

webhose.io

Protecting Fortune 500 Companies With Dark Web Monitoring

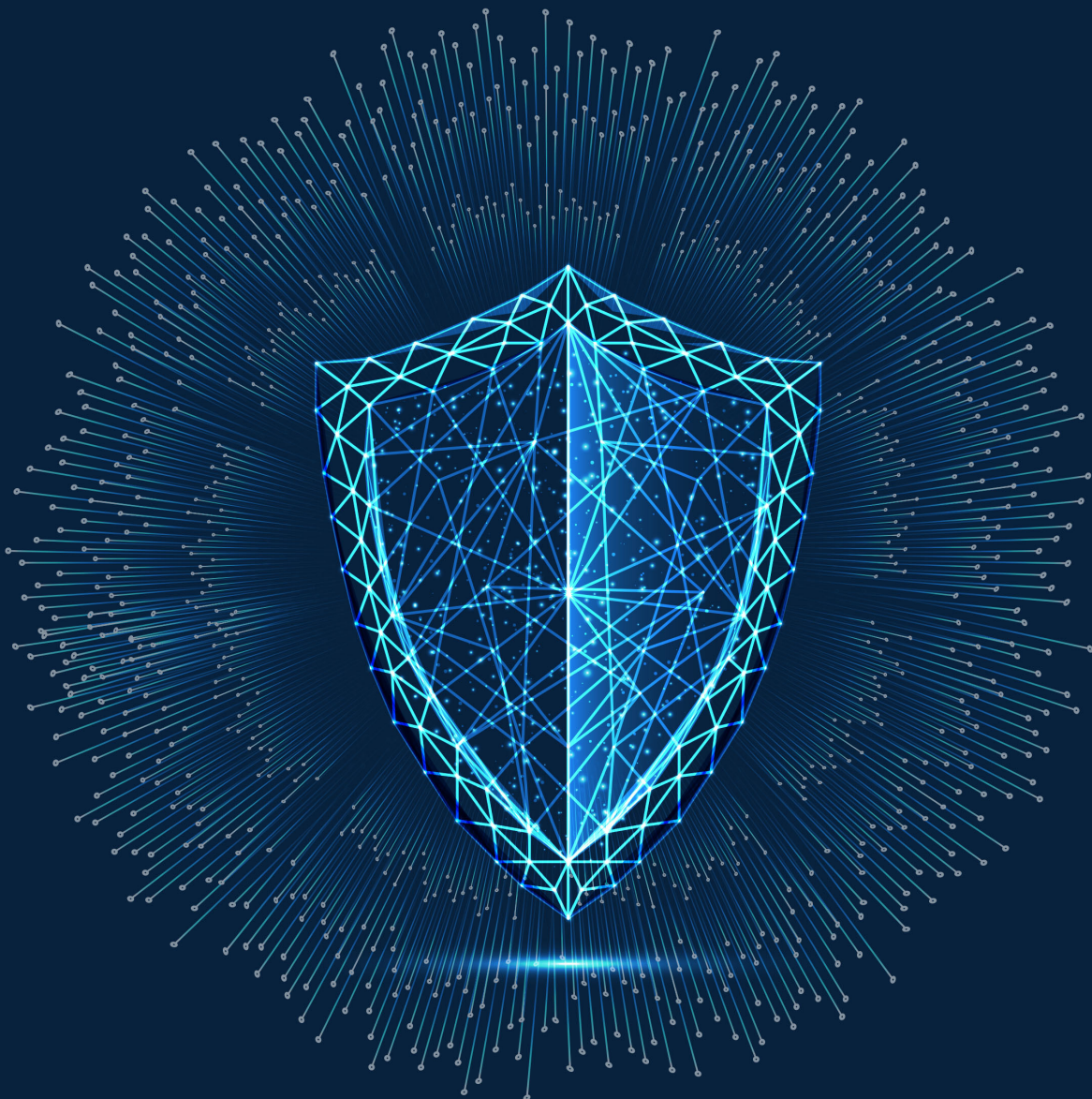


Table of Contents

Introduction	3
Executive Summary	4
Methodology	
Cyber Threat Categorization Across Multiple Industries	5
The top threats found in the Webhose Cyber API	
Threat categorization in the Cyber API and Data Breach Detection API	
Threats to the Technology Industry	7
Apple.com accounts leak discovered	
Exploitation of Microsoft vulnerability	
Threats to the Financial Services Industry	8
Western Union credit cards and PII leak	
OpenBullet configs to Paypal.com discovered in Cracking Pro forum	
Threats to the Retail and Wholesale Industry	9
Walmart carding methods exposed freely in the dark web	
Ebay gift cards for sale	
Threats to the Media Industry	10
Sharing of Netflix accounts revealed in Telegram	
Copyright infringement of a Disney movie	
Threats to the Telecommunications Industry	11
AT&T breach	
Verizon SIM swap exposed	
Threats to the Automotive and Manufacturing Industry	12
Executive threat to CEO of Tesla	
Threats to the Food and Supermarket Industry	13
Stolen Starbucks gift cards exposed	
Threats to the Apparel and Clothing Industry	14
Nike chargeback fraud	
Threats to the Aerospace Industry	15
Boeing emails leaking inside info from Pastebin	
Threats to the Insurance Industry	16
Revealing leaked records from Principal	
Threats to the Pharmaceutical and Healthcare Industries	17
Sale of Pfizer medicine revealed in the TOR network	
Aetna company database exposed	
The Future of Threat Intelligence	18
The Importance of Risk Monitoring	19
The goal of risk assessment	
About Webhose	20
Contributing Authors	20
Noa Hassidim	
Ziv Fried	
Liran Sorani	

Introduction

From the Tokopedia data breach compromising over 90 million users' personally identifiable data (PII) data, to the SolarWinds supply chain attack which affected approximately 18,000 companies and is still under investigation, hackers and dark web criminals clearly proved in 2020 that they are a serious threat to the security of many organizations. Not only are the digital assets of organizations in danger, but risks can also originate from their supply chain - as we saw in the recent Lockbit ransomware attack in December.

These attacks had wide-ranging consequences, both in monetary terms as well as in consumer trust. According to Cyber security firm [McAfee](#), cybercrime incidents could cost the world up to \$1 trillion in 2020. These damages continue to rise, as dark web security trends last year also showed an increase in ransomware attacks, costing \$8,100 per incident on average in 2020. Experts estimate that in 2021, a new attack will occur every 11 seconds. In addition, experts predict a rise in the data breaches that compromise PII information, with 540 data breaches occurring at the first half of the year alone and more than 100 million records being exposed.

