BITSIGHT

EBOOK

Tour of the Underground

Overcoming the Barriers to Extracting Dark Web Intelligence

Table of Contents

01 Introduction

The deep, dark web – the underground – is a haven for cybercriminals, rich with tools and resources that enable them to launch attacks for financial gain, political motives, and other causes. The underground is also a vast source of intelligence and information for cyber defenders, providing insights into the daily threats and tactics that target individuals and organizations. But for anyone attempting to continuously find and monitor the right dark web sources and intelligence, doing so through manual methods presents numerous barriers that can lead to analyst fatigue and delay appropriate action.

Accessing dark web intelligence can be frustrating for those on the front lines of cyber defense without proper knowledge of the underground and the necessary intelligence extraction tools.

This eBook offers an overview of the dark web and the many barriers to leveraging dark web intelligence to your advantage. It also describes steps to take to stay ahead of threats targeting your organization.

SPECIFICALLY, THE EBOOK COVERS:

Defining the dark web

Discovery and access

Extracting intel: manual vs. paid intelligence

Adding dark web intelligence to your CTI Arsenal

Re-Think Your Intelligence Strategy

Bitsight helps you take your cyber threat intelligence (CTI) program to the next level and better defend against the threats that pose the most significant risk to your organization through automated, proactive dark web intelligence. With a solid understanding of the dark web and ways to navigate the malicious activities in the underground, stopping bad actors before they launch an attack is more easily achievable.

Defining the Dark Web

The underground consists of many different types of sources from the deep, dark, and clear web, where threat actors engage in malicious activity, communicate with each other, and launch attacks. As these bad actors continue to adapt and expand their modes of communication, it's critical to stay up to date on where they sell and distribute malicious programs — many of which look similar to a legitimate online forum or marketplace.

"The dark web" is an overused term that can be a source of mystery and confusion for most cybersecurity professionals. Put simply, the dark web is any site, messaging platform, community, or other online entity that is not indexed by any search engine. Dark web sources typically require unique software to access them, such as Tor, I2Pd, and Zero Net, which enable people to engage and operate online anonymously. Because of the ability to remain anonymous, the dark web affords threat actors an easy way to communicate with each other and carry out malicious acts.

That said, not everything that occurs on the dark web is bad. For example, many dark web sites, such as gaming forums and online marketplaces, are used for legitimate purposes — and distinguishing between the good and the bad can be difficult without proper intelligence tools.

Types of sources

Clear Web	Paste sites (e.g. pastebin), Reddit, 8chan, NVD, Twitter (secondary+direct), GitHub (secondary+direct)
Deep Web	Open and closed (invite-only) forums, markets, credit card markets, paste sites and internet relay chat (IRC)
Dark Web	Open and closed (invite-only) forums, markets, credit card markets, paste sites and internet relay chat (IRC), and software such as Dread or Zeronet
Social Messaging	Open and closed (invite-only) groups and channels on Telegram, Discord and QQ, ICQ

Discovery and Access

When visiting dark web sources, it's essential to take precautions so you don't fall victim to threat actors' duplicity. To protect yourself and your organization, use an isolated device or sandbox, not your work or personal device. For example, you can use "dirty machines" that wipe themselves every time you log out of them or an OS system (e.g., Tails) that boots up on a flash drive and is wiped clean whenever you shut down.

There are many clear, deep, and dark web sites, forums and marketplaces where threat actors can access victims' online accounts. In addition, encrypted messaging platforms like Telegram and QQ provide a safe haven for communications about malicious acts and are, therefore, popular among threat actors.

One of the most significant barriers to finding deep and dark web sources is that you must use the exact URL to access sources that are not indexed — even with a browser like Tor.

For example, to access the popular dark web forum CryptBB, you must know the exact onion link; conducting a web search for the forum will not turn up anything useful. Some well-known underground sources can be easier to find because there are dedicated sites that share links and maintain regular status updates. But in many cases, finding the exact URLs through manual search methods can be next to impossible.

Registration and VIPs

Finding exact dark web links is one barrier to finding cybercriminals' activities. Another challenge is that many dark web sources require reference checks, payment, applications, or invites to access, so they're not readily accessible even if you have a link. For example, Genesis is a wellknown access broker where threat actors must pay thousands of dollars to gain access. RAMP is another prominent Russian- and Chinese-speaking forum that requires individuals to have an extensive background as a threat actor or pay large sums of money to be accepted. There are thousands more like these. Adding another layer of difficulty is that sensitive data is only available to the upper tier of hackers or VIP users, who must be trusted, verified threat actors on many of these sites.

