

Constella Intelligence 2023 Identity Breach Report

The Explosion of Infostealer
Botnets on the Dark Web
Threatening Individuals and
Corporate Networks



Table of Contents

About Constella's Identity Breach Report

01. Executive Summary

Section 1: Total Metrics

02. 2022 Total Breached Identity Metrics

- Geographic Distribution
- Most Impacted Sectors

Section 2: The Plague of Botnet Infostealers Flourishing on the Dark Web

03. The Explosion of the Infostealer Botnet Phenomenon

- What is an Infostealer and What Does It "Steal"?
- Why the Recent Boom in Infostealers' Success?
- Examples of How Users are Infected and How Infostealer Botnets Exfiltrate Data

04. Conclusion and Recommendations

Annex:

5.1 About This Report

5.2 Data Verification/Methodology

5.3 Glossary

Interested in learning more? Reach out to jan@constellaintelligence.com to speak with one of our threat intelligence experts.

Leveraging Constella's extensive data lake containing:



124B

curated identity breach records processed within Constella's data lake

*see annex for detailed description of curation process



180B

curated identity attributes

Our data spans



125 countries

&



53 languages

About Constella's Identity Breach Report

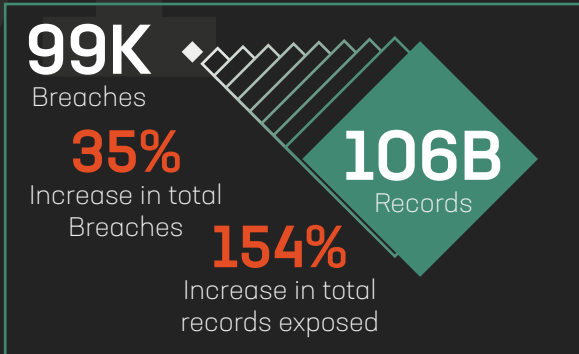
Constella's threat intelligence team continuously collects identity records from data breaches and leakages found in open sources, on the surface, social, deep, and dark web, to track data related company breaches and the specific personally identifiable information (PII) exposed that represents a risk to organizations and their employees and customers. Constella leverages the most extensive breach and social data collection on the planet, with +124 billion breach records and +180 billion curated identity attributes spanning 125 countries and 53 languages to help consumers and companies manage associated risks. Increasingly sophisticated tactics, techniques, and procedures (TTPs) employed by threat actors depend on the weaponization of billions of exposed personal data attributes as a vector through which both individuals and the organizations that they form a part of can be compromised.

In this report, we detail the implications of the proliferation of **infostealers and botnet malware** and what these threats mean for the security of **consumers and companies**. According to Constella's data and industry-leading analyses, infostealers:

- Are a backdoor to the corporate network of any company
- Consist of malware remotely controlled by criminals
- Are designed to optimize exfiltration, stealing credentials, messages, documents, and any other data on an infected device
- Began to be channeled and sold in the dark web in the past few years
- Are growing rapidly and are becoming one of the most dangerous cyber threats

This threat continues to grow and develop in sophistication, enabling cybercriminals to steal and maliciously exploit personal, private, and corporate data with increasing ease. Our findings are clear – most mid- and large-sized organizations have recurrent infostealer infections. The malware is a backdoor to corporate networks, often controlled by foreign state actor-linked groups and in many cases sold in the dark web. As the boom in infostealers, botnets, and the circulation of sensitive personal data exacerbated by data brokers and other actors continues to make its mark, it is critical to understand how individual risks are weaponized to compromise entire organizations.

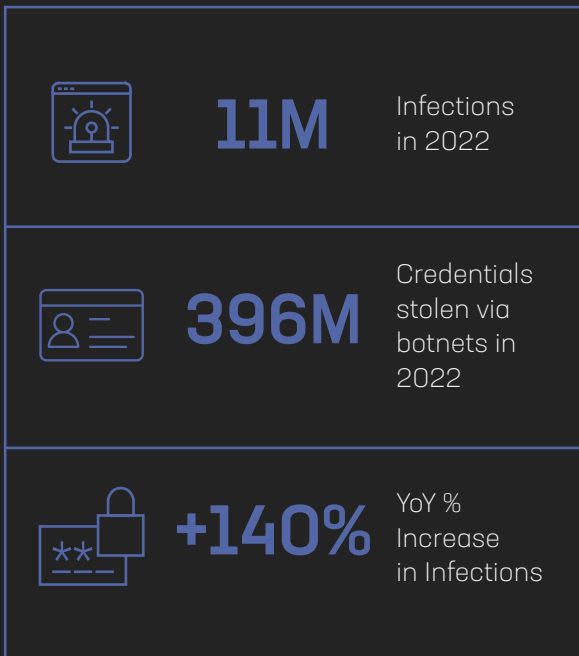
Executive Summary



1

BREACHES AND EXPOSURES SHOW SIGNIFICANT GROWTH IN 2022

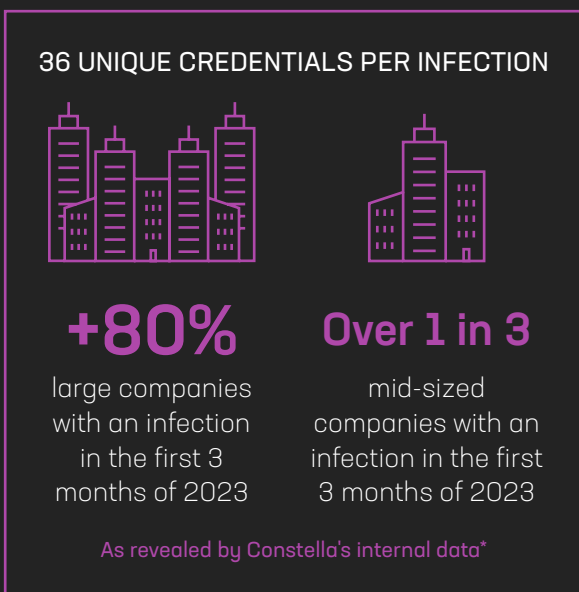
In 2022, Constella's threat intelligence team identified over 99K breaches containing approximately 106B total PII records circulating across deep and dark web sources. With a 35% increase in total breaches and a 154% increase in total records exposed, our research demonstrates how infostealers contributed to a year-over-year growth in breaches and records exposed.



2

INFOSTEALER BOTNET INFECTIONS INCREASE BY OVER 140%, COMPROMISING NEARLY 400M CREDENTIALS

Botnets of infostealer malware, a backdoor to the corporate network of any company consisting of malware remotely controlled by criminals, are designed to optimize data exfiltration stealing credentials messages, documents, and any other data on an infected device. Infostealers began to be channeled and sold in the dark web in the past few years and are growing rapidly and are becoming one of the most dangerous cyber risks. By analyzing a subset of total breaches and exposed records identified, Constella's threat intelligence team detected around 11M infostealer botnet infections, compromising and stealing approximately 396M personal or corporate credentials. These figures indicate a 140% increase in botnet infections since 2021, underscoring the rapid growth of this attack vector, serving as a highly effective back door into virtually any mid to large sized company.



3

MOST LARGE AND MANY MID-SIZED COMPANIES ARE REGULARLY COMPROMISED

Constella's internal data reveals that over 80% of large companies suffered an infostealer botnet infection in the first 3-months of 2023, while over one in three mid-sized companies had an infostealer botnet infection over the same period. Large companies with more employees (and more geographically distributed employees) who have remote access to corporate networks and digital infrastructure see increased risk of infostealer botnet infections. Accessing troves of stored data in browsers, these attacks steal an average of 36 unique credentials per infection. Further, the geopolitical asymmetry of this threat is key to note, as Russian companies appear to be less exploited by infostealer botnet malware, many of which are of Russian origin.

Further Patterns and Trends on Infostealer Botnets

Through sophisticated infection forensic analyses, Constella has surfaced a number of trends related to infostealer botnets. Our findings have revealed surprising patterns including:



1

PERSONAL, HOME, NON-COMPANY DEVICES EXPLOITED AS GATEWAYS TO ADMIN ACCOUNTS AND CORPORATE NETWORKS

Personal, non-company devices are frequently targeted as a gateway to access company resources and admin accounts. With the increase in digitalization and connected devices combined with virtual distributed workforces, this attack vector can be a challenge for many IT departments. In many cases, we find that the infected device is a home computer, outside the corporate infrastructure. Companies may not think this is relevant, however, through analyzing data exposed by infostealers we find that cybercriminals frequently access corporate networks via VPNs or intranets. Again, this is connected to the fact that virtually every role has been provided some degree of remote access during the COVID-19 years.



2

THE VOLUME OF CREDENTIALS EXPOSED PER INFECTION IS EXTREMELY HIGH

The amount of credentials from tech and security users can be astonishing, ranging from 500 to over 2,000 credentials in some cases. As such, we see several high-risk entry points like: AWS corporate accounts, GitHub, many corporate systems, and admin users within corporate network infrastructure. Our researchers have identified hundreds of corporate accesses, and dozens of them included admin or root users in just one user exposure. These credentials are stored in browsers which many times are synced within other computers and phones. For this reason as well, it's common to also see Android credentials, adding up over the years to these types of volumes. Exfiltrated information tends to include large volumes of credentials but also confidential documents, wallets, credit cards and cookies. Exfiltration of this sensitive data stored on browsers and devices means that high-risk information including financial account logins, bank and banking application credentials (PayPal, Venmo, etc.) and sensitive Crypto data can be compromised via this threat, even if many services use two-factor authentication.



3

SOFTWARE DOWNLOADS ARE A KEY ENTRY POINT FOR INFOSTEALERS

Many infections are coming from software downloads, tools for cracking software, and tech tools. In some cases, the installer asks the user to deactivate the antivirus momentarily. For this reason, we are finding several of tech and even security profiles infected. In some cases, we have detected infections from network administrators who are evaluating or playing around with tech tools. Although personal and home devices have been traditionally at greater risk, hybrid-virtual workforces mean that remote access has been granted to DevOps and many more types of profiles. These factors create situations where even the bad actors are inadvertently infecting their own devices and networks with botnets.

Section 1

Total Metrics

Most exposed attributes, sectors, geographies, and key meta-data

Interested in learning more? Reach out to jan@constellaintelligence.com to speak with one of our threat intelligence experts.

2022 Total Breached Identity Metrics

In 2022, Constella's threat intelligence team identified over 99K breaches containing approximately 106B total PII records circulating across the deep and dark web.