In response to these threats, Webhose has developed a data collection service that not only transforms unstructured dark web content into machine-readable data feeds but also provides threats signals from the darknet from a wide range of sources. This coverage includes millions of dark web posts over a wide range of networks (including TOR, OpenBazaar, Zeronet and I2P) as well as messaging platforms (including Telegram, IRC and Discord). Granular filtering and enriched entity capabilities allow the uncovering of specific data such as crypto addresses, phone numbers, emails, or IP addresses of dark web criminals, or any PII data that is found leaked online. This type of structured and unstructured web data is available in over 115 languages.

This report is intended to be a guide to how Fortune 500 companies in different industries can better understand the threats facing them and how they can use a web data service such as Webhose to detect these threats in advance.

Executive Summary

This report includes:

- How Webhose categorizes cyber threats across multiple industries
- Methodology and research in Webhose's Cyber API and Data Breach Detection API
- Examples of cyberthreats to Fortune 500 from 2020 in a wide range of industries
- Best practices for cybersecurity experts looking to guard against cyber threats in 2021 and beyond
- Key insights from 2020 from cyber threats in the deep and dark web for Fortune 500 companies
- The importance of risk monitoring for global enterprises

Methodology

Webhose examined hundreds of posts from both its [Cyber API](#) and [Data Breach Detection API](#) that includes sources from the deep web, TOR (.onion), Telegram channels, Discord servers, I2P, Zeronet forums, OpenBazaar, and IRC chat. Each of these sources contain illicit content of dark web activities related to hacking and cybercrime, illegal trafficking (drugs, weapons and humans), stolen credit cards and more.

Webhose's dark web coverage includes:

- Thousands of leaked credit cards detected daily from the Cyber API over the past year
- More than 100K posts from TOR network daily in 2020
- Access to and crawling of hundreds of closed, sensitive forums and groups
- Five times more content from Telegram now than we had in Q1 2020, with improved coverage of topics such as white supremacy, carding, hacking and data breaches

Webhose's Cyber API receives the searched terms either as freetext (e.g. illegal drugs OR MDMA) or as a filter (e.g. by language or domain). We also have a filter called enriched category which returns results related to a specific topic (e.g. illegal drugs, hacking, etc). With the filter, you can easily screen irrelevant content, focusing on results related to your specific query (for example results only related to drugs but not hacking).

Webhose's Data Breach Detection API is dedicated to leaked and compromised credentials and PII data, such as emails and passwords, phones, credit cards, social security numbers, passports and usernames. Querying and monitoring this endpoint will allow users to be aware of compromised entities of their customers or employees. The data is collected from leaked databases and leaked entities retrieved from our cyber coverage. All security threats we found and listed in this report for the Fortune 500 companies listed are from 2020.

While investigating the Webhose's extensive coverage of data in both the Cyber and Data Breach Detection endpoints, we found an average increase between 2019 and 2020 of about 150% in cyber threat mentions from the darkweb. We also saw from our data that the communication, cloud, e-commerce, and financial sectors were the most popular and most targeted industries in 2020.

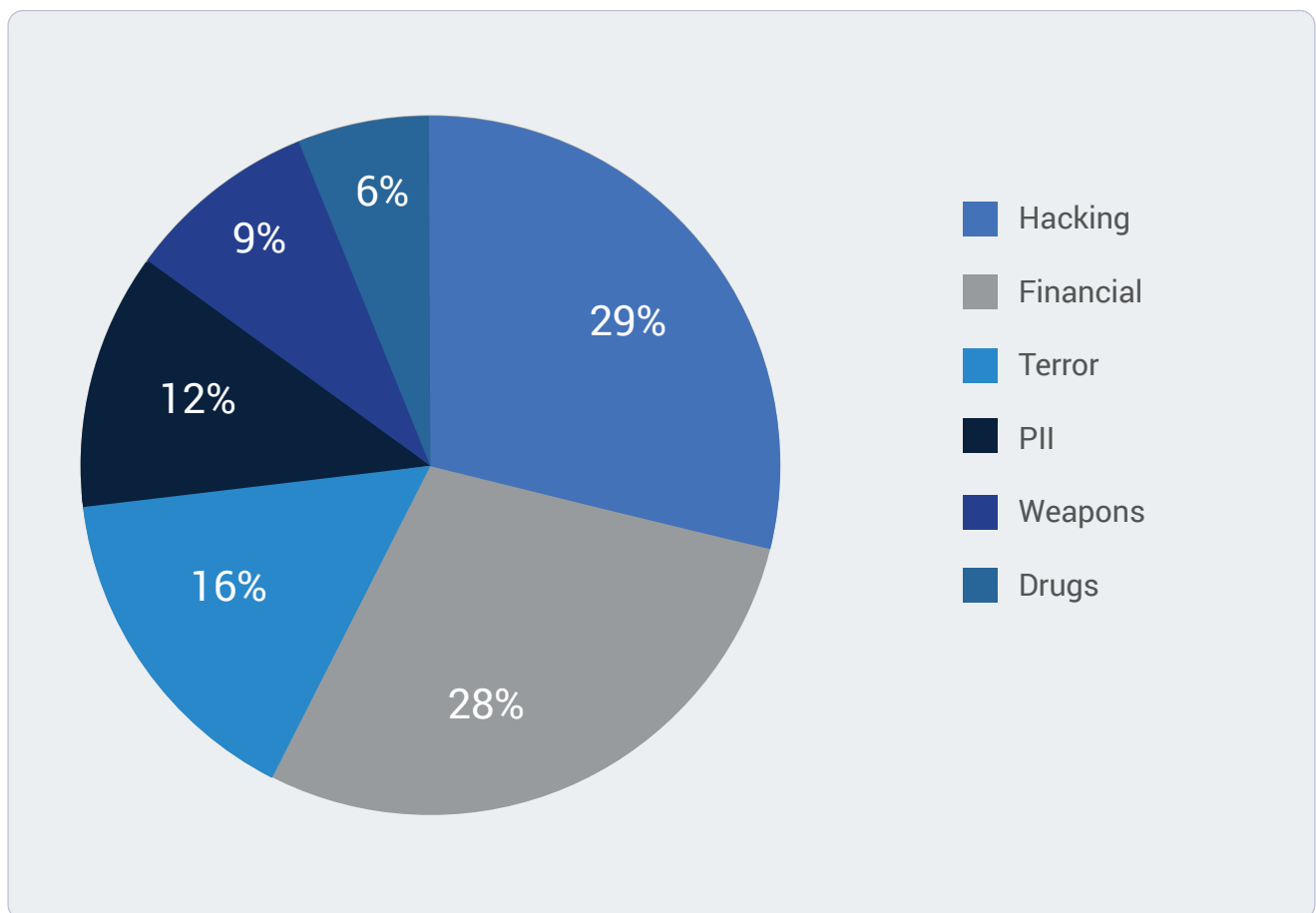
Cyber Threat Categorization Across Multiple Industries

For this report we have retrieved data from both our Cyber API and the Data Breach Detection API and categorized them across multiple industries. This report presents different examples of risks to Fortune 500 companies in each of these categories and explains how these threats should be monitored and identified so these companies can best defend themselves against those threats.

