

CYBERSECURITY REPORT

# 2023 State of the External Attack Surface

## Annual Threat Trends Analysis



CybelAngel

The external attack surface is cloud high, dark-web deep, supply-chain wide and internet infinite. It's our mission to detect and eliminate exposures and vulnerabilities our customers can't see...before cybercriminals can.



## Foreword

In 2022, after years of COVID-19 lockdowns, the world cherished the hope of returning to a more “normal” mode of operation. A needed break after the exhaustion of confinement. However, new conflicts soon erupted and tensions flared throughout the world on a variety of issues—and hacktivist and cyber criminal groups immediately exploited these pains in every way possible.

It's no surprise, really; after all, cybercriminals are inherently opportunistic. They systematically look for loopholes, and open doors that allow access to steal, destroy or blackmail. They rush to find the slightest exploitable cyber flaw to do the maximum damage. It's all about speed and stealth – a race against time to get in, get what they need, and get out undetected.

CybelAngel's *2023 State of the External Attack Surface: Annual Threat Trends Analysis* goes into this world to give you a glimpse into the myriad avenues hackers will take to get to their target. Businesses are becoming more and more decentralized, from the employee level to the supply chain, and that means the external attack surface is growing faster than ever. The data herein will help you understand what you can do to secure your organization against today's savvy cybercriminals.

I wish I could tell you that 2023 will be the year that you no longer have to worry about protecting your digital landscape but the data tells us otherwise. Still, knowledge is power, and this report will help support your business in your continued efforts to be safe, secure and resilient.



## Table of Contents

<b>1. Executive Summary</b>	<b>5</b>
<b>2. CybelAngel's Methodology</b>	<b>7</b>
<b>3. Overview of the Attack Surface</b>	<b>9</b>
3.1. SSL Certificates	9
3.2. Unknown Assets	9
3.3. Common Vulnerabilities and Exposures (CVE)	10
<b>4. Where Data is Vulnerable</b>	<b>12</b>
4.1. File Servers	12
4.2. Databases	15
4.3. Ransomed Servers	16
4.4. The Cloud	19
4.5. Credentials	21
4.6. Code Sharing	22
4.7. Dark Web	22
<b>5. The Exposure Landscape</b>	<b>24</b>
5.1. The External Attack Surface	25
5.2. Risk Areas by Industry	26
5.2.1. Average number of critical alerts	27
5.2.2. Relative percentage of assets with vulnerabilities detected	28
5.2.3. Average number of open ports	29
5.2.4. Relative percentage of unsecured databases	30
5.2.5. Average number of sensitive documents exposed	31
5.2.6. Average number of leaked credentials with passwords	32
5.2.7. Dark web credential activity	33
5.2.8. Average number of malicious sites	34
<b>6. Conclusion</b>	<b>36</b>
6.1. Trends for 2023	36
6.1.1. Proliferation of information stealers	36
6.1.2. Increase of shadow IT, including OT and IoT	36
6.1.3. Increase in unsecured/misconfigured clouds	36
6.2. Recommendations for 2023	37

<b>7. About CybelAngel</b>	<b>38</b>
<b>8. Appendix: Sample Findings</b>	<b>39</b>
8.1. Asset Discovery & Monitoring	39
8.2. Data Breach Prevention	42
8.2.1. Healthcare Exposure	42
8.2.2. Oil & Gas Exposure	42
8.2.3. Developer Exposure	43
8.3. Account Takeover Prevention	44
8.4. Dark Web Monitoring	47
8.5. Domain Protection	50
<b>About the Author</b>	<b>52</b>

# 1. Executive Summary

Every organization has policies, procedures and technologies in place to protect their environment and information. CybelAngel refers to the areas that a company can see and control as the perimeter. Outside of that perimeter is your external attack surface.

External attack surface management (EASM) is the fastest-growing area of critical cybersecurity exposures. It is the summation of multiple attack vectors coming from outside an organization's firewall, increasing the threat to security. These attack vectors are composed of assets, sensitive data and credentials that allow for access to your infrastructure and valuable data.

