

2021 Identity Breach Report

PII Fuelling the Threat Economy:
How Crisis Creates Targeted
Vulnerabilities for Individuals,
Executives, and Brands

Table of Contents

- 01. Introduction: The Cyber Threat Landscape
- 02. About This Report
- 03. Executive Summary: Breach Report Key Findings

Section 1: 2020 Identity Breach Data Deep Dive

- 04. Top Breaches and Leakages of 2020
- 05. Most Impacted Sectors
- 06. Geographic Distribution
- 07. Breach Metadata
- 08. Most Frequently Exposed Attributes

Section 2: The Real-World Impact of Data Breaches

- 09. Threats Targeting Major Brands
- 10. Vaccines and COVID-19-Related Items for Sale in Dark Markets
- 11. Dark Market Economy
- 12. Breaches, PII, and the Disinformation Ecosystem
- 13. Deepfakes
- 14. Risks to Individuals, Businesses, and Institutions
- 15. Conclusion and Recommendations

Annex:

- 16. Data Verification/ Methodology
- 17. Glossary

01 Introduction: The Cyber Threat Landscape

The world has watched powerful countries and seemingly indomitable companies thrown into crises virtually overnight due to breaches, ransomware, disinformation campaigns, and cyberattacks. The speed, precision, and scale of these attacks reveal the serious nature of threat actors and the significant vulnerabilities of all digital citizens. Incidents like the SolarWinds and Colonial Pipeline cyberattacks created geopolitical and economic aftershocks, making headlines across the globe – but these are only two examples of breaches. What about the breaches that do not receive media coverage? What can this breach data tell us about the evolving tactics, techniques, and procedures (TTPs) of threat actors today? With every advancement in digital transformation and every new service brought online come new weaknesses that threat actors are ready to exploit, leaving enterprises of all sizes, public institutions, and individuals wondering what they can do to protect their valuable assets.

“With over 100 billion attributes and 45 billion curated identity records spanning 125 countries and 53 languages, we help organizations anticipate digital risks and safeguard critical business interests.”

Constella Intelligence is home to the largest breach data collection on the planet. With over 100 billion attributes and 45 billion curated identity records spanning 125 countries and 53 languages, we help organizations anticipate digital risks and safeguard critical business interests. Further, Constella has identified over 16 million malicious actors and protected more than 30 million customer identities over the past 5 years. We developed this report based on the breaches and leakages discovered in 2020, and our findings represent far more data breaches and leakages than just those reported in the media. Leveraging data from underground communities and forums, black markets, and the deep and dark web, this report's findings will help the world better prepare for future attacks as we navigate the volatile cyber landscape.

Right now, there are billions of breached and leaked identity records circulating throughout open sources, and threat actors leverage these valuable compromised credentials to build digital profiles and personalize their attacks—including phishing scams, social media fakes, account takeovers, impersonations and more. And given the complexity of the ever-changing nature of networks, servers, applications, mobile devices, and the cloud, coupled with the probability of human error, no single system or process can fully stop a determined adversary. As a result, public institutions, enterprises, and consumer portals must implement resilient systems that can quickly detect and recover from attacks.

While experts in digital risk protection, cyberintelligence, and cybersecurity continue to track and analyze cybercrime activity, it is important to raise global awareness related to these trends and assist in reducing the associated risks. This begins with learning and operationalizing the signs of abnormal or malicious activity, from malign influence campaigns around narratives that can contribute to vaccine hesitancy and negatively impact public health to counterfeit COVID-19 certificates and beyond. The 2021 Breach Report explores the prevalence, methods, and incentives of threat actors and cybercriminals when it comes to the digital environment in the era of COVID-19.

Kailash Ambwani, CEO of Constella Intelligence



About This Report

Constella has watched the TTPs of threat actors closely and developed this report based on breaches and leakages identified in 2020. In addition to the known breaches and leakages reported in the media, Constella detects information found in data dumps posted in open, but often transient, sources in the deep and dark web. This information is critical for a number of reasons. For one, breached credential data helps identity theft protection providers and cyber insurance, security, and fraud vendors to alert consumers on their exposures. Organizations also rely on this data as financial intelligence for anti-fraud, anti-money laundering, and know-your-customer programs for preventing account takeover activity. Further, cybercrime investigators operationalize breached data to gain intelligence on adversaries and threat actors.

Many of these breach corpuses are not known to the general public. Constella's automated crawlers and subject matter experts use a variety of sources to authenticate and verify the data, including:

- Underground communities and forums
- Black markets
- The deep web
- The dark web

Constella analyzes, verifies, normalizes, cleans, and attributes the data to further understand the severity of risks facing consumers and companies. Constella then alerts the impacted parties in order to mitigate risks. We assess the severity of risk based on multiple factors, including:

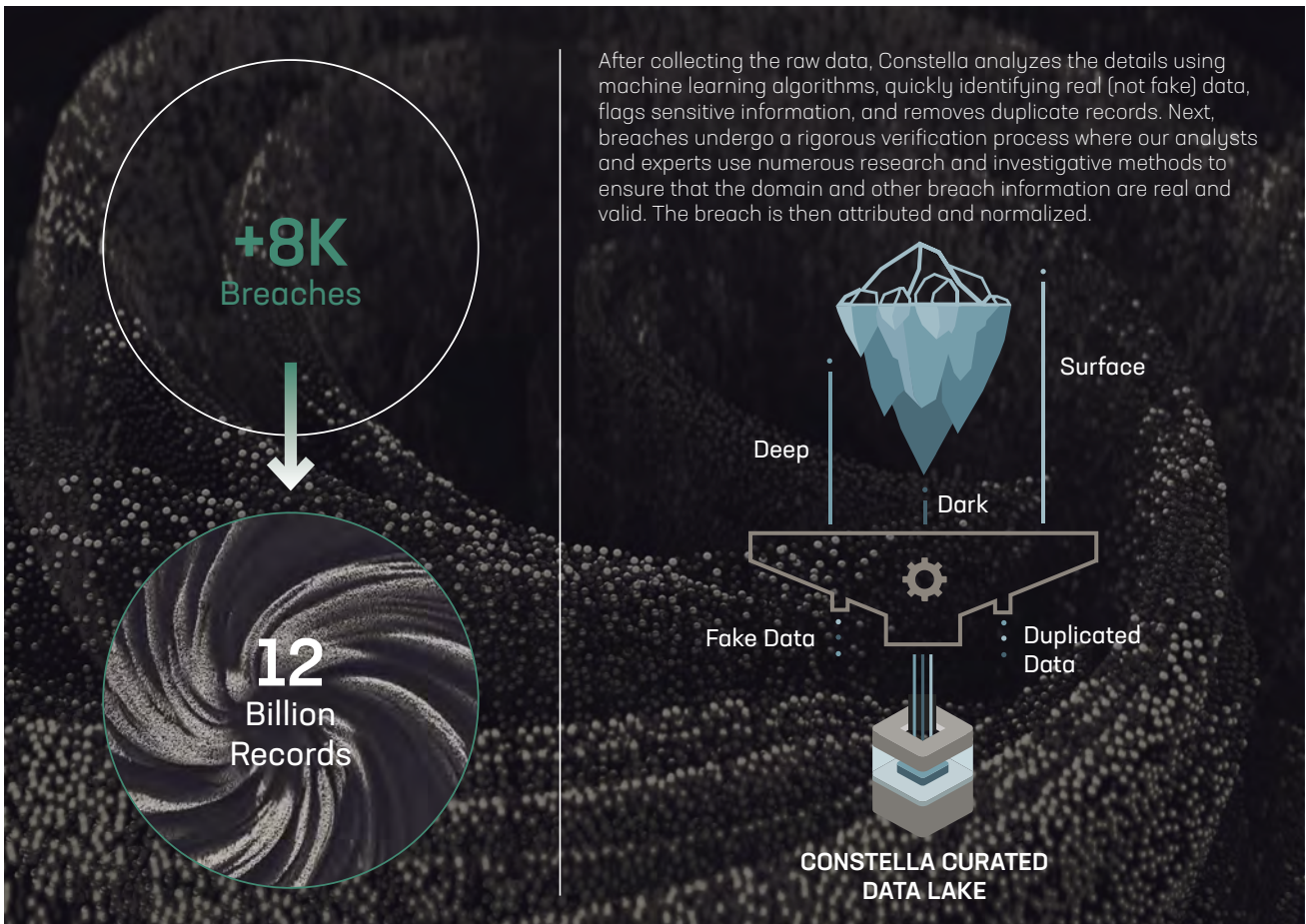
- Sensitivity of information
- Authenticity of the data
- Number of individuals impacted
- Age of each type of sensitive identity attribute exposed

Executive Summary: Breach Report Key Findings

Constella's threat intelligence team continuously collects identity records from data breaches and leakages found in open sources, on the surface, deep, and dark web, in order to track data related to reported company breaches and the specific personally identifiable information (PII) exposed. Consistently throughout the COVID-19 pandemic, cybercriminals have exploited heightened attention and anxieties produced by the global public health crisis, targeting individuals, brands, and high-profile individuals through a host of tactics and malicious cybercrime activity.

In 2020, Constella Intelligence's threat intelligence team detected over 8,500 breaches and leakages circulating in dark markets and underground forums, representing nearly 12 billion records. Constella analyzed a significant portion of the breaches and leakages detected in underground marketplaces in 2020, constituting a 32% increase in the total volume of breaches and leakages analyzed in 2019. The breaches and leakages analyzed in 2020 represented over 6 billion total records, comprising approximately 42.5 billion attributes, adding to a comprehensive data lake of analyzed breaches and breached identity records. Among the breaches and leakages analyzed, many of the most relevant breaches and leakages of 2020, in terms of volume and publicity, can be found.

Constella's 2021 Breach Report offers insights into these cyber threats and the impact of malign activities fuelled by breach data circulating on the deep and dark web. Below is a summary of Constella's key findings:





Key Findings:

1

Both brands and executives find themselves under attack.

Executives are being exploited as key attack vectors to inflict financial and reputational damage on companies and institutions. Targeting individuals to obtain access to corporate networks not only puts organizations at risk, but the reputations of executives as well, the two of which are inseparably tied.

2

2020-2021 has unarguably been the year of COVID-19.

Deep and dark markets proved this trend to be consistent, exemplifying the central significance of the pandemic to the public, private, and digital spheres. Constella observed the exploitation of the COVID-19 pandemic to be a recurrent theme in dark markets, including the sale of vaccine doses—such as AstraZeneca, Pfizer, Moderna, and Sputnik—in multiple dark marketplaces ranging from as little as \$8 to as much as nearly \$850.

3

The links between the disinformation ecosystem and the breach economy are growing stronger.

The threat of malicious information manipulation contributing to an environment of “information pollution”, as dubbed by many public multilateral agencies, continues to rapidly evolve. Constella Intelligence has noted a connection between the geopolitical, brand, and business-related risks engendered by the disinformation ecosystem and evolving tactics fuelled by deep and dark web activity.

4

Impacted sectors like Energy and Telecommunications evidence the dramatic growth in the breach economy, including breaches and leakages targeting executives.

Major increases were observed in sectors such as Crypto (+121%), News (+110%), and Social Media & Dating (+64%), Healthcare (+51%), and Services (+62%), while sectors like Services (a categorization that includes Utilities, Telecommunications, Energy, Food, and Transportation, for example) Gaming & Gambling, Social & Dating, and Retail stood out as the most affected sectors in 2020. Further, our deep dive into the Telecommunications and Energy sectors reveals increased employee and executive exposures in recent years.

Key Finding

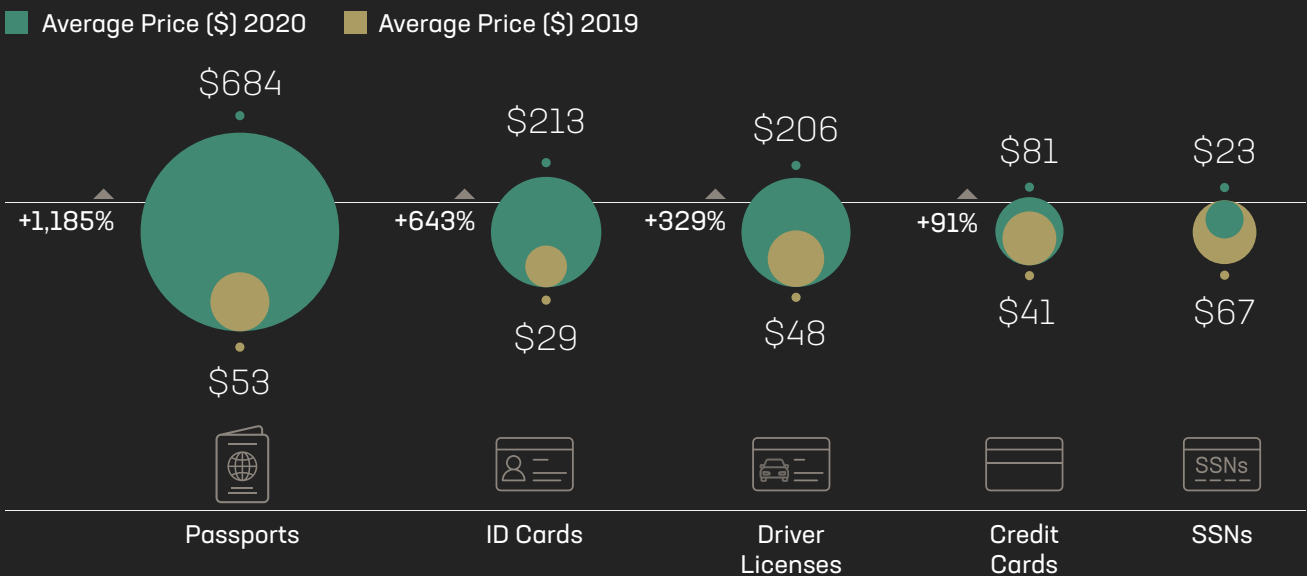
1



Both brands and executives find themselves under attack.

In 2020, Constella's threat intelligence analysts witnessed an exorbitant spike in the price of personal records transacted in dark marketplaces—compared to Constella's 2020 Breach Report price of data in dark markets including credit cards \$80.64 (+91%), passports \$684.29 (+1,185%), ID Cards \$213.49 (+643%), and driver's licenses \$205.71 (+329%) has increased significantly—indicating an increased demand for this sensitive personal data which can be used to commit fraud, launch impersonation attacks or coordinate even more sophisticated cyberattacks against individuals or critical corporate and organizational infrastructure. Further, from a sample of executives in the Energy and Telecommunications sectors, we found that more than 4 out of 10 had their credentials exposed in a breach in the past five years.