The top threats found in Webhose Cyber API

Hacking and financial fraud threats are the most common among the illicit topics covered in the Cyber API, followed by terror, PII data, weapons and drugs.

Threats by Category - 2020

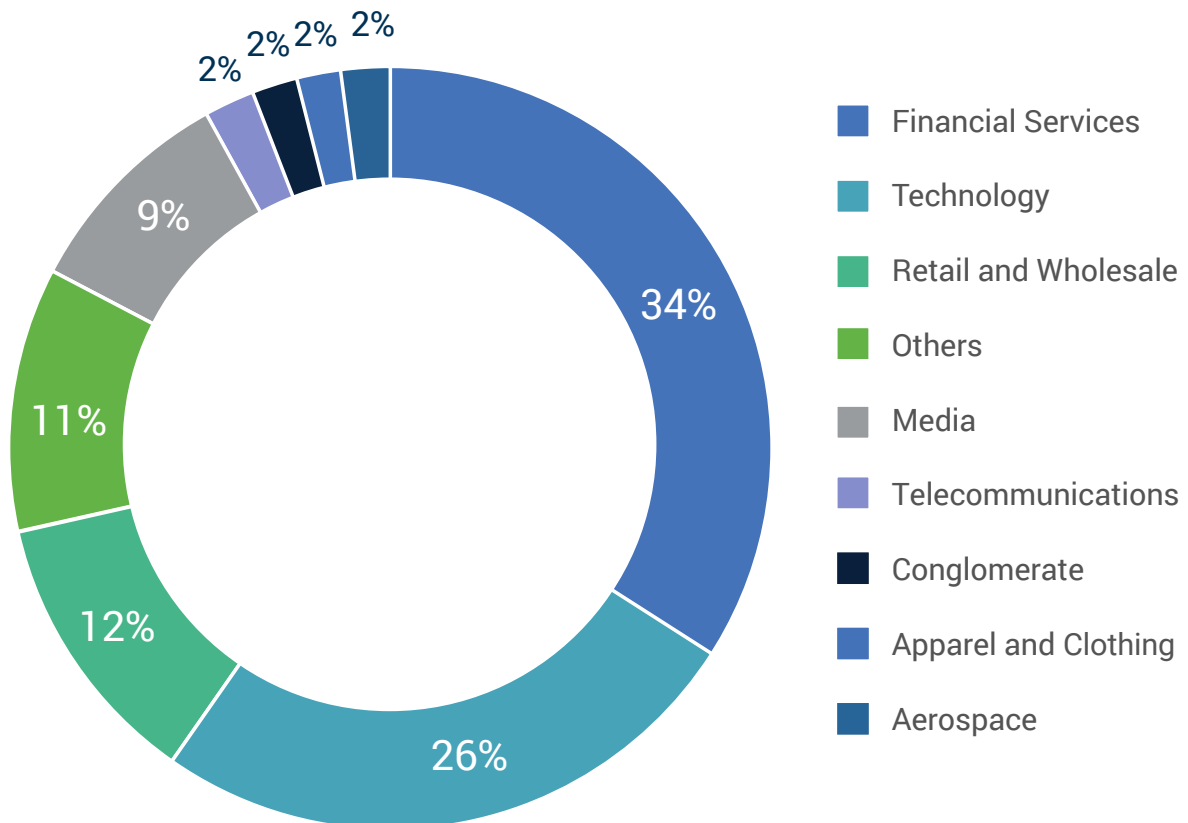


How Webhose categorizes threats in the Cyber API

Threat categorization in the Cyber API and Data Breach Detection API

The following pie chart shows the percentage of cyber threat mentions for each industry in the Fortune 500 companies both from our Cyber and Data Breach Detection endpoints over the past year. The chart shows that companies in the financial, technology, retail and wholesale fields are the most targeted and have the most cyber threat mentions from both endpoints. We will give examples of threats in each industry as well as in the pharmaceutical industry in this document.y.

Approximately 72% of the cyber threat mentions are focused on the financial, technology and retail and wholesale industries.



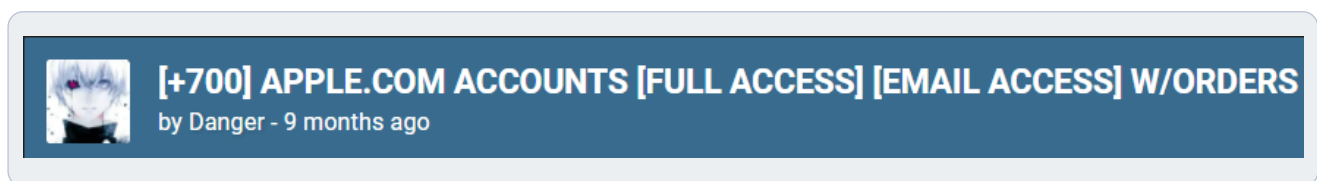
Webhose discovered leaked emails of 93% of the Fortune 500 domains in the last 6 months. In addition, 98% of Fortune 500 companies were mentioned in the dark web in the last 12 months.

Threats to the Technology Industry

This sector includes technology giants such as Apple, Microsoft, Facebook, Dell, Intel, etc. Threats to this sector most frequently include account leaks, PII leaks, cyberattacks, and illegal sales (and possibly counterfeit) of products.

Apple.com accounts leak discovered

This example shows an actor sharing hundreds of customer accounts from the official Apple site in a post published on Cracked Forum. This is a surprisingly common phenomenon in hacking forums, as those types of accounts are usually connected to multiple services (e.g., an Apple account can be an email address, an Apple Store account, an Apple music account, etc).



Post of sale of Apple accounts in a hacking forum from the Cyber API

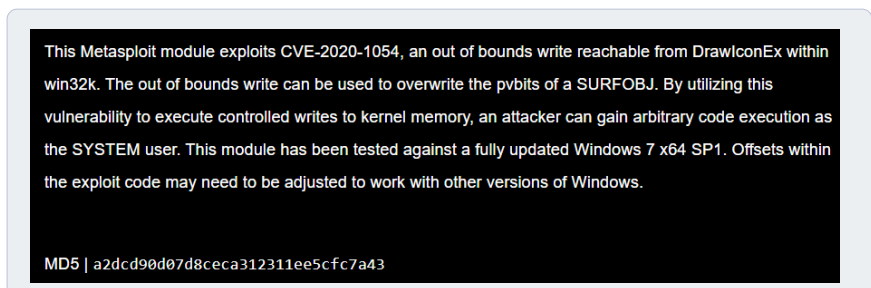
Approximately 12% of all cyber threat mentions of Apple and its products are intentions of selling Apple's products illegally online.