**This report is based on all exposures that were detected and scanned by CybelAngel in 2022. The extremely large sample size and volume of data allowed us to draw conclusions about the general state of the extended external attack surface in 2022.**

Raw numbers:

- 439M assets detected
- 740K unsecured/open databases
- 1.4M unsecured/misconfigured clouds
- 6.9M dark web detections
- In December alone we found:
  - 499K unsecured file servers containing over 70B files
  - 116K servers held by ransomware

Findings:

- 9% (or almost one in ten) of all detected assets had vulnerabilities associated
- 13% had expired SSL certificates, which can open up multiple attack vectors, including phishing attacks, man-in-the-middle attacks and data breaches
- 8% of all OT/IoT devices had vulnerabilities, which can act as a bridge to breach an otherwise secure network
- The top 10 common vulnerabilities and exposures (CVEs) were detected at least 12M times each



Based on our research, we predict the following trends for 2023:

1. A proliferation of information stealers
2. Increase of shadow IT, including OT and IoT
3. Increase in unsecured/misconfigured clouds

CybelAngel's research shows that 87% of all threats detected are from third-party or malicious actors. On the one hand, this means that most companies are doing the right things in securing their own perimeter from the inside, which is good. On the other hand, companies may be assuming there is nothing they *could* be doing to eliminate those threats, and that is not the case at all.

The external attack surface enables your managed perimeter to be breached and it happens with the (typically unwitting) help of your employees, partners, vendors, contractors and others via your trusted relationships. To regain control, you need to be aware of what your attack surface looks like so you can prioritize your limited security resources to stop attacks before they happen and stop leaks before they become breaches.

Our recommendation for CISOs in 2023 is to adopt a preemptive security strategy by taking control of your extended external attack surface. EASM is about being proactive rather than reactive.

In this report, we'll take a closer look at the overall external attack surface, then discuss key places where data is at risk, and dive into the exposure landscape and risk areas by industry. Finally, we'll share our thoughts on what these trends tell us about the year ahead in cybersecurity. We've also included an appendix with sample findings to further illustrate areas discussed in this report.

## 2. CybelAngel's Methodology

On a daily basis, CybelAngel's proprietary scanners combine with machine learning, high-speed scoring and over 10 years of data processing to provide actionable intelligence and alerts to protect our clients from external threats. These reports include context and investigation from our experienced analyst team, who work with the client to determine risk areas and prioritization with zero false positives. Those same inputs and sources are used in this report, along with opinions and recommendations from our industry experts.

### FASTEST IN-DEPTH SCANNING TECHNOLOGY IN THE MARKET

#### < 24 hours

**Fastest time-to-detect.** Other solutions take up to 60 days to detect an exposed database.

#### Deep Scanning

**Matches keywords inside documents & datasets.** Other solutions match at a metadata-level only.

### SOURCES MAY INCLUDE:



IPV4 connected SMB, NFS, RSynch, HTTP(S) filesystem, etc.



AWS S3, Google Cloud Storage, Azure Blob, Dropbox, OneDrive, etc.



MongoDB, MySQL, PostgreSQL, ElasticSearch, etc.



Codeslide, YouScribe, Slideshare, Prezi, Scribd, PDFArchive, Trello, etc.



Code Repositories, Collaborative platforms, etc.

This report includes an overview of the overall threat as well as data and results from our client base, which show real alerts, impact and actionability to today's threats. We also examine the speed and depth of attacks along with the specific vulnerabilities attackers seek—the "where" and "how" are extremely important.

Ethics and the privacy of our clients and potential clients are a big part of CybelAngel's DNA and are extremely important to us. While we do share examples of exposures, attacks, vulnerabilities and vectors, we do not and will not expose private or identifying information.

Detections or pre-filtered alerts refer to data our scanners provide around potential incidents. CybelAngel analysts then investigate the potential incident to determine that it is a true positive, i.e. contains information that is actually related to our client and that is truly sensitive or important to our client. We also undertake additional investigative work in order to deliver a fully contextualized incident report to the client. This report covers data pre- and post-filtering to show the depth and scope of the external attack surface along with the strength of CybelAngel's artificial intelligence (AI) and machine filtering.



## 3. Overview of the Attack Surface

How does the landscape look? Let's start with the entry point of an attack. If we can identify what entry points are vulnerable, like open assets, unsecured and accessible data, and domains, we can reduce these attack points before they are exploited.

**In 2022, CybelAngel's scanning capabilities detected over 439 million assets. Of those, over 39 million had an associated vulnerability.**

This means almost one in ten assets are freely detected in Internet scans and not behind a firewall or security feature—they are vulnerable to an attack.

### 3.1. SSL Certificates

In reviewing assets with SSL certificates (low-hanging fruit for a hacker), the numbers are alarming. SSL certificates ensure the website's identity via the digital certificate, which is used to encrypt data transmitted. This ensures sensitive information is protected from unauthorized access. Without a valid certificate, this can be an attack vector.

Without a valid or trusted certificate, the encrypted connection can no longer be established, which can leave assets exposed to a variety of cyberthreats. Examples include "man-in-the-middle" (MITM) attacks, with the attacker impersonating a legitimate website to steal sensitive information, or phishing attacks, where attackers reach out to individuals in an attempt to trick the unsuspecting into giving up key information. Organizations must regularly monitor and renew their SSL certificates.

