Constella

2022 Identity Breach Report

Exposed Data and the Convergence of Consumer, Business and Geopolitical Risk

2022 | Annual Report

Introduction:

Conflict, Crisis, and Threats to Critical Infrastructure

A crisis causes a ripple effect that impacts the cyber landscape; however, the long-term effects may be difficult to identify while the event is ongoing. Recent events, including aggressive vaccine disinformation campaigns, the Colonial Pipeline hack, and Russia's invasion of Ukraine, to name but a few, demonstrate the vulnerability of organizations, their people, and their personal data to nefarious forces.

Threat actors have embraced cyberattacks as a weapon of malign influence, disrupting essential services or infrastructures, and sowing discord. They often prey on communities susceptible to disinformation campaigns and propagandistic narratives, or target government services during periods of increased instability. Our most vulnerable moments present opportunities for fringe groups, hackers, or threat actors to strike. Industries including the financial sector, Healthcare, energy and telecommunications are just a few examples of prime targets for attacks. Any disruption leaves critical infrastructures at risk of paralysis or failure. As threats to IT and digital infrastructure become more deeply connected with risks to brands, individuals, physical infrastructure, and business continuity, to protect ourselves we must identify patterns in deception, theft, and operations related to cyber events.

As a leader in digital risk protection, Constella Intelligence is committed to raising awareness about the long-term and lesser-known implications of crises. Billions of breached identity records are being transacted and circulated on the deep and dark web right now. Malicious actors will use this private data to exploit executives, brands and governments for malign motives. Combatting this problem requires the private and public sectors to work together to implement safeguards that detect and respond to threat signals—but it all starts with identifying patterns and understanding the changing landscape of cybercrime.

Kailash Ambwani, CEO of Constella Intelligence

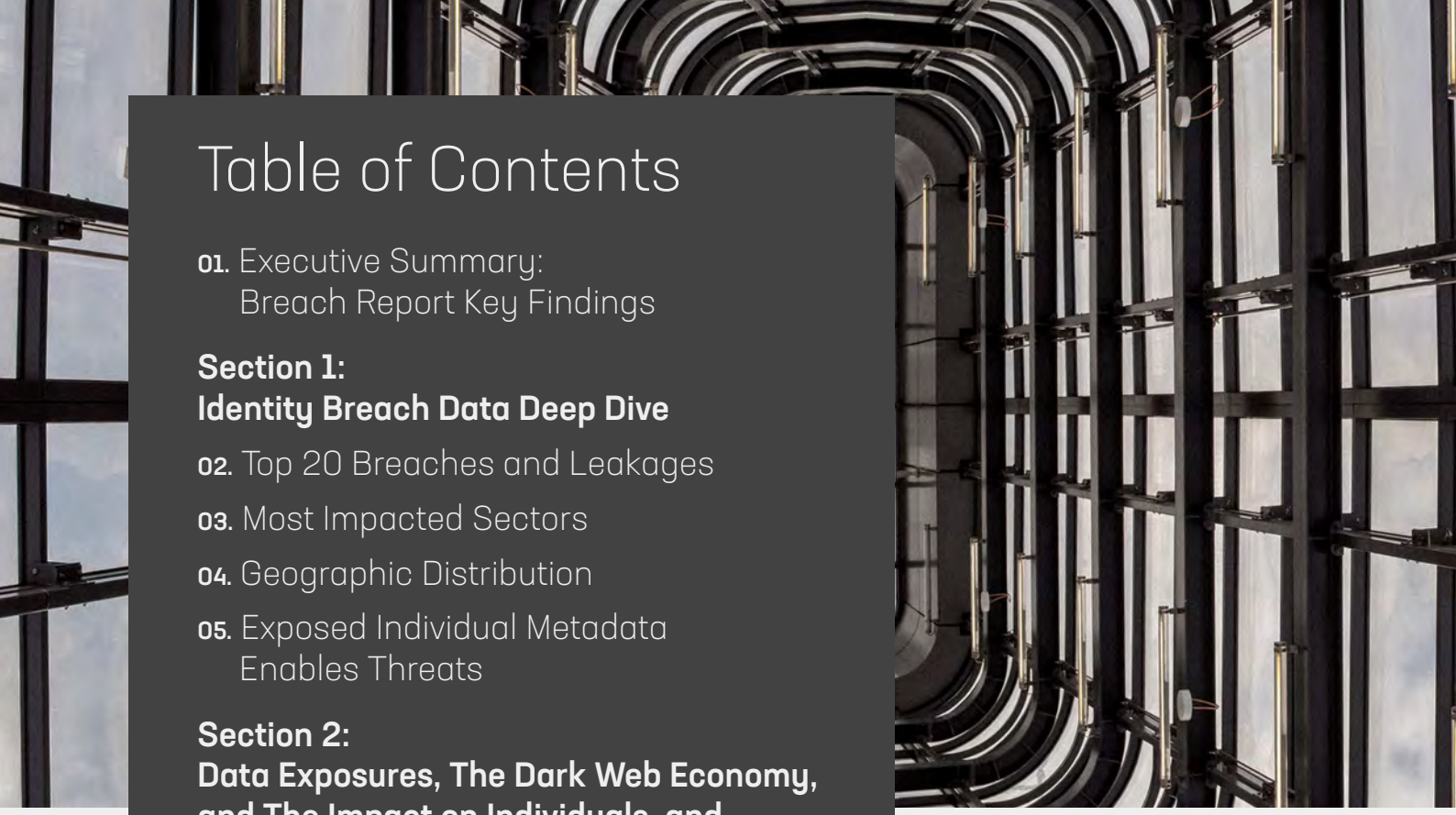


Table of Contents

Executive Summary

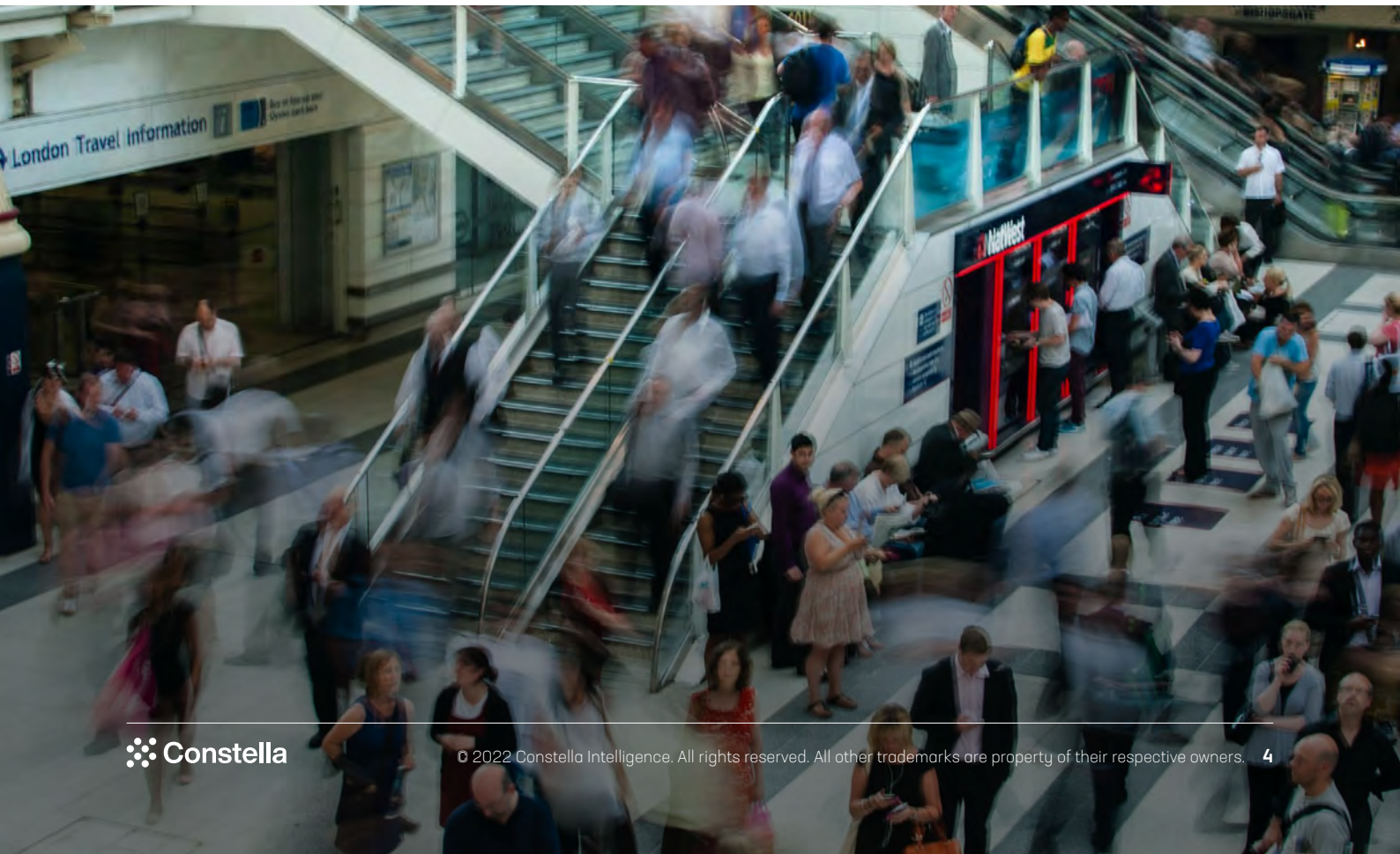
Over the past year, Constella Intelligence detected 66,000 breaches which contained 42 billion personal records. This information now circulates on the deep and dark web. Our 2022 Breach Report sheds light on the tactics, techniques, and procedures (TTPs) employed by threat actors in times of crisis—and how to prevent them.

Through a wide range of TTPs, malicious actors continue to improve their ability to carry out sophisticated attacks by weaponizing personal data. This threat cycle has far-reaching implications for individuals, companies, executives, brands, public institutions, and society at large. How can we detect compromised credentials as soon as the theft takes place? And proactively prevent the use of these credentials by malicious actors before they can do massive harm?

To better understand the key trends related to the metadata constituting these breaches and records, this report analyzes over 1000 of the most significant breaches in 2021, representing over 6M exposed records and 31M exposed attributes worldwide.

This report analyzes the nature of these breaches, their geographic distribution, and the potential consequences of unabated cyberattacks. Additionally, Constella presents a detailed analysis of the inner machinations of digital black markets and provides key context to understand what hackers do with the stolen information.

Constella's 2022 Breach Report offers key insights into these cyber threats and the staggering impact of malign activities fueled by breach data circulating on the deep and dark web. The following key findings represent the most significant and relevant trends for individuals, businesses, brands, and public organizations. This report also includes an extended analysis examining the ongoing conflict in Ukraine.



KEY FINDINGS 2021

1 The breach economy is expanding and diversifying, putting consumers at risk with massive volumes of sensitive personal data proliferating

Exposed sensitive information and personal data continue to proliferate. Our threat intelligence team identified nearly 42 billion exposed records in circulation in 2021, illustrating the high volumes of sensitive data on the dark web that make individuals and organizations more susceptible to fraud, infiltration, and identity-based attacks. Exposed personal attributes like email, name, address, passwords, and others are among the most frequently exposed in breaches, enabling further targeted attacks on individuals and the organizations to which they belong. Moreover, items like credit cards, passports, and IDs all saw significant price increases (>100%) in dark markets in 2021, demonstrating the increasing value of sensitive personal documentation for threat actors.

