with more – and better – options in a crisis

Inform your potential payment options

Enable IR teams with threat actor intel & attribution

BETTER PROCESSES, BETTER OUTCOMES

READY TO DEPLOY WHEN YOU MOST NEED HELP

Our negotiation experts mobilize at a moment's notice to **provide expert services during your ransomware event**. We assess the situation, communicate with IR teams & necessary stakeholders, and perform threat actor attribution.

OPEN COMMUNICATIONS AND DOCUMENTATION

Our team maintains **communications with IR teams, legal authorities, and other necessary stakeholders**. We also document the engagement for post-event compliance filings, insurance claims, and other recovery necessities.

REDUCED RANSOM DEMANDS BY 75%

The middle of a crisis is a bad time to learn how to negotiate with criminals. Our **negotiators know how to communicate with, assess, and understand your extortionists**, resulting in an average 75% reduction in ransom demand while giving IR teams more time to work.

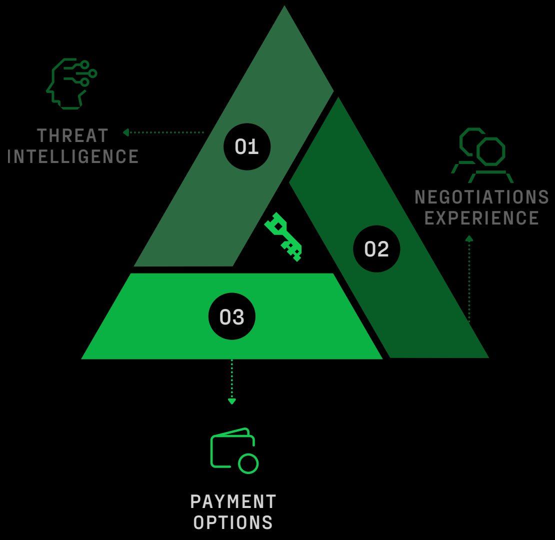
Digital
Asset
Redemption

Compliant Payment Services

FACT: CRIMINALS DON'T TAKE CHECKS.

When you're in the position of needing to make a payment to a threat actor, there are a lot of questions you need to answer, but the most important one is: **Who am I paying?**

When you're in the middle of a crisis, being able to make a crypto payment isn't enough. You need a payment provider who can perform **threat actor attribution, assess your sanctions risks, and keep your payments compliant**.



CRYPTO WALLET MANAGEMENT

When you need to make a payment, we're ready to go. Our team has years of experience managing crypto wallets and payments, and holds crypto reserves to **facilitate immediate payments to recover your stolen assets**. Our team makes sure your payment goes to the right person at the right time.

SANCTIONS AND COMPLIANCE SCREENS

We use our advanced threat actor attribution to **ensure your payments don't result in sanctions violations**. These screens include: The Office of Foreign Asset Control (OFAC), Global Affairs Canada, Security Council Consolidated List - United Nations, Consolidated List of Persons, Groups and Entities - EU, and more.

OPEN DIALOGUE WITH AUTHORITIES

We maintain **open lines of communication with domestic and foreign law enforcement and intelligence agencies** to provide you with the best guidance available. Some of these agencies include CISA, the FBI, the Secret Service, the UK National Crime Agency, the NSA, and others.

ADVANCED THREAT ACTOR ATTRIBUTION

It's no secret that professional extortionists – especially ones on sanctions lists – try to lie about who they are. And if you end up making a non-compliant payment without doing your due diligence first, your payment could result in even bigger **problems such as sanctions or compliance violations** later.

Before making a payment, we harness our **forward-deployed intelligence to perform advanced threat actor attribution**. During this process we work to understand their identities, activities, associations, IOCs, TTPs, and more. This helps **prevent you from making payments to sanctioned individuals or nation-state-sponsored actors** hiding as ransomware affiliates.

Digital
Asset
Redemption

You’ve been ransomed.

NOW WHAT?!

First: Take a deep breath. We’re on our way to help.

Next: Use this guide to make sure everyone on your team is on the same page while avoiding common pitfalls in the early stages of a ransomware attack.

✗ DON’T:

ENGAGE DIRECTLY WITHOUT EXPERTISE

Refrain from engaging with threat actors directly without the guidance of cybersecurity experts, legal advisors, and law enforcement authorities, as this can escalate risks and compromise negotiations.

PAY THE RANSOM IMMEDIATELY

Avoid rushing to pay the ransom without fully understanding the situation, assessing other options, and considering the potential consequences of rewarding criminal behavior.

IGNORE YOUR LEGAL OBLIGATIONS

Do not disregard legal obligations or regulatory requirements related to data protection, privacy, and incident reporting when responding to a ransomware attack, as this can result in legal liabilities and penalties.

NEGOTIATE WITHOUT A PLAN

Resist entering negotiations without a clear strategy, predetermined objectives, and an understanding of the organization's limitations, as this can lead to unfavorable outcomes or unnecessary compromises.

PROMISE IMMEDIATE PAYMENT

Avoid making promises or commitments to threat actors regarding payment or compliance with their demands before evaluating the situation and consulting with relevant stakeholders.

UNDERESTIMATE THE THREAT

Refrain from underestimating the severity or impact of the ransomware attack, as this can lead to delays in response efforts and exacerbate the situation.

PROVIDE SENSITIVE INFORMATION

Avoid disclosing sensitive information or sharing credentials with threat actors during negotiations, as this can further jeopardize cybersecurity and data privacy.

✓ DO:

ASSESS THE SITUATION

Evaluate the extent of the ransomware attack, including the scope of the data breach, potential impact on operations, and criticality of the affected systems.

ENGAGE INCIDENT RESPONSE TEAMS

Consult cybersecurity professionals and incident response teams to analyze the attack, identify vulnerabilities, and devise strategies for mitigation and recovery.

CONSULT LEGAL AND LAW ENFORCEMENT

Seek guidance from legal counsel and involve law enforcement agencies, such as the FBI or local authorities, to understand the legal implications and potential consequences of negotiating with threat actors.

ASSESS POTENTIAL VALUE

Begin to determine acceptable ransom amounts and negotiating terms by attempting to quantify the value of data stolen or encrypted.

EVALUATE BACKUP DATA

Determine if critical data is backed up and stored securely to prevent further loss in case negotiations fail or the ransom is not paid.

ESTABLISH PROTOCOLS

Keep internal stakeholders informed about the situation, including executives, IT staff, legal advisors, and relevant department heads, to ensure coordinated decision-making and response efforts.

Digital
Asset
Redemption