FRAUDWATCH
Digital Brand Protection

ENHANCED DEEP AND DARK WEB MONITORING

FraudWatch now offers an enhanced monitoring service of the deep and dark web. We provide a thorough and in-depth intelligence tool, that allows your organisation to get a detailed view of past, current, and potential future cyber threats targeting your organisation.

The resulting data can be accessed through an active dash-board, with the ability to view, download, sort and delete records. The dashboard will also present the user with visualised data results, allowing for swift presentation of the data.

Threat actors use various methods and platforms to communicate and share information via the surface, deep, and dark web, to avoid detection and remain anonymous. The deep web includes any regular websites that require authentication through account credentials, and contains information not picked up by search engines. We've developed proprietary tools that can infiltrate these sources to provide the most relevant and up-to-date intelligence daily.

Our enhanced deep and dark web monitoring service is an automated tool that collects data from various sources of interest, where threat actors are known to exchange information and communicate. In today's ever-evolving cyber threat landscape, large organisations are regularly targeted. With frequent data breaches occurring, it is vital to be aware of conversations between adversaries. Our platform will perform daily scans for any relevant mentions of a brand or individual and notify our clients of any relevant data that may have been leaked, allowing them to immediately mitigate the issue.

We offer secure access to the deep and dark web records and the ability to download sensitive information through encrypted channels. We can provide selected users access to the deep and dark web data to allow for easier control around which employees can access the results, to minimise risks internally.

Our high-threat sources include the various decentralised peer-to-peer anonymous networks including ToR marketplaces and forums, as well as I2P and ZeroNet. Our other sources include a range of deep web sources, such as authenticated hacker forums, high-risk surface web sources, encrypted chat rooms, Telegram groups, Internet Relay Chat networks, FTP Server Data, Data Leak records and Paste sites.

WHAT WE MONITOR

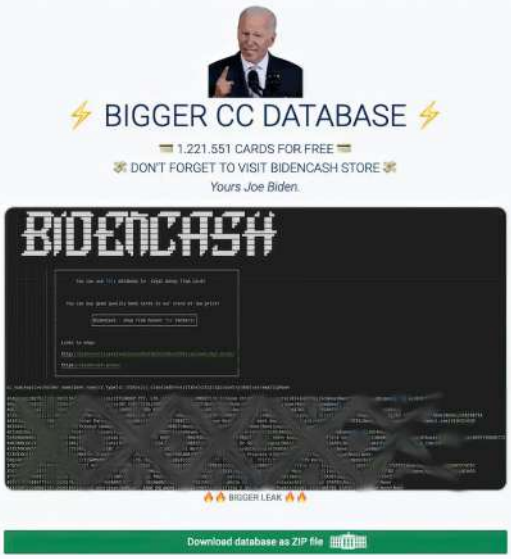
Our platform can scan for various mentions of targeted brands, intellectual property, domains, and Personally Identifiable Information (PII) of executives or employees such as email addresses, account credentials and identification documents. We also search for regularly updated data leak databases for PII relating to your organisation.

BANK IDENTIFICATION NUMBERS MONITORING

Monitoring the deep and dark web for Bank Identification Numbers (BINs), is an additional service we provide to financial institutions. Phishing pages are more prominent today than ever before, and that makes the theft of credit card numbers and personal information from individuals impossible to stop.

Stolen credit card details can be bought on dark web marketplaces for as little as $15 USD and PayPal account credentials are sold for a measly $10. Some dark web marketplaces even give away large numbers of credit card details for free as part of a promotion. For instance, in October 2022, a dark web carding market called 'Biden Cash' released over 1.2 million credit cards for free to promote their marketplace, allowing anyone with ToR access to download them for free and conduct financial fraud. We believe our monitoring tool can provide immense value, as knowing about a leaked credit card provides the ability to prevent the criminals from using it.

EXAMPLE OF THE 'BIDEN CASH' FAKE PROMOTION



sales@fraudwatch.com www.fraudwatch.com security@fraudwatch.com

FRAUDWATCH
Digital Brand Protection

TYPES OF DATA WE MONITOR

Brand Keywords/Domains:
- Brand, company, financial institution
- Domains
- Intellectual Property
- Data breach indicators

Executive Monitoring/PII:
- Name
- Email Address
- Account Credentials
- Personally Identifiable Information (such as ID/Drivers Licence or Passport numbers)
- Breached Data containing PII of an individual/executive

BINs/Credit Card Monitoring:
- Monitoring Bank Identification Numbers to identify stolen credit cards

CHANNELS / MONITORED SOURCES

High-Risk Surface Web - Dark Web:
- ToR
- I2P
- ZeroNet

Deep Web:
- FTP Server Data
- Data Leaks
- Authenticated Hacker Forums
- Encrypted Chat Platforms
- Telegram Groups
- Internet Relay Chat Rooms (IRC)
- Discord groups
- Paste Sites

What the Service Includes:
- Historical search option with potential to go back up to 8 years
- Access to billions of records
- Daily automated new scans performed for relevant intel across our extensive data set
- Notifications of new results
- Access to records via an active dashboard with visualised data
- Ability to securely access, download, view, sort and delete records

What Data Is Discovered:
- Compromised login credentials of internal users (executives/employees)
- Compromised personal information of internal users (executives/employees)
- Compromised login credentials of customers
- Compromised customer credit card information
- Legitimate or forged Bank Statements
- Payment application login credentials
- Mentions of a BIN in a targeted campaign
- Indicators of compromise (such as data logs)
- Indicators of Compromise through domains
- Intel on an upcoming or ongoing attack
- Leaked employee or customer data from a breach
- Compromised Crypto Wallet credentials
- Compromised Bank accounts
- Bank accounts used for money laundering
- Intellectual property
- Methods used by criminals to circumvent security measures
- Methods used by criminals to commit fraud
- Access to digital assets/artifacts (such as phishing kit, tutorials, config files)

GLOBAL SERVICE COVERAGE

Asia Pacific Head Office
+61 3 9887 6777

EMEA
+44 20 3974 1444

North America
+1 415 449 8800

sales@fraudwatch.com

www.fraudwatch.com

security@fraudwatch.com