Exploitation of vulnerability in a Microsoft component exposed

In this example we see an exploit kit for one of the latest Microsoft vulnerabilities is published at the end of 2020 in a site named 'Exploit Collector.' Early detection of those methods to exploit vulnerabilities can put a stop (and a patch) to those vulnerabilities being used by threat actors. Sharing of those kits online could lead to further exploitation of the vulnerability and could also lead to future attacks on the vulnerable component.



Post publicizing Microsoft vulnerability exploitation from the Cyber API



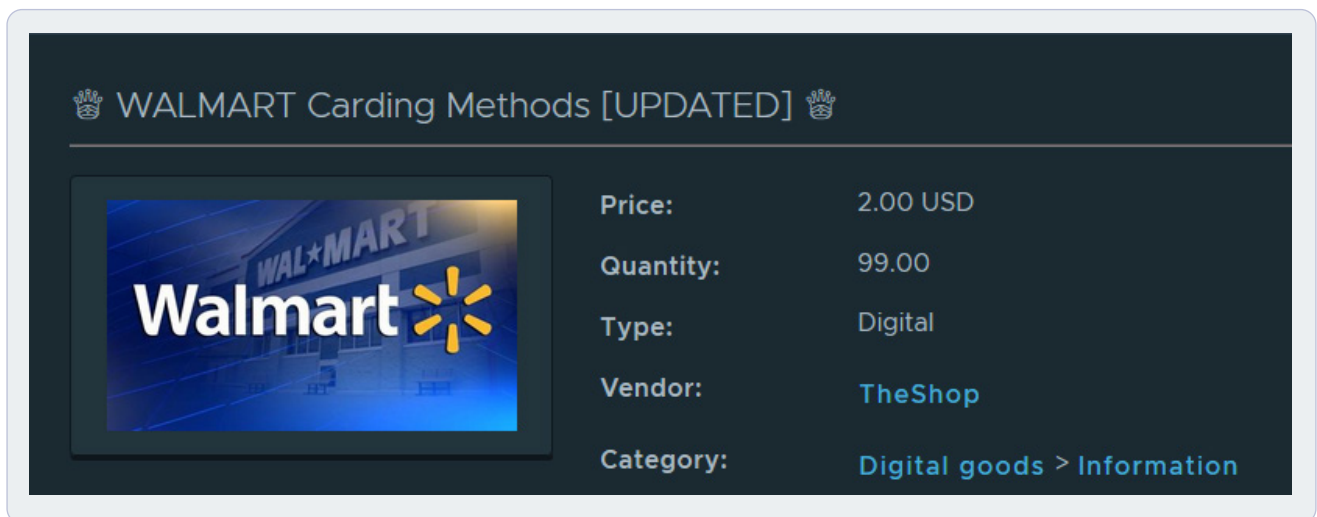
Post publicizing Microsoft vulnerability exploitation from the Cyber API

Threats to the Retail and Wholesale Industry

In 2017, the volume of retail spending worldwide was at \$23 trillion. According to Statista, retail sales are projected to amount to around \$30 trillion by 2023. The sheer magnitude of volume is what lures hackers to attack organizations in this sector. As a result, it faces continuous threats such as counterfeit, cyberattacks, carding fraud, financial fraud, and PII leaks.

Walmart carding methods exposed freely in the dark web

Founded in 1962 by Sam Walton, Walmart has a revenue of \$524 billion. In this example, we can see an actor who offers carding methods for sale on Walmart. Carding is a type of fraud in which a thief steals credit card numbers, validates that they work, and then uses them to buy prepaid gift cards. This could lead to both PII leaks for Walmart customers and loss of money for the company itself.

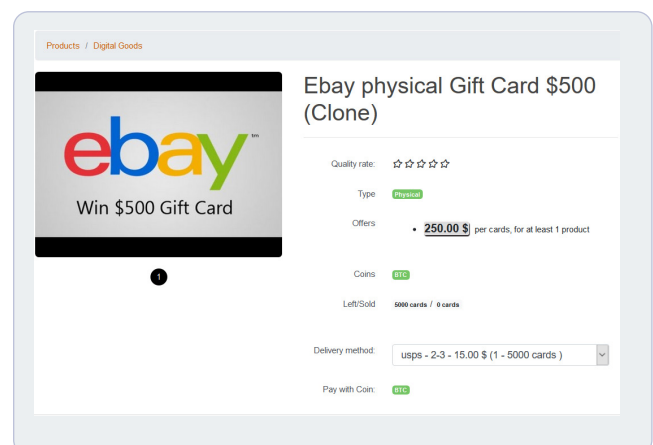


Post of sale of Walmart carding methods from the Cyber API

Of Webhose posts from the deep and dark web that are tagged as financial, PII or hacking, 2.5% are posts that mention Ebay or Walmart.

Ebay gift cards for sale discovered

Headquartered in San Jose, eBay is an e-commerce company with a market capitalization of \$42 billion. Here an actor offers for sale a \$500 eBay gift card at a price of only \$250. He claims to have 5000 cards in stock, which may indicate he stole them from eBay and may have a method of generating them in bulk. Stolen gift cards, especially if bought with stolen credit cards, can also cause damage to these types of major brands.



Post of sale of Ebay gift cards in the Cyber API

Threats to the Media Industry

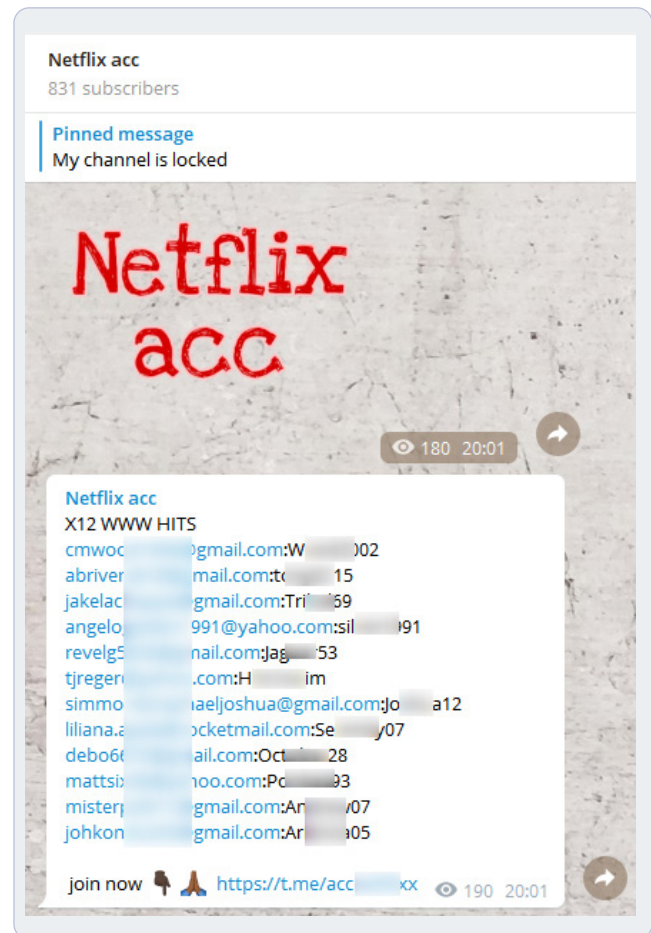
After the Disney+ hack just days after its launch in 2019, accounts were sold in the dark web for just \$3-11 each, and sometimes even leaked for free. With more than 10 million registered users in the first 24 hours, Disney+ and other popular media companies such as Netflix are targeted on a daily basis, mostly by actors selling counterfeit or fake Disney goods, but also for cyberattacks, PII leaks, carding fraud, and threats to their executives.