2 Individual, corporate, and geopolitical risk converge amidst global crises, with critical infrastructure in the crosshairs

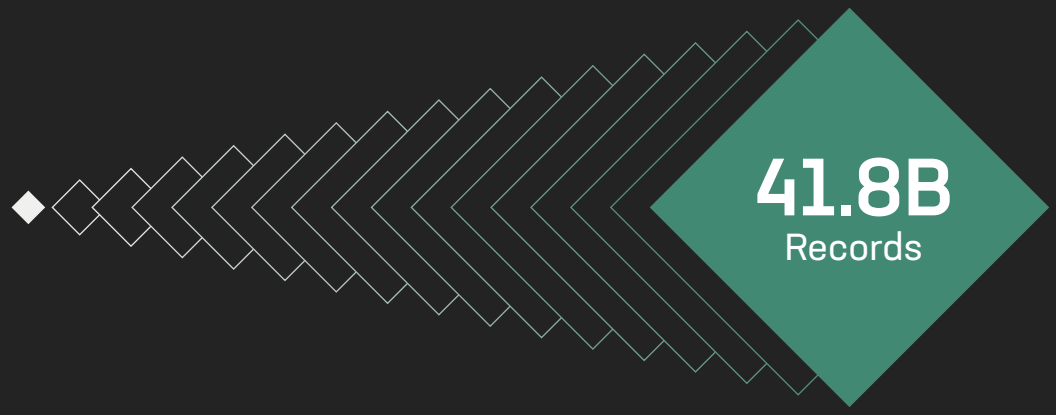
Critical infrastructure companies suffered every 1 in 3 breaches detected in 2021, reinforcing the imminent risks to essential services. Throughout the COVID-19 pandemic, threat intel experts observed increased ransomware attacks targeting healthcare systems. Together, sectors like Services (a categorization that includes Utilities, Telecommunications, Energy, Food, and Transportation), Financial Services, and Healthcare make up over one-third of all breaches and leakages identified. Risks to individuals, businesses and public institutions are converging—and breached sensitive personal data enables the proliferation of more targeted threats. Amidst the diverse TTPs and attack vectors, the individual is the fundamental unit at the center of personal, corporate, institutional, and geopolitical risk.

3 Brands are at greatest risk through their people—exposed executives and employees.

In an analysis of the 30 companies that make up the Dow stock exchange, Constella's threat intelligence team identified over 13K breaches and over 11M exposed personal records related to employee corporate credentials since 2018. The volume and diversity of exposed data from an organization have become a critical dimension of its risk profile, and the risks affecting these companies reach the highest levels. Astoundingly, out of a sample of more than 120 executives (C-suite profiles), 78% had their credentials exposed in a breach since 2018. As external threats expand due to shifting global dynamics—think COVID-19 or the Ukraine crisis—a central risk vector for corporate brands will be the individuals within their organizations.

1 EXPANDING BREACH ECONOMY

66.5K Breaches



41.8B Records

2 CRITICAL INFRASTRUCTURE SUFFERS TARGETED ATTACKS

34.9%

Services, Banking & Finance, and Healthcare make up over 1/3 of all breaches and leakages identified.

26.5%
Services
▲ (+49.1%)

4.9%
Banking & Finance
▲ (+123.8%)

3.5%
Healthcare
▲ (+61.9%)

3 EXPOSED EXECUTIVES AND EMPLOYEES ARE A SIGNIFICANT RISK VECTOR

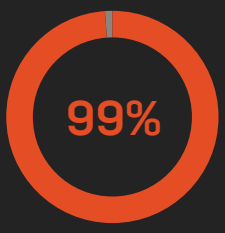
OUT OF A SAMPLE OF 124 EXECUTIVES OF 30 COMPANIES

DOW JONES

78%

have had their corporate credentials exposed in a breach or leakage.

Of those exposed

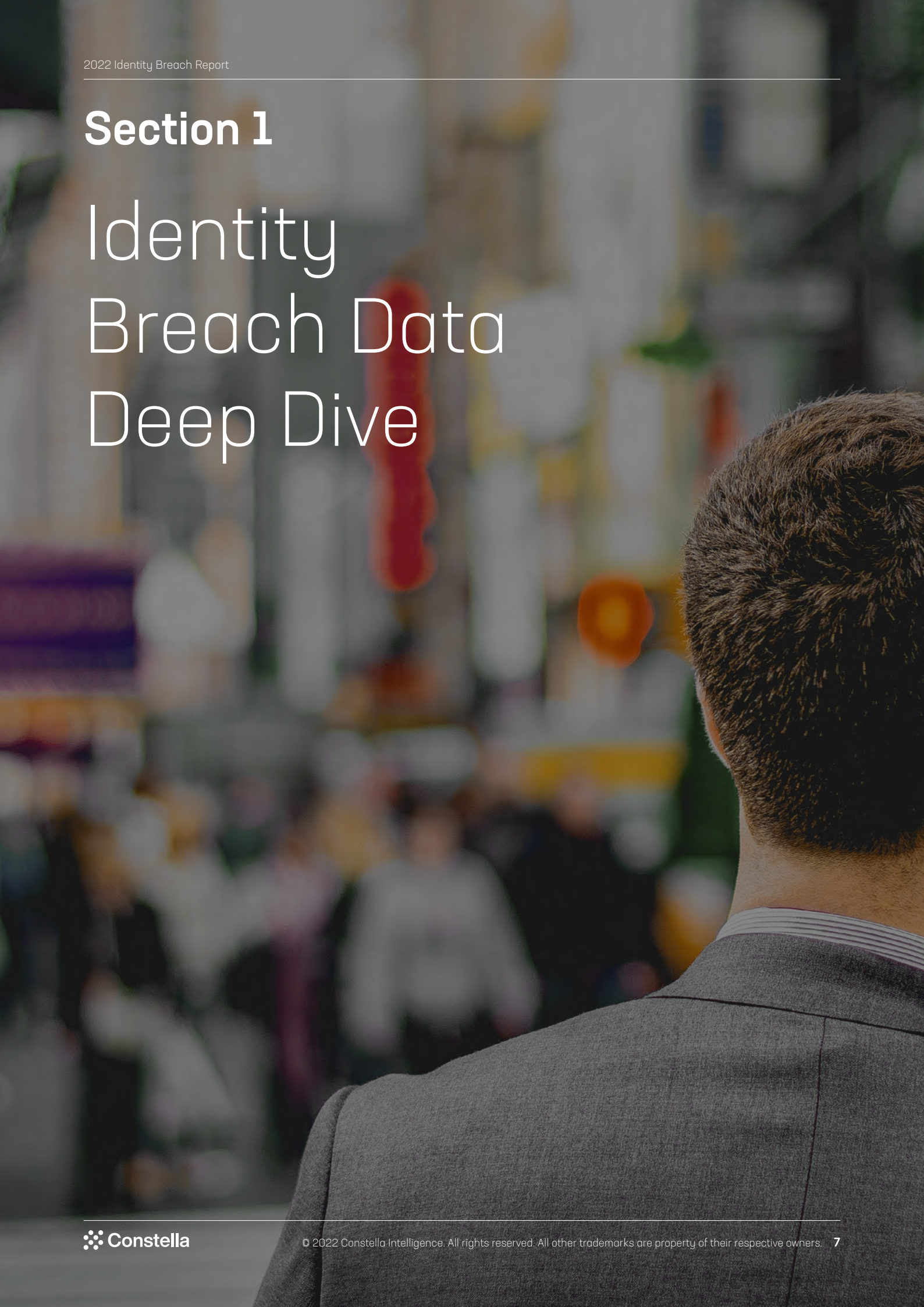


99% have been exposed in breaches or leakages with PII.

Over 1/4 have had their corporate password exposed.

Section 1

Identity Breach Data Deep Dive



02

Top 20 Breaches and Leakages

Internet- and app-based companies dominate the top breaches, exposing massive volumes of consumer data

Constella's threat intelligence team compiled a ranking of the breaches and leakages from 2021 that exposed the most records and personal data. These breaches exposed substantial volumes of personal information. Digital transformation of processes, productivity, and everyday activities increase vulnerabilities by expanding the possible vectors through which a cyberattack can be executed successfully. The high presence of internet- and app-based companies, including companies in the gaming, e-commerce, and technology industries on this list, presents an additional challenge.

raychat.io	157.7M	Customer support service and messaging platform that enables companies to communicate with their customers.
jd.com	118.7M	Internet company and online consumer electronics retailer.
carinfo.app (previously cuvora.com)	99.3M	India's leading RTO vehicle information mobile application.
actmobile.com	87.5M	Technology company and VPN service
gonitro.com	77.2M	Document productivity company which offers PDF document tools
iimjobs.com	65M	Online recruitment platform for middle and senior management positions in India
mmgfusion.com	45.6M	Technology company for dentists, oral surgeons and orthodontists.
bonobos.com	37.9M	E-Commerce driven clothing brand
ticketcounter.nl	33.4M	Technology company for e-ticketing software
rockettxt.com	32.1M	Technology company for SMS integrations
eskimi.com	26.3M	Adtech company
parkmobile.io	26.2M	Smart parking & mobility solutions
bigbasket.com	25.6M	Online food & grocery store
drivesure.com	24.2M	Provides car dealerships services for customers maintenance
indiamart.com	21.5M	Online B2B marketplace
adapt.io	18.4M	Provides access to millions of business contacts
telmex.com	18M	Provides telecommunication systems & telephony services
clearvoicesurveys.com	16.4M	Service to get paid taking surveys
yam.com	16.3M	Chinese e-Commerce
phonehouse.es	12.9M	Mobile phone, telco, and informatics B2C services

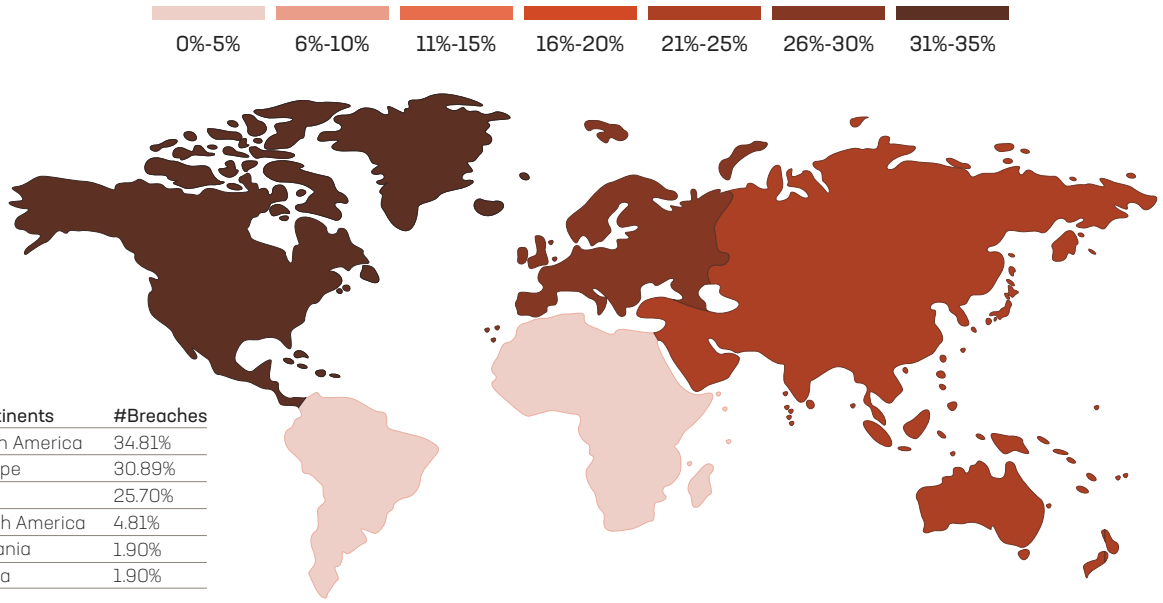
Most Impacted Sectors

Constella's threat intelligence team analyzed the sectors most impacted by the breaches and leakages throughout 2021. Banking & Finance (+123.8%) suffered a higher increase in breaches and leakages than other sectors. In a year when targeted attacks on critical infrastructure, such as Healthcare (+61.9%), characterized the cyber threat landscape, these increases are particularly relevant. Other sectors that saw significant increases included Cryptocurrency (+71.4%) and Travel (+70%).

