ZEROFOX®

A Hitchhiker's Guide to the **Dark Web**

Table of Contents

YOUR TRAVEL GUIDE

Adam Darrah

Director of Threat Intelligence Services
ZeroFox

INTRODUCTION

Your security team tells you that they've found ads for your organization's intellectual property (IP) for sale in dark web forums. As a business leader, I'm sure a lot of questions are going through your mind.

- Who's selling our IP?
- How long have the advertisements been up?
- Is it credible?
- If it's legit, can we get it removed from these forums before it's sold?
- What's the damage if it's made public?
- How do we fix this?

It's a scary situation. But here's the thing: the fear is made worse by the sheer volume of fear tactics surrounding the deep and dark web. Now, I'm not making light of the criminal activities that occur in the underground economy; it's a very serious business, and there are some undeniably dangerous adversaries operating there. But, the mystery around and misperceptions about the deep and dark web create a culture of terror-based clickbait. In a sincere attempt to provide some context around this underground economy, the ecosystem described is far too often a hyperbolic (and vague) caricature of what these environments are really like.

The mystery around and misperceptions about the deep and dark web create a culture of terror-based clickbait.

So is the dark web scary? Short answer: It depends but generally, maybe. Long answer? It can be scarier than the popular parts of the surface (indexed) web. The surface web, by the way, only accounts for about 10 percent of the internet. But not everything in the dark web is dangerous or even illegal. Because of its promises of anonymity, it does lend itself to criminal activity. Scary people do operate there, but it also provides a safe harbor to privacy advocates, curious dilettantes, and political, ethnic, or sexual minorities. Generally, I wouldn't recommend your average individual participate in unfamiliar dark web criminal forums. But the majority of activity that impacts enterprises takes place in the underground economy ecosystem of the deep and dark web – and in many ways, this ecosystem mirrors what we see in the above-ground economy.

There's no doubt the underground economy is a noisy place, filled with misinformation, misdirection, and criminal enterprises. But lacking tangible experience and significant time-on-target(s) in dark web forums make it seem exponentially more frightening – full of shadowy figures (in hoodies, naturally) making nefarious deals with nation-state actors, conducting espionage and world domination plots. It's true that some of these activities exist underground, stereotypes aside. But these activities also exist across the surface web. So what makes the deep and dark web different? And how can organizations navigate underground forums and prepared for potential attacks?

This Hitchhiker's Guide will shed light on the dark web and the environments most likely to target enterprises, organizations, and their people. Let's focus not on the fear but on the facts. Think of it as a guided tour, introducing you to…

- How the dark web economy functions
- Underground economy ecosystems and how they differ
- Relationships in the dark web
- Underground economy covert operations
- True(ish) tales from the dark web

Chapter 1

How the dark web economy functions

Operational functions

The dark web is a collection of online forums and communities that internet users cannot access via traditional web browsers. It requires a TOR (The Onion Router) browser to access, which allows users to obfuscate their identities, hide their locations, and protect and secure data transfers.

Think of the underground economy as a robust marketplace, selling information, tools, services, and more. Paste sites, chat apps, and malicious hacker forums make up this diverse ecosystem, catering to a broad range of adversary interests.

The underground economy operates much like the above-ground economy. The same volatile economic constraints we experience are also present in the underground. Supply and demand matter. There are winners and losers. There are innovators and leechers who recycle the ideas of the innovators. It also has its own language and identity, its own geographies, and within each, are very distinct cultures.

Economic functions

Whether sales are made directly or through a broker, there are two currencies used in underground deals – reputation and cryptocurrency.

Reputation matters because that is how you distinguish yourself from the overwhelming noise, time wasters, professional trolls, scammers, and the very worst within the ecosystem. Not only are threat actors vying for attention – some are also intentionally adding to the noise as a distraction, to force the uninitiated down a different path. Most adversaries know what sites threat intelligence companies scrape so all day, they post offensive and inflammatory comments publicly to keep the civilized world off-balance. To cut through that noise, you have to establish yourself as someone reputable. It takes time but once it's established, you will soon figure out how to get to the right people to deal with.