Sharing of Netflix accounts revealed in Telegram

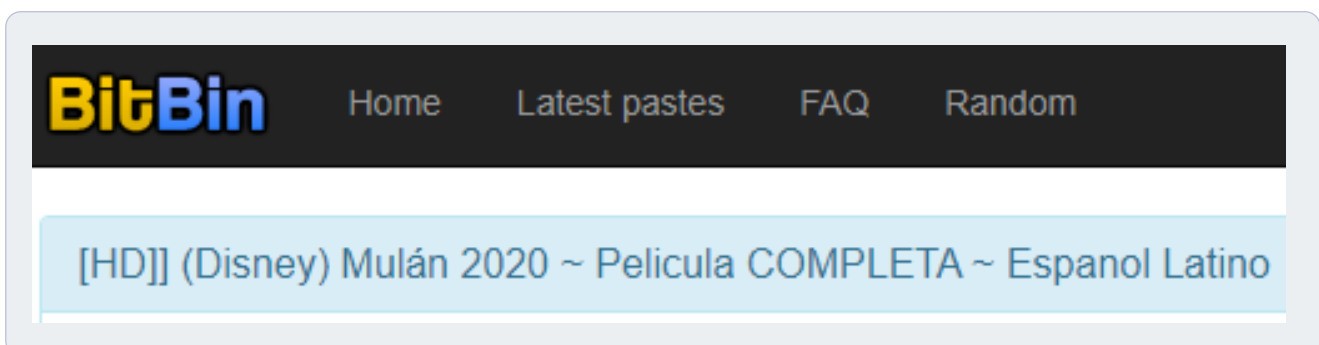
Headquartered in California and founded in 1997, Netflix now has a user base of 203 million. Here we see a Telegram channel that we have in our coverage and whose activity is to share Netflix accounts for free. The sharing of accounts can lead to theft of private information, leading to damage to Netflix's brand reputation.

Copyright infringement of a Disney Movie discovered

Founded in 1923, the Disney company has a global revenue of almost \$66 billion. In this example an actor is sharing links to free streaming of the Disney movie Mulan published last October. This example is only one out of many examples of copyright infringement cases appearing in the dark web. Copyright infringement can significantly affect company revenue, causing serious loss of income and harm the future activity of the company - especially if the infringement occurs before the official release.



Post of sale of Netflix account in Telegram from the Cyber API



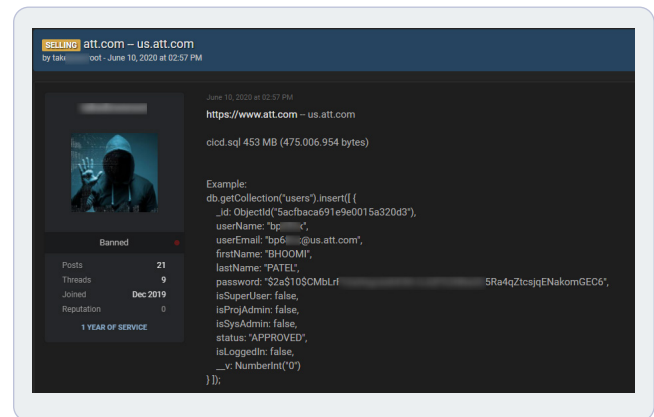
Links to Disney movie Mulan from the Cyber API

Threats to the Telecommunications Industry

After the phenomenal cyberattack on ten undisclosed telecom companies in Africa, Europe and Asia, we felt obligated to take a look at the risks on this sector in 2020. These include database leaks, cyberattacks and carding fraud.

AT&T breach revealed

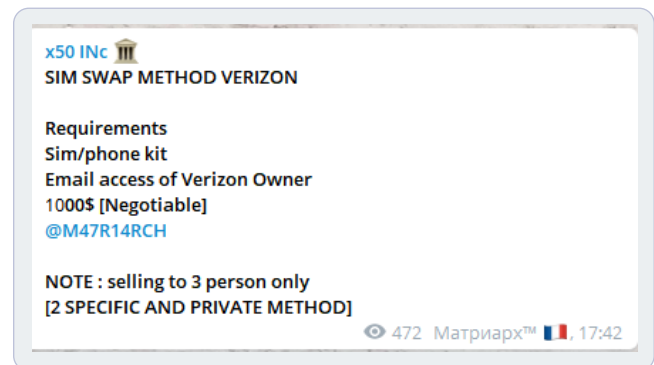
With a revenue of 181 billion, AT&T is a multinational communications company based in Dallas, Texas. In this example an actor is selling a database from the official site of AT&T - ".att.com." The actor posted an example of one record from this breach with details such as email address, user name and full name. Data breaches or early signs of the occurrence of one (e.g. selling a company's database, the existence of a phishing page of the company, known hacking methods and more) should be monitored. Gone unnoticed, the damage can increase and the impact on the company could be severe.



Publication of AT&T breach from the Cyber API

Verizon SIM swap exposed

Here we see an actor offer the sale of a method for a SIM swap fraud for Verizon SIMs. A SIM swap is a type of fraud that generally targets a weakness in two-factor authentication and two-step verification. This fraud method causes the phone to lose connection to the network and for the fraudster to receive all the SMS and voice calls intended for the victim. This could lead to real damage to the company's reputation and trust of its customers in their products.