AVERAGE PRICES OF RECORDS FOR SALE IN DARK MARKETS



Key Finding

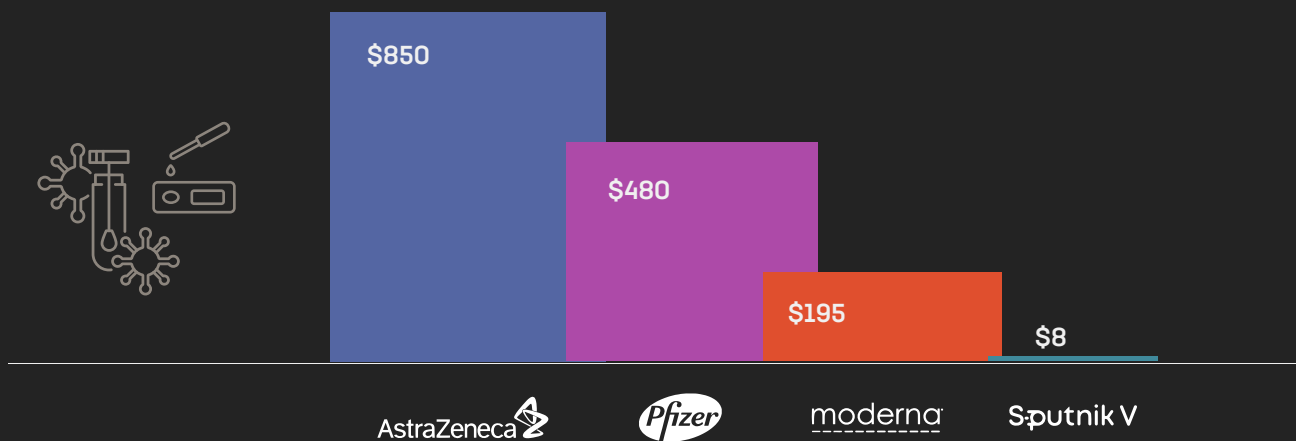
2



2020-2021 has unarguably been the year of COVID-19.

Deep and dark markets proved this trend to be consistent, exemplifying the central significance of the pandemic to the public, private, and digital spheres. Constella observed the exploitation of the COVID-19 pandemic to be a recurrent theme in dark markets, including the sale of vaccine doses—such as such as AstraZeneca, Pfizer, Moderna, and Sputnik. COVID-19 vaccine certificates, COVID-19 antigen tests, and COVID-19 PCR tests were also identified in underground marketplaces and on several Telegram channels sold by different users.

AVERAGE PRICE OF VACCINES FOR SALE IN DARK MARKETS





Key Finding

3

The links between the disinformation ecosystem and the breach economy are growing stronger.

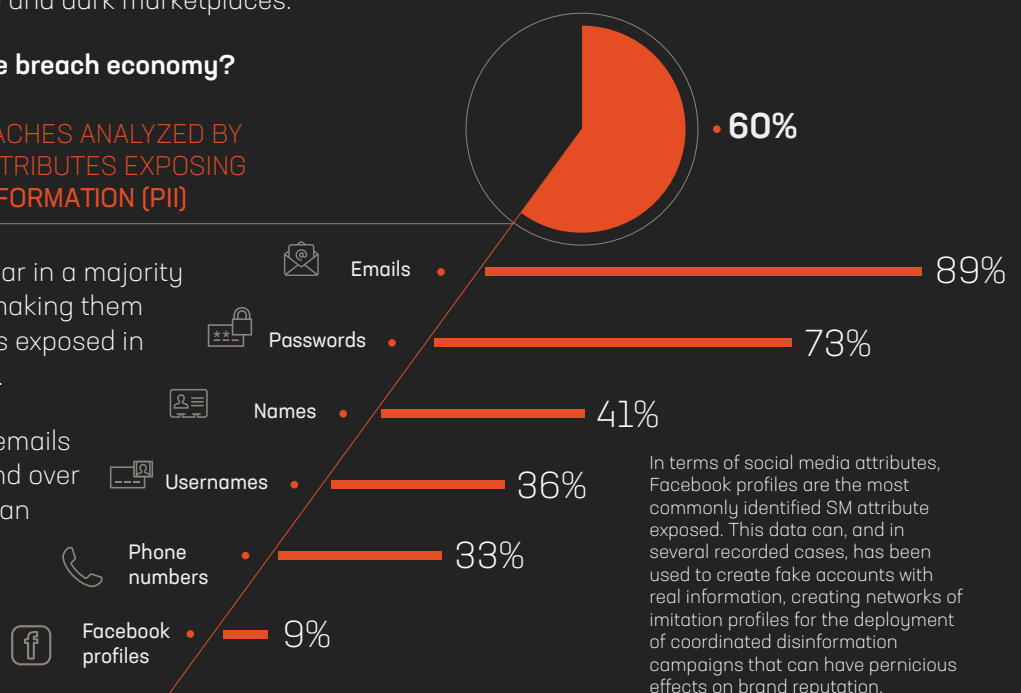
Spurred by the actors and tactics characterizing the disinformation ecosystem, this threat continues to rapidly evolve. Constella Intelligence has noted a connection between the geopolitical, brand, and business-related risks engendered by mis- and disinfo and evolving tactics fuelled by deep and dark web activity. The commodification of PII appears to be contributing to the commercialization of various building blocks of the disinformation ecosystem, including automated bots, false accounts, and deepfake production capabilities, all identified for sale in deep and dark marketplaces.

How is this connected to the breach economy?

PERCENTAGE OF DATA BREACHES ANALYZED BY CONSTELLA CONTAINING ATTRIBUTES EXPOSING PERSONAL IDENTIFIABLE INFORMATION (PII)

Emails and passwords appear in a majority of the breaches analyzed, making them the most common attributes exposed in breaches analyzed in 2020.

17.5% of records contained emails exposed more than once, and over 70% of breaches contained an email address.



In terms of social media attributes, Facebook profiles are the most commonly identified SM attribute exposed. This data can, and in several recorded cases, has been used to create fake accounts with real information, creating networks of imitation profiles for the deployment of coordinated disinformation campaigns that can have pernicious effects on brand reputation.

Key Finding

4











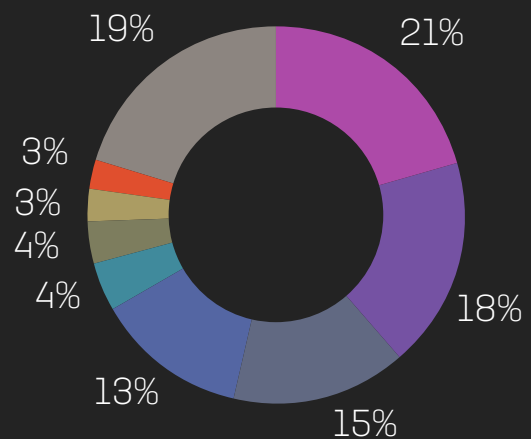
Impacted sectors like Energy and Telecommunications evidence the dramatic growth in the breach economy, including breaches and leakages targeting executives.

A few sectors accounted for over two-thirds (67%) of the total data breaches and leakages detected. Sectors like Services (a categorization that includes Utilities, Telecommunications, Energy, Food, and Transportation, for example) Gaming & Gambling, Social & Dating, and Retail stood out as the most affected sectors in 2020.

PROPORTION OF SECTORS MOST AFFECTED BY BREACHES AND LEAKAGES (2020)

▲ Increase (%) from 2019

●  21% Services (Energy, Telco, Utilities)	(+62%)
●  18% Gaming and Gambling	(+32%)
●  15% Social and Dating	(+67%)
●  13% Retail	(+37%)
●  4% News	(+110%)
●  4% Adult Sectors	(+97%)
●  3% Crypto	(+121%)
●  3% Healthcare	(+51%)
● 19% Others	

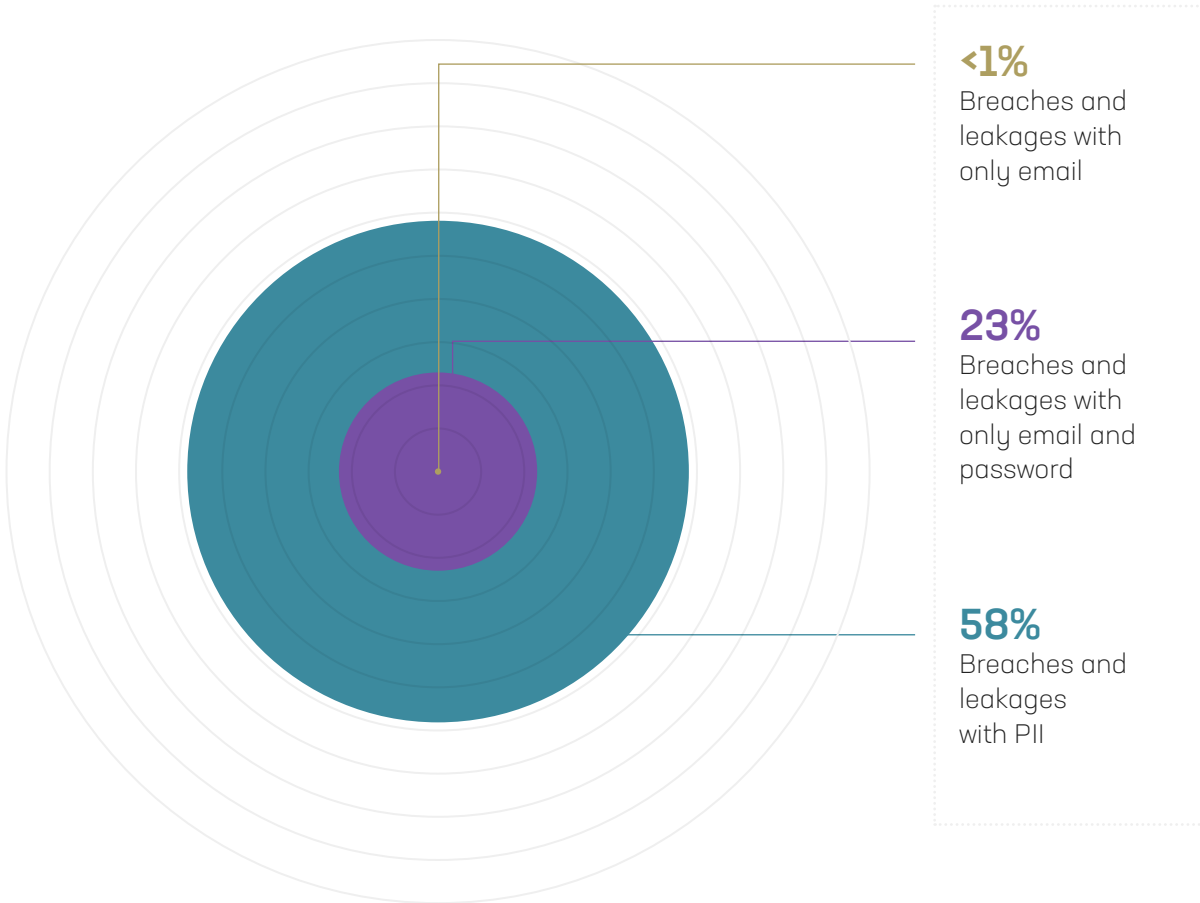


General Metrics & Data Composition

Figure 1 illustrates how data breach information in the Constella Intelligence data lake in 2020 has been classified based on the data analyzed and the sources from which these breaches were obtained.

FIGURE 1. TOTAL BREACHES COMPOSITION & PERCENTAGES

Figure 3 details the data composition of breaches analyzed in 2020. Note that nearly 60% of the breaches and leakages analyzed in 2020 include PII.

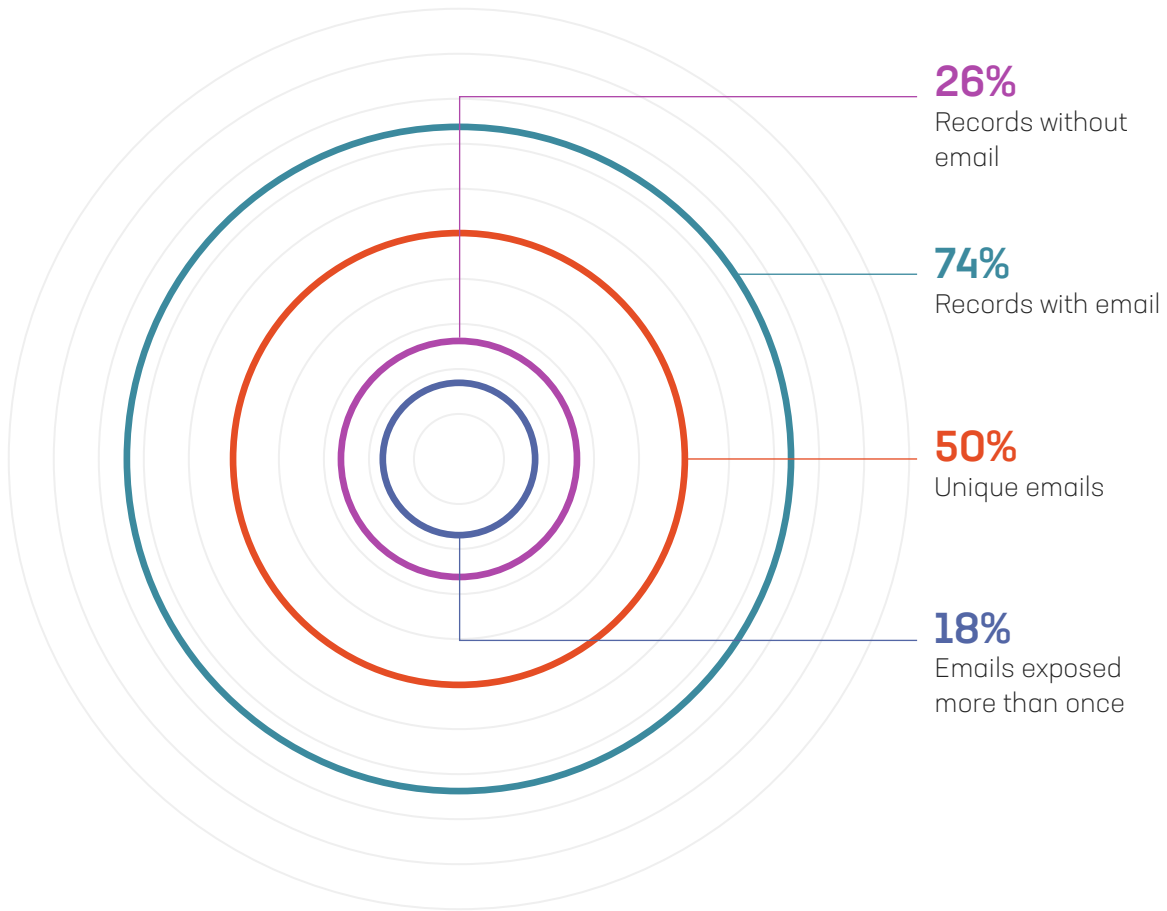


Threat actors gather PII from various sources, including breaches, leakages, social media and other publicly available information to create identity-based profiles, which they can weaponize to exploit businesses and individuals.