99K
Breaches

Identified circulating on the deep and dark web in 2022

106B
Records

35%
Increase in total Breaches

154%
Increase in total records exposed

BREAKDOWN OF TYPES OF BREACHES AND EXPOSED RECORDS

59%

Breaches /Leakages

61%

Records with email

41%

Combo Breaches

39%

Records without email

5%

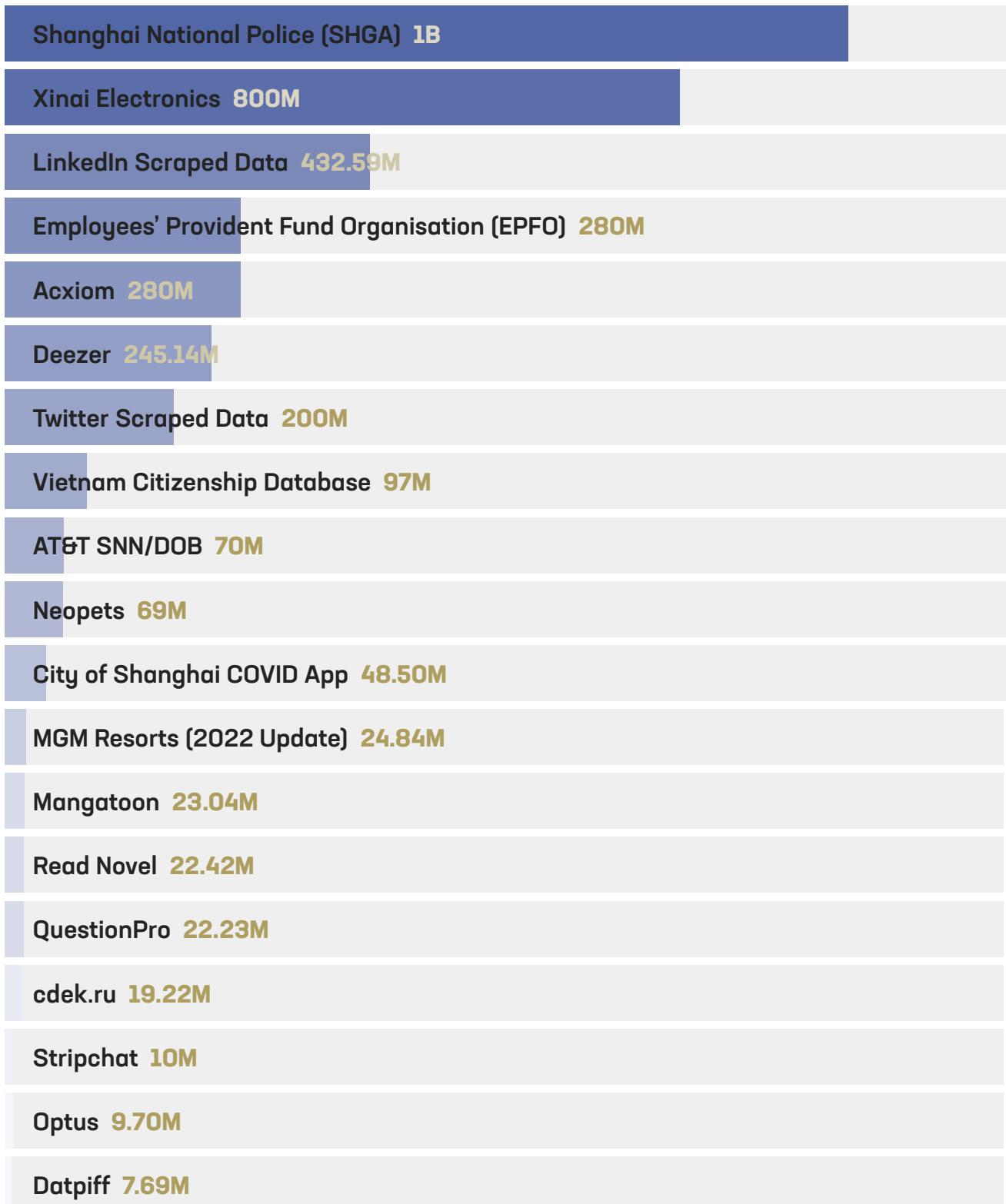
Breaches with only email

3%

Breaches with only email and password

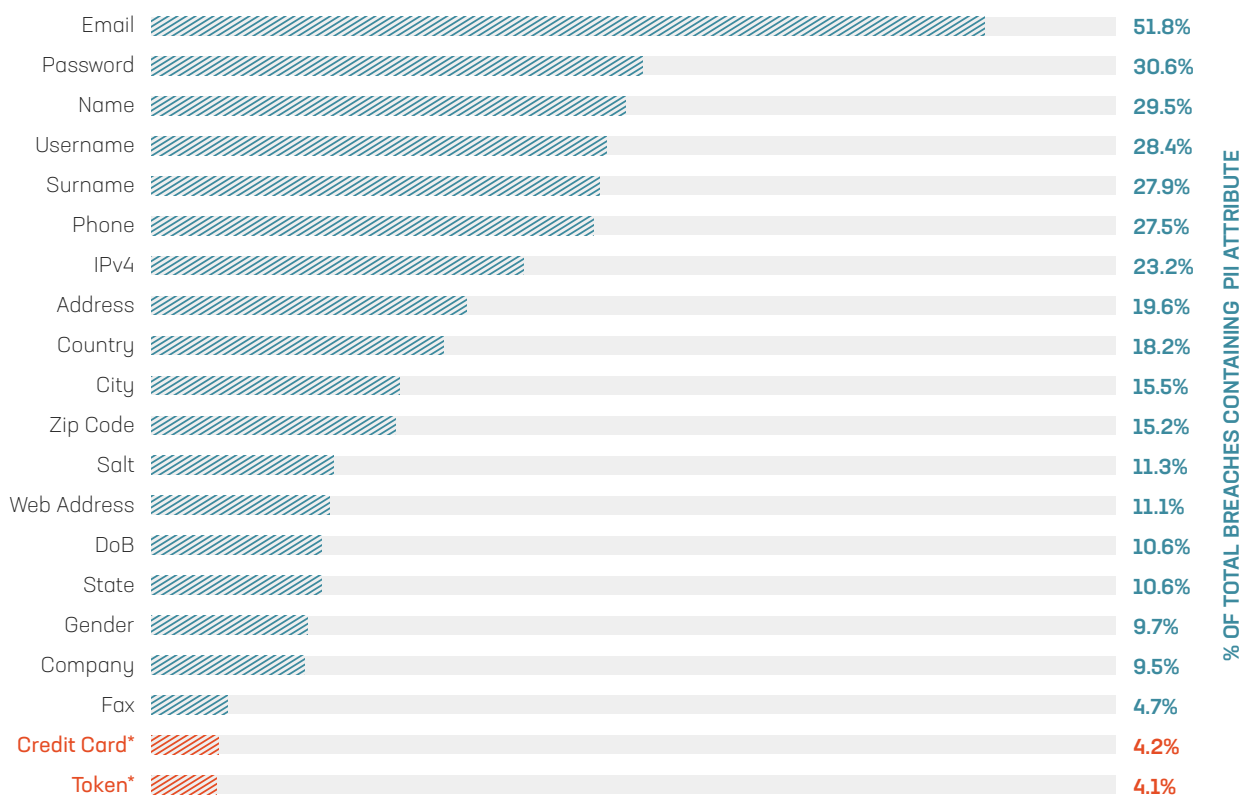
Constella's threat intelligence team compiled a ranking of the breaches and leakages from 2022 that exposed the most records and personal data. These breaches exposed substantial volumes of personal information. Digital transformation of processes, productivity, and everyday activities increase vulnerabilities by expanding possible sources of breached and stolen data increasing cybercriminals capabilities to execute sophisticated attacks.

BREACHES & LEAKAGES EXPOSING THE GREATEST VOLUME OF RECORDS: 2022

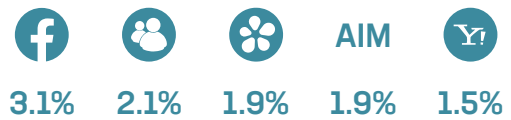


In analyzing the most exposed attributes related to breached or leaked personal records, our threat intelligence team identified that emails (52%) and passwords (31%) appear in most breaches and leakages. Following emails and passwords are attributes like names (30%), usernames (28%), and phone numbers (28%). Sensitive attributes like address (20%), zip code (15%), date of birth (11%), and company (10%) were frequently exposed, in addition to sensitive financial information, such as credit card information (4%). In 2022, credit card information and tokens appeared among the top attributes exposed, signaling both the increased use of digital financial assets by consumers and the increased impact of infostealers stealing financial data and using this to create combo breaches including tokens and credit card information*. Due to the diversity of sensitive data points and personal attributes that are exposed and weaponized on open sources and the deep and dark web, continuous monitoring of exposed personal data across a wide range of sources is critical for both personal and corporate protection. The number of devices and entry points that can be maliciously exploited by bad actors continues to expand. As such, more exposed personal data offers cybercriminals valuable resources to execute attacks.