The benefit of cryptocurrency is it's decentralized, but the problem with that is it is decentralized. Underground communities are moving to cryptocurrencies less traceable than Bitcoin but that still retain enough value to be cashed out for fiat currency. The same way that

KEY TERM

Fiat currency

Fiat currency is any type of currency that is declared legal tender by a government but that has no intrinsic value and is not backed by tangible assets.

above-ground money launderers have to find ways to creatively finance their illegal businesses are the same issues that underground actors deal with. But with market instability impacted by the war in Ukraine, crypto volatility, and more and more governments sanctioning crypto exchanges, threat actors are engaging in riskier transactions with less reputable exchanges.

The environments are also intentionally noisy. You have to stand out with your quality of goods and the way you interact with people. You'll find contemporary marketing tactics and advertising campaigns. Satisfaction guarantees and customer service support are all part of the business models. But to maintain operations, dark web vendors and brokers don't want to attract the attention of security researchers or law enforcement. So while running and promoting their businesses, they use misdirection and distraction to feed the chaotic nature of the ecosystem.

Enforcement functions

There are enforcement mechanisms, but they differ from the above-ground economy in that there's no judicial body that penalizes you. You have a sophisticated network of people who impose their own rules, and groups coalesce around the ones that have agreed to play the same game as them.

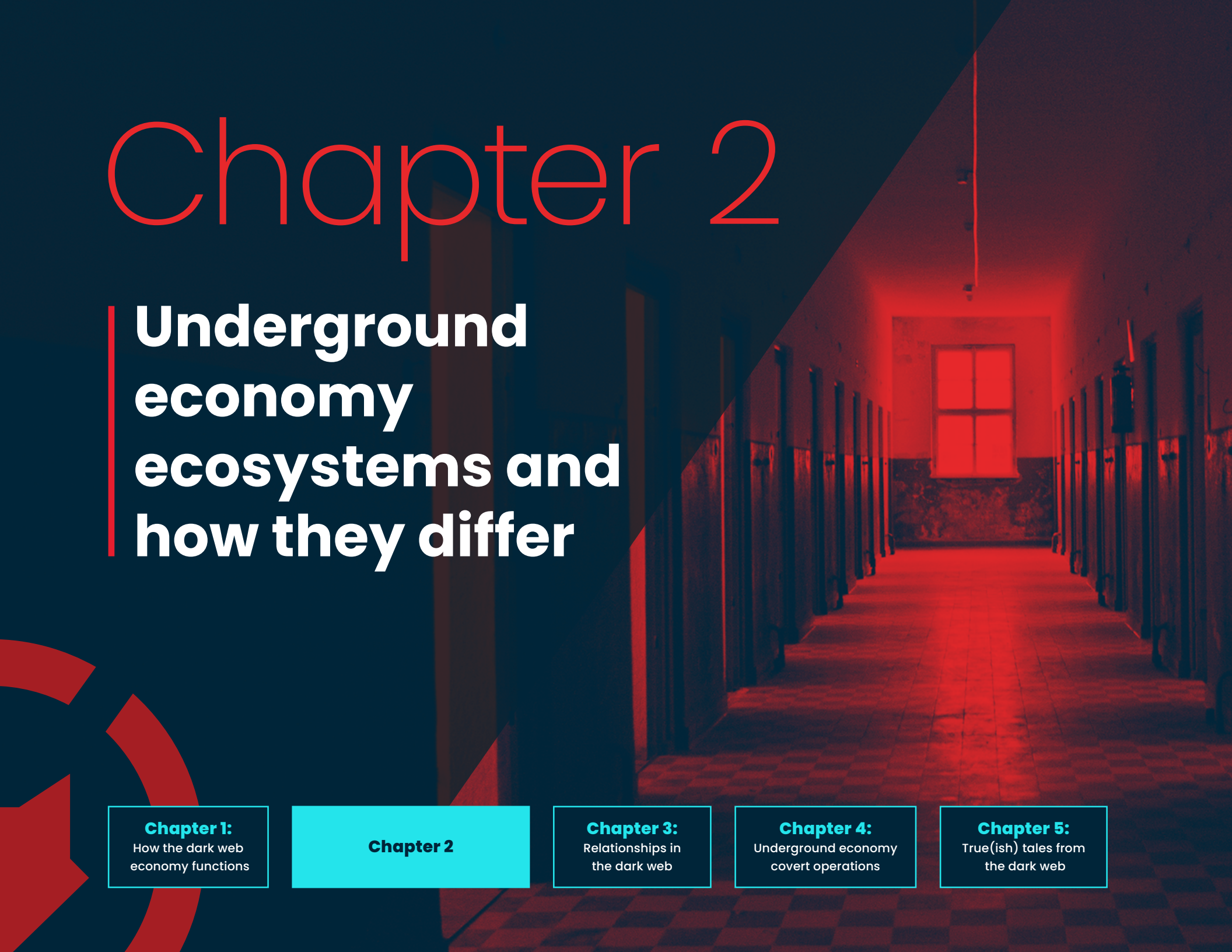
It's effectively mob rule.