Post about sale of Verizon SIM swap method from the Cyber API

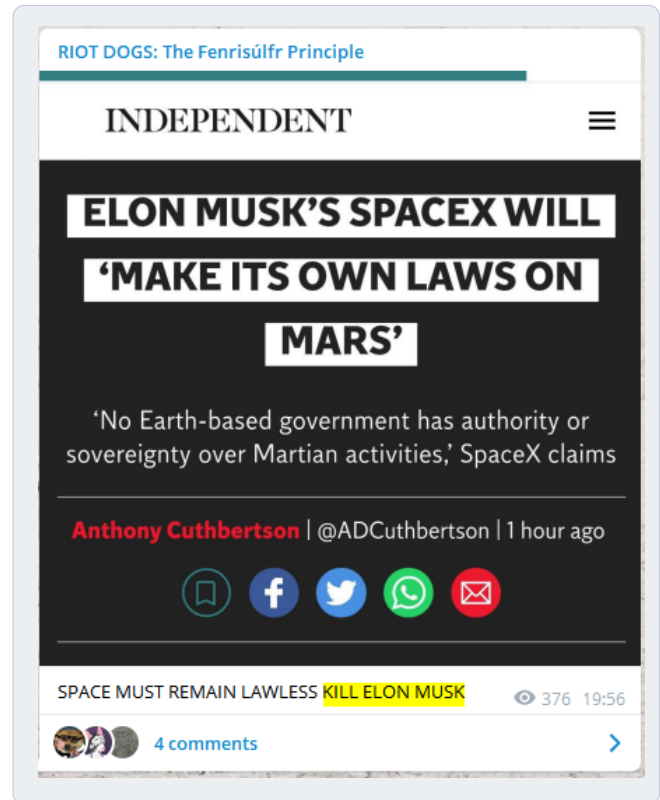
Approximately 78% of all cyber threat mentions of SIM swapping are guides and methods to perform this type of scam.

Threats to the Automotive and Manufacturing Industry

As people gain positions of power in high-profile companies, they risk greater exposure to the public. Public opinion of them can include extremist rhetoric such as conspiracy theories, defamatory calls and even threats of violence against them.

Executive threat to CEO of Tesla revealed

Founded in 2003 by Elon Musk, Tesla is a world leader in the manufacture of electric cars. In this example, an actor makes a threat against the CEO of Tesla, Elon Musk, in a Telegram channel. The data Webhose gathers helps organizations monitor those kinds of messages and gain increased executive protection for these types of high-profile companies.



Threats to the Food and Supermarket Industry

Scams against supermarkets and food suppliers usually appear as data leaks, such as account, credit card or gift card information, or as tutorials on how to perform such scams.

Stolen Starbucks gift cards exposed

Founded in 1971, Starbucks has become the largest coffeehouse chain in the world. Here we can see an actor sharing two Starbucks gift cards for free that were possibly either hacked or stolen and still have a balance in them. Sharing these types of gift cards for free could harm the revenue of the company and lead to harm to the company's reputation, particularly if these gift cards were stolen.

The screenshot shows a forum post with the following details:

- Title:** STARBUCKS GIFTCARDS
- Author:** [Profile picture] by [Redacted] - 10 months ago
- Post Content:**
 - OP 10 months ago
 - ☆☆☆
 - Image of a man blowing a pink bubble.
 - 21 REP
 - 1.153 LIKES
 - Buttons: Dems, Contributor
- Text:** Call Starbucks and check before using!
1 (800) 782-7282
Leave a like don't leech 🐸
- Hidden Content:**

6037	3054 - 10.88 USD
6135	7576 - 10.43 USD

Stolen Starbucks gift cards from the Cyber API

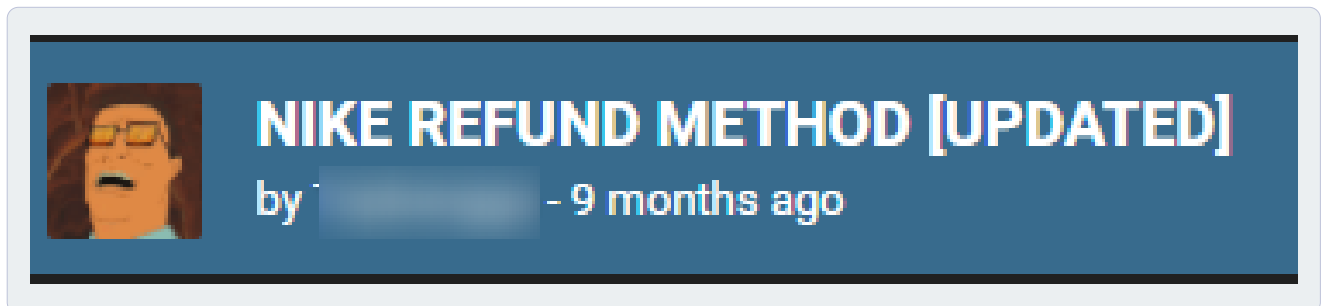
Threats to the Apparel and Clothing Industry

As COVID-19 struck and malls, shopping centers and street shops were closed, consumers started buying more clothes and footwear on the internet. [Research](#) shows an increase of 2% in the number of people ordering online at least one item of clothing or accessories. In our research at Webhose we were able to detect counterfeit items of high-end brands, fraud tutorials, and leaked databases of different fashion brands, etc, related to this industry from the past year.

Nike chargeback fraud

A global leader in footwear, Nike is headquartered in Oregon. In this example, the actor posted a comprehensive explanation on how to get a refund on Nike products without returning them to the company. With this type of fraud, also known as chargeback fraud, customers can resell their purchase, or worse - scam the company for a refund without returning the product. This is equivalent to stealing money from the company.

This type of fraud harms company revenue and could lead to a large black market of its products. Since new refund scams are constantly distributed and updated on the dark web, companies should consider dark web monitoring as a way to be aware of and defend themselves against the latest refund scams.



Nike chargeback fraud found in the Cyber API

Approximately 70% of Nike's cyber threat mentions are retrieved from chat applications, primarily on Telegram and Discord. These mentions are primarily related to carding scams against a brand or in a brand's website, leaked accounts, and illegal sales of a company's products.

Threats to the Aerospace Industry

In 2020 we witnessed the leaks of confidential information of several aerospace companies or subsidiaries in the dark web. One of these - executed by the [Maze](#) ransomware group - stole 1.5 TB of data.

Boeing emails leaking inside info from Pastebin

With its headquarters in Chicago, Boeing is the world's largest aerospace company. In some cases of data leaks, we can see internal email conversations of Boeing employees, such as this example from Pastebin. The exchanged leaked emails we see in the paste focus on issues and dilemmas of work modules between the company employees. In the email thread discussions we can also find information about the company's competitors. Leaks of internal communication and confidential information can lead to a serious PR crisis for the company.

boeing-mail-ussa-defects
pastebin.com | 2020-02-01

To:
CC:
Sent:
Subject:
Attachments:
Boeing Employee
j Boeing Employees j
2 / 26/2613 12:48:44 PM â€™™
RE: Synthetic Airspeed
737 Unreliable airspeed version 25 .pdf

To:!
Cc:i
Boeing Employees
Subject: RE: Flight Transition costs
Thanks
28
The only risk is that they will ask us to provide financial support to cover the worse case scenario... As you know, [redacted] is throwing money at the flip, so might a good strategy be to hold firm on the logic of the lower end scenario?