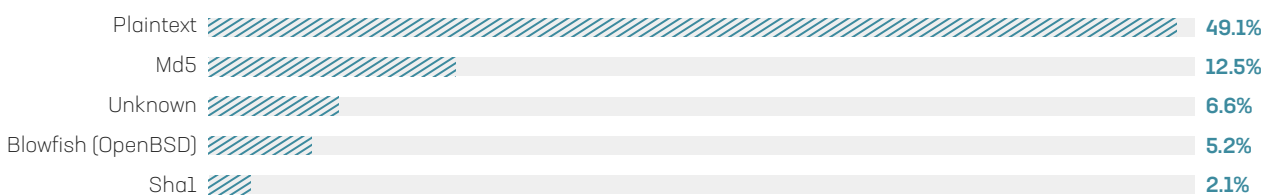
BREACHES EXPOSING THE GREATEST VOLUME OF RECORDS: 2022



Exposed attributes identified includes social media usernames, IDs (user identification numbers specific to a digital platform), and tokens, which can be linked to any identity inside the breach where they are exposed



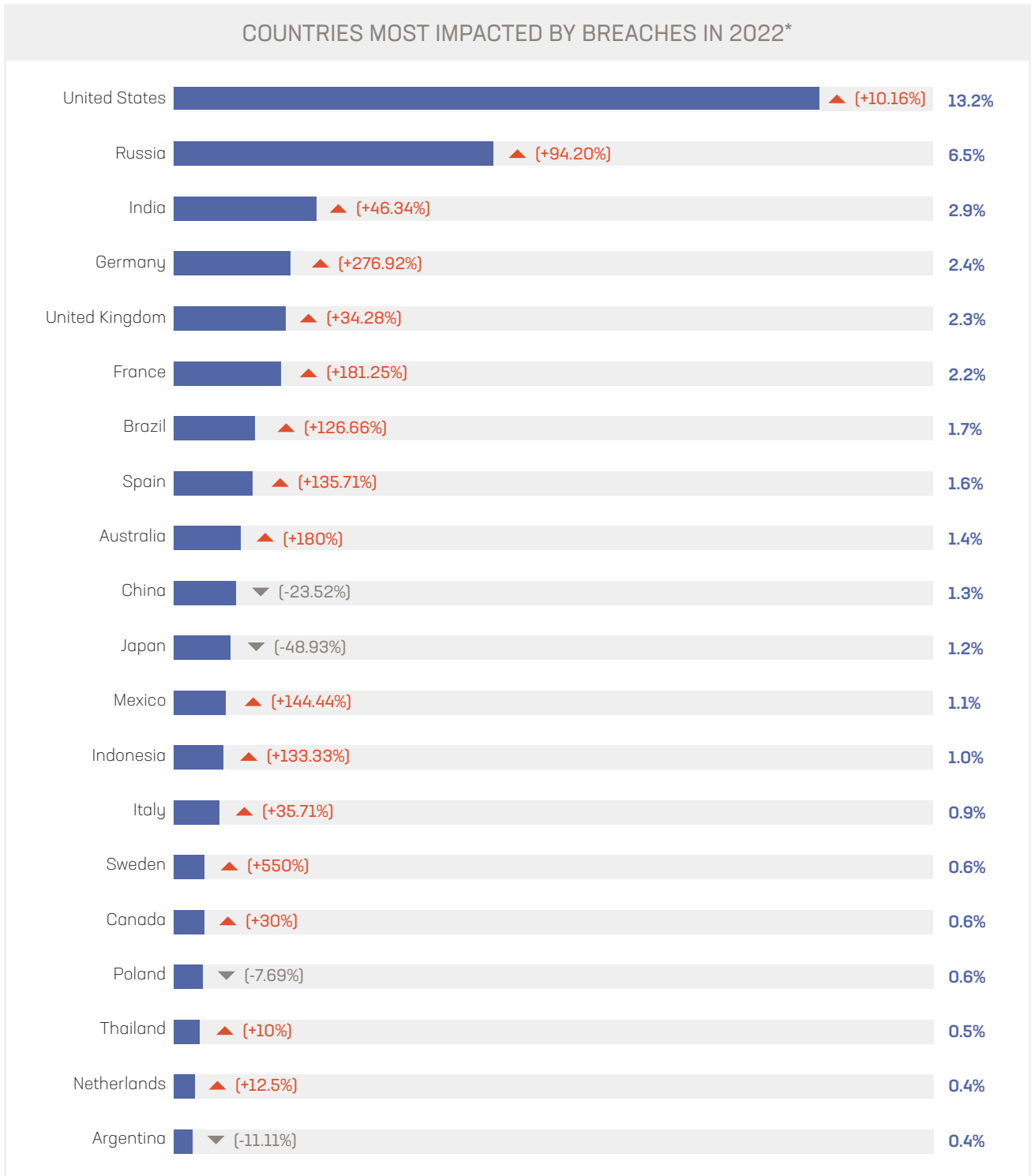
MOST FREQUENTLY DETECTED PASSWORD ENCRYPTION ALGORITHMS



* Password encryption algorithms including Dahua, Phpbbv3x, Snefru256, Mysql323, Sha512, Mysql5.x, and Adler32 were identified in less than 1% of breaches.

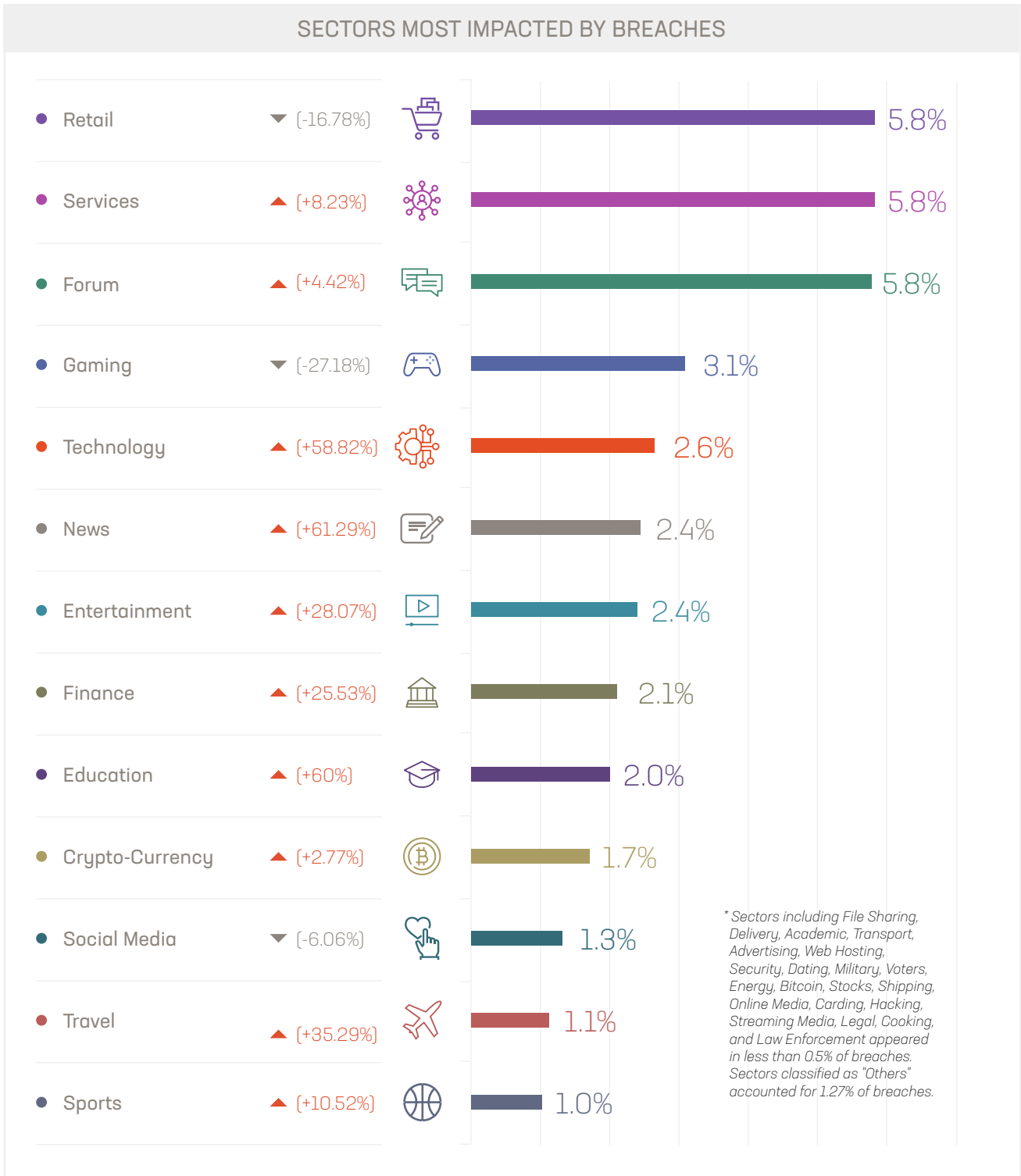
Geographic Distribution

The following map shows the total number of breaches and leakages analyzed in 2022, indicating the most affected countries based on the location of the impacted companies and the number of cyber incidents detected in each country. Breaches are classified by the country of origin of the breached company.* The most affected countries in terms of the total volume of breaches and leakages analyzed are the United States, followed by Russia, India, Germany, the United Kingdom, and France. In terms of total year-over-year changes from 2021, breaches from Sweden, Germany, France, Australia, Mexico, Spain, Indonesia, and Brazil increased notably.



Most Impacted Sectors

When consumers input their personal information to create accounts and conduct activity online, individuals' information can be exposed when these domains suffer data breaches or leakages. In this way, the security of consumers' data is linked to the domains and companies that are storing personal data. To better understand which sectors saw the most exposures in 2022, Constella's threat intelligence team analyzed the types of domains most impacted by the breaches and leakages throughout 2022. Companies or domains classified as Retail, Services, Forums, Gaming, and Technology made up the top 5 most impacted sectors. Significant increases from 2021 include sectors like News (+61%) and Education (+60%).



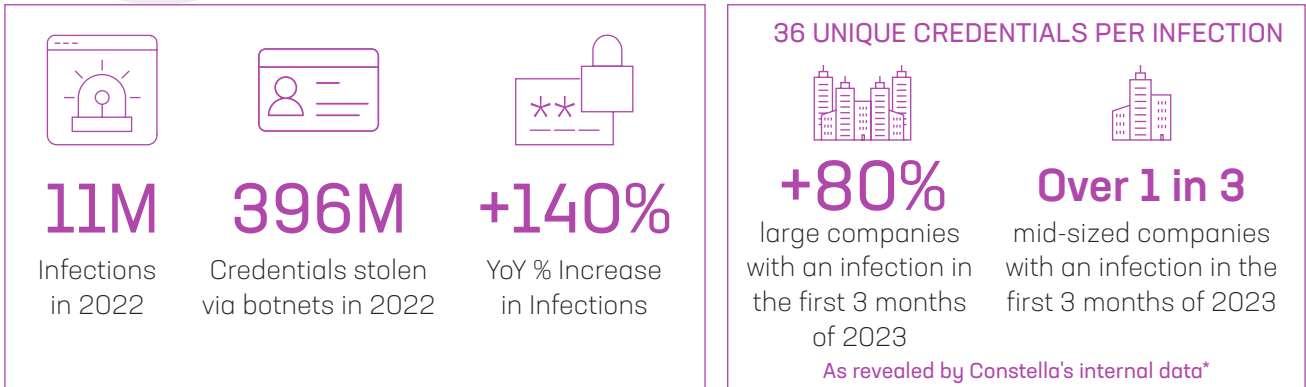
Section 2

The Plague of Botnet Infostealers Flourishing on the Dark Web

How the Trojan horse of infostealers serves as a backdoor to organizations and an efficient, sophisticated way of stealing credentials and PII

Interested in learning more? Reach out to jan@constellaintelligence.com to speak with one of our threat intelligence experts.