- **Julio Casal**, CTO at Constella Intelligence

FIGURE 2. TOTAL RECORDS COMPOSITION & PERCENTAGES

Figure 2 exhibits how the records are composed inside the breaches analyzed. 17.5% of records contained emails exposed more than once, and over 70% of records analyzed contained an email address, reinforcing the notion that email is the most prevalent PII exposed in breaches and leakages in 2020.



KEY TERMS*

- **Data Breach:** The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.
- **Data Leakage:** Unauthorized electronic or physical transfer of information from within an organization to external sources. This may not be with malicious intent; it could be accidental due to human error.
- **PII:** Personally, identifiable information (PII) is any data that potentially distinguishes, traces or identifies an individual.

This data can be sensitive or non-sensitive. Sensitive PII can result in harm to the individual if breached. Sensitive PII includes medical information, passport or security numbers, financial information, etc. Both sensitive and non-sensitive PII can be combined to aid in harmful exploits, including stalking, stealing the identity, or other criminal acts.

- **Executive Profile:** Digital footprint and exposed personal information of a company executive found in the surface Web, on social media, in the news, blogs, etc.

**Definitions of key terms can be consulted in the Glossary*

Section 1

2020 Identity Breach Data Deep Dive

Top Breaches and Leakages of 2020

By Total Records Exposed

Constella compiled the following leaderboard, as seen in Figure 8, based on breach/leakage size (number of records exposed by each breach) for company or website breaches/leakages analyzed in 2020.

- 1 People Data Labs**

This leakage was due to an unprotected ElasticSearch containing millions of personal information records from data enrichment company People Data Labs. The information exposed included PII (such as email addresses, usernames, employers, geographic locations, job titles, names, phone numbers)
- 2 Wattpad**

The website was breached in June 2020, exposing 270 million records. The information was initially sold on private networks and then published in underground forums. The information exposed includes names, usernames, email addresses, IP addresses, genders, birthdates, and passwords.
- 3 Adult Friend Finder**

AFF was breached two times (the first breach happened in 2015 and the second breach happened in 2016). This second breach exposed less sensitive information although it exposed a greater number of users (from 4M in 2015 to 220M in 2016). Despite the second breach happening in 2016, it was shared publicly in 2020. The information exposed in the second breach included: email addresses, passwords, and usernames.
- 4 Zynga.com**

Zynga suffered a data breach in 2019 by a hacker called “Gnosticplayers”, who stole data from Android and iOS users. Constella found the publicly shared data breach at the beginning of January 2020. The information exposed includes emails, passwords, phone numbers, usernames.
- 5 Tokopedia.com**

Tokopedia was hacked in March 2020 and the hacker obtained information from millions of users registered in Tokopedia’s online store. The information exposed includes email addresses, names, genders, birth dates, and passwords

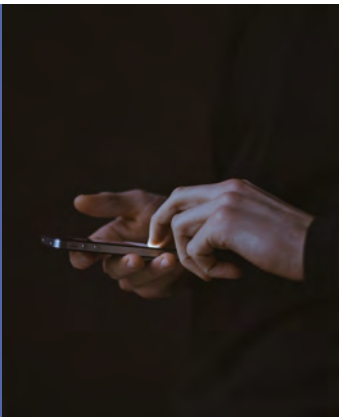
Our analysis indicates that most of the top breaches and leakages are from retail websites, gaming sites, and other digital services. Additionally, most of the relevant breaches/leakages detected and analyzed during 2020 resulted in exposed PII. Therefore, any attacker with access to this information would be equipped with the necessary data to create phishing campaigns, launch impersonation attacks, or produce fake accounts on social networks for disinformation and social engineering efforts.

Figure 3. TOP BREACHES AND LEAKAGES OF 2020 (BY TOTAL RECORDS EXPOSED)



Any time personal records and attributes are exposed due to a corporate security breach or leakage, corporate reputation and consumer confidence are a hefty but likely price to pay.

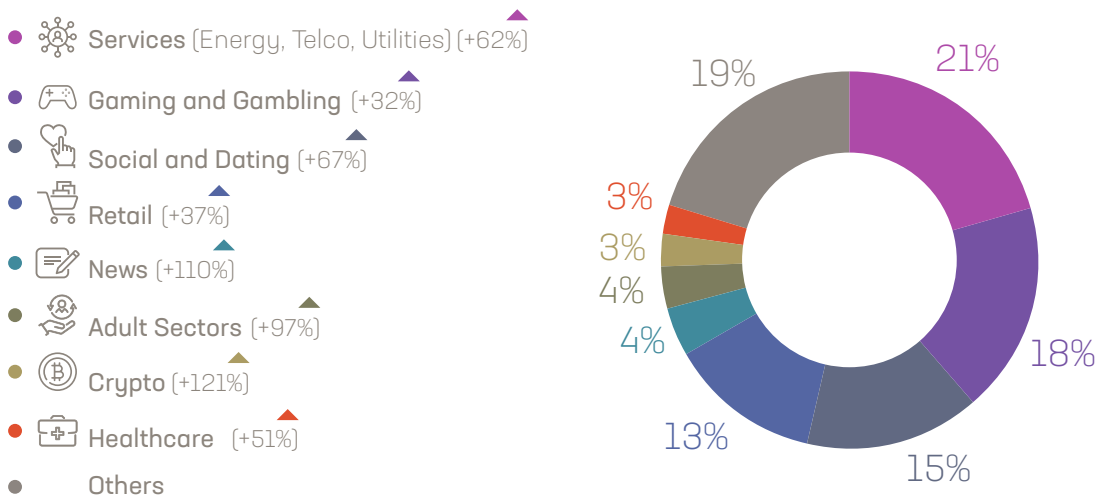
- **Cynthia Crossland**, CMO at Constella Intelligence



Most Impacted Sectors

Figure 4 shows the most impacted sectors based on the breaches and leakages analyzed by Constella in 2020. Notable increases from 2019 include companies from sectors such as Crypto (+121%), News (+110%), and Social Media & Dating (64%), Healthcare (+51%), Services (+62%), and the Adult sectors (+97%). In terms of the proportion of breaches analyzed and the sectors most impacted (based on the companies affected), sectors like Services (a categorization which includes Utilities, Telecommunications, Energy, Food, and Transportation, for example) Gaming & Gambling, Social & Dating, and Retail were the most impacted sectors based on this year’s analysis, together making up two-thirds (67%) of the companies suffering from the breaches analyzed in 2020.

FIGURE 4. MOST IMPACTED SECTORS IN 2020



One of the major long-term costs of data breaches is the disruption and loss of business. Large data exposure often leads to negative media exposure, which hurts brand reputation, eventually leading to loss of trust and confidence by customers. Other factors to consider include legal fees; insurance premium increases, ransomware payments (despite the U.S. government warning against doing so) and lastly, hefty fines.

- **Pablo Castillo**, Threat Intelligence Analyst at Constella Intelligence

Deep Dive into Critical Services: Energy and Telecommunications Industries

Attacks on critical infrastructure have been abundant in 2020-2021, including notable breaches and leakages in the cases of [SolarWinds](#), [Colonial Pipeline](#), [People's Energy](#), [Orange](#), and [Telecom Argentina](#). To better understand the impact of the breach economy on brands and executives in key sectors that deliver critical services, Constella's threat intelligence team conducted a deep dive into a sample of the top companies in the Energy and Telecommunications sectors. The following analysis includes the top twenty companies in the Energy sector and the top seventeen companies in the Telecommunications sector appearing in the [Fortune Global 500](#), a ranking of the top 500 companies worldwide in terms of total revenue.

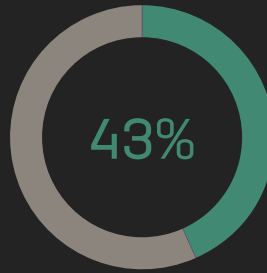


Energy Sector Fortune 500 Top 20 Companies

EXPOSED IN

+5,000

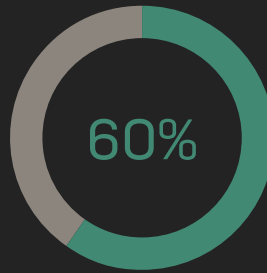
BREACHES OR LEAKAGES
SINCE 2016



Over 40% of breaches or leakages (+2,000) occurred since 2020, indicating a worsening usage of corporate domains among the companies analyzed.

+1,500,000

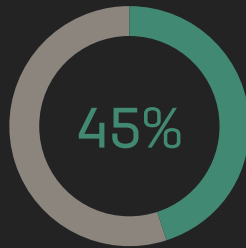
RECORDS EXPOSED
SINCE 2016



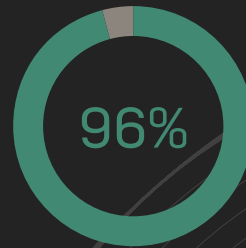
Around 60% (+900,000) of records exposed since 2020



OUT OF A SAMPLE OF 55 EXECUTIVES FROM FORTUNE 500 ENERGY COMPANIES



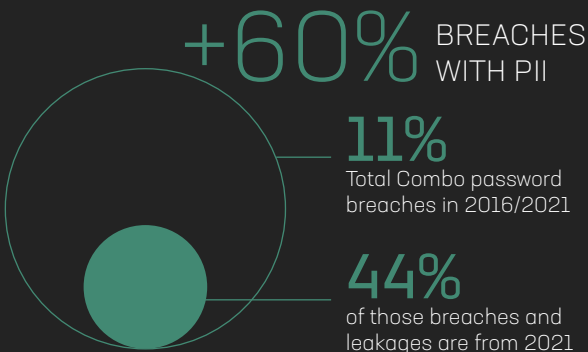
45% had their corporate credentials exposed in a breach or leakage since 2016.



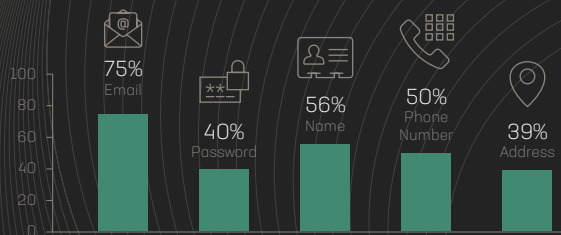
96% have been exposed in breaches or leakages from data brokers sites, including PII and no password.



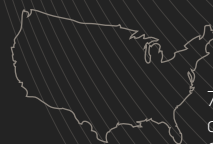
Nearly 1/4 have been exposed in breaches with password exposed.



What PII is most commonly exposed?

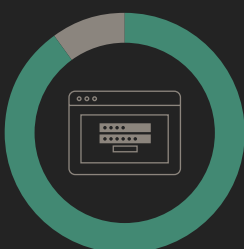


Where are these breaches taking place?



77% of breaches and leakages of employee credentials taking place in the US between 2016-2021 occurred in the last two years.

Weak Password Usage



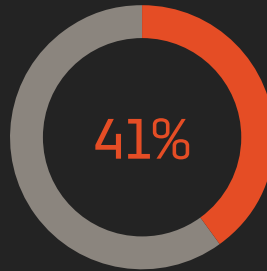
90% of breaches in 2020 include no password, are in plaintext, or use weak algorithms such as MD5 or SHA1

Telecom Sector Fortune 500 Top 17 Companies

EXPOSED IN

+6,000

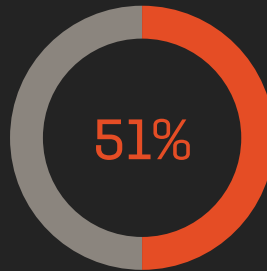
BREACHES OR LEAKAGES
SINCE 2016



Over **40%** of breaches or leakages detected occurred **(+2,500)** since 2020, indicating a worsening usage of corporate domains among the companies analyzed.

5,800,000

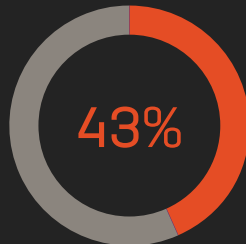
RECORDS EXPOSED
SINCE 2016



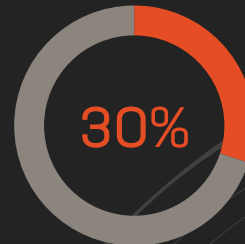
51% (+2,900,000) of records have been exposed since 2020.



OUT OF A SAMPLE OF 37 EXECUTIVES FROM FORTUNE 500 TELECOMMUNICATIONS COMPANIES



43% had their corporate credentials exposed in a breach or leakage since 2016.

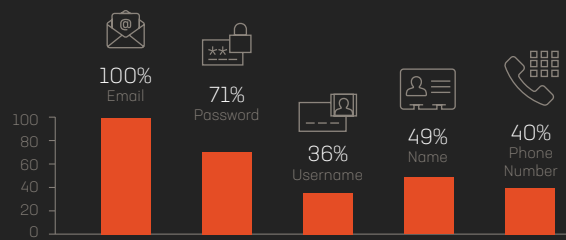


From this 43%, **over 30%** had their credentials exposed in breaches with passwords exposed.



100% of them have been exposed on breaches from Data Brokers sites which include PII and no password.

What PII is most commonly exposed?