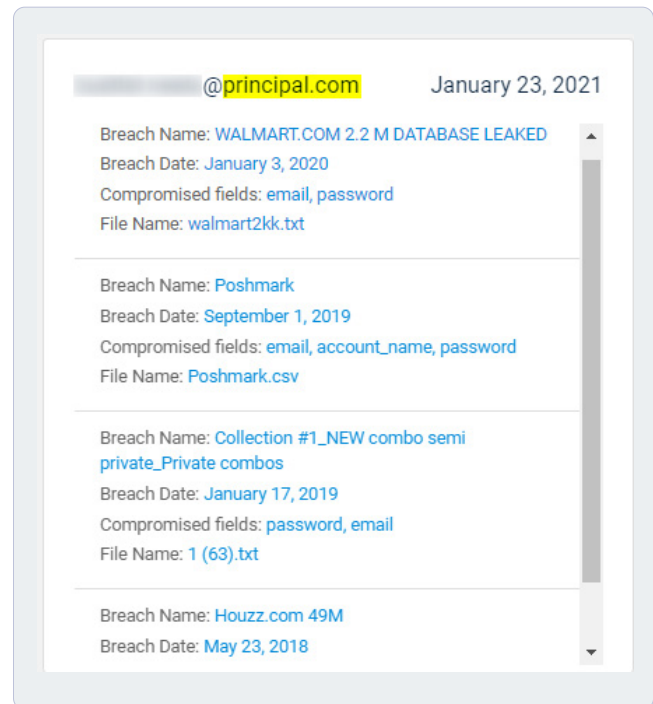
Boeing employee email from the Cyber API

Threats to the Insurance Industry

The most common threat to insurance companies in 2020 is leaked PII data. The data breach incident last December from the Israeli insurance company, Shirbit, is just one of the companies that have fallen victim to a cyberattack and had their data sold or shared online. Data of both employees of insurance companies or its customers are at constant risk.

Revealing leaked records from Principal

Principal is a global investment management and insurance company headquartered in Iowa. This example shows a screenshot from the Webhose Data Breach Detection API output that shows leaked records of a customer or employee of Principal, a global investment management and insurance company. We can see this leaked record appeared in four different leaks that occurred between the years 2018 - 2020. The leaked information can be used for future attacks, such as authorizations to operate (ATOs), business email compromise (BECs) or phishing.



Post of leaked records of Principal from the Data Breach Detection API

Threats to the Pharmaceutical and Healthcare Industries

Last year saw more data breaches hit the healthcare industry than any year previously. According to the Health and Human Services (HHS) Office for Civil Rights, a total of 616 data breaches of 500 or more records were reported, with approximately 28,756,445 healthcare records exposed, compromised, or disclosed without permission. The most common mentions in the dark web are related to brand abuse (mostly of counterfeit medicines or other products), medical records leaks, PII leaks, and cyberattacks.

Sale of Pfizer medicine revealed in the TOR network


With an annual revenue of over \$51 million, Pfizer is one of the world's largest pharmaceutical companies. The actor in this example offers Xanax, an antianxiety medication manufactured by Pfizer, for sale in a known dark web marketplace based in the TOR network. The sale of branded medications can seriously harm people who may consume this medication as well as Pfizer's brand reputation.

Almost 40% of the cyber threat mentions of Pfizer over the past year are related to illegal trade of its medications.

Pfizer Xanax 2MG Bars X10



(100%) Seller Level 0 (6)
Trust Level 0

Verified Seller :  / **Trusted Seller :** 

Positive Feedback : (100%)
Member since : Dec 02, 2019
Last Login : Sep 14, 2020
Sales : 6
Orders : 0

Sold : 3 Times
Origin Country : United Kingdom
Ship to : World Wide
Payment : Full Escrow
Product class : Physical Package
Quantity : Unlimited Available

Sale Price : 12.87 USD / 0.00123458 BTC
Sale Price : 12.87 USD / 0.14990256 XMR
Sale Price : 12.87 USD / 0.24050024 LTC