The Explosion of the Infostealer Botnet Phenomenon



What is an Infostealer and What Does It “Steal”?

Born in the 1990s, a botnet malware variant known as an “Infostealer” has boomed in recent years with the commercialization of the coordination and execution of this threat channeled via the Dark Web. Since the original discovery of botnet malware, both technology and threat actor skills have drastically improved, allowing botnets to scale in size and capability. As the name suggests, an Infostealer steals your information—and it takes it right from where you feel the safest keeping it: your own computer and mobile device. Much like a computer virus, an Infostealer is a form of malware that infects your computer or mobile phone. But unlike most viruses, an Infostealer’s purpose is to capture whatever data it can from your computer and relay it back to the botnet’s command and control servers. Furthermore, certain varieties of botnet malware can take control of your computer, take screenshots at any point, log your keystrokes, and much more. Often, this all happens without the machine’s user even knowing anything is wrong. While many viruses have very noticeable symptoms (poor computer performance, frequent crashing, etc), infostealers have become increasingly adept at operating without being detected by anti-virus software.

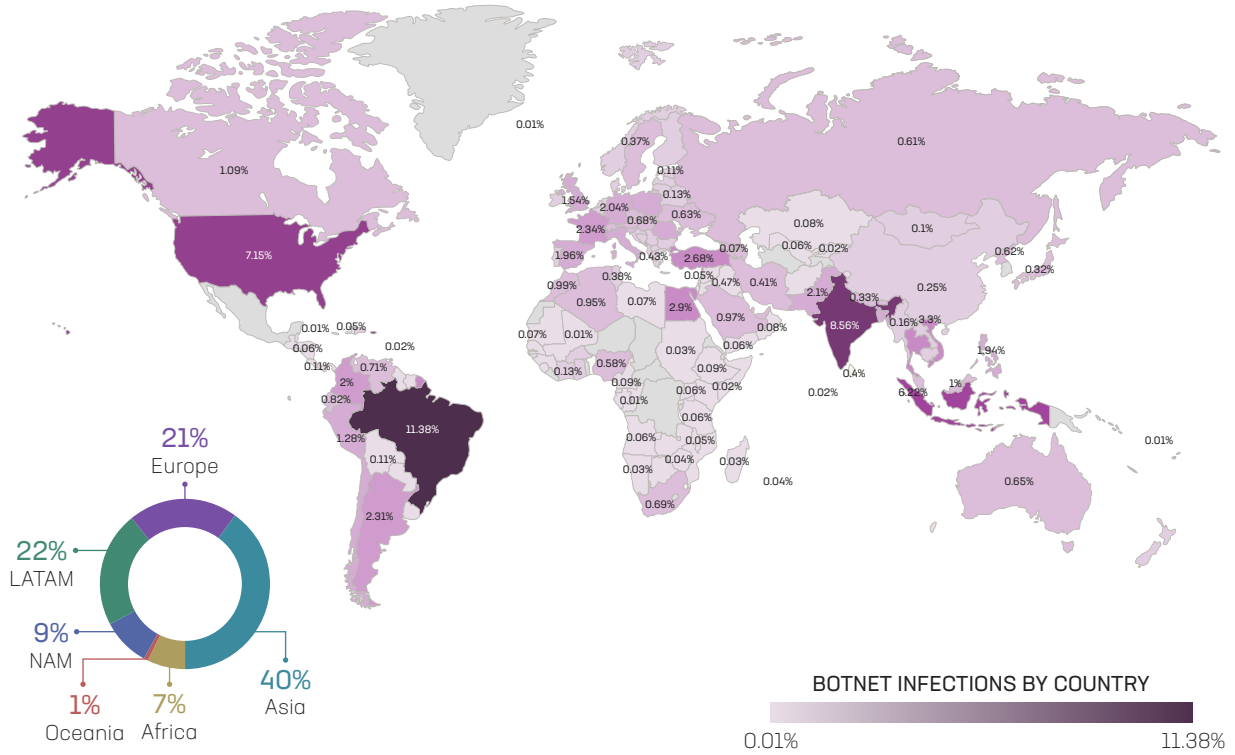
Our analysis demonstrates the prevalence of both infected users (infected users accessing third-party domains) and employees (an organization’s “infected” employee accessing a company URL/domain using their credentials). Analyzing 54 companies distributed across major regions (North America, LATAM, Asia, Africa, Europe, Oceania), our threat intelligence team detected over 15K total infected employees and approximately 14.2M total infected users visiting these organization’s domains. In 2022 alone, these figures reach 7.7K and 7.8M, respectively. There is also a critical geopolitical dimension to the infostealer phenomenon. Based on our findings, Russian companies are significantly less exposed to infostealer attacks. This is plausibly because botnets tend to be designed to detect the geographic location of an infected device, and as such are able to avoid stealing data from companies or individuals within specific geographic areas. In this way, the prevalence of Russian botnets corresponds with the relative lack of exposure of Russian companies when compared with other regions.

"There are many examples throughout 2022 of infostealer malware being used to harvest the credentials which serve as an entry point for further attacks."

- Paul Mansfield, cyber-threat intelligence analyst at Accenture

MAP OF BOTNET INFECTIONS

After analyzing millions of infostealer botnet infections, the following map displays the geographic distribution of incidents detected. Brazil, India, and the U.S. were among the countries with the most infected devices.



IN A SEPARATE ANALYSIS OF A SAMPLE OF 54 MAJOR COMPANIES WORLDWIDE, CONSTELLA'S THREAT INTELLIGENCE TEAM IDENTIFIED:

14,188,914

Total users

15,068

Total employees

7,774,270

User exposures in 2022

7,746

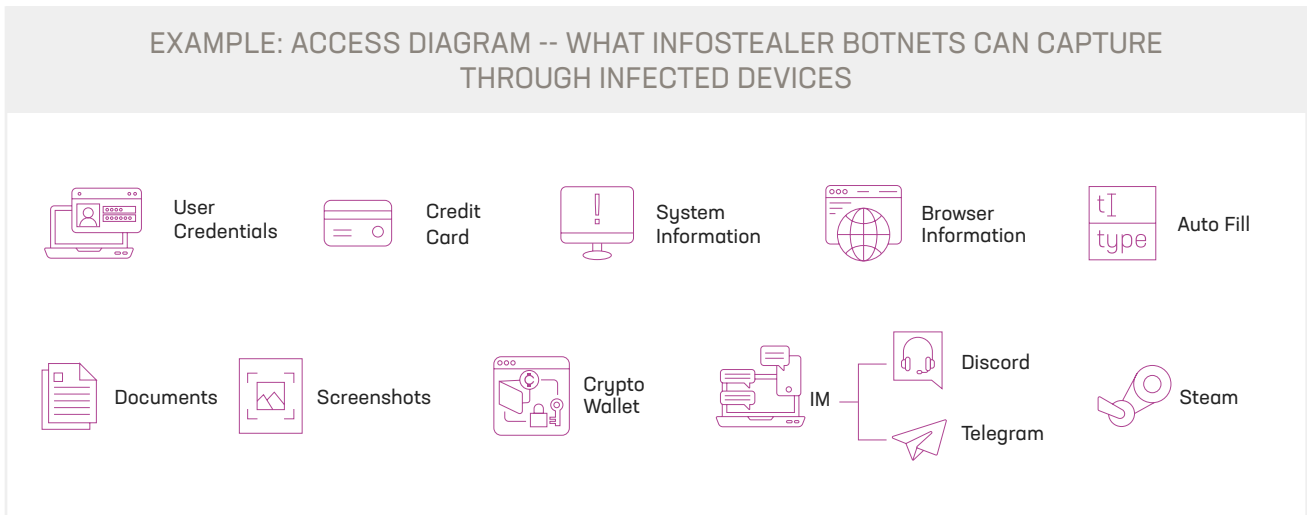
Employee exposures in 2022

To assess the prevalence of this threat and its impact on companies worldwide, Constella analyzed the domains of a sample of 54 top, publicly listed companies in all key regions (North America, LATAM, Europe, Asia, Africa, Oceania). The volume of exposures to infostealer malware impacting the domains of these major companies via compromised users and compromised employees is monumental. **Over 15K employees at these companies were detected as infected by infostealers, and over 14M users accessing these domains were identified. Over half of these user (7.8M) and employee (7.7K) exposures occurred last year, in 2022.**

***COMPROMISED USER:** A compromised user is a user infected by an infostealer who has accessed an analyzed domain, logging in with their credentials (email+password, username+password, or a saved cookie from their browser). This user is NOT a company employee. However, they may be a client or interested user.

COMPROMISED EMPLOYEE: A compromised employee is an employee infected by an infostealer that has accessed a URL of the company/domain analyzed by using their credentials (e.g., a company employee logging into their company account).

In short, infostealers are capable of capturing any information or meta-data on your device. The most lucrative is generally your stored credentials and Autofill data captured by your web browser. Every time you log in to a site and your browser offers to save your password, those saved credentials are what get snagged. We see an average of 36 different pairs of credentials captured per infected device—which includes on average 6 unique email addresses. Your browser’s Autofill feature also saves attributes like your name, address and credit card numbers for easy access the next time you need to fill out this information. Unfortunately, however, since an Infostealer is software that runs on your computer, it can quite easily extract the data saved in your Autofill database, and capture all your stored credentials, which sites those credentials work for, and any other personal detail you thought would stay private unless you decided otherwise.



Another important type of data an Infostealer can grab from your browser are your cookies. Cookies contain snippets of data stored locally in your web browser’s cache for convenient use later. This might be a website’s way of storing your preference for something, or it could be used for login purposes. Every time you log-in to a website, a “session” is created, and the session is said to be authenticated and depending on your preferences and how the web site you’ve accessed is designed, sessions can be valid for extended periods of time. Notice that you’re still logged in when you close your browser and return to certain sites? That’s thanks to sessions cookies that are responsible for keeping track of your session. The website you’ve authenticated with stores a token, or a code of some kind, in your browser’s cookies. When this cookie is present and you re-visit a site, the site checks the cookie, sees that the stored token is still valid and cross checks a few other parameters (like your browser version, operating system type and the geolocation of your IP), and if everything checks out, your session is still considered valid and you’re not required to re-authenticate. When an Infostealer captures your cookies, and some other relevant data from your computer, it is entirely possible they can leverage this to “hijack” your session and bypass the need to authenticate.