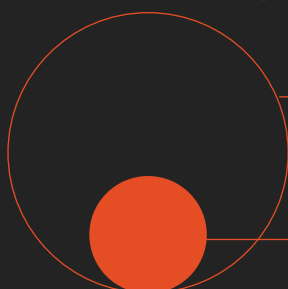


Weak Password Usage



+70% of breaches in 2020 include no password, are in plaintext, or use weak algorithms such as MD5 or SHA1

+60% BREACHES WITH PII



10% Total Combo password breaches in 2016/2021

42% of those breaches and leakages are from 2021

20%
2016-2020



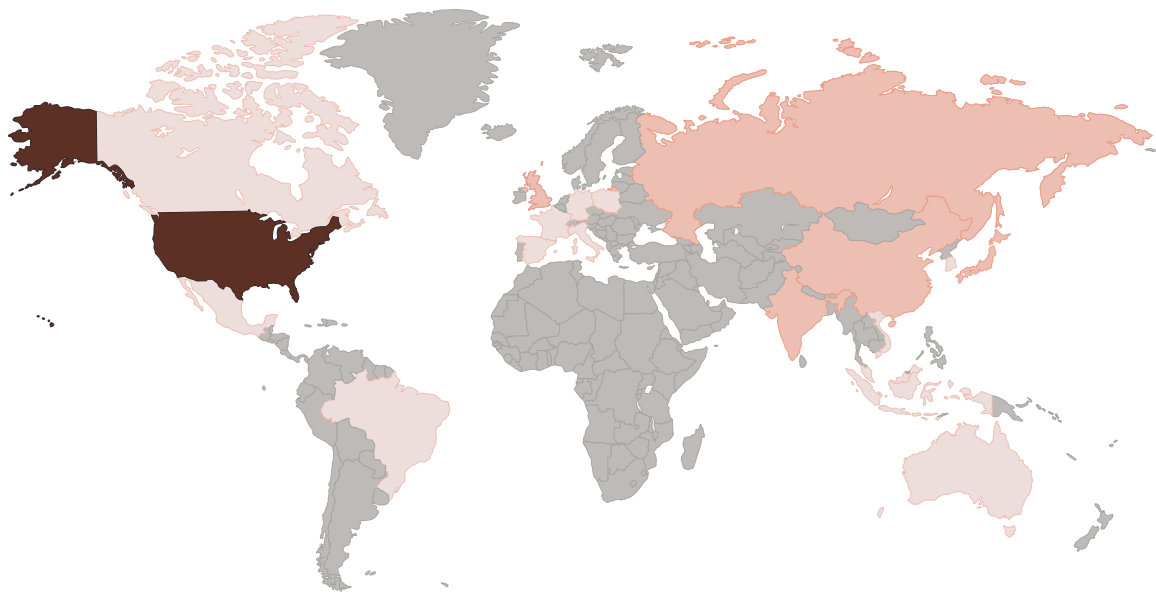
2020-2021

80% of exposures of employees in the Telecommunications sector since 2016 occurred in the past two years.

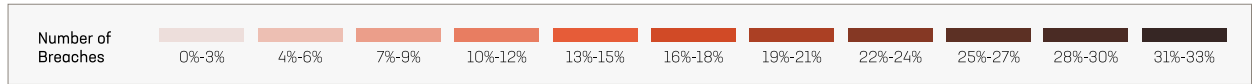
Geographic Distribution

The following map visualizes the total number of breaches and leakages detected in 2020, including the countries in which companies were most frequently impacted. The accompanying map visualization displays all breaches and leakages analyzed in 2020, sorted by country. This data indicates which countries were the most affected in the period of analysis—based on the location of the companies affected by the incidents—and the number of breaches and leakages that have been detected. The most affected countries in terms of the volume of breaches and leakages analyzed are the United States, followed by Russia, Japan, India, and the United Kingdom.

FIGURE 5. GEOGRAPHIC DISTRIBUTION OF BREACHES



Countries Affected	#Breaches	Countries Affected	#Breaches	Countries Affected	#Breaches	Countries Affected	#Breaches
United States	31.64%	China	4.25%	Spain	2.24%	Canada	1.42%
Russia	6.61%	Malaysia	3.90%	Germany	2.13%	Mexico	1.42%
Japan	5.90%	France	2.48%	Poland	1.65%	Indonesia	1.42%
India	5.31%	Brazil	2.48%	Australia	1.65%	Taiwan	1.06%
United Kingdom	4.84%	Italy	2.36%	Vietnam	1.53%	South Korea	1.06%



BREACHES DISTRIBUTION

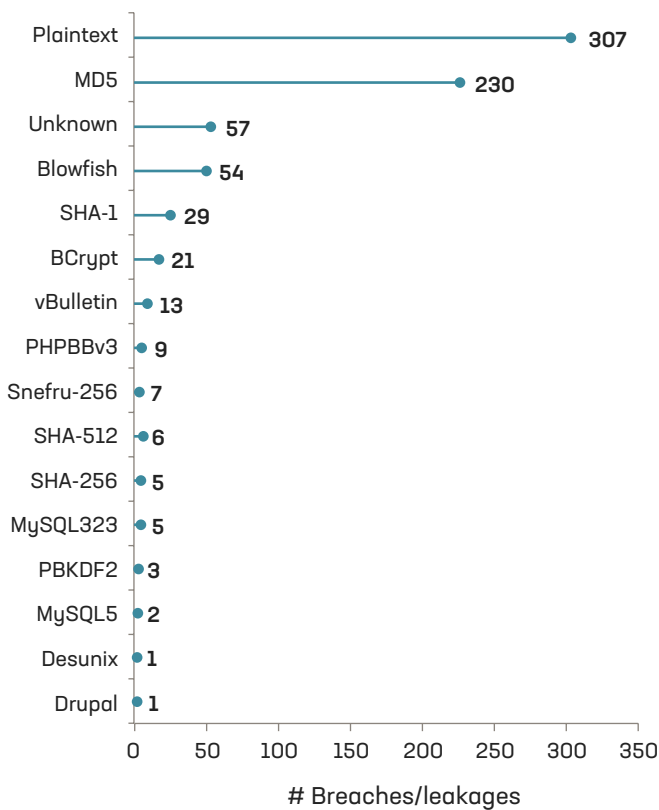


Breach Metadata

For the breaches and leakages analyzed in 2020, the different password algorithms detected are detailed in Figure 6.

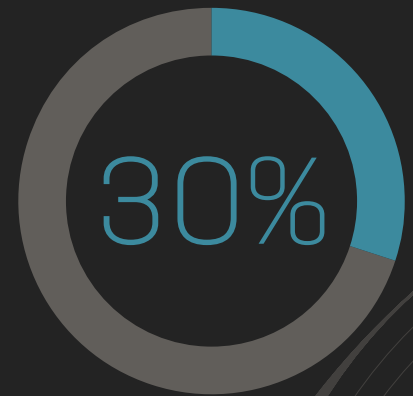
Password algorithms are relevant because the weaker a password is, the easier it is for cybercriminals to crack using wordlists. A wordlist is essentially a list of passwords collected in plain text. Wordlists are composed of a text file that includes a collection of possible passwords. As such, wordlists can be useful in helping threat actors crack passwords. As can be seen in the table, most breaches or leakages contain a password in plaintext or a password processed with the MD5 algorithm, which is an algorithm that tends to be easier to crack. It is significant to note that of the top five types of password encryption most identified in the breaches and leakages analyzed by Constella, 30% are unencrypted (in plaintext) and almost another 25% of the breaches and leakages contain passwords encrypted with weak algorithms such as MD5 or SHA1.

FIGURE 6. MOST FREQUENTLY DETECTED PASSWORD ALGORITHMS

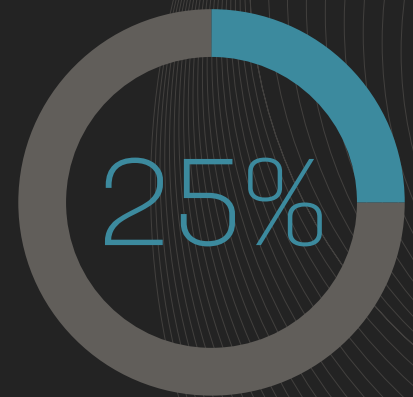


**No passwords were detected in 300 breaches.*

Of the top five types of password encryption identified:



are unencrypted (in plaintext)

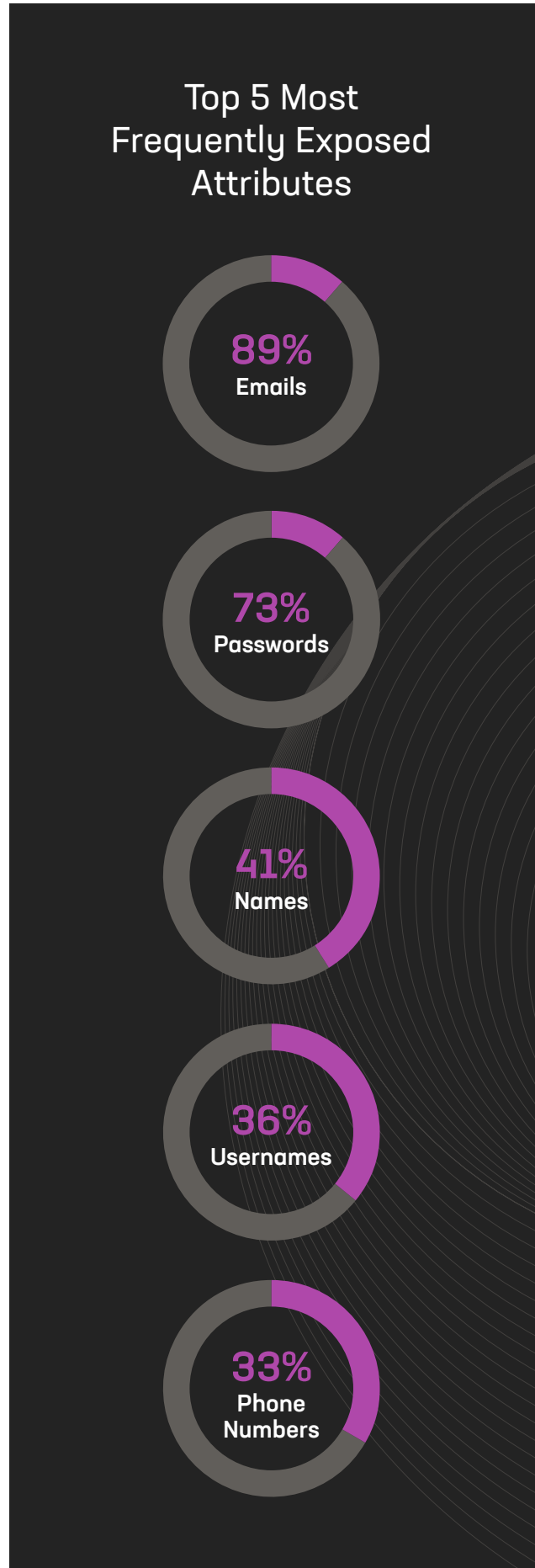
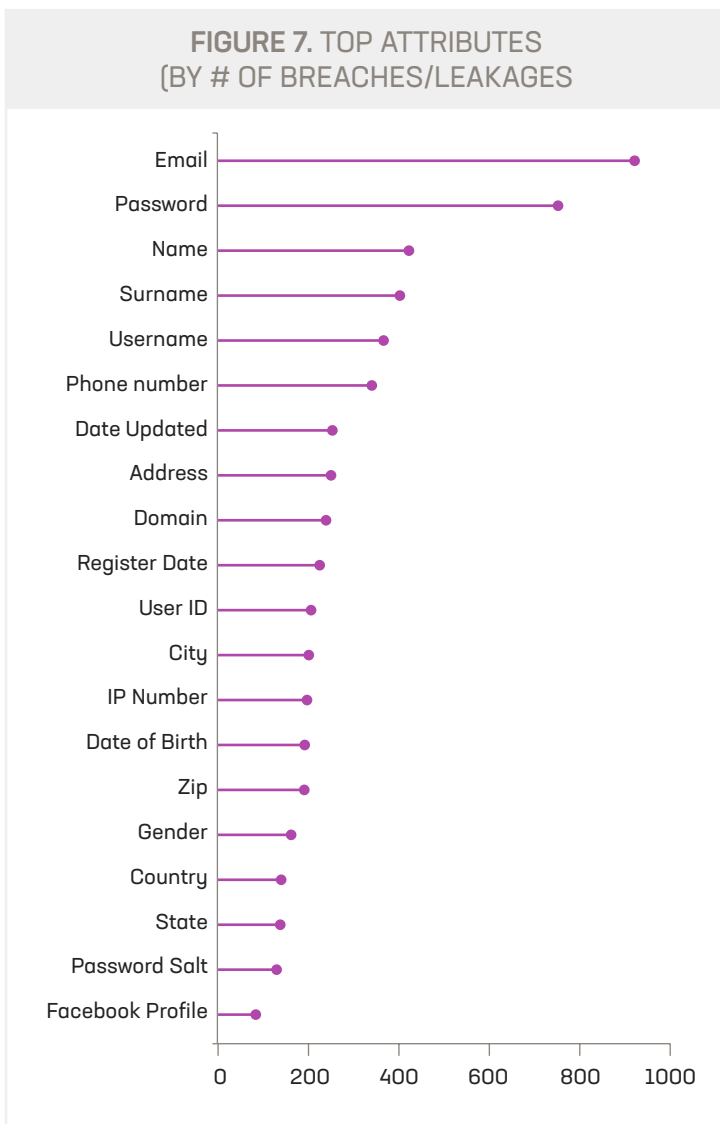


contain passwords encrypted with weak algorithms such as MD5 or SHA1

Most Frequently Exposed Attributes

The following data details the most recurrent attributes exposed in data breaches and leakages analyzed in 2020. Emails (89%) and passwords (73%) appear in a majority of the breaches and leakages analyzed, making them the most common attributes exposed in 2020. Following emails and passwords are names (41%), usernames (36%), and phone numbers (33%), which were exposed in more than 3 out of every 10 breaches/leakages analyzed.

Figure 7 shows the different types of PII exposed based on the breaches and leakages analyzed in 2020.



Top Social Media Attributes

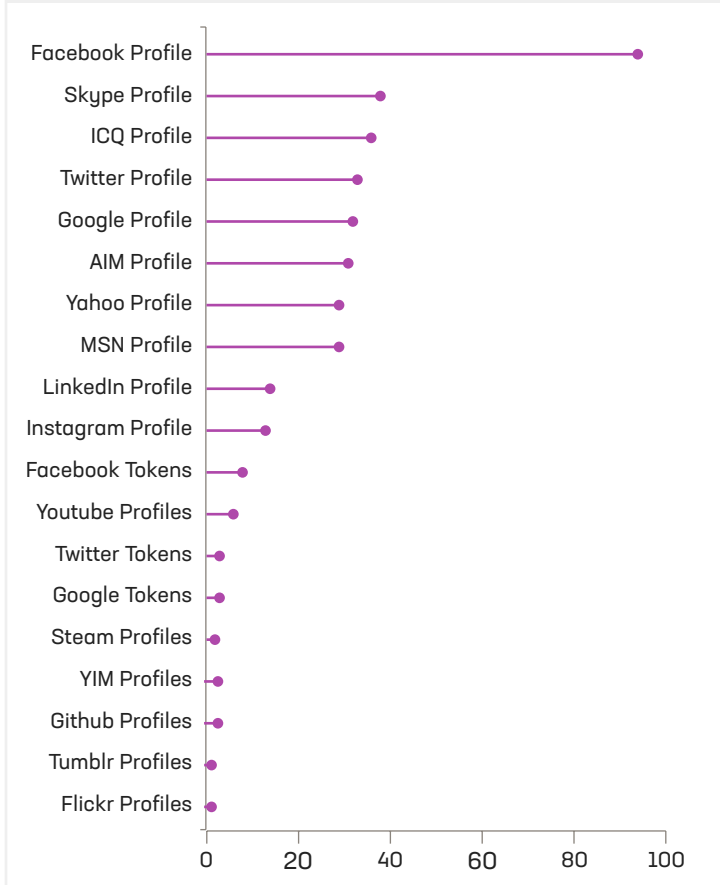
The data in Figure 8 compiles the number of breaches/leakages associated with a Social Media (SM) profile during 2020. These attributes include SM usernames, IDs, or tokens, that could be linked to any identity inside the breach where they are exposed. Among the SM attributes listed, Constella’s analysts have observed Facebook profiles as the most commonly identified SM attribute exposed, appearing in nearly one out of every ten breaches/leakages analyzed in 2020 (9%). Other commonly identified exposed SM attributes include Skype profiles, ICQ profiles, Twitter profiles, and Google profiles.