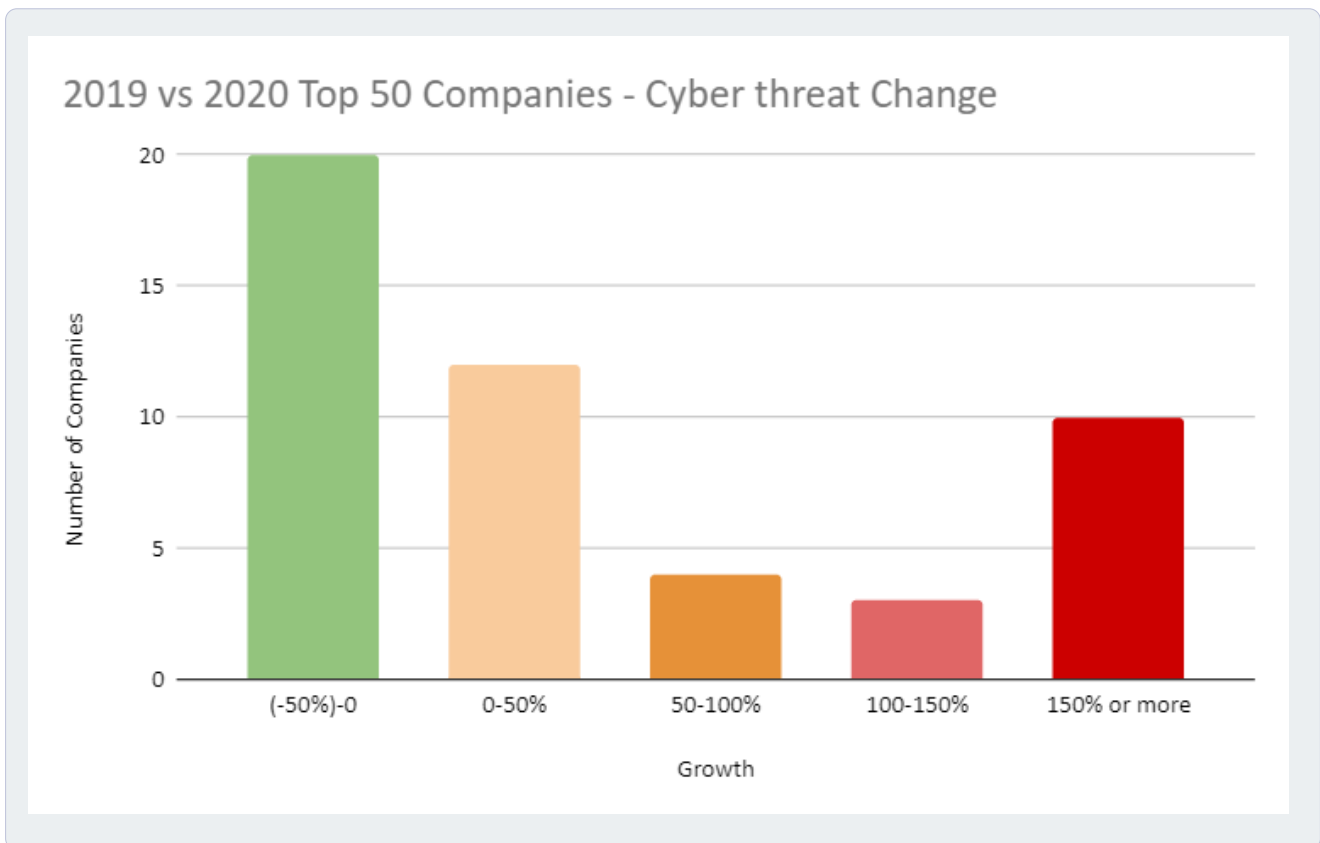
Aetna company database exposed

Aetna is a global healthcare company with a market capitalization of almost \$70 million. The actor in this example offers to sell website databases which include the "aetna.com" domain belonging to the Healthcare company Aetna. Although we aren't sure of the exact data contained in this database, we do know that the sale of it could lead to further hacking attacks, the leaking of personal information of its customers, and possibly the leakage of private medical information. These types of leaks that can cause damage to the Aetna brand.

<https://www.rtt.co.za/> RTT INTELLIGENT LOGISTICS. <https://www.scutum.fr/> SCUTUM. <https://www.aetna.com/> AETNA HEALTH INSURANCE. <https://mmwlaw.ca/> MORRISON WATTS L&E LAWYERS. <https://freschesolutions.com/> FRESCHÉ SOLUTIONS. <http://haverstock.com/> HAVER STOCK. <https://piaggiogroup.com/en/piaggio-automobile>. <https://www.dieffenbachs.com/> Dieffenbach's. <https://www.windwardssoftware.com/en-us/windwards-software>. <https://www.silverlake.com/> SILVERLAKE. <https://www.enrustenergy.com/> ENTRUST ENERGY. <https://www.misterfly.com/> MISTERFLY. **I have DB access to all the websites above, One website's DB price is \$275** and the price of them as a bundle is \$2500, if you wanna buy the bundle I can give you one website's DB as sample. If you need it, contact me at blackor@secmail.pro

The Future of Threat Intelligence

By thoroughly investigating extensive coverage of data in both the Webhose Cyber and Data Breach Detection API, we were able to compare the total number of cyber threats mentioned for the top [Fortune 50](#) companies in 2020 such as Walmart, Exxon Mobil, Apple, AT&T, etc., and found an average increase from 2019 to 2020 of almost 150% in cyber threat mentions from the dark web.



Cyber threats from Webhose Cyber and Data Breach Detection APIs 2019-2020

This graph represents the comparison in the growth of cyber threats between 2019 and 2020 for these top 50 Fortune companies. Although 20 of these companies were mentioned 0-50% less in the dark web, the remaining 30 had many more cyber threat signals. (i.e. gathered more risk). Ten of these companies had an increase of 150% in the number of cyber threats mentioned. In other words, they were identified as a highly valuable target for cyber attacks.

We also saw from our data that the communication, cloud, e-commerce, and financial sectors were the most popular and most targeted industries in 2020.

The Importance of Risk Monitoring

Cyber risks are used to identify, estimate, and prioritize risk to organizational operations, assets, individuals, organizations and nations. These risks are a direct result of the use of information systems.

Here are a few of the main benefits of cyber risk monitoring for global companies:

- **Mitigating cyber threats and preventing future attacks** - Implementing a cyber risk management strategy helps to identify the threats to an organization. Developing a risk treatment plan assists in addressing the risks and puts the correct defences in place, reducing future threats from cyberattacks.
- **Reducing costs and protecting revenue** - The motive of many attackers is financial gain. This means any organization can be affected. It is important for organizations to minimize the risk of falling victim to an attack and mitigate revenue loss. An added benefit is that complying with certain regulations as part of the cyber risk strategy will help organizations avoid hefty fines that can be given for non-compliance.
- **Increase business reputation** - Proving to your clients and customers that you take cyber security seriously gives your organization a competitive edge. Organizations who prioritize their customer data gain their trust, resulting in increased loyalty and long-term business success.

The Goal of Risk Assessment

The primary purpose of a cyber risk assessment is to help inform decision makers and support proper risk response. A cyber risk assessment will assess the likelihood of the business' vulnerability to cyberattacks.

Knowing the risks and monitoring threat signals can help a company take preventive actions, such as:

- Install relevant IT protection against specific threats
- Educate the employees toward specific attacks
- Identify the damage that can be minimized or even completely removed, such as:
 - Loss of sensitive data
 - Impact on the organization reputation
 - Impact on the revenue stream

Through careful risk assessment and risk monitoring, global organizations across a wide range of industries can better defend themselves and mitigate against the types of threats mentioned in this report.

About Webhose

Webhose is the leading web data provider transforming unstructured web content into machine-readable data feeds. Its data feeds and historical archives include multiple data sources such as news sites, online discussions, dark networks, and much more. Webhose delivers comprehensive, up-to-the-minute, relevant coverage of the open, deep, and dark web to enterprise-level customers in a wide range of verticals.

Contributing Authors



Noa Hassidim

Noa Hassidim is the Senior Cyber Analyst at Webhose. She is responsible for monitoring and research for VIP customers, professional cyber consulting and cyber product marketing, which includes researching cyber intelligence market needs and trends and for Webhose's cyber marketing content. She brings to Webhose her experience serving in the elite 8200 unit of the Israel Defense Force as an intelligence web and OSINT analyst and training lead for the new analysts in the unit.



Ziv Fried

Ziv Fried is a Cyber Analyst at Webhose responsible for monitoring cyber risks as well as research for cyber customers. His responsibilities include researching the major dark networks in the Cyber API and managing the custom processes in order to ensure stable and constant dark web data. Previously, he was a data analyst and commander of a technological intelligence team in the 8200 unit of the Israel Defense Force.



Liran Sorani

With over 10 years' experience in the Intelligence and Cyber solutions, Liran heads the Cyber Business Unit at Webhose. He is an expert in the deep and dark collection of data as well as new network discovery and has vast experience in social media and dark web analysis. He has built and deployed dozens of intelligence solutions and services for security organizations across the globe.

The background features a repeating pattern of light blue circuit lines and padlock icons on a dark blue background. The padlocks are positioned within hexagonal shapes, and the circuit lines form a complex, interconnected network.

webhose.io

For more information about Webhose
Dark Web Monitoring and Data Breach APIs

Please visit [Webhose.io](https://webhose.io)