This is particularly scary considering this often defeats multi-factor authentication too. Infostealers also capture information about your computer. This includes your machine name, IP address, operating system and version, which software you run and the type of anti-virus you use (if any). They often grab a screenshot of your desktop in addition to geolocating your machine as well.

Example - Infostealer Logs and Cookie Data Sold on the Dark Web

Around since 2018, Genesis Market's slogan was, "Our store sells bots with logs, cookies, and their real fingerprints." Customers could easily search for infected systems filtering by several options, including by IP address or by domain names linked to stolen credentials. Genesis Market made the process incredibly simple, selling and distributing novel products including "Genesis Security", a custom Web browser plugin capable of loading a Genesis bot profile so that the browser mimics virtually every key element of the victim's device – including details like screen size, refresh rate and even the unique user agent string connected to the victim's web browser. A law enforcement operation involving 17 countries resulted in 119 arrests and the takedown of Genesis Market in early April 2023.



What are some examples of how infostealers are spread that have been identified by Constella through forensic analyses?

- Ordinary users who accidentally download cracked software containing Redline malware.
- 3D digital artists who own coins and NFT tokens.
- Users who believe in the US's Folding@home campaign against COVID-19 (a distributed computing project to build Protein structure models for COVID-19 prevention research models) and are encouraged to download the Simulator app to accompany the project. At that time, the attacker will take advantage of this app to trick users into downloading a fake Simulator app containing Redline malware.

Why the Recent Boom in Infostealers' Success?

Infostealers are not a new concept, so why are they gaining traction now? In short, the underground community has matured and evolved rapidly. As technology has advanced, so have threat actor capabilities. And with these advancements, underground marketplaces, hacker communities and their respective exploits have increased in power and efficacy. It's important to remember there is a thriving economy supporting all of these digital nefarious activities. In addition to the previously outlined context of remote workforces/remote access which are key conditions for the explosion of this trend, there are other important factors that help explain the plague of infostealers:

- 1.** Underground marketplaces are robust and cater to threat actor demand. The underground hacking communities have benefitted from economic growth (of underground communities) the same way legitimate economies grow: demand for certain products and services increases the overall quality and creates competition. In short, demand for stolen credentials and PII creates demand for better tools to capture this data. Malware as a Service has emerged, allowing anyone with a nominal fee to gain access to these tools for their own malicious work.
- 2.** The cost and other barriers to entry are low, which build upon the growing community and concept of MaaS (malware as a service). Simply put, it's becoming easier to deploy botnet malware attacks, for very little upfront cost.
- 3.** Established "big game" threat actors are seeking Infostealer capabilities. As the underground community scales up, well-known and established cybercriminals are looking to expand their game using Infostealers.
- 4.** Infostealers are successfully impersonating legitimate software, which seeds infections. Simply put, botnet malware creators are doing a better job at disguising their Infostealer as legitimate software, making it both harder for antivirus software to detect, and more likely a user will download and install the software.
- 5.** Tactics like MFA fatigue are being successfully deployed: The report highlighted the growing effectiveness of MFA fatigue attacks, which involve repeated attempts to log on to an MFA-enabled account using stolen credentials, thereby bombarding a potential victim with MFA push requests.

Examples of How Users are Infected and How Infostealer Botnets Exfiltrate Data

EXAMPLES OF FILES OR FOLDERS WITH STOLEN DATA

```

URL: https://accounts.google.com/v3/signin/challenge/pwd
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown

URL: https://twitter.com/i/flow/login
username: ****@paoe
password: ****@17
Browser: Opera GX_Unknown

URL: https://users.nexusmods.com/auth/sign_in
username: ****@gmail.com
password: ****@21
Browser: Opera GX_Unknown

URL: https://www.netfilx.com/login
username: ****@gmail.com
password: ****@paoe
Browser: Opera GX_Unknown

URL: https://www.amrdoco.com/alternate-life
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown

URL: https://betteranime.net/login
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown

URL: https://www.loverslab.com/register/
username: ****@huh
password: ****@17
Browser: Opera GX_Unknown

URL: https://auth.riotgames.com/login
username: ****@zal7
password: ****@zal7
Browser: Opera GX_Unknown

URL: https://rizomaclass.com.br/login-membros
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown

URL: https://guaporizoma.fastcorban.com.br/login/autb
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown

URL: https://steamcommunity.com/openid/login
username: ****@aic
password: ****@pc
Browser: Opera GX_Unknown

URL: https://vendas.qrporizoma.com.br/aceso/login
username: ****@9
password: ****@711
Browser: Opera GX_Unknown

URL: https://www.payspal.com/br/welcome/sigmp/
username: ****@gmail.com
password: ****@17
Browser: Microsoft_Edge_Default

URL: https://www.twitch.tv/login
username: ****@paoe
password: ****@hun
Browser: Microsoft_Edge_Default

URL: https://br.pinterest.com/
username: ****@gmail.com
password: ****@hun
Browser: Microsoft_Edge_Default

URL: http://sh.tnxtbrasil.com.br/candidato/login.aspx
username: ****@43
password: ****@843
Browser: Microsoft_Edge_Default

URL: https://www.amordoco.com/high-school-life
username: ****@mail.com
password: ****@17
Browser: Microsoft_Edge_Default

URL: https://login.rvgs.nvidia.com/v1/login/password
username: ****@aic
password: ****@zal7
Browser: Microsoft_Edge_Default

URL: https://auth.abye.tech/login
username: ****@gmail.com
password: ****@19
Browser: Microsoft_Edge_Default

URL: https://steamcommunity.com/openid/login
username: ****@paoe
password: ****@pc
Browser: Microsoft_Edge_Default

URL: https://accounts.google.com/signin/v2/challenge/pwd
username: ****@gmail.com
password: ****@234
Browser: Microsoft_Edge_Profile 1

URL: https://twitter.com/i/flow/login
username: ****@paoe
password: ****@iki
Browser: Microsoft_Edge_Default

URL: https://vendas.qrporizoma.com.br/aceso/login
username: ****@9
password: ****@711
Browser: Opera GX_Unknown

URL: https://betteranime.net/login
username: ****@gmail.com
password: ****@17
Browser: Opera GX_Unknown
    
```

→Image #1
Example of a Password File Stolen Via an Infostealer

```

Telegram

Name
Profile_1
  7E6F400AB8824E47s
  90B5FD02AC0489FES
  A7FDF864FBC10B77
    configs
  A7FDF864FBC10B77s
  countries
  D877F783D5D3EF8C
    5DC4616165E0947Es
    6A279BE16762E85Es
    6D1CBD747474A09As
    7B91D86FFB2564E7s
    316E4FA63834CCAAs
    496E51DC5F850D53s
    936FF16A1E3CA27Ds
    A668E95F60FBDE0Bs
    B8769272F55B6358s
    configs
    maps
  D877F783D5D3EF8Cs
  DDA17E36C3424A26s
key_datas
    
```

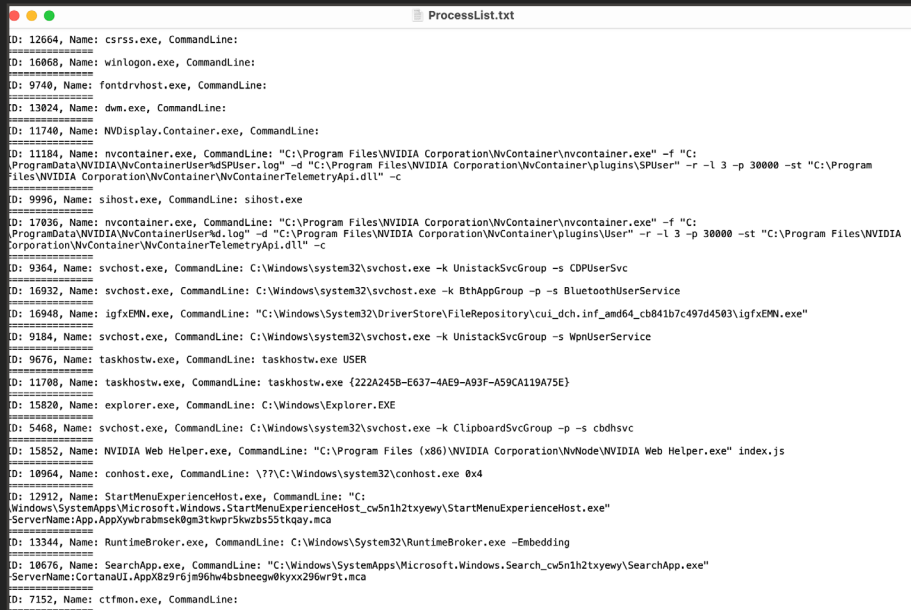
→Image #2
Example of a Telegram folder stolen from an infected user. This folder contains personal user data, chats, groups, channels, etc.

```

InstalledSoftware.txt

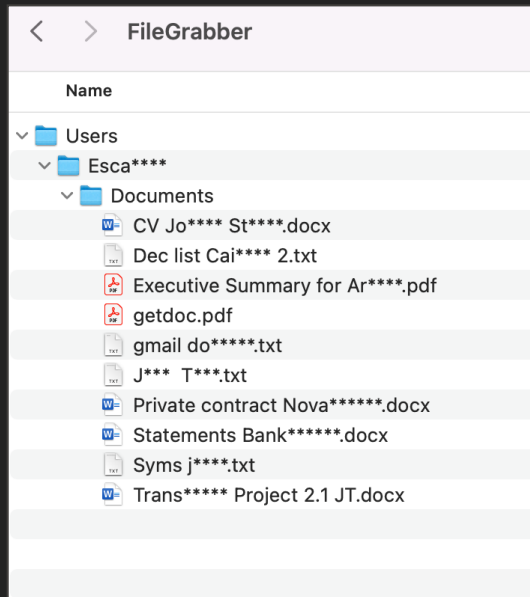
1) 3uTools [2.62.020]
2) 4G Mobile Hotspot [1.0.0.2]
3) 4MeKey 4.0.8.4 [4.0.8.4]
4) AnyDesk [ad 7.0.13]
5) Apex Legends [1.0.2]
6) ApowerEdit V1.7.8.9 [1.7.8.9]
7) ApowerREC V1.5.6.20 [1.5.6.20]
8) Apple Software Update [2.7.0.3]
9) Brave [104.1.42.97]
10) Days Gone MULTi23 - ElAmigos versin 1.06 [1.06]
11) ExpressVPN [10.26.0.4]
12) ExpressVPN [10.26.0.4]
13) Google Chrome [104.0.5112.101]
14) Google Chrome Dev [106.0.5245.0]
15) Internet Claro [22.001.29.00.1074]
16) IObit Uninstaller 11.5.0.3 [11.5.0.3]
17) Magick Checker versin . [.]
18) MEMU+/MEMUQQ 0 [0.1.0.0]MEMU+/MEMUQQ0
19) Microsoft .NET Core Host - 3.1.16 (x86) [24.64.30112]
20) Microsoft .NET Core Host FX Resolver - 3.1.16 (x86) [24.64.30112]
21) Microsoft .NET Core Runtime - 3.1.16 (x86) [24.64.30112]
22) Microsoft Edge [104.0.1293.63]
23) Microsoft Edge Update [1.3.167.21]
24) Microsoft GameInput [10.1.22621.1011]
25) Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219 [10.0.40219]
26) Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61830 [11.0.61830.0]
27) Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.30501 [12.0.30501.0]
28) Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.30501 [12.0.30501.0]
29) Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005 [12.0.21005]
30) Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005 [12.0.21005]
31) Microsoft Visual C++ 2015-2019 Redistributable (x64) - 14.28.29913 [14.28.29913.0]
32) Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.28.29913 [14.28.29913.0]
33) Microsoft Visual C++ 2015 x86 Additional Runtime - 14.28.29913 [14.28.29913]
34) Microsoft Visual C++ 2015 x86 Minimum Runtime - 14.28.29913 [14.28.29913]
35) Microsoft Windows Desktop Runtime - 3.1.16 (x86) [24.64.30112]
36) Microsoft Windows Desktop Runtime - 3.1.16 (x86) [3.1.16.30112]
37) Minimal AOB and Fastboot version 1.4.3 [1.4.3]
38) Nmap 7.92 [7.92]
39) NoxPlayer [7.0.3.3]
40) Ncpap [1.50]
41) OBS Studio [27.2.3]
42) Origin [10.5.115.51547]
43) Overwolf [0.204.0.1]
44) Python Launcher [3.10.7751.0]
45) qBittorrent 4.4.3.1 [4.4.3.1]
46) Realtek High Definition Audio Driver [6.0.9205.1]
47) StreamElements SE.Live [22.3.5.805]
48) Surfshark [4.0.1999]
49) Surfshark [4.0.1999]
50) Surfshark TAP Driver Windows [1.0.1]
51) Technitium MAC Address Changer v6.0 [6.0]
52) Tioo [01.005.15.02.222]
    
```

