Computer Troubleshooters®
TECHNOLOGY SOLVED

OUR BLOG

Dark Web Marketplaces: How Cybercriminals Buy and Sell Your Data

Introduction

The dark web has become a notorious marketplace for cybercriminals engaging in the trade of stolen personal data. This hidden segment of the internet is accessible only through specialised software like Tor, enabling criminals to operate anonymously.
This guide explores:

- How the dark web marketplaces work (Source: Scoop
- The types of stolen data sold online
- Methods used by hackers to steal sensitive information
- The economic impact of cybercrime
- Protective measures to safeguard personal and corporate data

Understanding these illicit activities is crucial for cybersecurity awareness, risk mitigation, and developing stronger digital defenses.

What Is the Dark Web?

The dark web is a part of the deep web that requires special tools like Tor (The Onion Router) to enable access to the dark web . Unlike the surface web, which is indexed by search engines, the dark web operates in an anonymous, unregulated environment, making it a hotspot for illegal activities.

Dark Web Statistics (2025)

- Estimated 30,000 active dark web websites. (Source: Scoop Market)
- Global dark web market revenue projected to reach $1.3 billion USD by 2028. (Source: KBV Research)

22.3% CAGR (Compound Annual Growth Rate) in dark web activities. (Source: KBV Research)

What Data Is Sold on the Dark Web?

Stolen data is sold by cybercriminals using underground marketplaces, often categorised into different types:

1. Personally Identifiable Information (PII)

- **Data Included:** Name, address, phone number, Social Security Number (SSN), medicare numbers, car license details, passports, and dates of birth.
- **Purpose:** Identity theft, financial fraud.
- **Price:** Can range from US $1 to $100 per record.

2. Financial Information

- **Data Included:** Credit card numbers, bank account details.
- **Price Range:** Complete financial profiles sell for US$100-US$1,200, individual credit cards US$5-US$30, with an average of US$12 (ZipDo Education Reports, 2024).

3. Login Credentials

- **Data Included:** Email, social media, corporate login credentials.
- **Price:** Regular accounts typically sell for US$5-US$20, while corporate accounts can go up to US$1,000.

4. Medical Records

- **Data Included:** Patient history, insurance details, prescriptions.
- **Why So Valuable?** Medical records can be used for insurance fraud and fake prescriptions.
- **Price:** US $250 - $1,000 per record (as low as $1 for basic details)

5. Corporate & Government Data

- **Target:** Trade secrets, proprietary technology, intellectual property.
- **Price:** Corporate data ranges from US$2,000 to US$4,000, with government/military records varying significantly based on sensitivity.

How Cybercriminals Steal Data

Hackers use various techniques to harvest and sell stolen data:

1. Data Breaches

- Large-scale cyberattacks on companies expose millions of records.
- These records are later sold in bulk on dark web forums.

2. Phishing Attacks

- Cybercriminals trick users into revealing login credentials.
- Phishing kits (used for scams) are available on the dark web for as low as US $3.

3. Malware & Ransomware

- Hackers deploy spyware, keyloggers, and ransomware to steal sensitive data.
- Some malware can be bought on the dark web for $30 or less.

4. Social Engineering

- Exploiting human psychology to manipulate users into sharing passwords or confidential details.

5. Cryptocurrency Payments

- Transactions on the dark web occur via Bitcoin (BTC) and Monero (XMR) to maintain anonymity.

How Cybercriminals Steal Data

Hackers use various techniques to harvest and sell stolen data:

1. Data Breaches

- Large-scale cyberattacks on companies expose millions of records.
- These records are later sold in bulk on dark web forums.

2. Phishing Attacks

- Cybercriminals trick users into revealing login credentials.
- Phishing kits (used for scams) are available on the dark web for as low as US $3.

3. Malware & Ransomware

- Hackers deploy spyware, keyloggers, and ransomware to steal sensitive data.
- Some malware can be bought on the dark web for $30 or less.

4. Social Engineering

- Exploiting human psychology to manipulate users into sharing passwords or confidential details.

5. Cryptocurrency Payments

- Transactions on the dark web occur via Bitcoin (BTC) and Monero (XMR) to maintain anonymity.

Dark Web Marketplaces: How Cybercriminals Trade Stolen Data

Several dark web marketplaces facilitate the sale of illicit data:

Marketplace	Year Established	Commission	Total Listings	Business Volume (Figs in US$)
TorZon	2019	0.15% - 0.25%	100+	$10M+
Nexus	2023	0.10% - 0.20%	110+	$20M+
Flugs	2016	0.00% - 0.10%	400+	$40M+
Abacus Market	2022	0.05% - 0.15%	100+	$20M+
Elysium	2024	0.10% - 0.20%	50+	$5M+

These marketplaces function like e-commerce platforms, but for stolen data, illegal drugs, weapons, and hacking tools.

Economic Impact of Dark Web Transactions

- **Annual Revenue:** US $6 billion
- **Daily Transactions:** Estimated US $250,000 - $500,000
- **Increasing Demand:** Reports show a 300% rise in stolen login credential sales from 2022 to 2023.

Computer Troubleshooters Basic Tips for Protecting Yourself From the Dark Web

1. Strengthen Your Passwords

- Use strong, unique passwords for each account.
- Utilise password managers to store credentials securely.

2. Enable Multi-Factor Authentication (MFA)

- Adds an extra security layer against hackers.

3. Monitor Your Financial Accounts

- Regularly check bank and credit card statements for unauthorised transactions.

4. Be Wary of Phishing Attacks

- Avoid clicking suspicious links or downloading unknown email attachments.

5. Use Dark Web Monitoring Services

- Services like HaveIBeenPwned notify users if their data has been compromised. For a business often it is more efficient and effective to have your local Computer Troubleshooter monitor and perform regular checks on a monthly plan. This would enable a business to focus on doing business while your business IT is in good hands.

Challenges Faced by Law Enforcement

Despite efforts to combat cybercrime, law enforcement faces multiple hurdles:

- **Decentralised Platforms:** Hard to shut down completely.
- **Evolving Criminal Tactics:** Hackers constantly adapt to avoid detection.
- **Advanced Encryption:** Makes it difficult to trace transactions and identify criminals.

Future Trends in Dark Web Marketplaces

- **Increased Fragmentation:** Major marketplaces shut down → Small niche markets rise.
- **Advanced Security Measures:** Dark web sites adopt better encryption & decentralised hosting.
- **Regulatory Scrutiny:** Governments strengthen cryptocurrency monitoring.
- **AI in Cybercrime:** Hackers & law enforcement both use AI-powered tools.

Conclusion

The dark web remains a critical threat to cybersecurity, facilitating the illegal trade of stolen data. As cybercriminals evolve, individuals and businesses must stay informed and implement robust security measures to protect sensitive information.

Hence, the time to act is now. Begin by securing your personal data; use strong, unique passwords for each account, enable multi-factor authentication, and avoid sharing sensitive information online. Moreover, keep your operating systems, applications, and antivirus programs up-to-date to protect against vulnerabilities through regular software updates. Encrypt your internet connection and monitor network traffic to help block unauthorised access by deploying a VPN and Firewall. Additionally, monitor your digital footprint by regularly checking your financial and personal accounts for suspicious activity and also use dark web monitoring services for early detection.

Get in touch with us at contactus@ctaustralia.com.au or call us on 1300 28 28 78 for an initial assessment at no charge. Our experts are ready to guide you through every step of the process. Let's protect your IT infrastructure together!

Contact Us

contactus@ctaustralia.com.au

1300 28 28 78