STATE OF THE DARK WEB 2025:

GET AHEAD OF CYBERTHREATS WITH THE LATEST DARK WEB INSIGHTS

ID AGENT
A Kaseya COMPANY

INTRODUCTION

The dark web is often depicted as a seedy virtual back alley where lone wolves peddle illegal goods and stolen data. However, it is so much more than that. It is a thriving marketplace where all manner of goods and services are bought and sold by everyone from nation-state threat actors to teenage hackers. This economic juggernaut forms the world's third-largest economy[1] and is a clear and present danger to businesses that IT professionals must wrestle with daily.

Bad actors are constantly refining their techniques, tactics and procedures (TTPs) to outmaneuver defenders to attack organizations and steal valuable data. Now, they've embraced advances in artificial intelligence (AI) technology to supercharge their efforts and increase the pressure on businesses.

Threat intelligence is essential if IT professionals want to stay a step ahead of bad actors. Organizations must understand how today's dark web ecosystem functions and how emerging trends in technology may shape its evolution if they hope to protect their businesses from a costly cyberattack or data breach.

THE DARK WEB DEMYSTIFIED

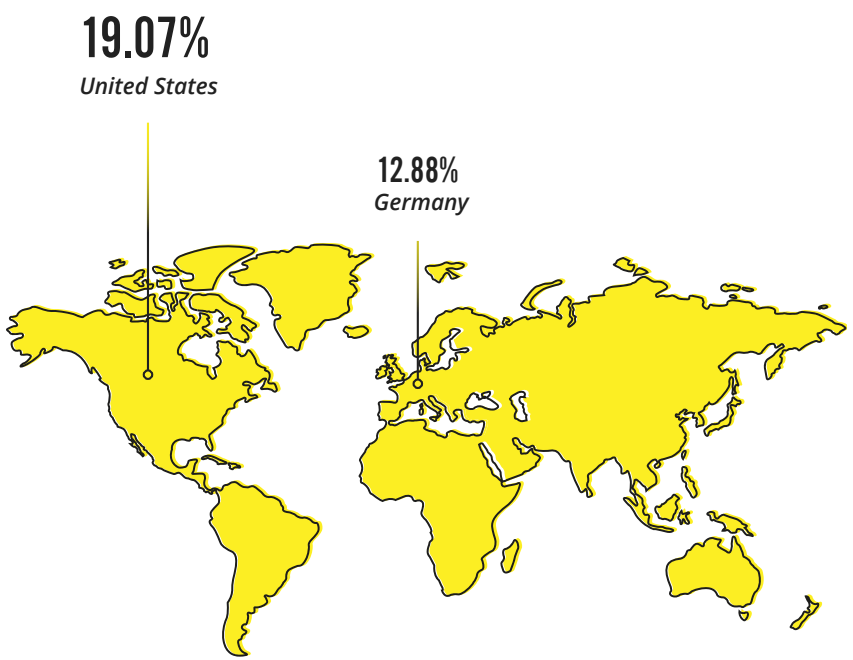
The dark web is a flourishing economic juggernaut. To shield businesses from trouble, defenders must familiarize themselves with the people, commodities, services and transactions that shape it.

MAPPING DARK WEB USERS

The dark web is a hidden network attracting a range of users, from seasoned cybercriminals to opportunistic amateurs. The Onion Router (TOR), an open-source network that enables anonymous internet browsing, is the primary gateway users around the world use to access the dark web worldwide. This breakdown illustrates the top locations for daily dark web access via TOR.[2]

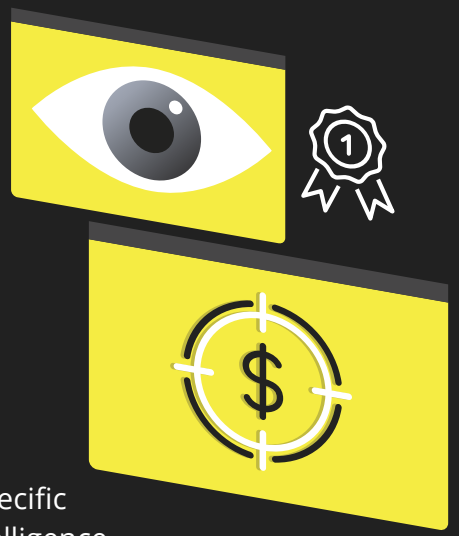
Top 10 countries with the highest daily dark web access via TOR

Country	Mean daily users	% of total users
United States	458,986	19.70%
Germany	300,044	12.88%
Lithuania	98,186	4.21%
Finland	96,147	4.13%
India	91,105	3.91%
Netherlands	69,864	3.00%
Republic of Korea	68,534	2.94%
Indonesia	67,783	2.91%
United Kingdom	56,145	2.41%
France	53,777	2.31%



POWER BROKERS OF THE DARK WEB

The dark web is a busy hub with a diverse population, and these are the major players:



CYBERCRIMINAL GANGS

These organized groups, either independent or state-sponsored, lead the cybercrime world, providing affiliates with resources like malware and intelligence to carry out attacks.