→Image #3
An example obtained from an infostealer with all software installed by the user on their device and their respective versions



→Image #4

Example of a file obtained by an infostealer, capturing all processes executed by the infected device



→Image #5

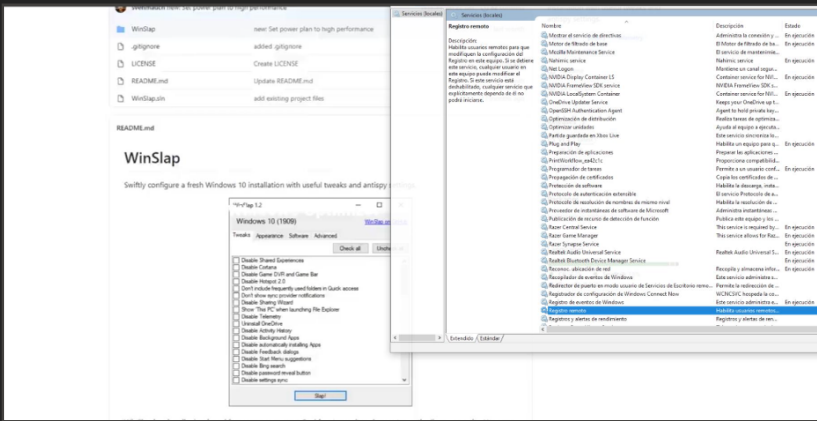
Example of a folder with files and personal documents stolen from the infected device by an infostealer



→Image #6

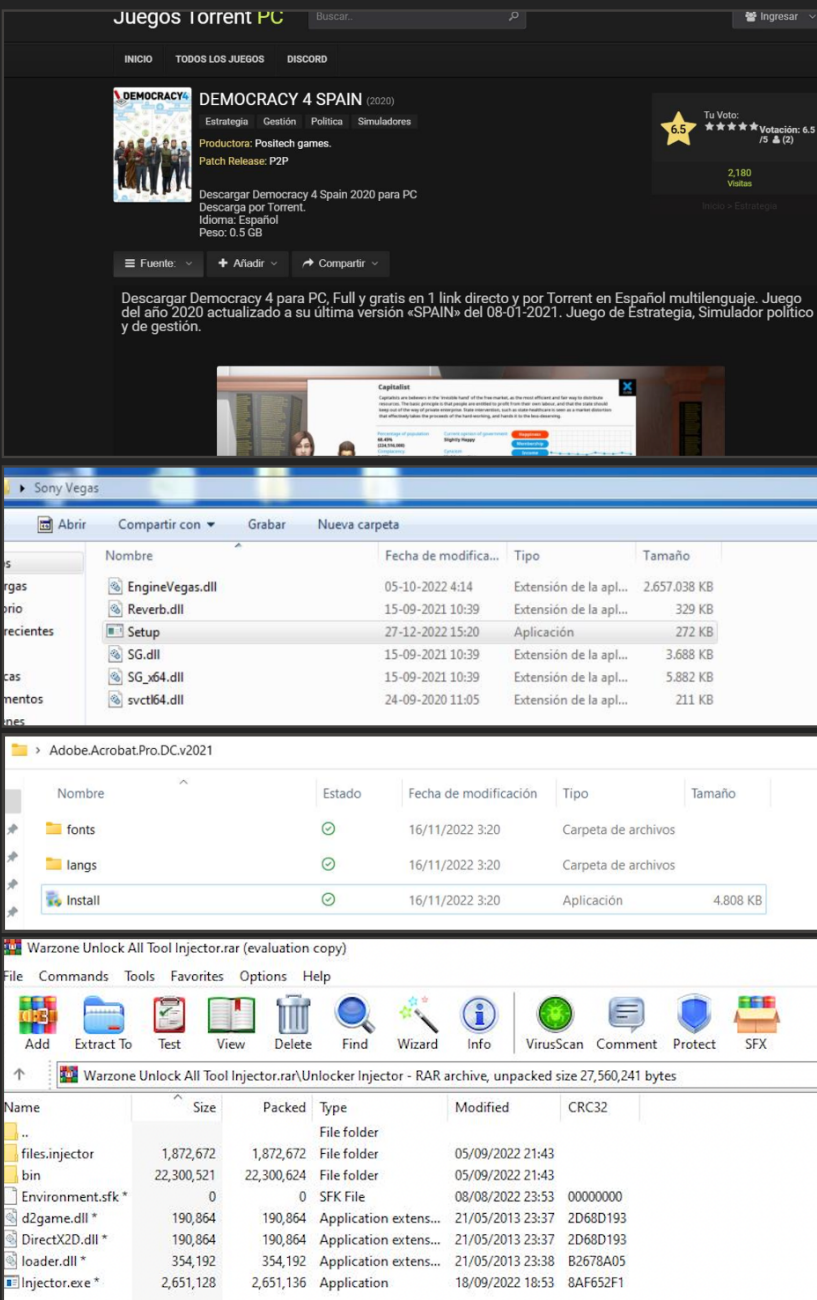
Example of a file captured by an infostealer including all session cookies of the web navigator used by the user/infected device.

EXAMPLES OF SYSTEM REGISTRIES DEMONSTRATING DATA THAT AN INFOSTEALER CAN CAPTURE



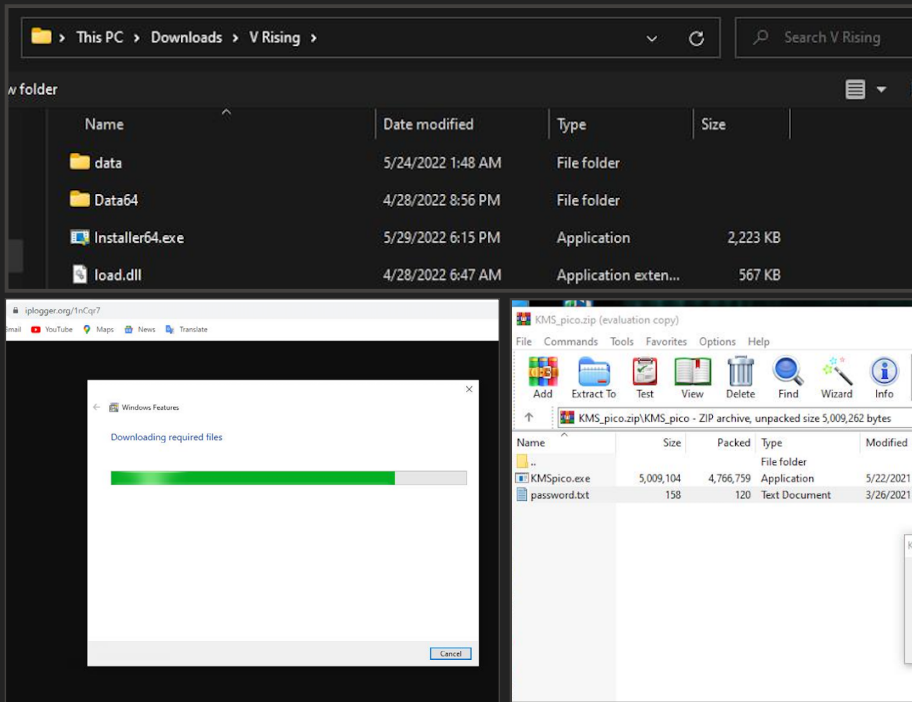
→Image #7
Example of the system log, system information that an infostealer usually obtains