Forums regularly appear and disappear, contributing to the dark web's transient nature. When forums shut down, this typically happens in at least one of two ways. First is via law enforcement. If law enforcement agencies track illegal activity to the underground source, they may seize the infrastructure and shut it down. The second way is for the forum admin to run an exit scam. An exit scam is when a forum admin sees all the money sitting in escrow – the account holding the cryptocurrency that is transferred between buyers and sellers – then shuts down the forum, takes the money, and runs. If there are signs law enforcement has discovered the forum, an admin may run an exit scam. If the forum is populated with inexperienced users, they may run an exit scam. Exit scams aren't common since once executed, the user loses all credibility in the underground economy. Still, they do happen.

The mystery around and misperceptions about the deep and dark web create a culture of terror-based clickbait.

Chapter 2

Underground economy ecosystems and how they differ



Navigating the dark web is difficult, even for regular visitors. There's a lot of turnover so destinations shift without notice. Each community has its own culture, language, and playbook. The rules depend on where you go, and even minor missteps can have major consequences. It's a big marketplace, right?

Let me show you what's behind the popular "doors" across the dark web.

DOOR 1

The Boardroom

DOOR 2

The Workshop

DOOR 3

The Shark Tank

DOOR 4

The Rave

DOOR 5

The Bazaar

DOOR 6

The House of Mirrors

DOOR 1

The Boardroom

Behind Door Number 1, you'll find the truly elite hackers. They enable everything. They're the visionaries – and ruthlessly intelligent when it comes to business. These are the leaders who authorize how stolen goods, services, and tools are shared more broadly. So after data has been brokered and exploited, the adversaries behind this door determine if and how it will be used and for what purpose. Could its release embarrass a public target? Could it boost their reputational currency? These are the decision makers who are strategizing and delegating.

NEXT DOOR > BACK TO ALL DOORS >

DOOR 2

The Workshop

This is where the inventors "build" zero-day exploits. Think of these adversaries as Q from James Bond. They build innovative "gadgets" no one has seen before. The reputation and respect these actors have in underground forums garners respect and top dollar from trusted buyers. Not just anyone gets into this world. Actors in these forums are extremely cautious about who gets invited here and who they'll do business with. They want to sell to the highest bidder and operate strictly within their criminal circle.

< PREVIOUS DOOR | NEXT DOOR > | BACK TO ALL DOORS >

DOOR 3

The Shark Tank

Behind this door, you'll find the entrepreneurs. It's a robust ecosystem focused on malware and how it can be used against broad groups of people to steal their information or shut down systems. It's noisy. It's also sophisticated. This is perhaps the most closely reflective of an above-ground economic business. Here, you'll find buyers, tech support, marketers, competition, and a variety of products and services for sale (ransomware, botnets, etc).