Geographic Distribution

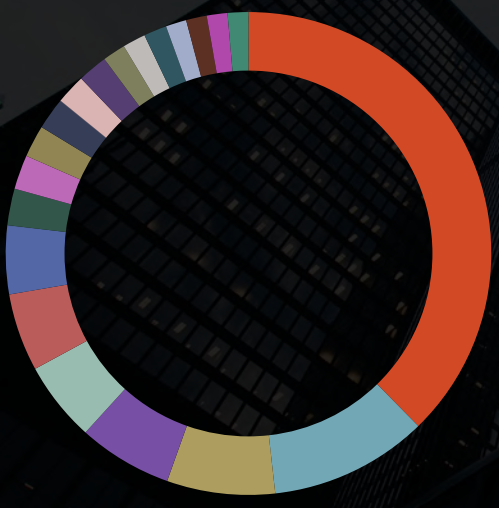
The following map shows the total number of breaches and leakages analyzed in 2021, including the countries in which companies were most frequently impacted. This data indicates which countries were the most affected—based on the location of the impacted companies—and the number of cyber incidents detected in each country. The most affected countries in terms of the volume of breaches and leakages analyzed are the United States, followed by India, Russia, France, Poland, the United Kingdom, Japan, Brazil, Mexico, China, and Germany.

GEOGRAPHIC DISTRIBUTION OF BREACHES



Continents	#Breaches
North America	34.81%
Europe	30.89%
Asia	25.70%
South America	4.81%
Oceania	1.90%
Africa	1.90%

BREACHES DISTRIBUTION



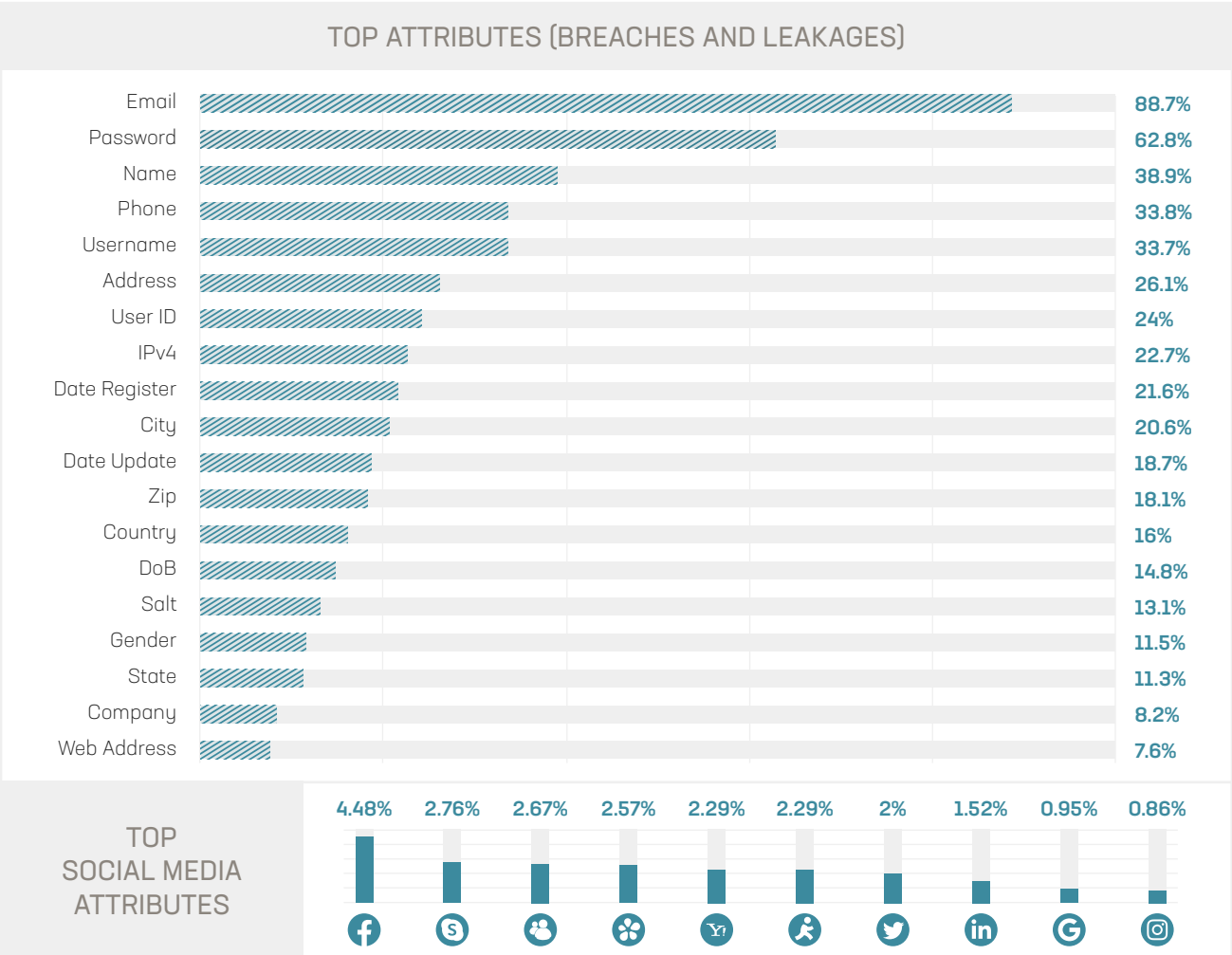
- United States **(31.14%)**
- Russia **(5.95%)**
- Poland **(4.43%)**
- Japan **(3.8%)**
- Mexico **(1.9%)**
- Germany **(1.77%)**
- Canada **(1.65%)**
- South Korea **(1.27%)**
- Indonesia **(1.14%)**
- Turkey **(1.14%)**
- India **(8.73%)**
- France **(5.19%)**
- United Kingdom **(4.3%)**
- Brazil **(2.03%)**
- China **(1.77%)**
- Australia **(1.65%)**
- Italy **(1.27%)**
- Thailand **(1.27%)**
- Argentina **(1.14%)**
- United Arab Emirates **(1.14%)**

05 Exposed Individual Metadata Enables Threats

In analyzing the most frequently exposed attributes related to exposed personal records, our threat intelligence team identified that emails (89%) and passwords (63%) appear in most breaches and leakages. Following emails and passwords are names (39%), usernames (34%), and phone numbers (34%), which were exposed in more than three out of every ten breaches. Additional exposed attributes included personal data like company, gender, registration and update dates, and location-related attributes. This data is beneficial for cybercriminals who harvest credentials and personal information to monetize on the Dark Web or weaponize to commit fraud, account takeover, impersonation, identity theft, and other cybercrimes.

Privileged data tied to an individual and related to social media profiles also proves valuable for threat actors. By connecting exposed social media data with information identified on open sources, threat actors can obtain personal information about their targets, such as locations, workplaces, hobbies, relatives, etc. Cybercriminals can launch more effective and sophisticated impersonation attacks that target associated individuals and entities by procuring this data.

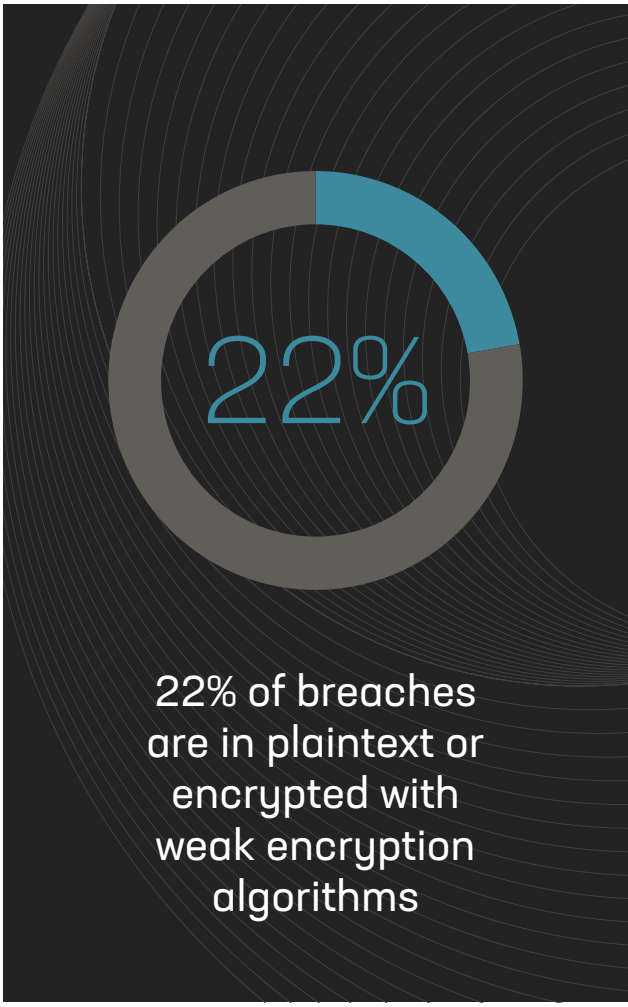
Constella's threat intelligence team observed Facebook, Skype, MSN, ICQ, Yahoo, AIM, Twitter, LinkedIn, Google, and Instagram profiles associated with breaches among the social media attributes detected.



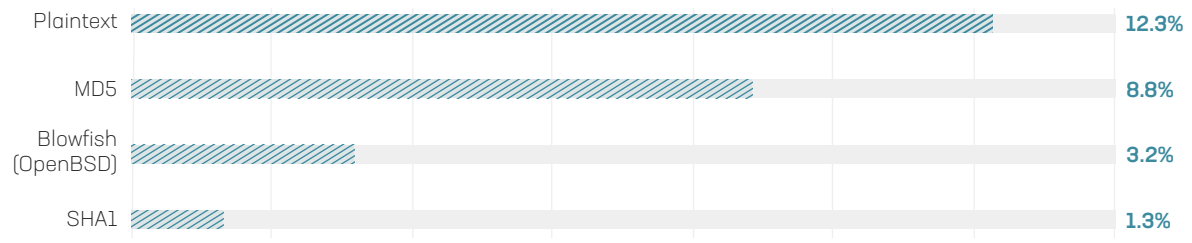
Weak Password Algorithms Increase Personal and Corporate Risk

The graph below details the most frequently detected password algorithms from the breaches analyzed. Password algorithms determine the complexity and uniqueness of passwords, making them more difficult for cybercriminals to crack using targeted tactics, such as wordlists. A wordlist is an index of possible passwords collected in plain text that can enable threat actors to attempt numerous passwords or variations at scale. Together, passwords in plaintext or encrypted with the MD5 or SHA1 algorithms were identified in around 22% of breaches.