EXAMPLES OF ILLEGALLY DOWNLOADED SOFTWARE/FILES/VIDEOGAMES



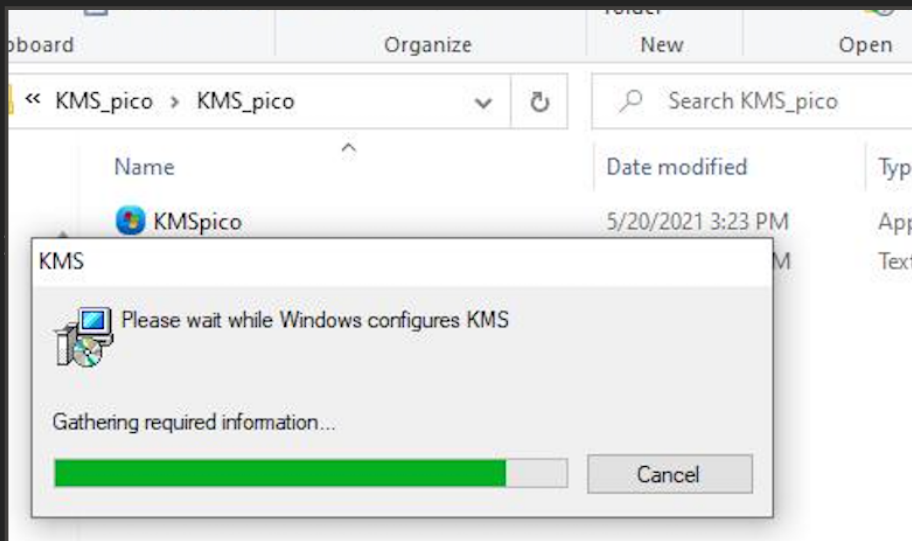
→Image #8 #9 #10
Example of illegally downloaded software that can be an entry point for an infostealer infection

→Image #11
Example of software to modify a videogame that could be an entry point for an infostealer infection



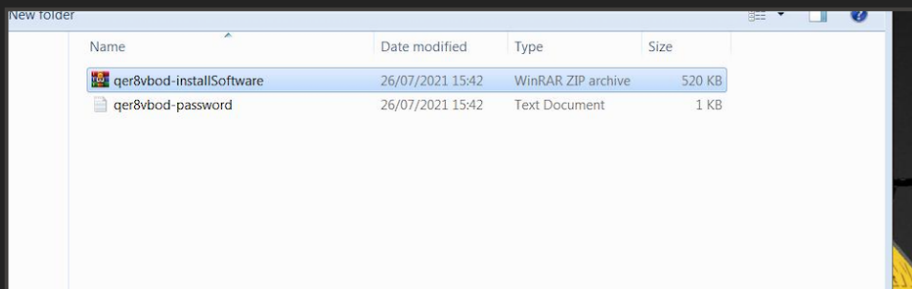
→Image #12

Example of illegally downloaded software that can be an entry point for an infostealer infection



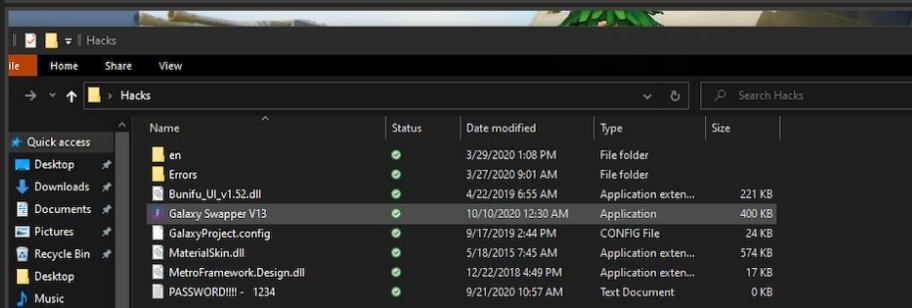
→Image #13 #14 #15

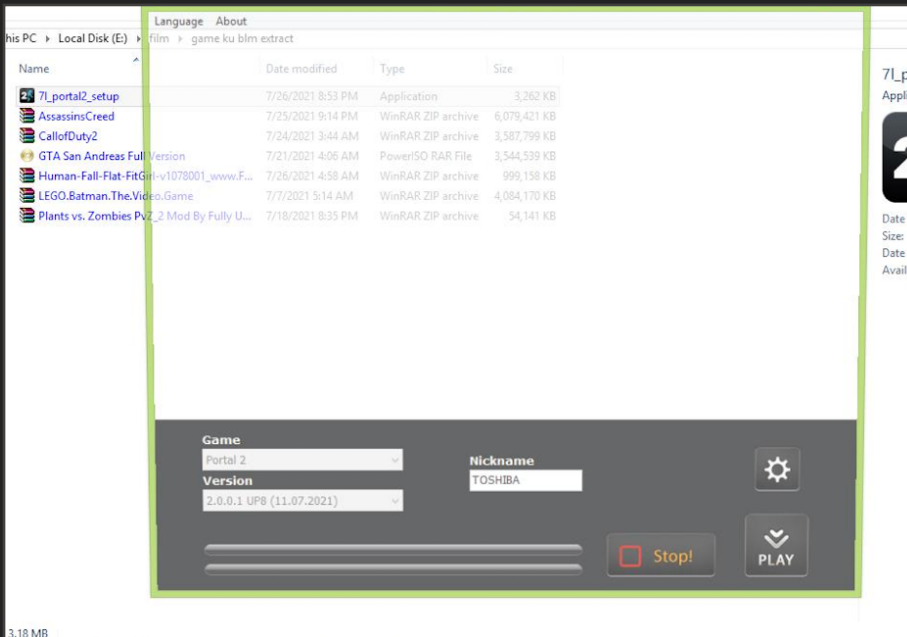
Example of an illegally downloaded software and its installation, demonstrating the moment in which a user is infected by an infostealer



→Image #16 #17

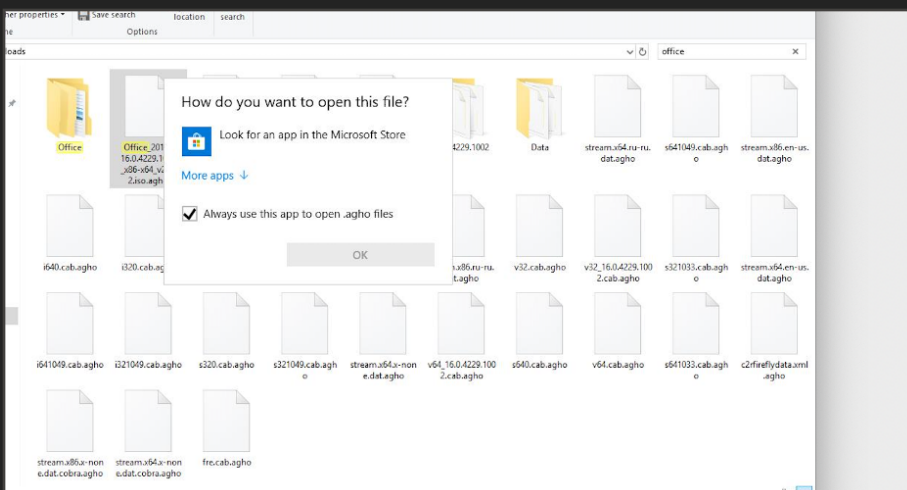
Example of illegally downloaded software that can be an entry point for an infostealer infection



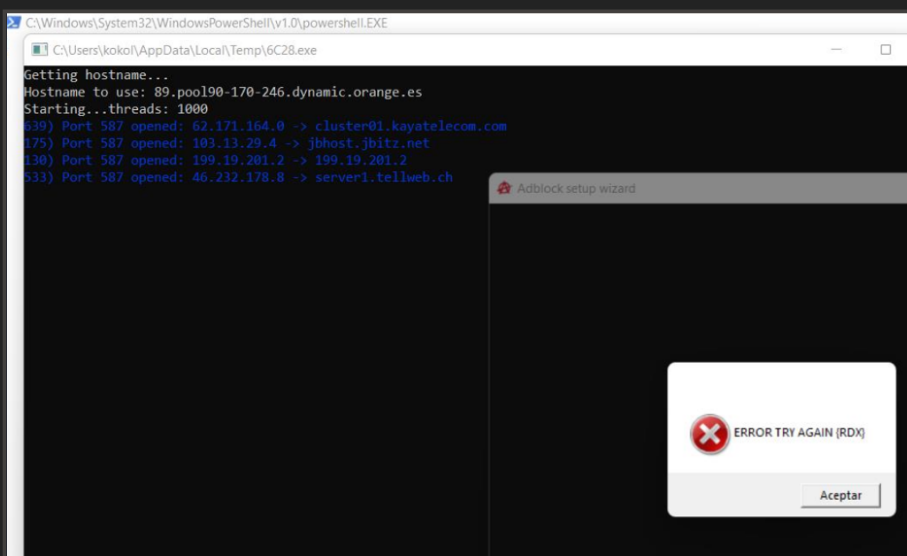


→Image #18 #19

Example of videogame software in which a user, upon executing the software, is infected



EXAMPLES OF INSTALLATION ERRORS



→Image #20

Downloaded software can contain errors that make it unable to complete the installation process. In this way, the user is infected and is unable to use the software. This creates the possibility of an additional infostealer infection upon downloading another illegal software.

04 Conclusion and Recommendations

Infostealer botnets are malicious networks of infected devices controlled by cybercriminals. Due to their low barriers of entry for purchase and execution, infostealer botnets have resurged as key tools in cybercriminals' arsenal. These botnets are designed to steal sensitive information, such as usernames, passwords, credit card details, and other personal or financial information from individuals and companies they belong to. The risks posed by infostealer botnets are numerous and can be significant. Examples include:

- 1. Identity theft:** Infostealer botnets can steal login credentials and other personal information, which can be used for identity theft. Cybercriminals can use this information to access bank accounts, credit cards, or other financial accounts.
- 2. Financial loss:** Infostealer botnets can be used to steal money from bank accounts or credit cards. This can result in significant financial losses for individuals and companies.
- 3. Data breach:** If an infostealer botnet gains access to sensitive information such as customer data or trade secrets, it can result in a significant data breach. This can lead to reputational damage and legal liabilities.
- 4. Malware infection:** Infostealer botnets are often used to distribute other types of malware, such as ransomware or spyware. This can result in further damage to individuals and companies.
- 5. Compliance violations:** Companies that are subject to regulatory compliance requirements, such as HIPAA or PCI DSS, may face fines and other penalties if they are found to be non-compliant due to an infostealer botnet attack.