For hackers, SM attributes can prove useful for a few important reasons:

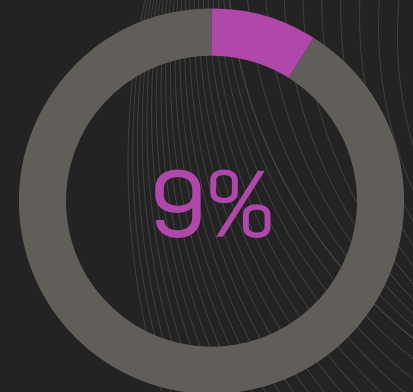
1. Threat actors can obtain personal information about their targets, such as locations, workplaces, hobbies, family members, or friends.
2. By obtaining a victim’s personal information, threat actors can launch more effective and sophisticated impersonation attacks in efforts to obtain sensitive information. These attacks could be targeted towards several possible entities including company of employment, bank accounts, other financial information, and much more.

Using similar methods, albeit for different objectives, security analysts and researchers can leverage these attributes to better understand the potential correlation between an email or user and a real identity, making it more efficient and easier to establish a network of connections that can aid in the identification of malicious actors.

FIGURE 8. TOP SOCIAL MEDIA ATTRIBUTES (BY # OF BREACHES/LEAKAGES)



Facebook profiles are the most commonly identified SM attribute exposed, appearing in nearly one out of every ten breaches/leakages analyzed in 2020 (9%).



Section 2

The Real-World Impact of Data Breaches

Threats Targeting Major Brands

Figure 9 lists a sample of some of the most valuable companies and brands breached in 2020, highlighted below for their presence in the Forbes Global 2000 ranking. The companies listed have publicly acknowledged suffering a breach or leakage during 2020.

FIGURE 9. THE EFFECT OF BREACHES ON BRAND REPUTATION



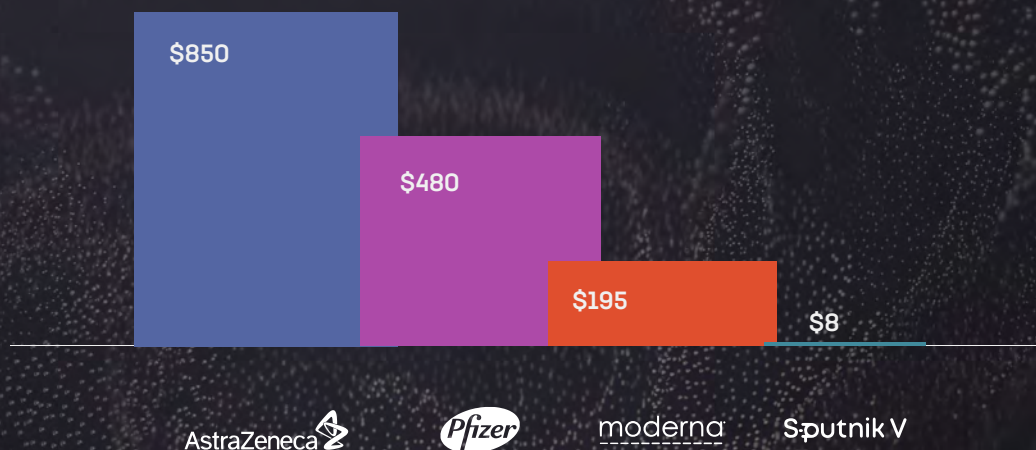
Vaccines And Covid-19-Related Items for Sale in Dark Markets

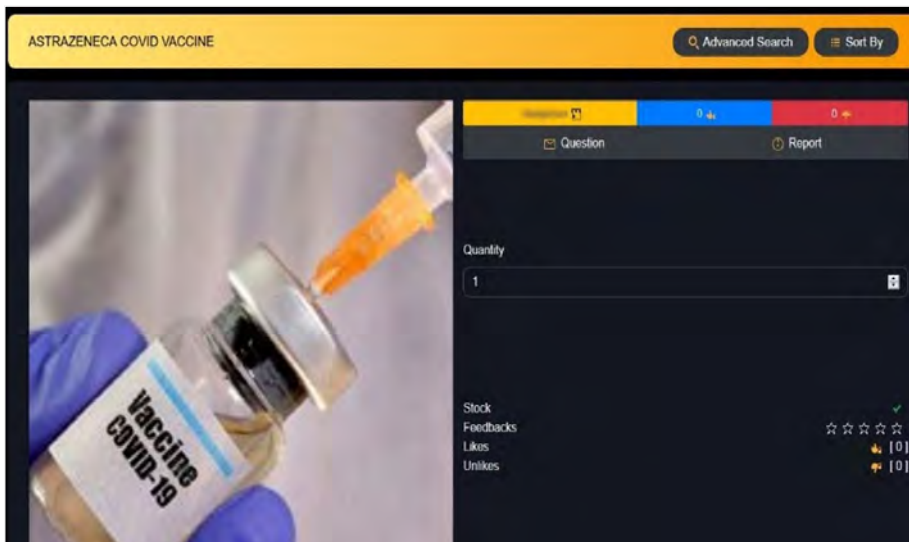
Threat actors are exploiting the pandemic for profits in underground markets, as has been well-documented by public and private research outputs since early 2020. Our threat intelligence teams have identified vaccines—real or otherwise—and fake vaccine certificates for sale in underground markets such as “Liberty Market” and “Televend,” as well as by various users on different Telegram channels. The images below show some examples of vaccination certificates and other COVID-related records found for sale in black markets.

The World Health Organization (WHO) held a press conference earlier this year to address this very issue, warning that “some falsified products are also being sold as COVID-19 vaccines on the internet, especially on the dark web.” The WHO would go on to say that it was aware that ministries of health and regulatory agencies across the globe “have received suspicious offers to supply COVID-19 vaccines.”

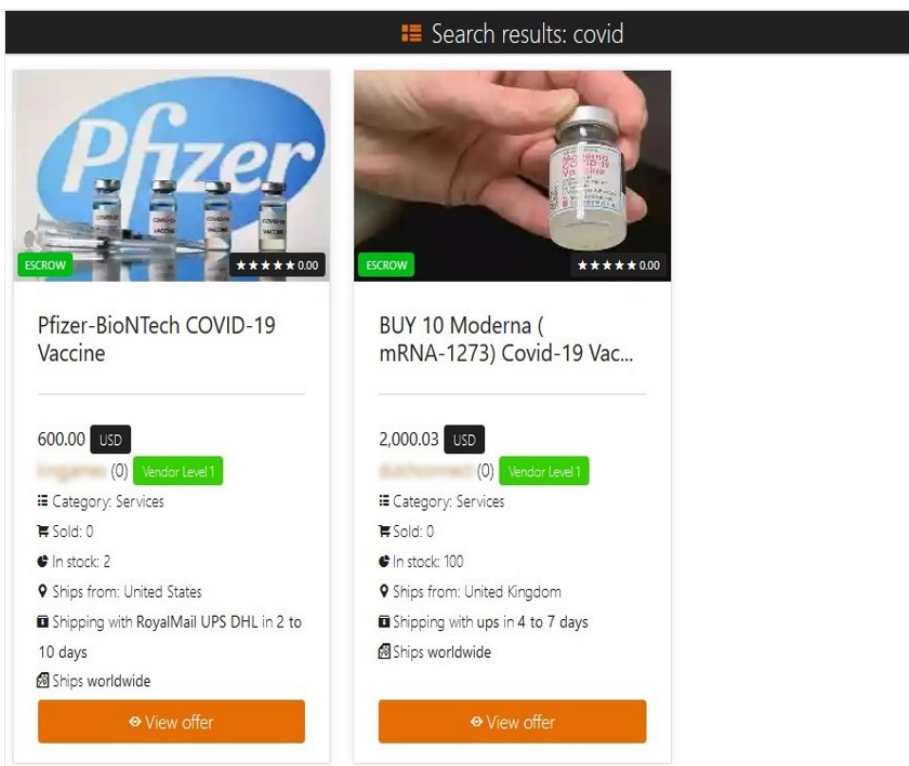
The prices of vaccines for sale in several dark markets (such as Steroid King, Cartel Marketplace, Tor Door Marketplace, DarkFox, and Invictus) are indicated in Figure 16. Our threat intelligence analysts have seen that the average price in several dark markets—including Steroid King, Cartel Marketplace, Tor Door Marketplace, DarkFox, and Invictus—for AstraZeneca is an exorbitant \$848.50; Pfizer is selling for \$483.75; Moderna goes for \$193.60; while Sputnik costs an average of only \$8. As far as certificates go, German vaccine certificates are being sold for an average of \$22.35, and COVID-19 antigen tests sell for an average \$25 flat. Cryptocurrency is the exclusive form of payment.

FIGURE 10. AVERAGE PRICE OF VACCINES FOR SALE IN DARK MARKETS

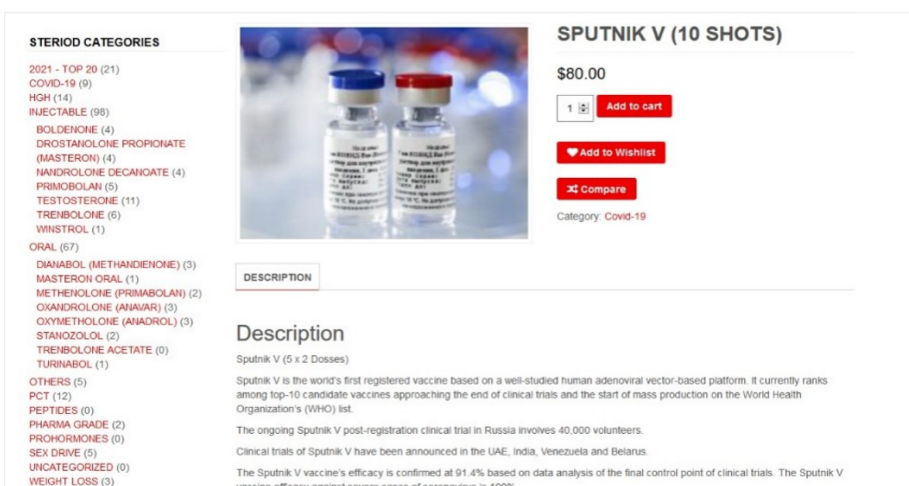




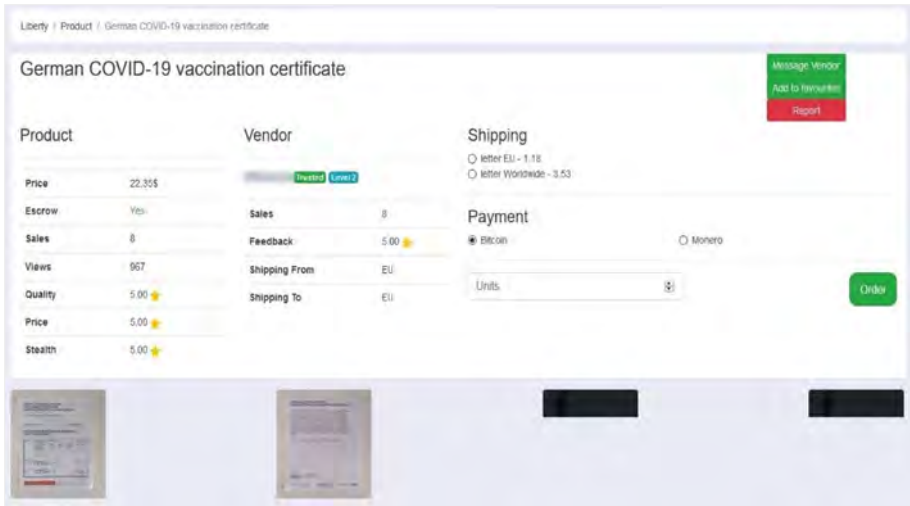
→Image #1
AstraZeneca Vaccine



→Image #2
Pfizer and Moderna Vaccines



→Image #3
Sputnik V Vaccine



→Image #4
COVID-19 Vaccination Certificate

We work directly with medical institutions. We need 4-5 hours to issue the document.

Wir arbeiten unmittelbar mit verschiedenen medizinischen Einrichtungen.
Die Erstellung dauert ca. 4-5 Stunden.

Price/Preis: 100 euro.

PCR-Test Nachweis wird für Auslandsreisen benötigt.

All certificates are registered in the laboratories accordingly. Alle Zertifikate werden in der Labor registriert.

We require following data :

Name, family name
Passport Number
Date of birth
Place of birth
Place of Residence

Wir benötigen folgende Angaben von Ihnen:

1. Vorname, Name
2. Pass mit Seriennummer
3. Geburtsdatum
4. Wohnort/Stadt

Feel free to write to us, we respond quickly. Schreiben Sie uns, wir werden Ihnen schnellstmöglich antworten.