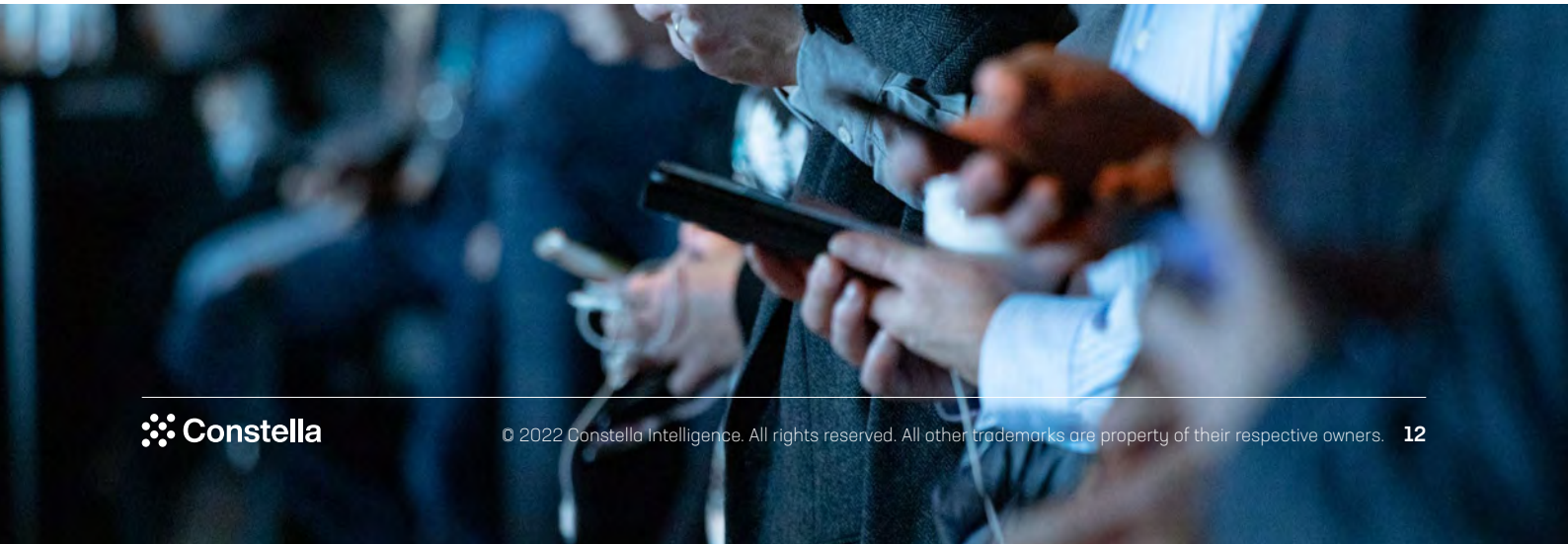
Threat actors target individuals with the intent to steal consumers' identity information or employees' corporate credentials to access enterprise systems and data. Although techniques may vary, the objective is the same—the collection of credentials and personal data that can be monetized or weaponized for future attacks. Attacks like phishing trick users into revealing personal or sensitive information, like usernames or passwords. Once cybercriminals have this information, they can access devices, accounts, or other resources to commit fraud or identity theft, even infecting devices with botnets, or credential-stealing malware, without the user's knowledge.



MOST FREQUENTLY DETECTED PASSWORD ALGORITHMS



*No passwords were detected in 37.19% of breaches.



Section 2

Data Exposures, The Dark Web Economy, and The Impact on Individuals, and Companies

World's Largest Companies Impacted by High-Risk Employee Exposures

Constella's threat intelligence team analyzed personal data from companies on the Dow 30 stock exchange circulating on the deep and dark web to better understand the vulnerabilities of major global companies. The Dow 30 tracks the performance of 30 large-cap stocks in the U.S. that generate significant economic activity. These vulnerabilities represent a combination of human-, technology-, and data-centric risks. Our findings illustrate the vast volumes of personal records tied to corporate credentials that are out there – with 11.3M personal records from more than 13K breaches identified since 2018.

What did our analysis find?

- **11.3M exposed records from over 13K breaches and leakages**, exposing the PII of employees and executives from companies on the DOW 30 stock exchange were identified since 2018.
- **62% of breaches and leakages included PII**, with the most common attributes being email, password, name, username, phone number, address, location-based data (city, state, zip) date of birth. Although to a lesser degree, sensitive data, including credit card information, bank information, relatives' information, and medical information, were also identified.
- A sample of 124 executives (C-suite profiles) from these companies found that **78% of executives were exposed in a third-party breach or leakage** since 2018.

30
COMPANIES

+13,000
BREACHES OR LEAKAGES SINCE 2018

+11,300,000
RECORDS EXPOSED SINCE 2018

OUT OF A SAMPLE OF 124 EXECUTIVES

78%
have had their credentials exposed in a breach or leakage.

Threat actors took advantage of these vulnerabilities throughout the pandemic, increasing efforts to steal data and money through phishing, ransomware, and other attacks. As global geopolitical tensions rise, state- and non-state actors will again take advantage of opportunities to weaponize personal data to compromise companies' cyber-infrastructures. As our research shows, the largest and most essential organizations to the American economy are by no means immune to these risks.

Dow 30 Exposures Related to Corporate Credentials

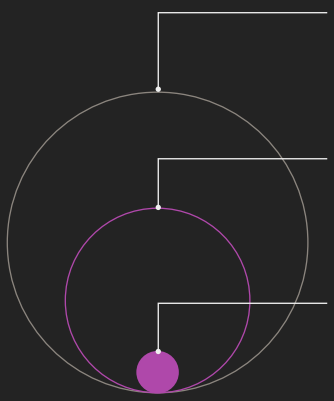
30
COMPANIES

+13,000
BREACHES OR LEAKAGES SINCE 2018

61%
percentage of total breaches or leakages occurring since 2020

+11,300,000
RECORDS EXPOSED SINCE 2018

79%
percentage of total records exposed since 2020

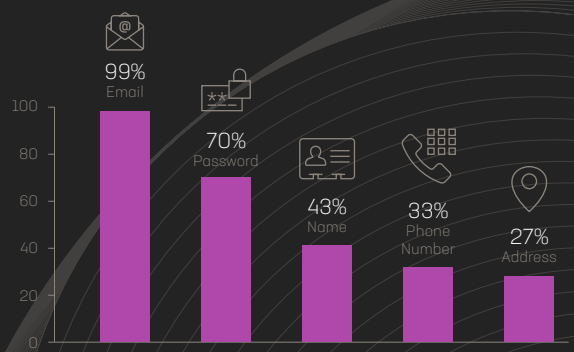


+60%
BREACHES WITH PII

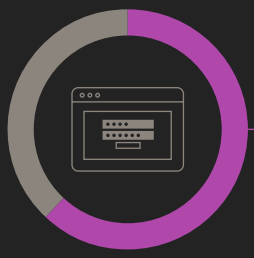
36%
Breaches with only email and password

2%
Breaches with only email

What PII is most commonly exposed?

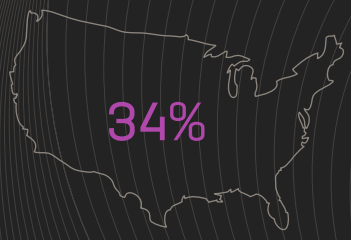


Weak Password Usage



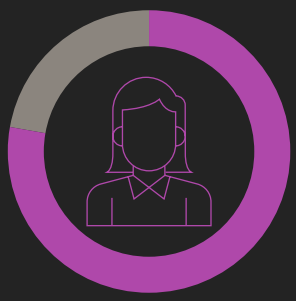
62%
of breaches in 2020 include no password, are in plaintext, or use weak algorithms such as MD5 or SHA1

Where are these breaches taking place?



Over 30% of breaches and leakages of corporate credentials from Dow 30 companies are from sites in the U.S.

OUT OF A SAMPLE OF 124 EXECUTIVES AT COMPANIES LISTED ON THE DOW



78%
have had their corporate credentials exposed in a breach or leakage.

Of those exposed

99%

99% have been exposed in breaches or leakages with PII.

Over 1/4 have had their corporate password exposed.

07 Exposed Data and Illicit Personal Documents Circulating in Dark Markets

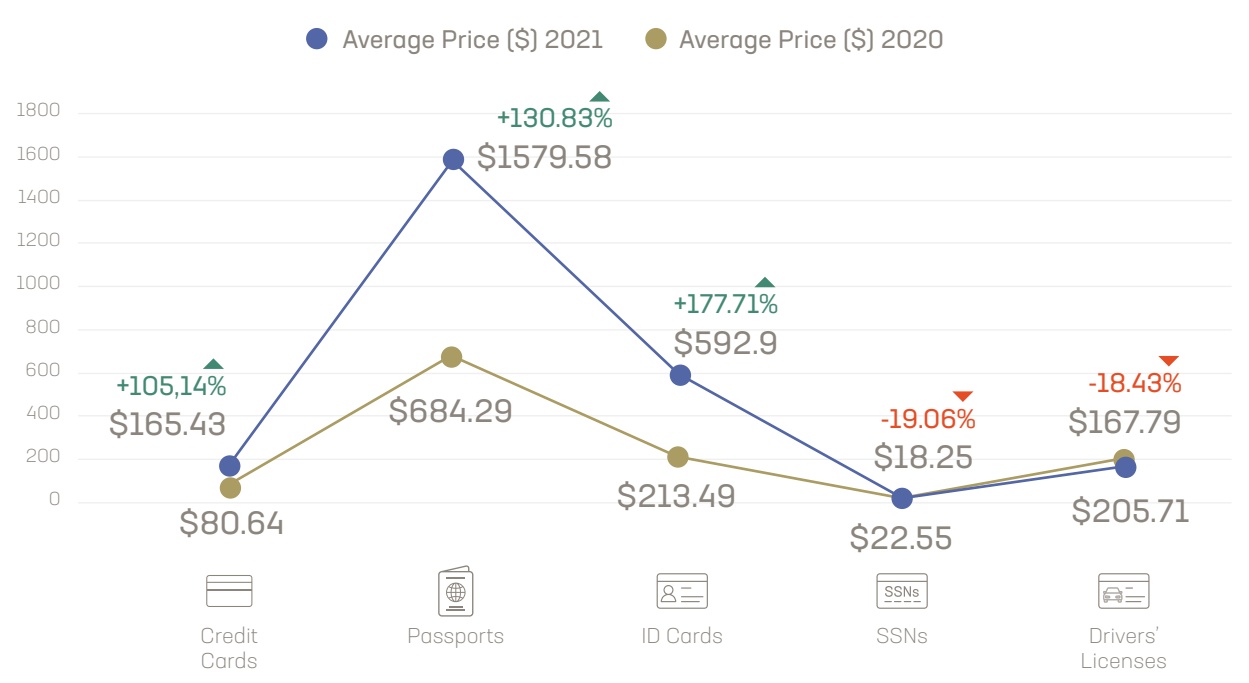
Constella's threat intelligence team analyzed the price of personal identification and financial documents such as credit cards, passports, ID cards, Social Security numbers, and driver's licenses for sale on dark markets. Overwhelmingly, the price for IDs increased substantially (+178%), passports (+131%), and credit cards (+105%) compared to the previous year's data. This jump is likely caused by the need for forms of identification for COVID-19 passports or certificates permitting international travel to countries that require this public health documentation. Dark web sellers perceive this increased instability and reliance on documentation for travel as an opportunity to sell false identification documents. Alongside passports and IDs, credit card price spikes have also likely been driven by a combination of factors, including:

1. **The increased risk of obtaining false or stolen records:** General public awareness about cybersecurity and data protection means that individuals tend to be exposed in less egregious ways. As companies and individuals improve their cybersecurity postures, hackers and threat actors must incur greater risk to obtain this type of data, improving and refining their TTPs to obtain credit card-related data.

2. **The increased benefits for buyers who use false or stolen records:** Credit cards usually contain significant amounts of personal information, which can aid in financial fraud. If one method of attack proves unsuccessful—such as money laundering or making a money withdrawal from an account—there are generally multiple alternative approaches (like impersonation, extortion, and others) through which attackers can benefit.

3. **Global inflationary trends:** Worldwide inflation coinciding with the COVID-19 pandemic corresponds with upward price shifts in dark markets for several types of records and data.