Detecting and cleaning an infection rapidly is key to contain the damage. Knowing details of the stolen data and documents allows companies and users to evaluate and contain the risk. In order to protect against these risks, individuals and companies should take steps to protect their devices and networks. This includes implementing strong passwords, keeping software up to date, using antivirus software, and being cautious when clicking on links or downloading files from unknown sources. Additionally, individuals and companies should be vigilant and report any suspicious activity to their IT security teams or law enforcement.

As the breach economy and the sophisticated methods of attack employed by cybercriminals continue to expand Constella's experts offer several recommendations for prevention of associated risks. These recommendations are tailored towards employees and individuals—a major attack vector for cybercriminals seeking to infiltrate and compromise corporate networks via individual exposures and vulnerabilities.

- 1. Keep your software up-to-date:** Ensure that your computer's operating system, anti-virus software, and other applications are updated regularly. Cybercriminals exploit security vulnerabilities in outdated software to launch cyberattacks. Set up automatic updates whenever possible to ensure that you have the latest patches and security fixes.
- 2. Use strong passwords and multi-factor authentication:** Strong passwords are critical to preventing ATO attacks. Use unique, complex passwords for each online account, and avoid reusing passwords across multiple accounts. Enabling multi-factor authentication (MFA) can provide an extra layer of security against ATO attacks.
- 3. Be cautious of suspicious emails:** BEC attacks usually start with a phishing email, so be careful when opening emails from unknown senders. Never click on links or download attachments from suspicious emails. Check the sender's email address carefully to make sure it's legitimate before taking any action.
- 4. Backup your important data:** Ransomware attacks can lock up your files and demand payment to restore access. Back up your critical data regularly to a secure, offsite location to ensure that you can recover it in case of a ransomware attack. Test your backups regularly to make sure they are working correctly.
- 5. Educate yourself and your employees:** Educate yourself and your employees about the latest cybersecurity threats and best practices. Conduct regular security awareness training sessions to help them recognize and avoid potential cyber threats. Develop and implement clear security policies, guidelines, and procedures for your organization.
- 6. Use a Virtual Private Network (VPN) when accessing the Internet:** VPNs create a secure, encrypted tunnel between your device and the Internet, protecting your online activity from prying eyes. Use a VPN, especially when using public Wi-Fi, to prevent cybercriminals from intercepting your data.
- 7. Monitor your accounts regularly:** Keep a close eye on your online accounts, especially financial and email accounts, to spot any unusual activity. Review your transaction history and account settings regularly to ensure that there are no unauthorized changes.
- 8. Enable device encryption:** Use encryption to protect the data stored on your devices, such as laptops, smartphones, and tablets. Encryption scrambles your data and makes it unreadable without the correct decryption key.
- 9. Use caution when downloading software and apps:** Only download software and apps from trusted sources, such as official app stores or the developer's website. Be wary of free software or apps that seem too good to be true, as they may contain malware.
- 10. Limit access to sensitive data:** Limit access to sensitive data, such as financial or personal information, to only those who need it. Use access controls, such as passwords and user permissions, to restrict access to sensitive data. Monitor and audit access regularly to detect any unauthorized access attempts. DRPS (Digital Risk Protection Services) can help companies identify, monitor, and mitigate digital risks that can impact their executives and key employees, such as brand impersonation, social media impersonation, and other online attacks. By partnering with a DRPS provider, companies can proactively protect their key employees' digital identities and reduce the risk of cyberattacks that use their identities as a stepping stone to gain access to sensitive information.

Annex

Interested in learning more? Reach out to jan@constellaintelligence.com to speak with one of our threat intelligence experts.

ANEX 5.1

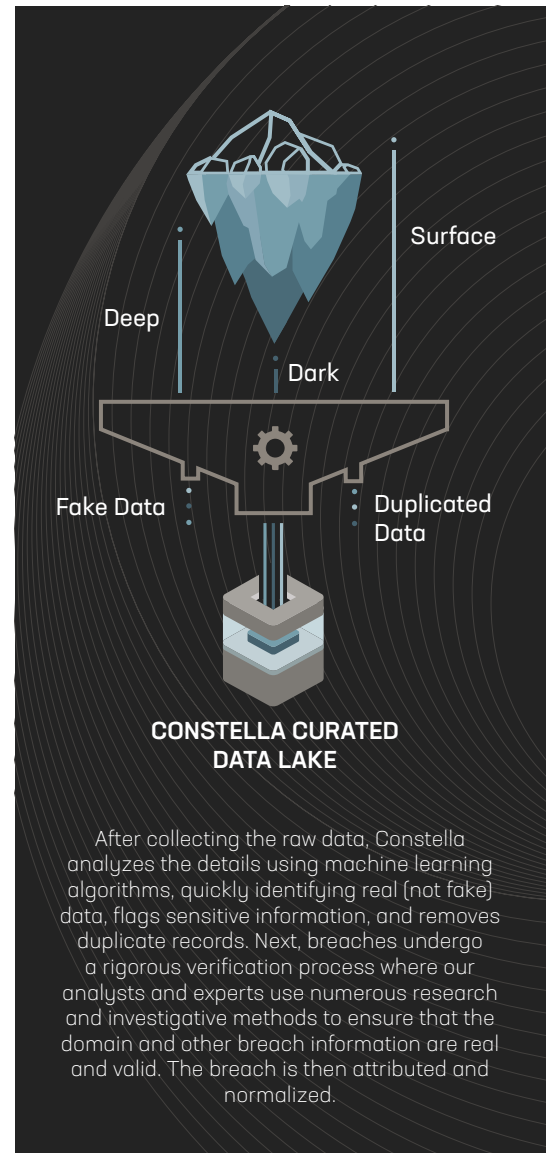
About This Report

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**



ANEX 5.2

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 5.3

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.

INFOSTEALER: Information stealer (infostealer) malware—malicious software designed to steal victim information, including passwords and other sensitive data.

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 people, 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 124B breach records and 180B curated identity attributes spanning 125 countries and 53 languages. This richness and breadth enables detection of diverse threats and risks emerging from breach data, surface web and open source threats, social engineering, botnets, phishing data, data brokers, and more to uncover and protect against the diverse tactics, techniques, and procedures (TTPs) employed by threat actors.

Our recent work has been featured in major mainstream media like [Reuters](#), [the World Economic Forum](#), and [Forbes](#), in addition to other notable media.

[Reach out to us](#) for a demo to learn more about Constella's 360-degree approach to proactively anticipating, identifying, and remediating targeted threats to your people, your assets, and your brand.

WHY CONSTELLA

OUR TEAM

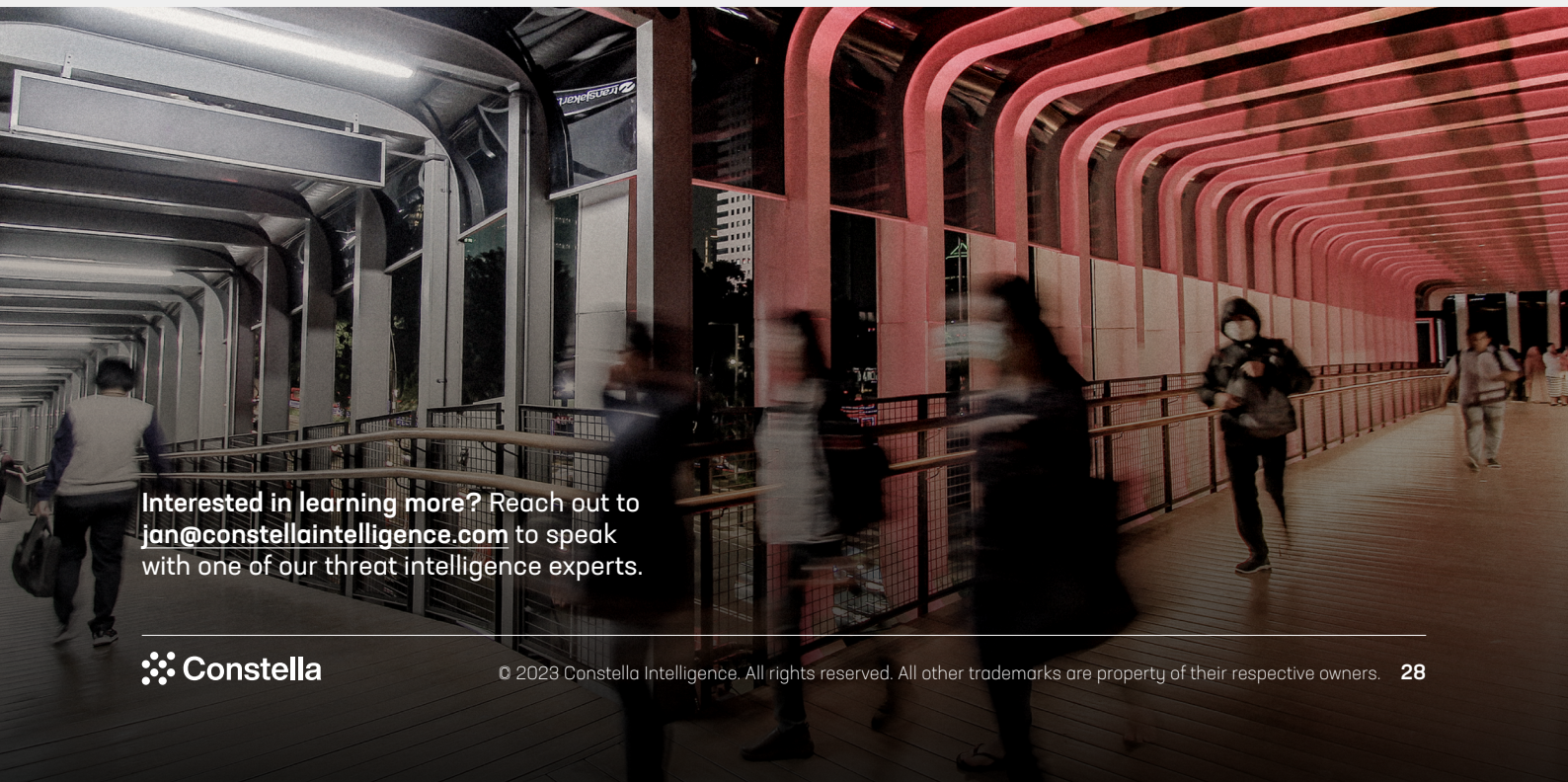
We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web 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 social media, 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 employees, and their critical assets. Because, the best way to overcome future digital threats is by facing them today.



Interested in learning more? Reach out to jan@constellaintelligence.com to speak with one of our threat intelligence experts.