491 edited 7:56

Image #5
COVID-19 Certificate

Vaccination certificate
PROOF OF COVID19 VACCINATION CARD WITH STAMPS

Hello everybody. Not everybody will like to take the COVID19 vaccine and we provide proof of haven been vaccinated. For more detail is inbox me

Price for 1 set 150 \$

Discounts apply when ordering several sets. 140 17:07

Vaccination certificate

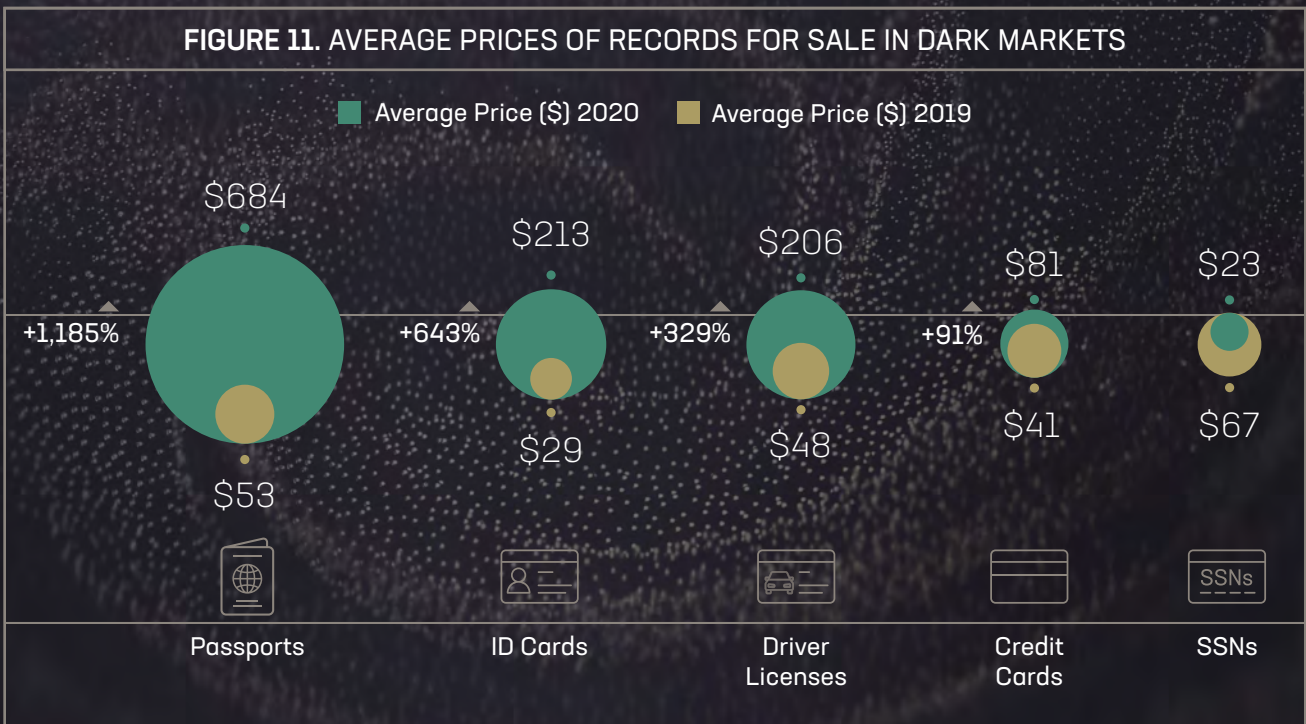
Vaccine	Product Name/Manufacturer Lot Number	Date	Healthcare Professional or Clinic Site
1 st Dose COVID-19		mm / dd / yy	
2 nd Dose COVID-19		mm / dd / yy	
Other		mm / dd / yy	
Other		mm / dd / yy	

Image #6
COVID-19 Vaccination Card

Dark Market Economy

The data in Figure 11 indicates the average prices of credit cards, passports, ID cards, Social Security numbers, and driver's licenses traded or sold in dark markets in 2020. During a year in which cybercriminals leveraged new tactics and methods to exploit the global health crisis for financial gain, the prices of credit cards (+91%), passports (+1,185%), ID cards (+643%), and drivers licenses (+329%) increased dramatically from Constella's research in 2019.

Although it is difficult to conclude the causal factors behind the substantial increase in records for sale in dark markets, we can point to certain trends that may have influenced this trend. It is plausible that, due to the COVID-19 pandemic and limitations on travel and movement among countries, the demand for false documentation (such as passports, personal identification cards, and other types of identification documents) that permit access to foreign countries may have increased. Given this increased demand, restrictive international and domestic contexts characterizing travel and mobility during 2020 may have contributed to black market document sellers seeking an opportunity to further profit from the pandemic.




SSN CARD



Category: Services -> Fake Documents (Physical)
 Price (Fiat): USD 65 (€64.13 £46.90 AUD84.99 CAD81.34)
 Price (XMR): 0.189140429494
 Measurement unit: Piece
 Shipping: from: United States to: United States
 Views: 38
 Shipping methods:
 - USPS PRIORITY 2-3 DAYS : USD 9 (XMR 0.026188674853)
 Available: In stock
 Vendor: [Redacted] 100.00 % positive / 5 reviews Disputes: 0 won / 0 lost [0 - 10 sales]
 Finalize early (FE): Listing is Escrow
 Vendor last seen: Today
 Minimum order amount: XMR 0.215329104347 (0.189140429494 for products + 0.026188674853 for shipping).
 Vendor's PGP key fingerprint: [Redacted] Show Key

→Image #7
SSN Cards

0★ Escrow ID, pasport , permit and drivers license available + Favorite stockup' (5★)



Shipping from	United States of America
Shipping to	Worldwide
Sold	0x, 0 orders
Views	8
Stock	Unlimited
Payment System	Escrow

1x 500.00 USD
 \$ 500 / 0.008805 BTC / 1.447515 XMR

Quantity:


Select Shipping

Order BTC

Description
 WELCOME TO STOCKUP CARTEL MARKET PLACE ,
 We are a Group of suppliers who have access to very high quality products, we wish to deliver these products to you at very competitive rates, Best prices you can ever find in the market that's what we will give you.
 We strive in being the best! we are focused on building a reputable vendor account on this marketplace with extremely high grade products and exceptional customer service.
 We're Shipping Top Quality Products in great stealth Packaging to ensure safe and perfect shipment.

→Image #8
Passports, ID Cards,
Driver's Licenses

HQ Credit Cards (Australia) VALID



Valid number (100%)
Seller Level 2 (182)
Trust Level 2
 Verified Seller : ✔ / Trusted
 Seller : ✔
 Positive Feedback : (100%)
 Member since : [Redacted]
 Last Login : [Redacted]
 Sales : 182
 Orders : 0

Sold : 5 Times
 Origin Country : World Wide
 Ship to : World Wide
 Payment : Finalize Early
 Product class : Digital Goods
 Quantity : 3 Items Available

Sale Price : 24.99 USD / 0.00042980 BTC
Sale Price : 24.99 USD / 0.10482383 XMR
Sale Price : 24.99 USD / 0.12868177 LTC
Sale Price : 24.99 USD / 0.04813267 BCH

Shipping Options :

Digital 1 Day - 1 Day - 0.00 USD / 0.00000000 BTC
▼

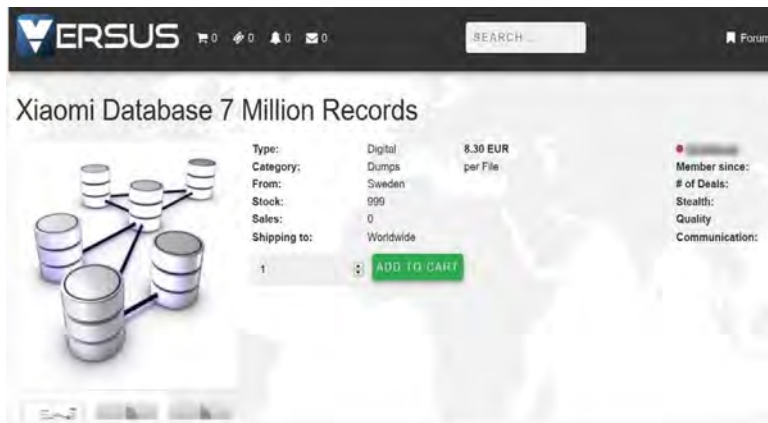
→Image #9
Credit Cards



→Image #10
Clubhouse.com
Data Breach/Leakage
Sale



→Image #11
Ledger.com
Data Breach/Leakage
Sale



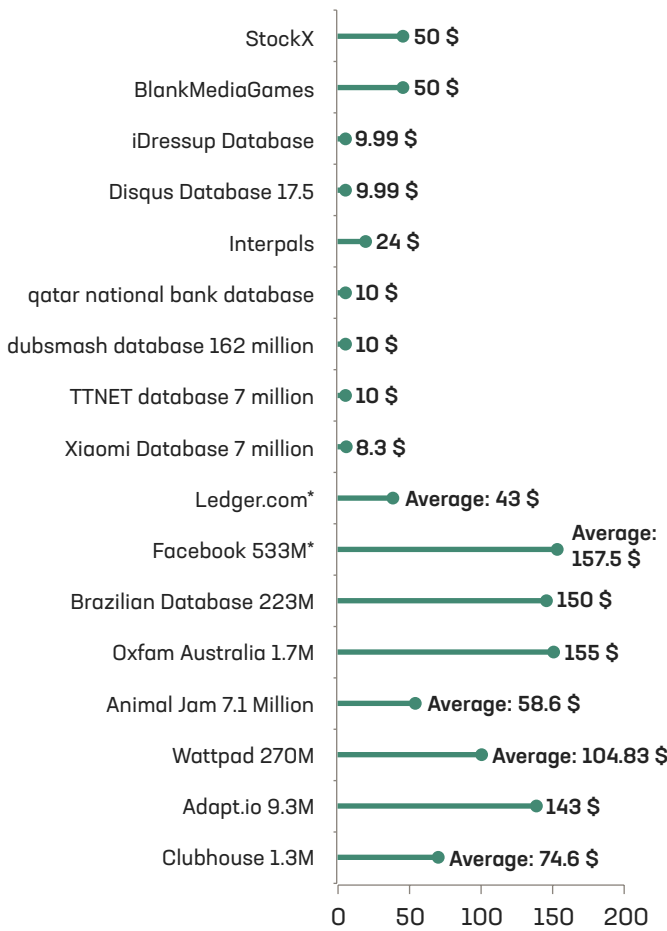
→Image #12
Xiaomi 7M
Data Breach/Leakage
Sale

Breach Databases: Higher Value Breaches Sold on DDW Forums

Figure 12 indicates the price of databases being traded or sold in dark markets, while Figure 20 shows the price of the breaches and leakages for sale in deep and dark web forums. Over the period analyzed, Constella's threat intelligence analysts observed a trend of hackers putting their hacks for sale more frequently in forums and less often in black markets. This trend can be observed related to the price of the databases and concerning the specific databases sold in each underground location.

Further, in the dark markets analyzed, databases are sold at a much lower price than the databases sold in the forums. This is likely because of their relative age (2-3 years old), meaning that the data has already been accessed by several users, devaluing the price. As such, more recent and more expensive breaches/leakages are being sold more frequently in forums rather than dark marketplaces.

FIGURE 12. BREACH DATABASES FOR SALE IN DARK MARKETS



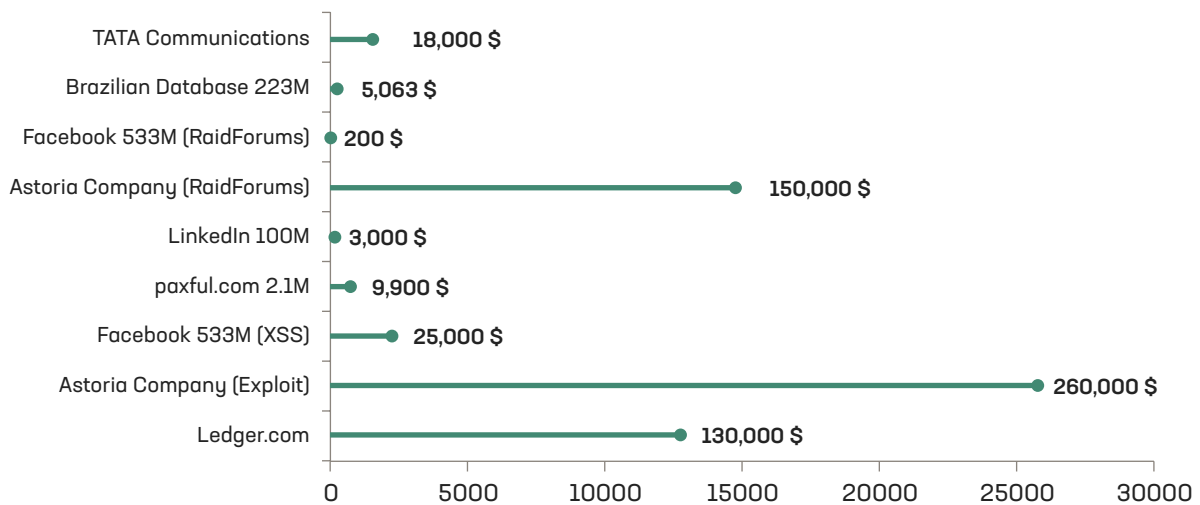
*Databases for sale by different users at a range of prices

Within this context, a DDW forum has a few distinct advantages. Sellers migrating the sale of recent breaches from Black Markets to deep and dark web forums could be due to several of these advantages, including:

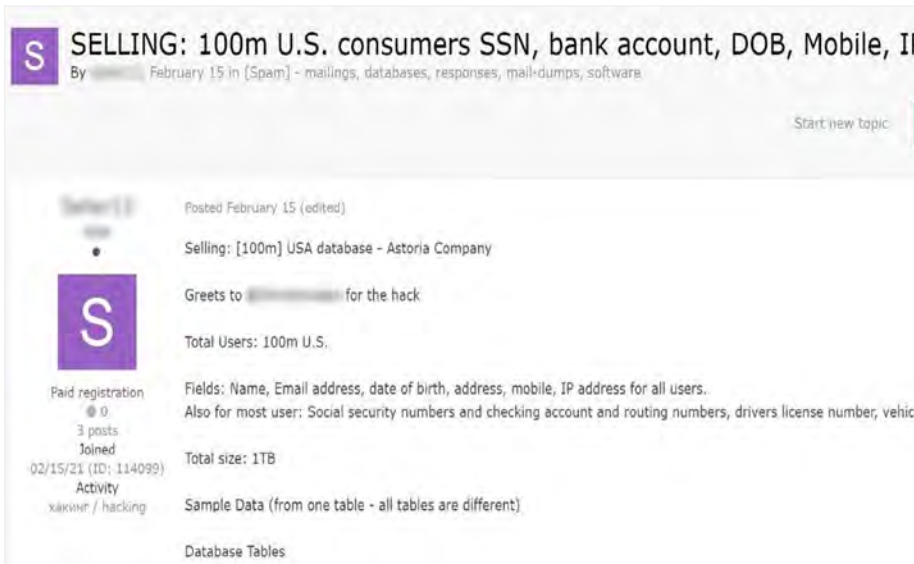
- 1 Black Markets usually have a service through which the buyer pays for a breach, while the Black Market retains the payment until the seller sends the information to the buyer. This makes the payment and transaction process slower.
- 2 Compared to deep and dark web forums, Black Markets tend to have less traffic and a more limited audience than deep and dark web forums. This is due in part to the closures of Black Markets in recent years.
- 3 Deep and dark web forums tend to attract higher concentrations of users, conversations are more direct, and sellers are able to offer secure, personal channels of communication, allowing for easier and quicker communications between sellers and buyers. Moreover, transactions are made directly between a buyer and seller, without an intermediary.