CYBERCRIME AFFILIATES

These small groups or individuals subcontract with major cybercriminal gangs to execute specific attacks, sharing a percentage of their profits for access to advanced tools, expertise and intelligence.

INITIAL ACCESS BROKERS

An initial access broker (IAB) specializes in gaining unauthorized access to networks or systems. IABs then sell that access to other criminals for further exploitation, such as deploying ransomware or stealing data.

SPECIALISTS

These independent operators cover a range of cybercriminal needs, such as developing malware, providing data, laundering money or creating clever phishing messages. Many specialists provide only support services and do not actively engage in direct hacking or cyberattacks.

HACKTIVISTS

Activist individuals or groups may be motivated by a cause instead of profit. They often target high-profile organizations or governments. Hacktivists typically steal and expose sensitive data or mount DDoS attacks to cause disruption.

MALICIOUS INSIDERS

Disgruntled employees or contractors may turn to the dark web to sell their access credentials or sensitive company information. It can be challenging for companies to detect a malicious insider at work.

NATION-STATE ACTORS

Often referred to as advanced persistent threats (APTs), these operatives are government-backed hackers who engage in cyberwarfare and espionage activities. They typically concentrate on strategic targets like critical infrastructure or defense assets.

STEP INSIDE THE UNDERGROUND MARKETPLACE

The bustling economic landscape of the dark web may be chaotic, but several elements remain consistent about how business is done. Digital currencies rule, primarily Bitcoin and Monero. Buyers and sellers typically negotiate deals through encrypted messaging tools like Signal or in digital venues like these:

01

DARK WEB MARKETS

are centralized platforms for buying and selling goods and services that function like e-commerce sites complete with search filters, product categories and even seller reviews.

02

MESSAGE BOARDS OR FORUMS

are hubs where users share tips, tutorials, gigs and listings, serving as key platforms for connecting with other users.

03

LEAK SITES

typically run by ransomware-oriented gangs, are used to pressure extortion victims to claim attacks, publicize ransom demands and publish stolen data.

A CATALOG OF THE GOODS AND SERVICES AVAILABLE ON THE DARK WEB

A wide variety of goods and services, from hacking to designer knockoffs, are available on the dark web. These examples illustrate the breadth of dark web markets.

CYBERCRIME-RELATED SERVICES

CaaS

Cybercrime-as-a-Service (CaaS) is an umbrella term that encompasses a galaxy of specialized cybercrime service providers. The industry has transformed the cybercrime landscape, making it a snap for even novice cybercriminals to conduct dangerously sophisticated attacks against businesses.

RaaS

Ransomware-as-a-Service (RaaS) platforms, run by cybercrime gangs or independent operators, offer preconfigured ransomware tools that enable bad actors to launch attacks with ease while the platform operator takes a share of the ransom.

PhaaS

Phishing is cheaper and easier than ever. A subscription to a Phishing-as-a-Service (PhaaS) platform gives bad actors access to everything they need for successful phishing from slick branded email templates to full-service concierge operations.

The CaaS world also includes Distributed Denial-of-Service (DDoS) attack tools, exploit kits, credential stuffing services and brokers selling stolen credentials and data.

HOT COMMODITIES

Shoppers can easily purchase just about anything on the dark web, from fake designer purses to medical records or even a whole new identity. These are some of the major commodities that are bought, sold and traded on the dark web.

FULLZ

Complete sets of personally identifiable information (PII), often referred to as fullz, are hot items. Bad actors can use fullz to facilitate identity theft and commit fraud, like opening a fake bank account to launder money.

INTELLECTUAL PROPERTY AND PROPRIETARY DATA

Proprietary business data, including contracts and invoices, can fuel business email compromise (BEC) attacks. Intellectual property like patents, trademarks blueprints and proprietary designs are also highly valued.

NATIONAL SECURITY DATA

Sensitive government information, including schematics for power stations, military capacity data and intelligence reports, is valued by nation-state actors.

PII, PMI AND OTHER PERSONAL DATA

PII, protected medical information (PMI) and similar data is highly sought after on the dark web. Medical records can be used for insurance fraud and blackmail while personal details power spear phishing and identity theft.

ZERO-DAY EXPLOITS

Software vulnerabilities that are unknown to the vendor are very desirable and often used for espionage or major cyberattacks.

ILLICIT TRADE

Non-cybercrime illicit commerce on the dark web includes designer knockoffs, weapons, drugs, endangered species and human trafficking.

By staying informed about what's being sold, who's buying it and how transactions occur, IT professionals can better anticipate risks.