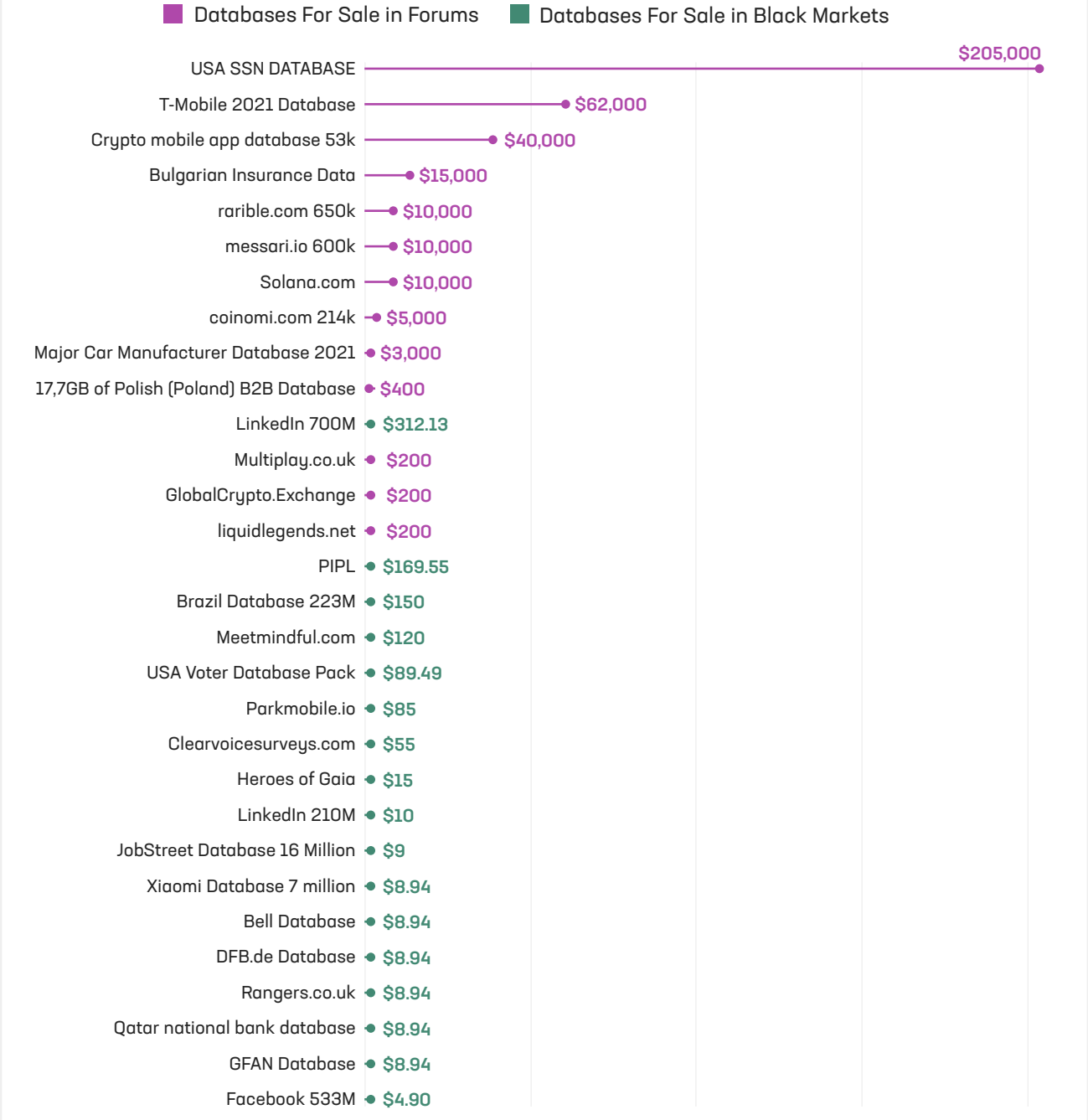
AVERAGE PRICES OF RECORDS FOR SALE IN DARK MARKETS



The Economy of Exposed Data: Breach Databases

When threat actors acquire databases containing massive volumes of personal data, they are often later sold for profit. The circulation of this sensitive data increases individual and corporate risk, as more cybercriminals can use this information maliciously to execute targeted attacks. The differences between the distinct channels where these databases are transacted can be significant. The average price of databases sold in black markets was $61.78, while the average cost of databases sold in deep and dark web forums was $27,769. Recent, high-value breaches appear to be sold more frequently in forums, hiking up the price. Additionally, forums tend to have higher traffic and do not depend on intermediaries for transactions. The following table shows the price of traded or sold databases in dark markets and deep and dark web forums.

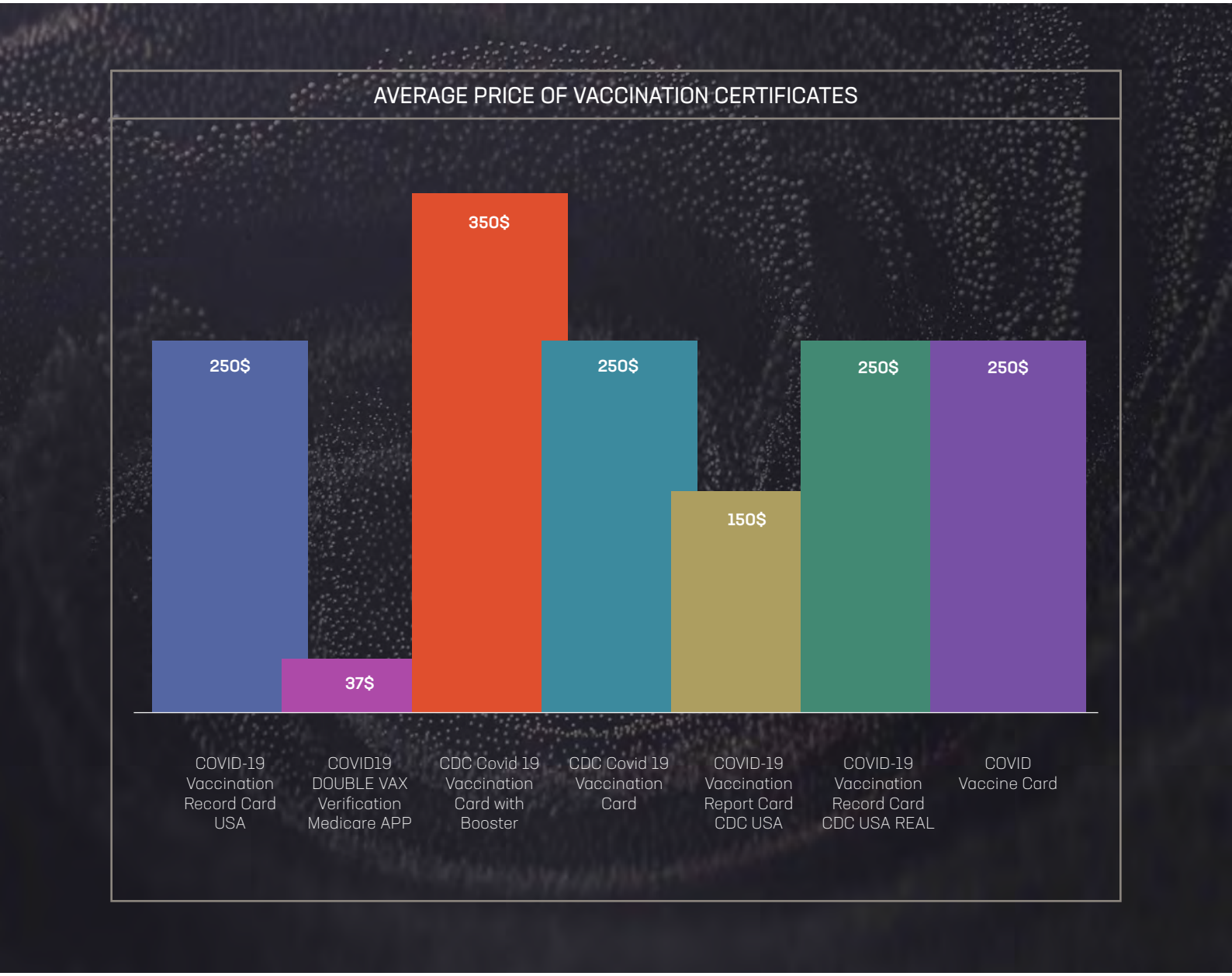
DATABASES IN BLACK MARKETS VS. DATABASES IN FORUMS



COVID-19-related items continue to drive dark market activity

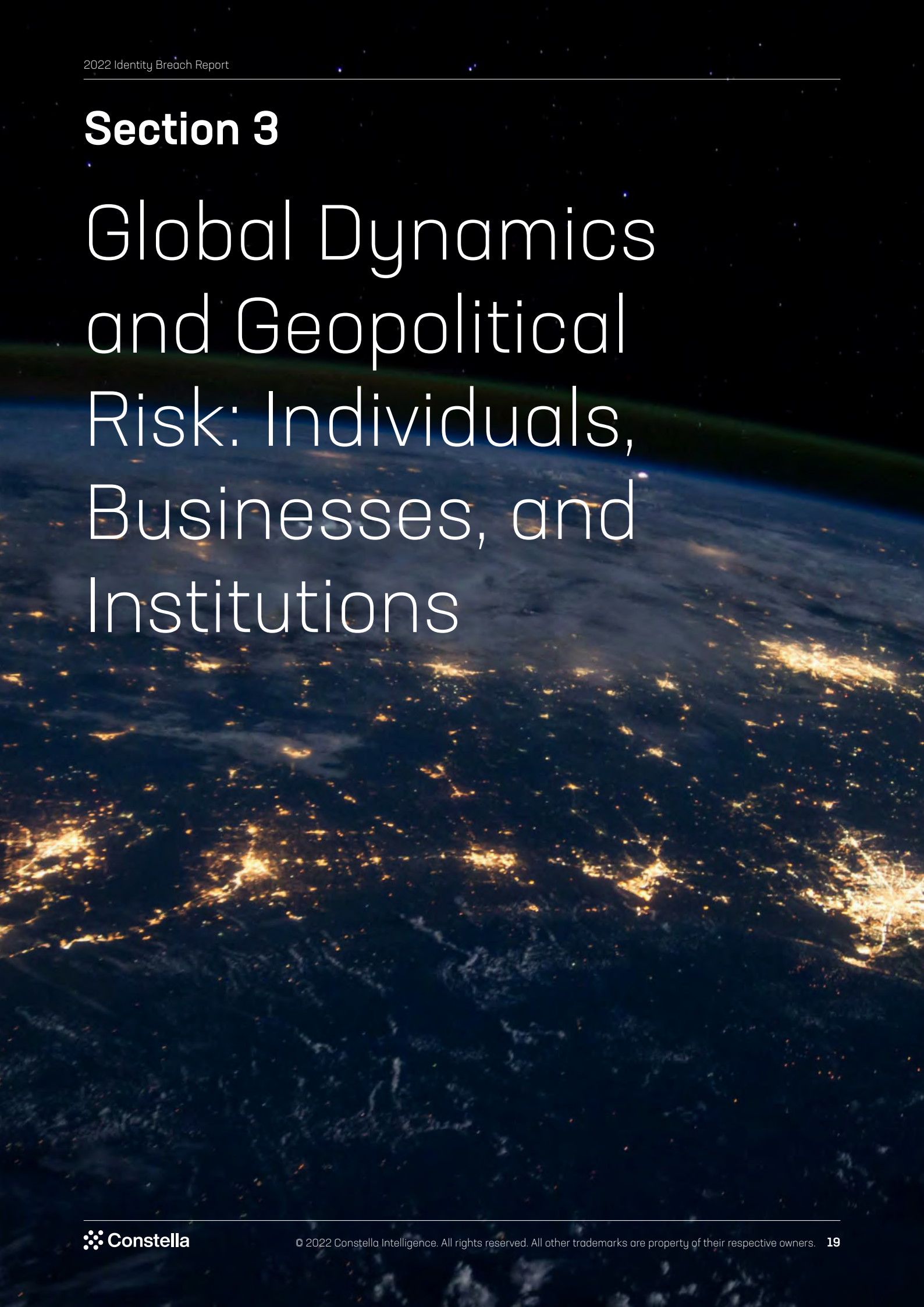
Vaccination certificates and COVID treatments

A significant increase in fake COVID vaccination certificates for sale in 2021 was identified in comparison to the previous year. This shift is likely due to the requirement to show proof of vaccination for travel, work, and other social activities in many countries. Given the rise in anti-vaccine sentiment across segments of the population, the demand for fake COVID-19 certificates and alternative treatments like Ivermectin and Actmera has grown correspondingly. False vaccination certificates, such as counterfeit vaccination cards, were also detected in dark markets and even Telegram groups for sale and purchase. These certificates were identified in black markets like AlphaBay, Incognito, WorldMarket, and ASAP Market.