The following table shows the price of the breaches/leakages which are for sale in deep and dark web forums:

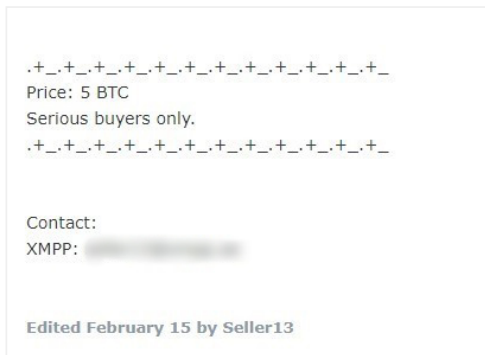
FIGURE 13. BREACH DATABASES FOR SALE IN UNDERGROUND FORUMS



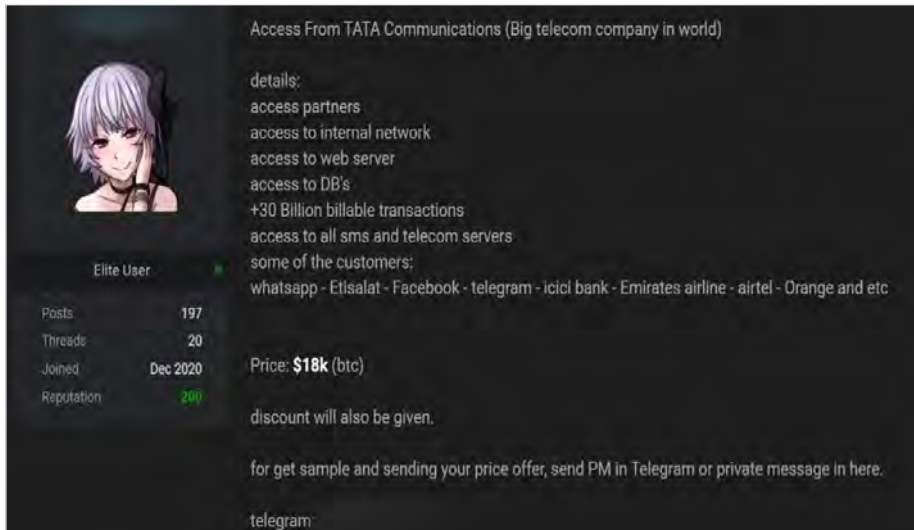
*Databases for sale by different users with different prices



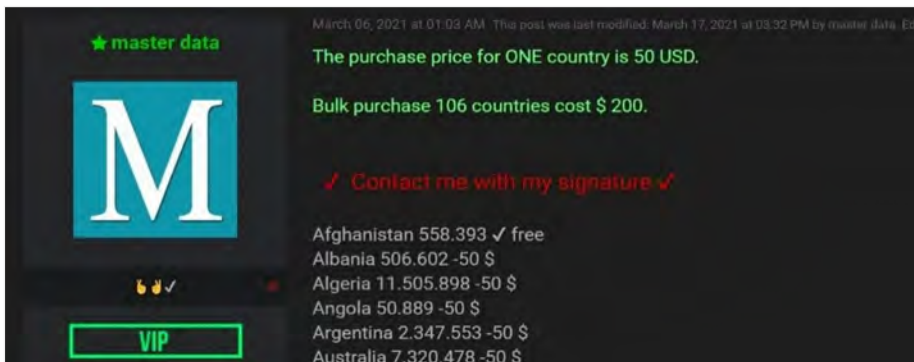
→Image #13
 Xiaomi 7M
 Data Breach/Leakage
 Sale



→Image #14
 Astoria Company
 Data Breach/Leakage
 Sale



→Image #15
 TATA Communications
 Data Breach/Leakage
 Sale



→Image #16
 Facebook 533M
 Data Breach/Leakage
 Sale



During the past year and a half, I've observed increased cybercrime activity in the dark web, as well as the surface, social, and deep webs. Right now, there are billions of breached and leaked identity records circulating throughout these open sources. Threat actors leverage these compromised credentials to build digital profiles and personalize their attacks—phishing scams, disinformation campaigns, account takeover, and more—while targeting enterprises and individuals alike.

Identifying and tracking sources of criminal activity, specifically in the dark web, is a worthwhile investment to: stay one step ahead of attackers to proactively identify exposures; identify breached credentials to prevent further damage; and gain insights into all stages of criminal activity, from planning to attack. The sooner organizations and individuals know about the breach, change credentials, and lock down networks, the less damage occurs.

- **Alberto Casares**, VP of Risk Protection at Constella Intelligence



Breaches, PII, and the Disinformation Ecosystem

Through analyzing deep and dark web forums, Constella's intelligence analysts identified several threads related to social media accounts for sale or social media bots for automating account interactions in order to generate likes, views, subscribers or post customized comments. Table 2 details threads on distinct forums selling software that enables bots with a diverse and comprehensive list of features. Capabilities offered by software identified for sale can include post scheduling, hashtag and captions generators, and other automated elements. Additionally, entire accounts have been identified for sale, varying in price based on the account's creation date.



“Entire accounts have been identified for sale, varying in price by the account’s creation date.”

- **Constella** 2021 Identity Breach Report

TABLE 14. BOTS FOR SALE IN UNDERGROUND FORUMS

BOTS FOR SALE IN UNDERGROUND FORUMS				
Thread/Topic	Forum	Price		Comments
Dimension Bots	Nullified Raidforums	Basic	Free	For several Social Networks, software allows: <ul style="list-style-type: none"> - Proxies - Captcha bypass - Live chat - Auto-start - Anti-ban - Automated account login - Advanced tasks configuration
		Pro	\$3.5/month	
		Ultra	\$5/month	
Efface Instagram Bot	Nullified	Regular License ● \$19		For Instagram social network, software features are: <ul style="list-style-type: none"> - Likes/Dislikes - Make comments - Follow/Unfollow users - Mention users - Hashtag Generator - Captions Generator - Custom Profile URL or Custom Hashtag
SMMVerse	Raidforums	Depending on the volume of interactions needed the prices are: Min. \$10 Max. \$500		For Instagram, Twitter, Youtube, Facebook, Tiktok or Twitch, software features are: <ul style="list-style-type: none"> - Likes/Dislikes - Views - Comments - Shares - Followers - Watch Time - Retweets - Traffic
2008 - 2019 Created Twitter Aged Accounts	Nullified	Prices per account: 2015-2019 \$3 2010-2014 \$8.7 2009 \$15 2008 \$30		Account for sale: <ul style="list-style-type: none"> - Have zero or less than 50 followers - Gender can be both male and female - May or may not have profile pic and tweets
Jarvee	Nullified	For free in forum thread. Prices in website: Starter \$29.95/month Regular \$49.95/month Professional \$69.95/month		Software features: <ul style="list-style-type: none"> - Posts Scheduling - Social Media Automation - Scraping tool - Auto-hashtag

Nearly 60% of breaches/leakages analyzed by Constella in 2020 contain an attribute exposing personal information such as first and last names, phone numbers, addresses, email addresses, and much more. Although some breaches and leakages are from lesser-known websites, data exposed in all of these incidents could potentially be used for the creation of fake social profiles with real information to produce networks of inauthentic accounts for the deployment of coordinated disinformation campaigns.

Deepfakes

A deepfake is content created using human image or audio synthesis based on artificial intelligence - this means that it's an image, video, or audio impersonation of someone powered by AI, usually making it more convincing and difficult to distinguish as false. This is achieved by merging or superimposing existing audio, image, and video content onto source content by applying an advanced machine learning technique known as a generative adversarial network (GAN). Given these characteristics, deepfakes have already been used in a wide array of contexts, including in the production of “fake news” and manipulated content or malicious impersonations with the objective of obtaining sensitive data for financial gain (also known as “social engineering” within this context) or influencing public opinion for corporate or political reputational damage.

Our threat intelligence analysts identified several capabilities related to the production of deepfake content online. Tools including DeepFakeWeb, FaceSwap, FakeApp, DeepFaceLab and others can be found on the Surface Web and are available to any user. These tools can be accessed via Github or even in mobile app stores, allowing any user to access, download, and even modify the source code of the application. Despite their availability on the Surface Web, underground users post on deep and dark web forums about the tools detailed below, making recommendations or discussing the relative quality and functionality of different tools. Some tools that were identified explicitly advertise “manipulation of politicians lips” as a functionality, for example.

Constella’s intelligence analysts have also identified users that offer to produce deepfakes, although the price is not mentioned, as the users solicit private channels like ICQ and Telegram for requests. Deepfakes are highly effective tools for cybercriminals engaging in social engineering—or duping employees into sharing confidential information—which can lead to exposure of sensitive data or the facilitation of unapproved transactions. There have already been cases of corporate funds being transferred to malicious actors using synthetic audio content to impersonate high-level executives seeking additional credentials or the direct transfer of funds by employees.





The ability to influence public opinion at key moments can negatively affect stock prices and even client or consumer confidence, not to mention the integrity of electoral processes and citizen confidence in public institutions in general, as many experts have noted. Most importantly, deepfakes are simply one building block of multiple ways in which an executive or brand can be attacked by leveraging current—and often easily accessible—capabilities within the digital ecosystem. We predict that as these digital attacks become more sophisticated, they will employ deepfakes as an additional building block in distributed, multi-layered efforts to target high-profile individuals and brands.

- **Alex Romero**, COO at Constella Intelligence



Risks to Individuals, Businesses, and Institutions

The inundation of the digital ecosystem with a combination of malicious actors and compromised personal data exfiltrated from government, enterprise, consumer, and market aggregation databases, reinforces the illicit activities of cybercriminals. In 2020, two critical macro-level forces combined to contribute to an environment that increased the vulnerability of both individuals and organizations operating with a growing dependency on the digital sphere: digital transformation and the COVID-19 pandemic. Digital transformation—already an unstoppable force fundamentally reshaping the way that businesses, governments, and individuals operate—has been dramatically accelerated by the unanticipated circumstances of the COVID-19 pandemic. For continuity and simply to stay afloat, organizations have had to rapidly adapt for the viability of their businesses.

Below, we highlight some of the most notable threats that have been evidenced throughout this report and that are emerging from these new dynamics characterizing the digital ecosystem.

Account Takeover

Criminals are leveraging password combo breaches (email addresses or usernames and associated clear text passwords) to take over personal and business accounts. Account takeover (ATO) is a form of identity theft perpetrated by fraudsters using stolen personal data, such as usernames, passwords, email addresses, or other PII, to illegally gain access to a victim's online account - which can lead to unauthorized transactions, extraction of sensitive data or infiltration of an organization's infrastructure. These attacks primarily occur using two techniques: credential cracking and credential stuffing. Credential cracking uses automated brute-force to identify the correct login credentials, whereas credential stuffing takes troves of exposed credentials to "stuff" them into a login page. When people re-use login credentials for many different accounts, threat actors can access multiple accounts with one credential.

A 2021 report by Security.org examining the prevalence of ATO found that 22% of U.S. adults have been victims of account takeovers, 60% of account takeover victims used the same password as the compromised account across multiple accounts, and social media accounts made up 51% of the accounts taken over, while bank accounts were the second-most common at 32%.

To get ahead of cybercriminals, people should use unique, complex passwords for all accounts. Making use of a reliable, trusted password manager to keep track of this information and opting for multi-factor authentication whenever possible is a best practice that everyone should adhere to. Consumers should also invest in identity protection services for themselves and their families to offer an additional layer of security.

Business Email Compromise (BEC), Email Account Compromise (EAC), and Impersonation Attacks

ATO can be carried out in several ways, including Business Email Compromise (BEC), one of the most financially pernicious digital crimes. BEC exploits our personal and professional dependencies on email to conduct business, creating particular vulnerabilities for organizations that frequently use wire transfers or have suppliers abroad. The 2020 IC3 Internet Crime Report cited BEC as the number one cybercrime reported to the FBI—causing \$1.8 billion in confirmed losses, or 37% of all cybercrime losses in 2020.

Impersonation attacks can be both a threat to executives as well as a dangerous form of brand abuse. In recent years, impersonation attacks have been executed with increasing complexity and sophistication, employing TTPs including imitation domains, fake social media accounts, fraudulent applications, and fake customer support services. Once again, the proliferation of PII circulating in the digital ecosystem enables threat actors to launch more successful targeted and multi-vector attacks.

In an EAC attack, messages come from a trusted source due to attackers obtaining access to user inboxes through credential theft (using malware, phishing, or other methods). This allows attackers to steal data from within an organization and even send emails within and outside of the organization, potentially to employees or clients. The major difference between BEC and EAC is that in a BEC attack, the cybercriminal is outside of the organizational infrastructure, while in an EAC attack the attacker has infiltrated the corporate network. In addition to the oft-recommended cybersecurity best practices, businesses and institutions should proactively assess their employee and domain email vulnerabilities leveraging breached identity intelligence to effectively safeguard their organization's infrastructure, finances and company assets.



Ransomware

In May 2021, Colonial Pipeline paid hackers almost \$5 million in ransom to restore its systems and get gasoline flowing again after a ransomware attack held the USA's largest pipeline hostage, resulting in widespread disruption of gasoline supply. If you are in the healthcare, financial services, or public administration sectors, there's a high probability that you will be hit with a ransomware attack if it has not already occurred.

Payments to ransomware attackers rose 337% from 2019 to 2020, rising to more than \$400 million worth of cryptocurrency, according to figures by Chainalysis, a blockchain analysis company. Hackers have collected more than \$81 million, and the average ransom payment has skyrocketed from \$12,000 in the fourth quarter of 2019 to \$54,000 in the first quarter of 2021. Given a choice between losing sensitive data or paying money to cybercriminals, there is a serious likelihood that you will pay. "This creates a collective action problem—the bad guys win so they'll go out and hit someone else," said Betsy Cooper, director of Aspen Tech Policy Hub at the Aspen Institute. "As an organization, you have to take into account the immediate costs versus the cost of your data. The less prepared you are, the worse it's going to be."

However, this segment of the criminal ecosystem has been evolving into a commodified and specialized ecosystem, with new providers offering rich technical PII as a service. "We saw this approach evolve out of the ransomware space," he says. "I don't need to be a programming expert anymore. I can buy a kit, or I can buy the information, or I can buy access. All I need to do is execute my scheme—someone else is providing the crime technology as a service." It's undeniable that this challenge is rampant and creates complex situations for cybersecurity and risk and reputational teams alike, and it appears that ransomware groups are getting more hostile and are less likely to restore systems, even when they are paid the ransom.