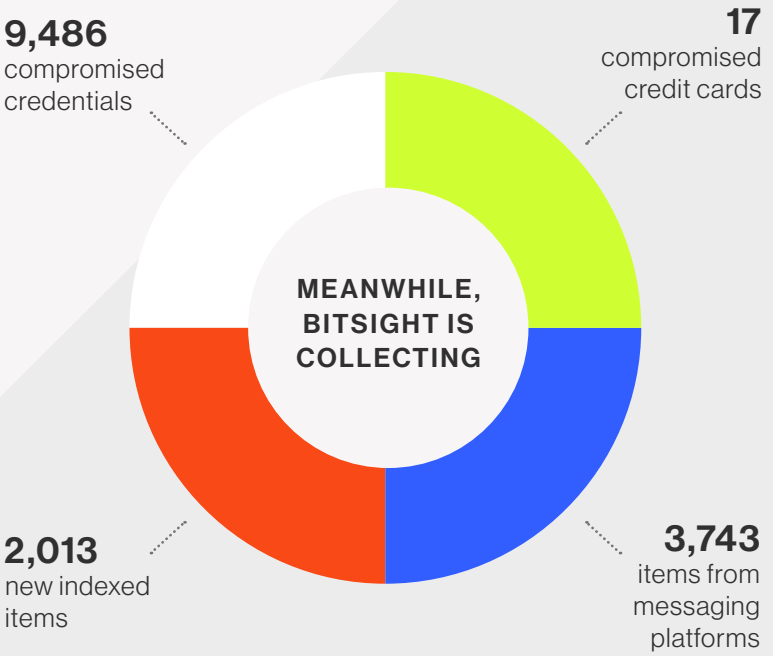
Language barriers and communications

Many dark web sources use foreign languages (such as Chinese or Russian), which makes it difficult to find relevant information and prevents communication with threat actors if you don't know the language. Communication among bad actors is how they acquire sensitive data or attain an invite to a protected source. If you cannot communicate with them in their language, you'll have difficulty building trust and discovering plans and activities that pertain to you and your organization.

For dark web sources where language is not an issue, you need to know where and how threat actors communicate. Often, they rely on private messaging functions on a specific dark website, or they use messaging platforms like Telegram or Jabber where they can quickly burn anonymous accounts when needed. Communication with threat actors is both a challenge and a risk for cyber defenders because you must maintain anonymity and ensure you're not compromising their trust.

Extracting Intelligence: Manual vs. Paid Intelligence

From fraudulent credit cards and compromised endpoints offered for sale to Zero Days and malicious programs being sold and distributed, vast volumes of data are posted to underground sources every minute of every day. No matter the topic or use case, finding and extracting this intelligence efficiently is challenging for any cyber investigator.



Adding to the challenges already discussed, many dark web sites deploy tools that prevent bots and web crawlers from accessing the site. Unfortunately, when encountering these mechanisms, you may be put in a queue and have to wait to be admitted to the source, or you may have to click through a series of questions and challenges to prove that you're a human (e.g., clicking specific images or checking the "I'm not a robot" box). Overcoming these roadblocks can be one of the most laborious aspects of dark web investigations. On top of this, dark web sources are often unreliable and unstable and may go down without warning. In this case, any data that you've accumulated will instantly vanish.

An easier way

Bitsight gives you a powerful tool for overcoming the many obstacles to finding useful dark web sources and intelligence. We continuously collect information from a vast range of sources, including closed forums and limited access markets, translating any language and enriching each item of intel with rich context so you can instantly learn more about the threat or threat actor it relates to. We automatically map this intelligence to your priority assets and immediately alert you of any suspicious activity. We spot malicious activities across dark web sites, forums, marketplaces and messaging platforms targeting your IP assets, different web domains, executives' names and titles, products and more.

By leveraging proactive, automated dark web intelligence, you can get ahead of threats targeting you, learning about malicious activity in the planning phases before an attack is launched. This helps you to concentrate on the vulnerabilities exposing your environment to specific-and-real risks, closing the door to a threat actor as they are about to strike.

Recommendations: Getting Ahead of Threats

To further up-level your cyber threat intelligence (CTI) program and protect your organization, we recommend the following:

Enable your CTI team with resources that provide the earliest indication of risk through automation of collection and alerting.

Ensure that your team has complete visibility into the threats and surrounding context to spend less time sorting through data.