Section 3

Global Dynamics and Geopolitical Risk: Individuals, Businesses, and Institutions



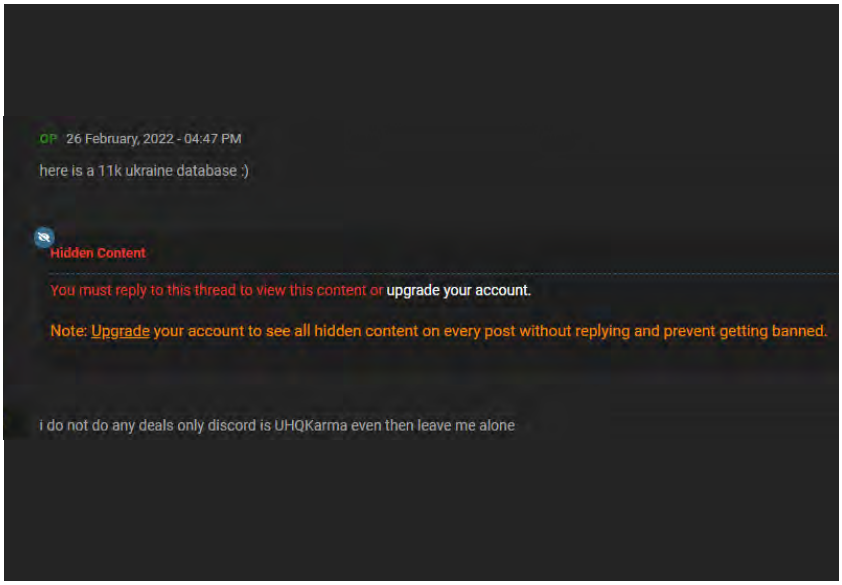
Geopolitical Conflict Drives DDW Activity and New TTPs

The cyber threat landscape directly impacts governmental institutions, public and private organizations, and individuals who make up the general public. Understanding the depth of the deep and dark web (DDW) and the breadth of interactions across these landscapes is an essential asset in effectively anticipating emerging risks and threats. Constella's threat intelligence team extended the period of analysis of the Identity Breach Report (2021) to analyze the TTPs of threat actors relevant to the current geopolitical conflict in Ukraine via deep and dark web activity. Our research offers additional examples of the continuity and commodification of the cyber threat ecosystem, showing how early signals related to the current geopolitical conflict and threat actor activity provided insight into the trends visible today.

Exposed Data and Threat Signals Related to the Ukraine Conflict

Conversations related to the Ukraine-Russia crisis were detected in different DDW underground communities.

Most of the conversations consist of opinions about the current situation, although, to a lesser extent, publications related to passports, data leakages and threats were also detected. Numerous threads were found in DDW forums where users share data leaks affecting both Russian and Ukrainian targets, including companies and websites. Some of these leaks and sales were posted before the Russian invasion, demonstrating the relevance of threat actor activity in dark markets preceding the current conflict.



UKRAINIAN IDENTITIES FOR SALE IN DARK MARKETS

Databases of sensitive data pertaining to Ukrainian identities for sale in dark markets demonstrates the nature of the underground threat economy and the types of transactions that empower the endeavors of threat actors.

26/02/2022 - Database for sale containing data related to 11K Ukrainian identities

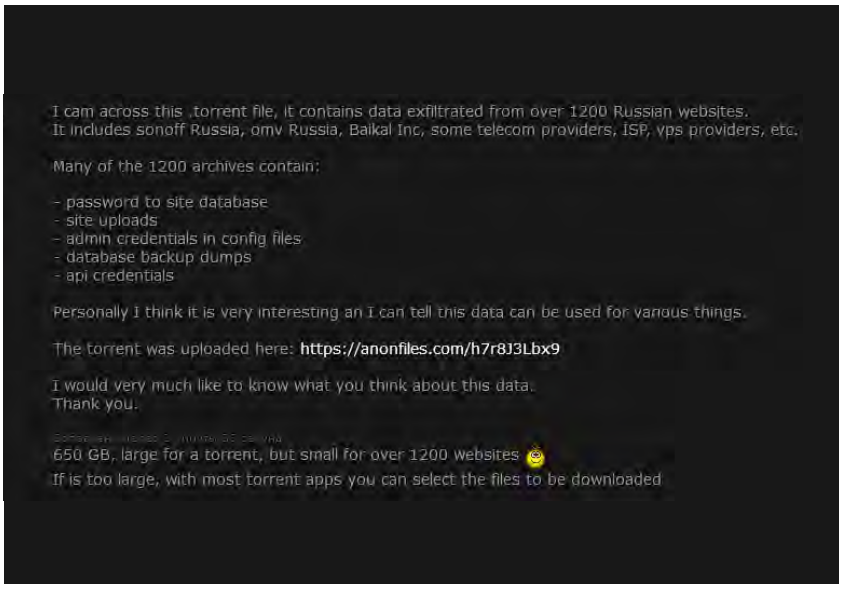
```
Database: People.
Date: up to 04.2020 +-
Format: Cronos.
Language: Ukrainian + Russian.
Quantity: DB count 63M or less unique contacts + 130M aditional records.
Fields:

Full name;
Date of birthday;
Country of birth;
Phone number;
Adress(by 2005, 2006, 2007, 2008, 2014, 2018 and up to 2020) - up to 6 fi
```

UKRAINIAN PII DATABASES FOR SALE IN DARK MARKETS

Before the February 2022 Russian invasion of Ukraine, massive volumes of sensitive citizen data were available for sale in dark markets

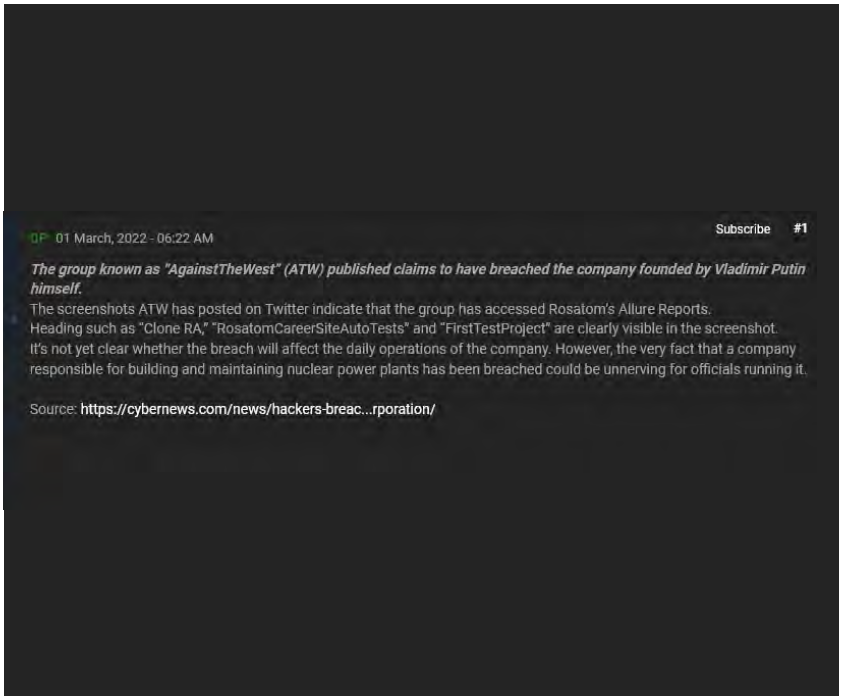
17/01/2022 - Ukraine combo database



WEBSITE DATA EXFILTRATION

Sensitive data that can aid in cyber espionage and cyberattacks exfiltrated from websites of Russian companies. The sale and purchase of this type of data contribute to a robust economy where both Ukrainian and Russian data have been identified.

08/03/2022 - Recent data from 1200 Russian websites



CRITICAL INFRASTRUCTURE BREACH

Anti-Russian hackers claim to have breached a Russian critical infrastructure company responsible for the construction and maintenance of nuclear power plants. The proliferation of this type of sensitive data means that it can be made available to wider communities of individuals with diverse motives.

01/03/2022 - Hackers breach Rosatom, 'Russia's state nuclear energy corporation

Groups & TTPS

At the time of publication of this report, Constella's threat intelligence team had identified 72 groups that had announced their involvement in the conflict (either through taking responsibility for attacks or by leaking information), or have expressly proclaimed their position. Of these 72 identified groups, 47 of them are pro-Ukrainian and 25 are pro-Russian.

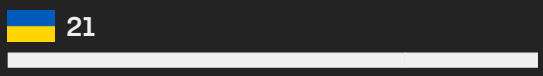
Some of these groups have carried out actions against Ukrainian or Russian targets, while other groups have only shown their support for one of the two sides and their intention to commit solely defensive hacktivist acts.

Due to the sensitivity of the conflict and implications of the participation of state and non-state actors, this section focuses on profiling the most commonly identified tactics, techniques, and procedures of these groups, rather than explicitly naming those identified.

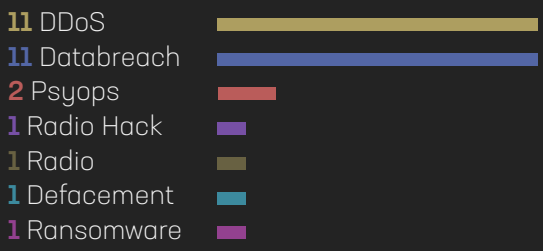
ANONYMOUS-ASSOCIATED ACTORS

of groups: **21**

Supporting:



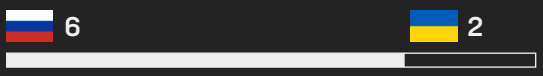
TTPs identified:



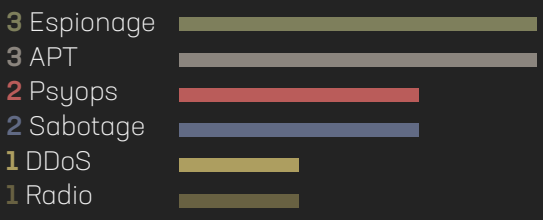
NATION STATE ACTORS

of groups: **8**

Supporting:



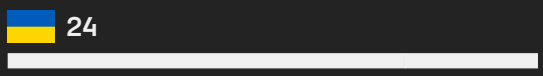
TTPs identified:



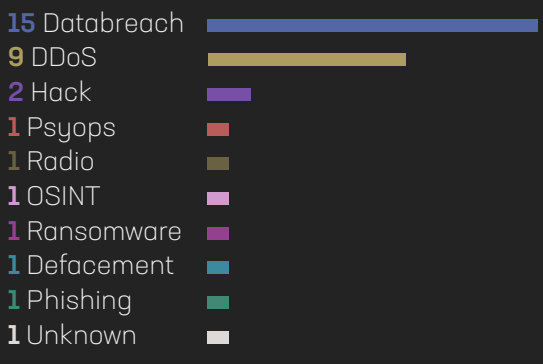
PRO-UKRAINE ACTORS

of groups: **24**

Supporting:



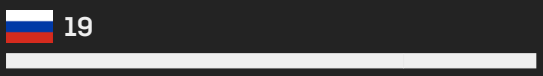
TTPs identified:



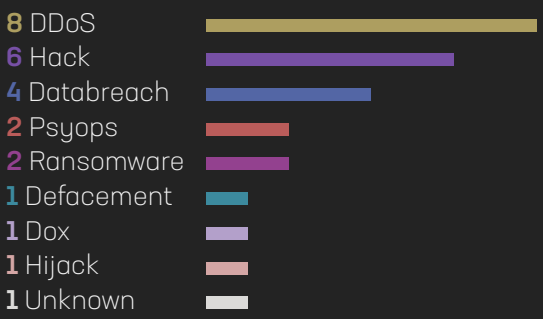
PRO-RUSSIA ACTORS

of groups: **19**

Supporting:



TTPs identified:



Identified TTPs of Engaged Groups

DDoS and Defacement

RISK LEVEL: LOW | MEDIUM | HIGH

Threat actors conduct reconnaissance phases on their targets before deploying a DDoS attack. Those targets are often shared publicly in a list via websites like Pastebin or AnonPaste. Some actors also share scripts inviting other members in the hacking community to conduct DDoS attacks on designated targets, sometimes indicating the level of exposure, sharing Shodan information.