< PREVIOUS DOOR | NEXT DOOR > | BACK TO ALL DOORS >

DOOR 4

The Rave

Loud music. People are having fun. Some are upset. Some are just staring at a glow stick. Everyone's doing their own thing, but you've got a DJ who's organized and knows what they're doing. Nothing behind "The Rave" door is new – here, you'll find stolen data dumps of user data. These are commodities – mostly user credentials from streaming services, online stores, and porn sites. We've all seen this stuff before. Here, you might find data that originated behind the malware door – after it's been used for more lucrative, sophisticated scams – has ended up at the rave.

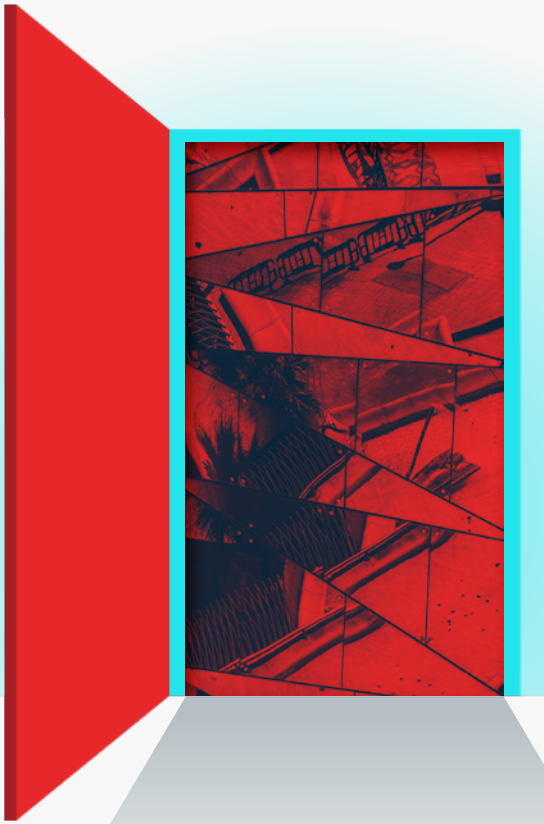
< PREVIOUS DOOR | NEXT DOOR > | BACK TO ALL DOORS >

DOOR 5

The Bazaar

The bazaar may be the most welcoming ecosystem, but that doesn't mean it's friendly or easy to navigate. Behind this door, you'll find all things fraud. Everyone wants to sell to you. If you've ever been to an open-air bazaar, you may have had countless vendors approach you, eagerly pitching their products – and their products are remarkably similar to their neighboring vendors' products. You hear lots of big claims; dealers applying pressure to make a sale, but ultimately, there's not a lot of differentiation. This is what it's like behind "The Bazaar" door within the dark web – lots of counterfeit goods, lots of chaos, no real distinctive products.

< PREVIOUS DOOR | NEXT DOOR > | BACK TO ALL DOORS >



DOOR 6

The House of Mirrors

You probably hear about what's behind this door, but I'm hesitant to say what you've heard is correct. Nation-state actors. It's scary stuff. When a government uses its resources to target something or someone, it's extremely serious. There is a lot of inaccurate information that circulates around nation-state threats. These claims are often too casually and liberally applied to activity in the underground economy. This door leads to other doors and to rooms filled with mirrors. It's a labyrinth, lacking clarity and often offering more questions than answers.

This is not to say nation-state threats should not be of concern. But it is like a house of mirrors – intentionally confusing and rife with misdirection. Because cybercriminals can operate in countries where nation-state threats originate, it's easy to conflate the two. But a threat actor who happens to operate out of Russia is not the same as a threat group sponsored by Russia's government. You need to understand and be able to recognize the difference to determine the best course of action.

Questions to consider when assessing the threat and if it could be state-sponsored include:

- Are there relationships between specific financially motivated adversaries and state-sponsored actors?
- Are these attacks about economic self-interest, direct nation-state intervention, or nation-state cooperation?
- Does the adversary's actions serve a geopolitical agenda?