Relieve analysts and engineers from manual persona management and investigations and allow them to focus on providing valuable insights.

Provide proper training and services to help with investigations and data acquisition.

Adding Dark Web Intelligence to your CTI Arsenal

Given the high volume of malicious activities occurring daily in the underground, automated, proactive dark web intelligence gives you a tremendous advantage by identifying threats targeting your organization without burdening already strained resources. Access to the places where threat actors meet, buy and sell their ill-gotten gains and discuss their plans means security, governance, risk and compliance teams can analyze the data they need in several ways to protect their environment. The following use cases are just a few of the most common applications by threat analysts:

Vulnerability Management
Know which vulnerabilities will be targeted and get insights around emerging threats.

Ransomware Protection
Get real-time alerts and essential context to combat ransomware, malicious malware, and vulnerability exploits.

Compromised Credentials
Stay ahead with automatic notifications in the event of leaked employee credentials, system passwords, and brand assets.

Incident Response
Analyze and detect threats earlier. Perform investigations on the dark web to optimize the incident response lifecycle.

Threat Hunting
Seek the highest-priority potential cyber threats to your organization and take remediating action to protect your environment before they attack.

Data Leaks
Customize automated alert warnings of leaked organizational data, including OCRextracted text from images to identify logos and designs.

Brand Protection
Receive advanced warnings of brand abuse, such as rogue applications on app stores and typosquatting activity.

Compromised Credit Card Detection
Stop leaks fast with real-time alerts in the event credit card credentials are leaked or sold on underground markets, IM apps, or IRC chats.

Re-Think Your Threat Intelligence Strategy

Bitsight automates the process of identifying and monitoring threats across the deep, dark, and clear web from the broadest range of sources in real-time to proactively block threats before they materialize into attacks. Our market-leading threat intelligence can be consumed through various solutions and integrations, depending on your needs. Each solution is scalable, searchable, and seamlessly integrates into your existing security stack.

DVE Intelligence

Our Dynamic Vulnerability Exploit (DVE) Intelligence is an end-to-end solution that spans the entire Common Vulnerabilities and Exposures (CVE) lifecycle, streamlining vulnerability analysis, prioritization, management, and remediation. With DVE Intelligence, your teams gain critical insight and context to accurately identify and prioritize the vulnerabilities that pose the greatest risk to your organization. This significantly reduces your mean time to remediate.

API Integration

Our API suite provides direct, programmatic access to our market-leading threat intelligence data, integrating seamlessly into your existing workflows and system architectures. Supporting multiple data types, use cases, and processes across departments, our seamlessly integrated machine-readable threat intelligence optimizes the efficiency of your cybersecurity operations.

Investigative Portal

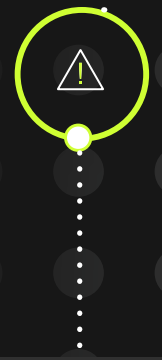
With Bitsight's SaaS Investigative Portal, you have secure, covert access to our complete body of collected intel from the clear, deep, and dark web. Combining unparalleled threat data collection capabilities with unlimited search functionality means you can monitor emerging cyber risks threatening your organization in real-time and accelerate your mean time to detect them.

07 The Bitsight Difference

	BITSIGHT	OTHER VENDORS
Threat Intelligence Collection	Fully automated, real-time intelligence collection, extraction, and indexing – promising more data, fewer blindspots, and greater value generation for customers.	Collect data using obsolete, manual approaches that rely on humans to search for and extract intelligence and fail to continuously detect threats.
Access to Threat Intelligence & Data	Provides complete and unrestricted access to our comprehensive body of contextual threat intelligence, empowering customers to conduct their own independent investigations and regain control of their cybersecurity program.	Manually curated reports and feeds which do not provide the full intelligence picture regarding the nature and source of each threat, forcing clients to make critical decisions with little information.
Speed of Collection	Provides actionable and relevant threat alerts in real-time, minutes after activities have surfaced on the underground, along with actionable recommendations for remediation.	Significant time lag from collection to detection to alert, by which time the threat has likely been weaponized and the incident may have already occurred.
Scalability & Cost	Fully scalable solution with transparent pricing and no limits to search results.	Limited ability to scale. Complex pricing packages are tied to a restricted number of search results.

To learn how Bitsight's cyber threat intelligence solutions empower you to detect threats quickly, efficiently, and early, schedule a demo today.

Book a demo



sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BITSIGHT