This agile adaptation has been remarkable and commendable. However, the normally gradual process of digital transformation expands the digital footprints of organizations and increases threat surfaces. This process was accelerated in a way that did not allow for the necessary evolution in both the security culture and infrastructure to ensure the protection of companies and individuals.

- **Jonathan Nelson**, Media, Partnerships, and Special Projects at Constella Intelligence

Conclusion and Recommendations

2020 was a tumultuous and painful year across the globe—but it was undoubtedly a productive year for cybercriminals. As the world suddenly shifted toward hybrid and remote work models, and thousands of brands pivoted toward a greater reliance on digital services, cybercriminals went to work, harvesting PII, finding new sources of value amidst the COVID-19 epidemic, and positioning themselves for the next wave of attacks, on higher value, more critical infrastructure.

The trends identified by Constella through this comprehensive analysis of breached and leaked data circulating in underground forums and the deep and dark web offer unmatched insight into the landscape of digital risks and the evolving tactics of threat actors emerging from the digital sphere. As organizations expand their digital reach, virtually all operations and communications are becoming deeply embedded within and dependent upon this shared digital ecosystem. In this environment, effectively all companies, individuals, and institutions are experiencing a dramatic expansion in their digital infrastructures, constituting an expanding attack surface and overall digital risk.

Constella's findings in the 2021 Identity Breach Report demonstrates how threat actors exploit crises as opportunities. The anxieties and concerns associated with the public health crisis that has gripped the globe over the past year and a half have been converted into vectors of attack and exploitation. Cybercriminals are equipped with easier access to the tools necessary to target citizens, executives, high-worth individuals, and the organizations they belong to—as identified in our report with the availability of deepfakes production technology and the availability of botnet networks for sale online. This commodification and general availability of resources that can be used to launch targeted attacks signals significant reputational and financial risks associated with the malicious use of these technologies in the digital sphere.

Constella expects these threats to continue accelerating, with the commercialization of various elements of the breach economy, fuelled by valuable PII, driving greater accessibility and variation of tactics for cybercriminals and threat actors.





Recommendations

Constella's experts' recommendations fall into two categories, **prevention** and **remediation**.

PREVENTION



FOR COMPANIES

- Secure internal corporate systems through a strong, multi-factor authentication password policy.
- Enforce a policy for backup storage, ensuring backups are kept separate from critical corporate systems.
- Implement strong encryption algorithms for corporate databases. Frequently used encryption algorithms, including MD5 and SHA1, have been proven relatively vulnerable.
- Invest in education and awareness of employees and executives regarding digital threats and cyberattacks including but not limited to phishing, fraud, online scams, malware, ransomware, account takeover, impersonation, and more.
- Leverage advanced threat intelligence to understand and protect attack surfaces through proactive monitoring of risks across the surface, deep, and dark web.



FOR EXECUTIVES AND INDIVIDUALS

- Avoid the use of corporate email outside of the corporate environment. This will reduce the likelihood of corporate credentials being exposed in future data breaches.
- Limit the use of personal data (including data related to the private or family spheres) in both the corporate environment as well as on social networks.
- Use a secure and strong password that meets the established security policies of your organization.

REMEDIATION



FOR COMPANIES

- Request that employees or clients affected by an attack change and reset their passwords
- Implement cyberattack prevention policies if they have not been already implemented. Review existing prevention policies and analyze the attack or possible security breach to identify and improve the flaws or vectors of attack that permitted the security incident.



FOR EXECUTIVES AND INDIVIDUALS

- Reset and change passwords of affected accounts.
- Communicate the attack and/or theft of any account or information. Attackers imitate executives or employees to obtain more information or infiltrate internal systems. As such, warning of attacks or thefts when they are identified can prevent future successful phishing or impersonation attacks.

About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to safeguard what matters most and defeat digital risk. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your executives, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45B curated identity records spanning 125 countries and 53 languages.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your executives, your assets and your brand visit us at constellaintelligence.com

Why Constella

OUR TEAM

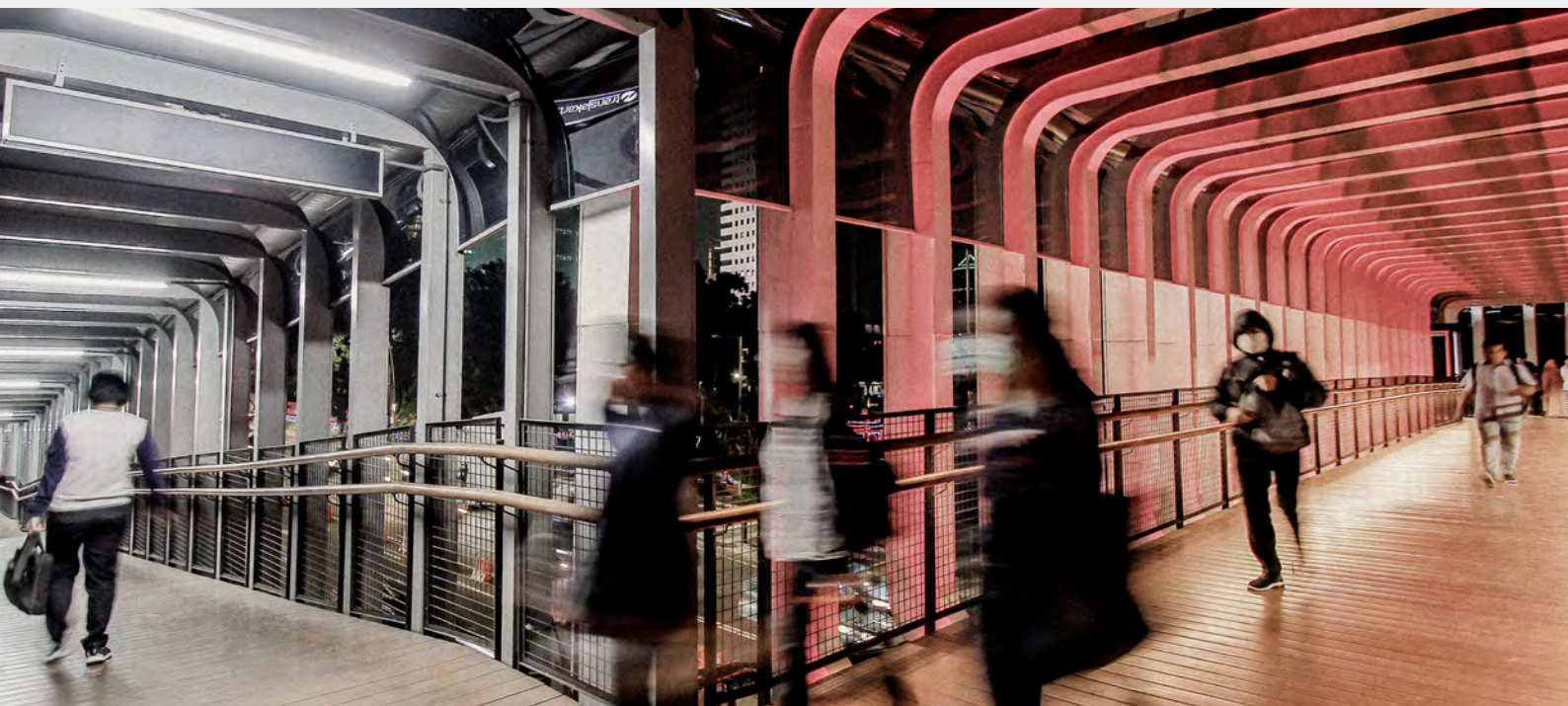
We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify threats and reduce risks emerging from the surface, deep, and dark web.

OUR DIFFERENCE

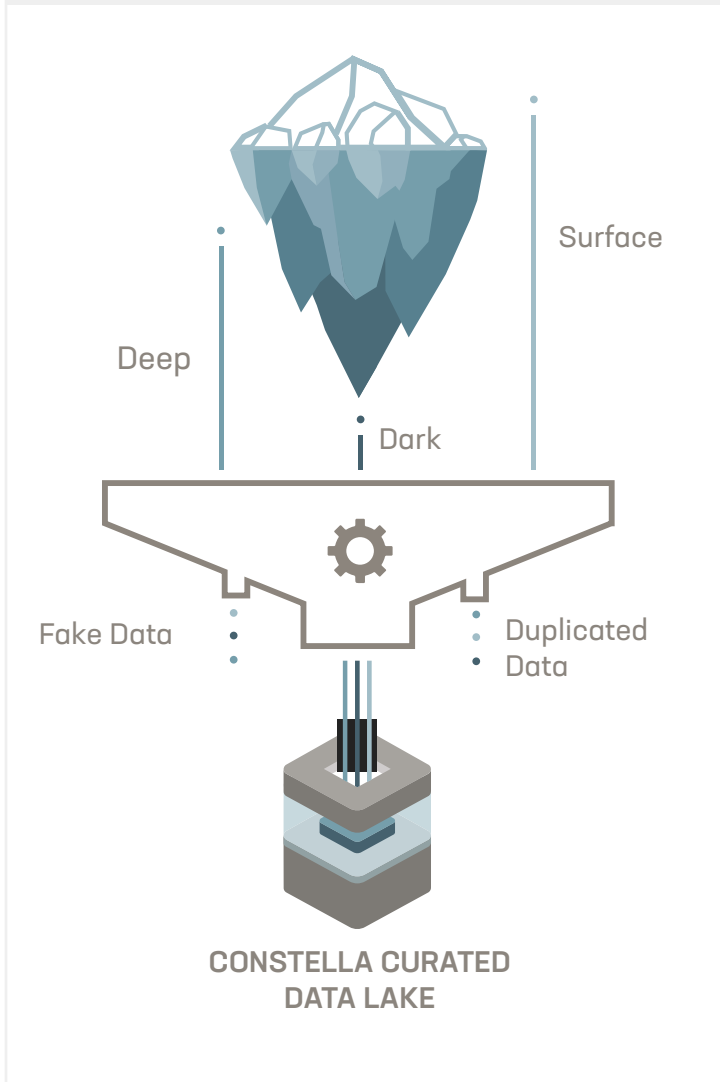
Our unique technology empowers advanced analysis across the entire risk surface for superior anticipation, protecting organizations, their individuals, and their critical assets. Because, the best way to overcome future threats is by facing them today.



Annex

16 Data Verification/Methodology

FIGURE 15. CONSTELLA DATA VALIDATION AND CURATION



While the number of accumulated raw identity records provides insight into the exposure of activity of identity-based data, it is not the best indicator of overall risk.

This is because not all of the data gathered is authentic or unique. After collecting the raw data, Constella analyzes the details using machine learning algorithms, quickly identifying real (not fake) data, flags sensitive information, and removes duplicate records.

Next, breaches undergo a verification process where our analysts and experts use numerous research and investigative methods to ensure that the domain and other breach information are real and valid. The breach is then attributed and normalized.

After a breach is verified, the Constella platform calculates a risk score based on several variables, including types of attributes, date, and password strength.

Glossary

BOTNET

A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer. A collection of these infected computers is known as a “botnet” and is controlled by the hacker or “bot-herder”.

BRAND ABUSE

Ranging from unintentional misuse to intentional impersonation, brand abuse occurs across a range of channels such as email, domains, instant messaging, social media, SMS, mobile apps, and more. Brand abuse for example domain abuse or Typosquatting can be used for phishing. Brand abuse can damage reputation, impact financials and disrupt customer communications.

COUNTERFEIT

An imitation of something with the intention to deceive. Examples of counterfeit products: driver’s license, social security card, passports and other documents, checks, currency, software, shoes and other branded products.

CREDENTIALS

In Internet security, credentials are a form of identification or tools for authentication that proves a person’s identity. Credentials are typically in the form of a user ID (or username) and password to prove a person’s identity in order to allow access to a website or account.

Accounts of employees and executives are often hacked and their usernames and/or passwords published and even sold in the deep and dark Web for fraud or scam purposes.

DATA BREACH

The occurrence of disclosure of confidential information, access to confidential information, destruction of data assets or abusive use of a private IT environment. Generally, a data breach results in internal data being made accessible to external entities without authorization.

DATA LEAKAGE

Unauthorized electronic or physical transfer of information from within an organization to external sources. This may not be with malicious intent; it could be accidental due to human error.

DATA LOSS

When valuable or sensitive information is compromised, or destroyed due to error, malware, theft or system failures.

DATA LOSS INCIDENT

An information security incident that puts institutional data at risk. Incidents can include data being copied, transmitted, leaked, lost, viewed, or stolen and used by an unauthorized individual(s).

FRAUD, SCAM, ETC

Any fraudulent business or scheme that takes money or goods from an unsuspecting person.

EXECUTIVE PROFILE

Digital footprint and exposed personal information of a company executive found in the surface Web, on social media, in the news, blogs, etc.

HACKTIVISM

Hacking as a form of activism, either politically or socially motivated. Hacktivism has several meanings, and “was coined to characterize electronic direct action toward social change by combining programming skills with critical thinking.” - Wikipedia source.

HIDDEN SERVICES

Also Known as Onion sites. Anonymous hidden websites reachable via the Tor network. The purpose of this network is to provide various kinds of services while the identities of the provider and the user are hidden and anonymous.

HIJACKING, FAKES

A type of network security attack in which the attacker takes control of a communication - just as an airplane hijacker takes control of a flight - between two entities and masquerades as one of the entities.

IDENTITIES

User and / or account names and personal information WITHOUT passwords published on the Internet. When found with a password, the combination is called a 'credential'.

IDENTITY FRAUD

A form of identity theft in which a transaction, typically financial, is performed using the stolen identity of another individual. The fraud is due to the attacker impersonating someone else.

INSIDER DAMAGE

An employee leaking information from inside the company.

PII

Personally identifiable information (PII) is any data that potentially distinguishes, traces or identifies an individual. This data can be sensitive or non-sensitive. Sensitive PII can result in harm to the individual if breached. Sensitive PII includes medical information, passport or security numbers, financial information, mother's maiden name, etc. Both sensitive and non-sensitive PII can be combined to aid in harmful exploits, including stalking, stealing the identity, or other criminal acts.

TYPOSQUATTING

Typosquatting, also called URL hijacking, a sting site, or a fake URL. It is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typographical errors made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL, including an alternative website owned by a cybersquatter.

This technique is used by a cybersquatter to attract website traffic by redirecting common types of popular search terms or major websites to their own sites. For example: google.com, etc.