DARK WEB PRICE POINTS

Like in legitimate economies, pricing on the dark web reflects a dynamic interplay of supply, demand and competition. These examples illustrate typical pricing for the common items and services available in dark web markets. Understanding these price points can help IT professionals anticipate threats and prioritize cybersecurity defenses to protect valuable assets.[3]

Example pricing of goods and services on the dark web as of 2024

US ID (PHYSICAL FORM)

$150 – $160

EU PASSPORT (PHYSICAL)

$3,800

DDOS ATTACK: 20-50K REQUESTS PER SECOND FOR 24 HOURS ON A PROTECTED WEBSITE

$200 and up

HIGH-SUCCESS RATE MALWARE

1,100 to $1,800

MASTERCARD (PIN INCLUDED)

$20

THE AI REVOLUTION ON THE DARK WEB

AI has been a major disruptor for the dark web. Cybercriminals have been quick to adopt AI-enhanced tools that help them to do their dirty work efficiently and effectively. Here are some ways AI is making cybercrime easier:

01 Creating malware and ransomware that can autonomously adapt and evolve, improving the effectiveness of attacks and making them harder to detect and block.

02 Conducting phishing attacks that can flawlessly mimic the style and tone of trusted individuals or companies, increasing the likelihood of success.

03 Data mining and rapid analysis allow bad actors to rapidly analyze vast amounts of information to swiftly identify valuable targets or potential vulnerabilities.

04 Making deepfake videos or audio recordings that can be used to impersonate individuals, such as executives, in fraudulent schemes like BEC or other scams.

05 Improving encryption methods, making it harder for authorities to trace transactions or infiltrate dark web marketplaces.

06 Bots can assist with scanning for vulnerabilities in financial systems and execute automated attacks when they identify the right conditions for success.

07 Predicting trends and identifying new vulnerabilities to launch zero day attacks.

ESSENTIAL SOLUTIONS FOR A SMART DARK WEB DEFENSE TOOLKIT

As businesses become increasingly aware of the dangers posed by the dark web, IT professionals must take proactive steps to mitigate these risks. By leveraging the right tools, strategies and best practices, they can significantly reduce the likelihood of organizations falling victim to dark web-related threats.

ILLUMINATE A COMPANY'S RISK WITH DARK WEB MONITORING

Dark web monitoring is a key strategy in reducing dark web risks by proactively identifying exposed data, credentials or sensitive information. Regular scans of dark web marketplaces, forums and data dumps allow businesses to detect breaches early and take action to prevent malicious use of compromised data, such as changing passwords or implementing additional security measures.

Dark Web ID provides round-the-clock monitoring of business and personal credentials, including domains, IP addresses and emails, using both human and machine-powered detection. It uncovers compromised credentials in dark web markets and data dumps, alerting you quickly to enable proactive action against cybercriminals.

With Dark Web ID , IT professionals get the valuable intelligence they need to close security gaps and gain peace of mind about an organization's dark web risk.

STOP PHISHING BEFORE IT STARTS

Phishing is the most common method cybercriminals use to launch cyberattacks. Reducing risk starts with reducing employee exposure to phishing messages. An AI-driven anti-phishing solution can detect and mitigate phishing attempts before they reach end users. By analyzing patterns and identifying suspicious emails in real-time, an AI-powered anti-phishing solution adapts and improves its detection capabilities over time without human intervention, freeing up valuable tech time.

Graphus is an AI-powered anti-phishing solution that shields employee inboxes from ransomware, BEC, and other threats with patented automation. It features EmployeeShield for easy threat identification and reporting.

Graphus integrates seamlessly with Microsoft 365 and Google Workspace via API, with no complex configurations or email rerouting, enhancing an organization's email security to withstand today's sophisticated threats.

MITIGATE YOUR BIGGEST RISK WITH COMPREHENSIVE TRAINING

Human error is one of the greatest vulnerabilities businesses face. Security awareness training and phishing simulations are critical in educating employees on how to recognize and respond to potential threats. Employees who understand how to spot phishing attempts, avoid social engineering and safely handle data become security assets instead of liabilities.

BullPhish ID is an affordable security awareness training and phishing simulation platform that provides comprehensive education about cyberthreats and data breach risks, empowering employees to spot and stop phishing threats and follow cybersecurity best practices. It's the perfect training solution to help businesses bolster compliance with cyber insurance requirements and industry regulations.

With BullPhish ID, IT professionals gain access to a variety of engaging, multilingual training materials and customizable phishing simulation kits. Smart automation enables set-it-and-forget-it training and effortless reporting. Meet cyber insurance requirements and industry regulations with ongoing security awareness training, reducing non-compliance risks and associated fees.

STAYING AHEAD OF THE CURVE

As the dark web evolves, IT professionals must stay vigilant and adapt to ever-changing threats. Cybercriminals are refining tactics with advanced tools like AI, requiring proactive defenses such as dark web monitoring, AI-driven security and employee awareness. By staying agile, IT teams can better protect against emerging dangers.

Let us show you how our smart, affordable solutions can help you mitigate dark web risk.

LEARN MORE

BOOK A DEMO

ID AGENT
A Kaseya COMPANY

SOURCES

[1] ID Agent - Dark Web Exposure From These 9 Sources Increases Cyberattack Risk

[2] TOR Metrics

[3] Privacy Sharks - Dark Web Price Index 2024