There is geographical and motivational crossover between nation-state threat actors and financially motivated threat actors. Each situation requires tremendous amounts of intelligence, experience, and context. Outside of critical infrastructure, the likelihood of a state-sponsored adversary targeting your business is low. Can it happen? Certainly. But it isn't what businesses are most likely to encounter, and giving it equal consideration, on par with cybercriminals, creates fear and distractions that lead to ill-informed engagements.

‹ PREVIOUS DOOR BACK TO ALL DOORS ›

Chapter 3

Relationships in the dark web

Chapter 1: How the dark web economy functions

Chapter 2: Underground economy ecosystems and how they differ

Chapter 3

Chapter 4: Underground economy covert operations

Chapter 5: True(ish) tales from the dark web

Relationships in the underground economy matter above everything else. To succeed in the dark web – whether it's to remove your organization's stolen assets or to acquire a tool that could be leveraged against your business – you must have solid, established relationships within these unique ecosystems.

ZeroFox operatives are embedded in dark web environments and have been building relationships for a decade. It's important to know the adversaries – not just the actions they take. We know about their lives, their likes and dislikes, their families. It's easy to vilify threat actors because of their crimes. But as counterintuitive as it seems, looking at an adversary as a complex person versus a one-dimensional enemy enables us to provide important context around the human. Significant time on target leads to more efficient identification of situational nuances that fundamentally impact an engagement.

Questions you want to consider when evaluating dark web intelligence include:

- How well can your researchers distinguish between legitimate threats and trolls?
- Do you know how to avoid traps adversaries set to root out researchers?
- How do you confirm whether or not a threat is legitimate?
- Do you know enough about the threat actors to recognize when an innocuous brand mention is cause for concern?
- How well does your dark web research team work together?
- Can your dark web researchers assist with asset recovery?

"Relationships in the underground economy matter above everything else."

Chapter 4

Underground economy covert operations

Chapter 1: How the dark web economy functions

Chapter 2: Underground economy ecosystems and how they differ

Chapter 3: Relationships in the dark web

Chapter 4

Chapter 5: True(ish) tales from the dark web

Returning to our task at hand – there are advertisements on the dark web that claim to be selling your intellectual property. What do you do now?

What are your goals?

In this scenario, your security team wants to understand your brand's deep and dark web (DDW) exposure, including the brokerage of your company's data. Before beginning an engagement, it is important to define what insights and advantages you hope to uncover. Do you want to understand how your brand is discussed among cybercriminals? Do you want to acquire tools that can potentially be used against your environment? Are you interested in intelligence around specific communities operating in the underground economy?

The dark web is not a homogenous collection of underground criminals. It's a diverse group of ecosystems, each with its own culture, language, rules, and activities. It requires specialized expertise to develop the right plan for the right situation.

"As counterintuitive as it seems, looking at an adversary as a complex person versus a one-dimensional enemy enables us to better serve organizations and provide important context around the human."

Is the threat legitimate?

DDW intelligence is just one piece of the security and decision-making puzzle aimed at filling intelligence gaps. To that end, context around the threat matters, including the reputation of the actor and the accompanying chatter. For example: Who is advertising that data set or tool aimed at your brand? Is it from an established dealer or broker? On what forums are these ads posted? How are communities reacting to the claims? Dark web researchers should be able to activate operatives using established personas to determine the legitimacy of the threat and advise on what actions would be most advantageous to protect your business.

How do you engage with cybercriminals?

First, don't. Not on your own. Experts with hands-on experience operating in the dark web should conduct engagements on your behalf. Covert operations require deep engagement. Acting without the appropriate access, experience, context, and reputation can lead to additional and unnecessary risk to your organization.

Chapter 5

True(ish) tales from the dark web

Chapter 1: How the dark web economy functions

Chapter 2: Underground economy ecosystems and how they differ

Chapter 3: Relationships in the dark web

Chapter 4: Underground economy covert operations

Chapter 5

THESE TALES ARE TRUE, ALTHOUGH SOME DETAILS MAY BE CHANGED TO PROTECT IDENTITIES.