The sophistication level of these attacks is generally low and the impact does not last long, mainly because the infrastructures used to launch these attacks are usually self-hosted.

After successful DDoS attacks, hacktivist groups claim ownership by showing the target name on social media (mainly on Twitter and Telegram), posting links to the "downed website" and sharing screenshots as "proofs".

Databreach

RISK LEVEL: LOW | MEDIUM | HIGH

A data breach is a security violation in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, or used by an unauthorized individual.

Several criminals and activist actors specialized in leaking sensitive information such as RDP, VPN access, and databases have been identified. The majority of the targets have been Ukrainian and Russian government institutions.

Although the threat actors are mostly targeting Russian and Ukrainian institutions or companies, many Russian companies are linked to European companies through subsidiaries or partnerships. Thus, some databases can contain data about European customers.

Moreover, all countries that support the sanctions against Russia are potential cyber targets, and there is a high risk that data leakage attacks will increase in NATO member countries.

Ransomware

RISK LEVEL: LOW | MEDIUM | HIGH

Ransomware is malware employing encryption to hold a victim's information at ransom.

The ransomware group Conti published a message threatening to target the critical infrastructures of states that would go against Russia.

Conti remains the only group openly pronouncing its position related to the conflict in the case of the ransomware groups. This has been notable amid the relative silence of other ransomware gangs, excluding the announcement of LockBit 2.0, which claimed to remain strictly apolitical in its activities.

APT

RISK LEVEL: LOW | MEDIUM | HIGH

An Advanced Persistent Threat (APT) is a type of stealth and continuous hacking that targets a specific entity.

The most important APT threat actor identified is the Gamaredon Group, which is known to be active since at least 2013 and has been attributed to Russia. Gamaredon would have been potentially involved in the conflict with Ukraine since the summer of 2021.

The group is believed to be operating out of Crimea with objectives consistent with cyber espionage. More generally, it appears that their aim is to target various critical actors that could intervene in an emergency context in Ukraine.

Frequent TTPs Employed by Multiple Threat Actors Involved in the Ukraine Crisis

TACTIC	TECHNIQUE
Resource Development	Acquire Infrastructure
Initial Access	Phishing Spearphishing Attachment
Execution	Command & Scripting Interpreter Native API
Defense Evasion	System Information Recovery
Lateral Movement	Remote Services
Command & Control	Application Layer Protocol: Web Protocols

Malware identified includes DinoTrain, DesertDown, DilongTrash, ObfuBerry, ObfuMerry, PowerPunch, Cyclops Blink, SunSeed, Reaper (malware shared by IT Army of Ukraine to conduct DDoS attacks), and Wiper. The above table highlights how phishing and spearphishing are commonly used by these actors to gain initial access to networks, laterally moving within a network to gain access to more sensitive data and high-value assets.

09

Constella's Outlook

The Convergence of Individual, Corporate and Geopolitical Risk

The rapid pace of digital transformation has forever changed how we work, communicate, and do business. While bringing innumerable benefits, digitization and technological progress offer ample opportunities for cybercriminals to exploit an organization's vulnerabilities for malign purposes.

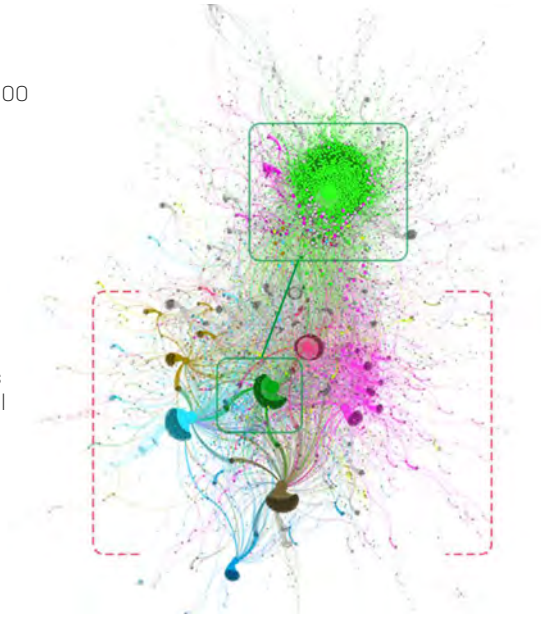
Risks to individuals, businesses and the public sector are converging. Individuals—as consumers, employees, and executives—are targeted for their sensitive personal data. This data powers an increasingly commodified threat economy where personal information is transacted for profit. Consequently, the availability of this data empowers threat actors to leverage it to launch cyberattacks against the companies, institutions, and networks that individuals are a part of. This ecosystem is becoming even more intertwined as geopolitical risks intensify, and critical infrastructure is targeted by state and non-state actors for a combination of economic and political motives. Amidst diverse TTPs and attack vectors, the individual is the fundamental unit at the center of personal, corporate, and institutional risk.

As global trends and instability continue to precipitate cyber risk, organizations will increasingly need to focus on security holistically, connecting the dots in anticipation of digital and physical threats to critical assets—including people and infrastructure. Moreover, the expected increase in attacks targeting individuals and businesses at the periphery of dynamically changing global trends will likely produce further situations in which:

A. Private individuals and organizations will be targeted in cyberattacks and suffer the reputational repercussions of diverse public narratives, exemplifying a core connection between brand defense and cyber risk.

B. Countries may see the deterioration of digital discourse, influenced by conspiratorial narratives and unsubstantiated allegations related to the impact of affected critical infrastructure and vulnerable businesses and individuals within the context of continued geopolitical crises.

USERS: 8,718
INTERACTIONS: 12,862
MAX. AUDIENCE: 13,200,000



— Support for affected company

- - - Mixed conversations in which reputational risk narratives and propaganda are diffused

The size of the node represents its influence within the user's network

The direction of the edge represents the direction of influence (clockwise) between users

The color of the nodes defines the community to which they belong

This community network analysis demonstrates how, after a cyberattack, the proliferation of propagandistic and false narratives were disseminated at speed and scale across the digital public sphere, sowing discord and distrust in both the affected company and the regional digital conversation, thus producing additional layers of risk at the corporate and geopolitical levels.

The rapidly increasing relevance of these threats must be a strategic priority for private companies and public institutions—especially those in sectors delivering and administrating critical infrastructure services.

10

Conclusion and Recommendations

Constella's 2022 Identity Breach Report analyzed the inner workings and dynamics of the surface, deep and dark web, demonstrating the varied nature of threat actors' efforts. Our threat intel experts also spent considerable time analyzing what these hackers do with the data troves that they have stolen. While some simply seek a quick payout by selling credentials online, others exploit this data for sociopolitical motives, which are not always independent of economic incentives—exploiting a combination of social and political vulnerabilities through malign influence. Indeed, the "breach economy" is expanding and rapidly diversifying at the same pace as our digital transformation.

In addition, our research found that critical infrastructure has become a prime target, especially during times of crisis. Our healthcare systems are vulnerable to cyberattacks, and Constella's experts found that critical infrastructure services suffered 1 in 3 breaches in 2021. Moreover, an organization's greatest asset—its people—are principal risk vectors for breaches and other forms of cyber infiltration. In a survey of over 120 leading executives from companies listed on the Dow index, nearly 78% had been exposed to a data breach. Of those exposed, almost all (99%) had their personal information stolen.

Constella anticipates continued geopolitical instability to precipitate breaches and cyberattacks based on our findings and identified trends. Moreover, these attacks will likely happen to our most critical infrastructure—during our most vulnerable times. Preparation and a robust cyber defense will remain essential as organizations venture into the ever-expanding cyber world. Though no breach is entirely preventable, advanced warning and early detection will help to minimize the damage while ensuring a coordinated response against myriad threat actors.

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

Recommendations

PREVENTION

FOR COMPANIES

- Ensure corporate policies include a strong, multi-factor authentication password requirement for all employees and a policy for backup storage, ensuring backups are kept separate from critical corporate systems.
- Incorporate a response strategy for attacks on critical infrastructure in the business continuity plan – including alternative forms of internal communication in the event of an attack. Communicate with partnering agencies or third-party vendors to ensure continuity and preparedness.
- 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 for employees and executives regarding digital threats and cyberattacks, like phishing, fraud, online scams, malware, ransomware, account takeover, impersonation, and others. This should include simulation and tabletop exercises for cyberattacks, cyberwarfare, and threats to critical infrastructure.
- Leverage advanced threat intelligence to understand and protect attack surfaces through proactive monitoring of risks across the surface, social, deep, and dark web.
- Invest in employee protection at all levels, including monitoring leaked credentials of executive leadership and lower-level employees.

FOR INDIVIDUALS, EMPLOYEES, AND EXECUTIVES

- Avoid the use of corporate email accounts outside of the corporate environment. This will reduce the likelihood of corporate credentials exposure in future data breaches.
- Change passwords regularly and encourage others to do the same. Avoid re-using company passwords for personal accounts.
- 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.
- Attend and participate in corporate training exercises in preparation of potential cyber threats.

REMEDIATION

FOR COMPANIES

- Request that employees or clients affected by an attack change and reset their passwords.
- Utilize an alternative communications platform (alternative emails, devices, etc.) in the event of a system shutdown. Ensure that employees are aware of the alternate platform before an incident occurs.
- Implement cyberattack prevention policies if they'venot 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.
- Alert your organization of a potential attack – whether personal or from corporate credentials – immediately to ensure swift remediation efforts can be made, if necessary.
- 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.

Annex

ANEX 11.1

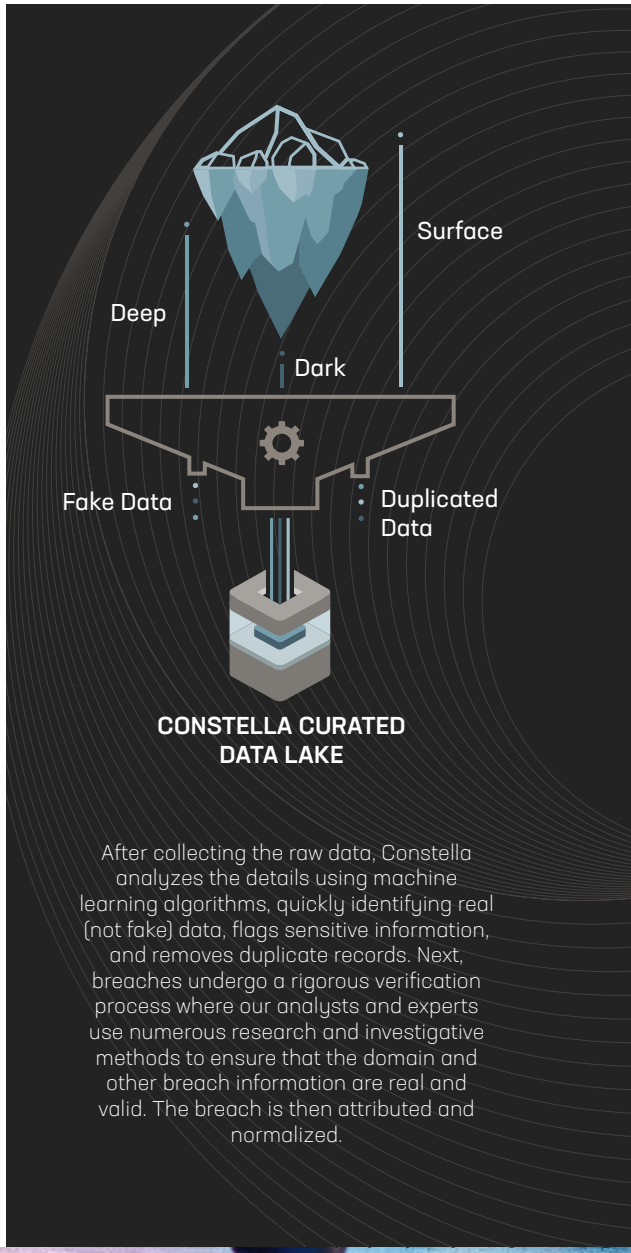
About This Report

Constella has monitored the TTPs of threat actors closely and developed this report based on breaches and leakages identified in 2021. In addition to the known breaches and leakages reported in the media, Constella detects information found in data dumps posted in the open, but often transient, sources in the deep and dark web. 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, cleans, and attributes the data to further understand the severity of risks facing consumers and companies. Constella then alerts the impacted parties 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



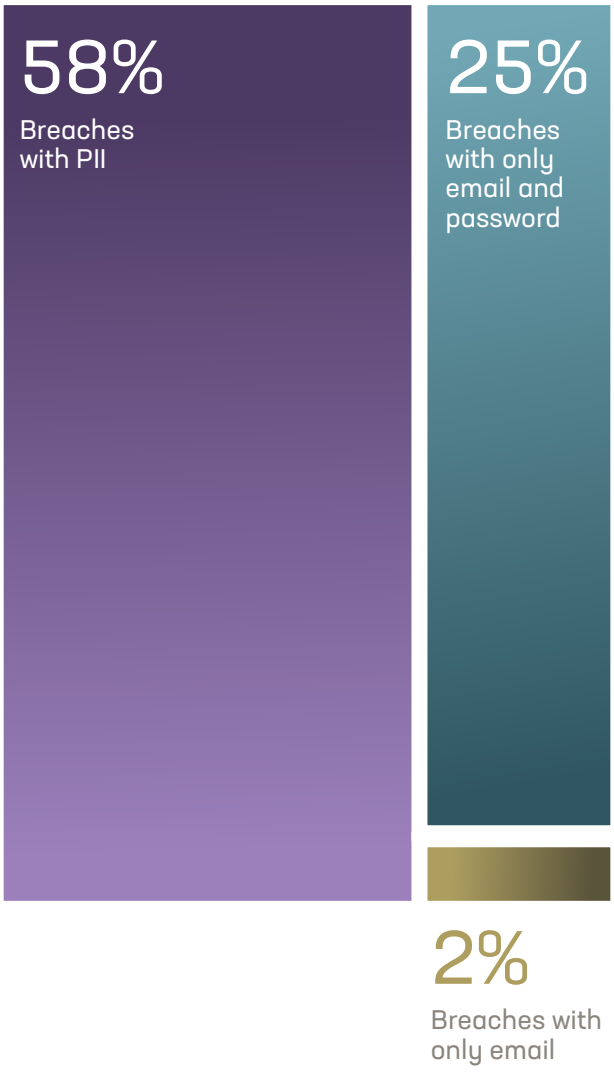
After collecting the raw data, Constella analyzes the details using machine learning algorithms, quickly identifying real (not fake) data, flags sensitive information, and removes duplicate records. Next, breaches undergo a rigorous verification process where our analysts and experts use numerous research and investigative methods to ensure that the domain and other breach information are real and valid. The breach is then attributed and normalized.

ANEX 11.2

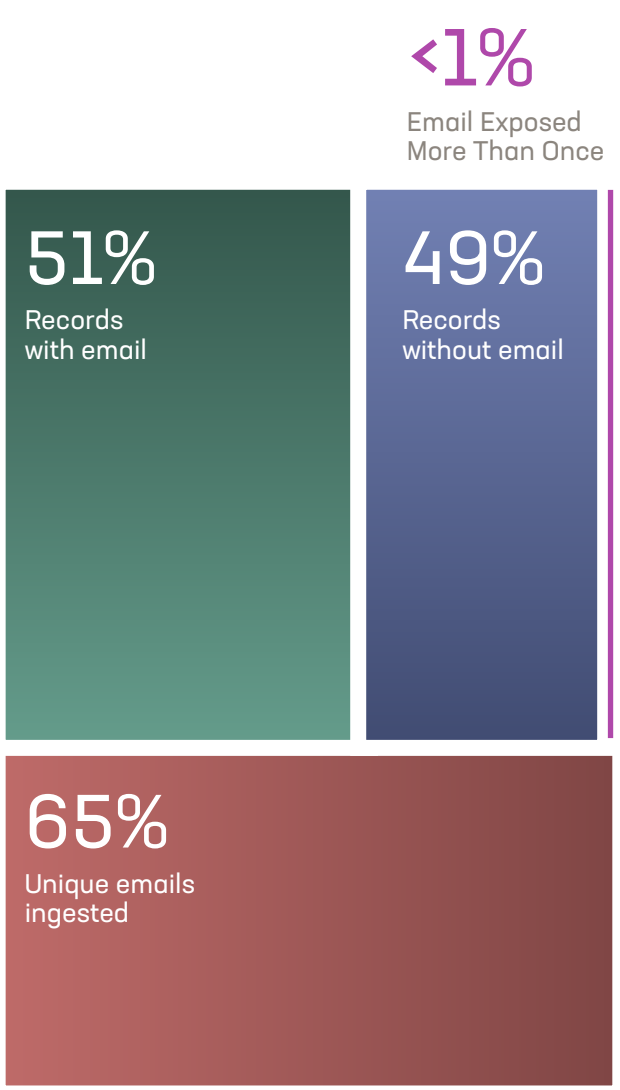
General Metrics & Data Composition

The below graphics illustrate the breakdown of breach data in the Constella Intelligence data lake based on the data analyzed and the sources from which these breaches were obtained. Notably, nearly 60% of breaches contained PII.

TOTAL BREACHES COMPOSITION & PERCENTAGES

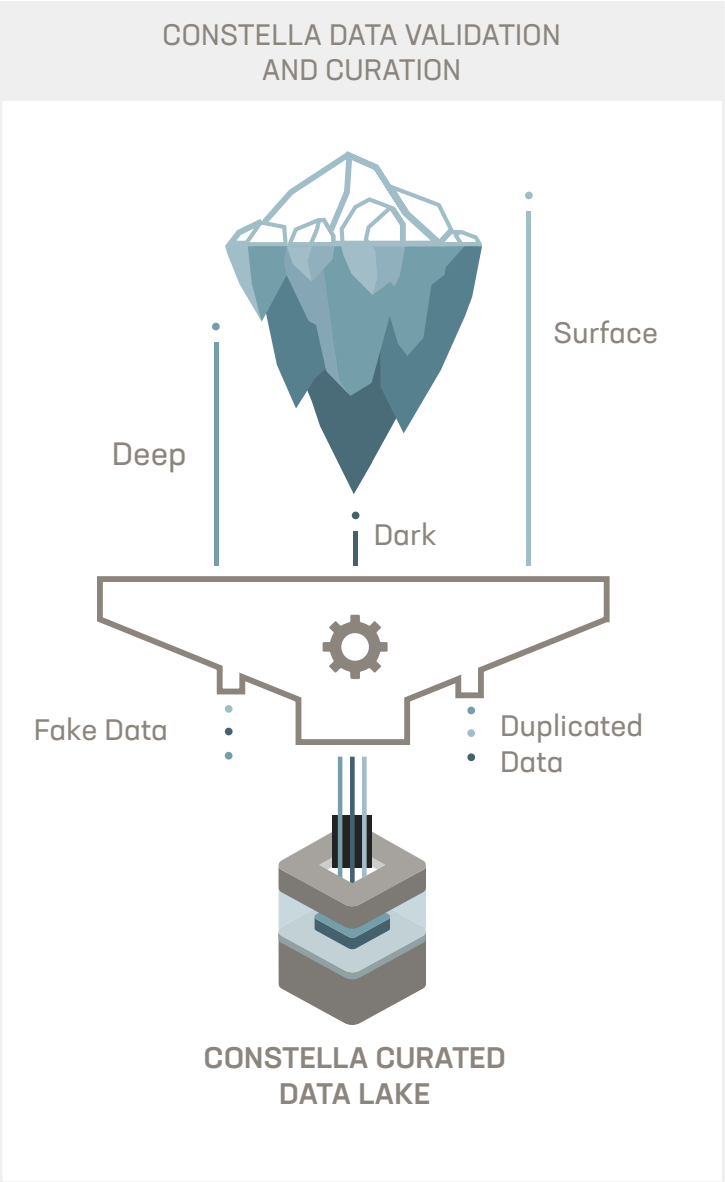


TOTAL RECORDS COMPOSITION & PERCENTAGES



ANEX 11.3

Data Verification/Methodology



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.

ANEX 11.4

Personal Records and Documents for Sale

→**Image #1** SSN Cards

→**Image #2** Passports, ID Cards, Driver's Licenses

→**Image #3** ID Cards

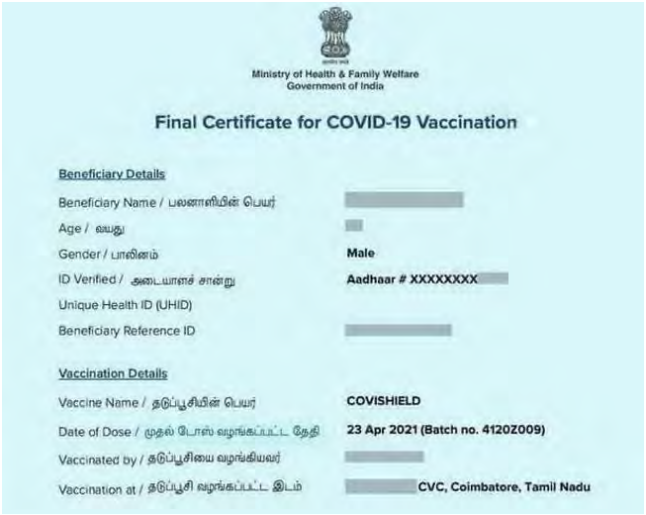
Data Breaches for Sale

→**Image #4** heroesofgaia.com- Data Breach Sell

→**Image #5** Car Manufacturer - Data Breach Sell

COVID Vaccine Certificates for Sale

→**Image #6** COVID-19 Vaccination Certificate



→**Image #7**- COVID-19 Certificate

→**Image #8** Actemra (Tocilizumab)

ANEX 11.5

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.

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 45 billion 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.