TALE 1: **Avoiding an exit scam**

Our team is often asked to procure an item in a DDW forum or marketplace on behalf of a client – intellectual property, compromised data, or tools that could be used to attack the client or the client's users. DDW forums and marketplaces have a shelf life and are taken offline without notice regularly, leaving its users confused and robbed of their money. There have been several occasions where our team identified signals that an exit scam was coming. We advised our clients to hold off on procuring an item so as not to get scammed, and sure enough, within a week, our suspicions were confirmed. We were able to save our clients money and perhaps more importantly, provide peace of mind.

TALE 2: **Contextualizing the adversary beyond the actions**

While presenting to a client, our team noted that one of the most prolific and well-known English-speaking adversaries was advertising his interest in several IP addresses, one of which was connected to the client. They informed us that the IP address had been decommissioned so they believed no action was needed. If we didn't know this hacker – really know him – we wouldn't have been able to add important context. We said, "We hear you, and we're glad the IP address is locked down. The reason we highlighted this in our findings is because the most well-regarded, scary English-speaking hacker on the planet is thinking about your company. He has your company's name on his lips." Because of the circumstances, our team recognized and because we focus on building strong, trust-based relationships with our customers – who know we never cry wolf – we were able to reassure, with a high degree of confidence, that this customer's security team should reexamine their security and tighten things up around their networks.

TALE 3: **Facts, not fear-mongering**

We were conducting DDW research for a large client. They provided a broad task to look into this specific ecosystem within the underground economy ahead of a big event they had planned. We engaged and found it was full of trolls and speculators. It was really an immature subsection of the dark web community. Most conversations were, in a way, satirizing the bigger dark web ecosystem.

After writing our brief, we presented our findings to the client – that this was an immature group, making jokes and venting. They told us, "You're the only vendor that didn't lie to us. You are the only vendor that didn't fan the flames."

Our tradecraft is unique. Because of our techniques, our time on target, and our decade-long history in the underground economy, we can quickly identify the difference between satire and serious threats. Those nuances take time to recognize and understand, but the actions you take based on the assessment have real consequences. Our experience translates to tangible results – cost savings, peace of mind, and the thorough context needed to know if a situation will escalate or deescalate. We're here to simplify security decision-making. And to do that, trust is everything.

"SO LONG, AND THANKS FOR ALL THE *PHISH*"

There you have it – a hitchhiker's guide through the dark web economy. It's a diverse, noisy, chaotic ecosystem with more in common with the above-ground economy than one might think. But of course, this is just an introduction. It's constantly evolving. Like with any complex environment, small changes can have big consequences. Engagements across the dark web economy are more successful with an experienced team who can not only navigate conditions as they are today but whose background is so robust, they can anticipate how it will adapt tomorrow. And, as long as adversaries are putting organizations and individuals at risk, we'll be there to light the way into and out of the dark.

CONTRIBUTORS

Author: Adam Darrah - Director of Threat Intelligence Services, *ZeroFox* | Editor: Emily L. Phelps - Director of Content Marketing, *ZeroFox*

About ZeroFox

The leader in External Cybersecurity

ZeroFox (Nasdaq: ZFOX), an enterprise software-as-aservice leader in external cybersecurity, has redefined security outside the corporate perimeter on the internet, where businesses operate, and threat actors thrive. The ZeroFox platform combines advanced AI analytics, digital risk and privacy protection, full-spectrum threat intelligence, and a robust portfolio of breach, incident and takedown response capabilities to expose and disrupt phishing and fraud campaigns, botnet exposures, credential theft, impersonations, data breaches, and physical threats that target your brands, domains, people, and assets. Join thousands of customers, including some of the largest public sector organizations as well as finance, media, technology and retail companies to stay ahead of adversaries and address the entire lifecycle of external cyber risks. ZeroFox and the ZeroFox logo are trademarks or registered trademarks of ZeroFox, Inc. and/or its affiliates in the U.S. and other countries.

See ZeroFox in action

zerofox.com/demo | zerofox.com

Get in touch with us today

sales@zerofox.com | 855.736.1400