CybelAngel detection capabilities found **over 91 million web assets** on open ports with either valid or invalid/expired certificates in 2022. Almost 13% of those detected had an invalid or expired certificate.

### 3.2. Unknown Assets

Understanding the composition of your external environment is the first step in knowing what to protect and what to prioritize for risk. For example, in 2022, CybelAngel detected hundreds of millions of unknown assets that were forgotten or had been undetectable by our customers' existing tool sets. Unknown assets often carry an inherent cost to

keep and/or maintain—a cost that the organization could be putting to better use. However, the real issue is that 8% of every internet-facing device detected by CybelAngel had an associated vulnerability.

### 3.3. Common Vulnerabilities and Exposures (CVE)

The race between awareness of an exposed vulnerable asset and making sure it is secure is not just an internal competition; it's between you and cybercriminals as well. When an asset has an associated CVE, this multiplies the risk. The CVE lets security professionals know what the risk and associated threat is, but also the roadmap to an attack. Here are the top 10 CVEs CybelAngel detected with associated detected assets in 2022 in volume.

Top 10 CVEs detected in 2022		
CVE	Description of CVE	# of times detected
CVE-2017-15906	OpenSSH which allows attackers to create zero-length files	17,211,891
CVE-2018-15919	Remote attacker could use this bug to test for the existence of particular usernames on a target system	15,340,767
CVE-2016-20012	Username and public key test in login	12,913,079
CVE-2021-36368	Attacker can silently modify server to support the “none authentication” option	12,913,079
CVE-2020-15778	Ability to move files to a remote server via scp program	12,856,076
CVE-2019-6110	MITM attacker manipulates client output	12,848,862
CVE-2019-6109	Malicious server or MITM can manipulate client output	12,848,862
CVE-2018-20685	Attack can bypass intended access restrictions via filename	12,848,862
CVE-2019-6111	A malicious SCP server or MITM attacker can overwrite arbitrary files in the SCP client target directory.	12,848,862
CVE-2018-15473	Not delaying bailout for an invalid authenticated user until after the packet containing the request has been fully parsed. Vulnerability is to data confidentiality.	12,697,428

The bigger problem: **Each one of these was detected at least 12 million times in 2022!** Of the thousands of CVEs, CybelAngel detected 987 of them at least one million times in 2022. Many of the CVEs are related and assets often have multiple CVEs. Determining what you have and mapping it to critical assets is essential to determine what you do and do not prioritize.

Even though the number of CVEs is alarming, it is the critical ones like Log4Shell and Exchange that grabbed the attention of every security professional in 2022. Sifting through all external-facing assets in a crisis is nearly impossible. CybelAngel was able to inform and direct our clients to the most vulnerable assets in their time of need, allowing them to isolate and to remediate and therefore reduce the risk associated.

Interestingly, 100% of the most-discussed CVEs had at least one public proof of concept (POC) freely available on Github<sup>1</sup>. While this may not be a surprise in 2022, sharing POCs has long been reserved to closed-access communities in the past. Nowadays, researchers and security aficionados team up to share their knowledge on platforms such as Github, Pastebin or personal blogs, as well as directly embedded in security tools such as Metasploit<sup>2</sup>.

Regardless of a CVE disclosure, POCs for most—if not all—discussed vulnerabilities make them exploitable from a broader community, including low-level actors (script kiddies). This, in turn, adds criticality to one-day flaws.

---

<sup>1</sup> <https://www.github.com>, a Microsoft-owned public code-sharing platform used by developers worldwide

<sup>2</sup> <https://www.metasploit.com>, a popular open source penetration software pre-equipped in hacking operating systems such as Kali Linux

## 4. Where Data is Vulnerable

Never assume your company data is safe. That's not to say it's your fault—there are simply too many vendors, partners and independent contractors in your supply chain. The weakest point in your security is those you need to trust, and the further your data is separated from you in your supply chain ecosystem, the less you can control its safe storage, transfer and use. Let's explore how exposed the world is when it comes to data.

In the previous section, we shared some alarming numbers involving your external attack surface and the exposed assets that can be entry points into your environment. Now, we are going to look at numbers that are downright scary.

### 4.1. File Servers

File servers hold our data, intellectual property, personally identifying information (PII), protected health information (PHI), legal agreements and more. They embody the critical functions, the very life of companies and of their employees'. Bad protocols and misconfigurations can expose all of it to the whole world.

Again, these exposures don't necessarily come from your own company but instead from your partners, employees, supply chain and vendors. Let's dive into the facts...

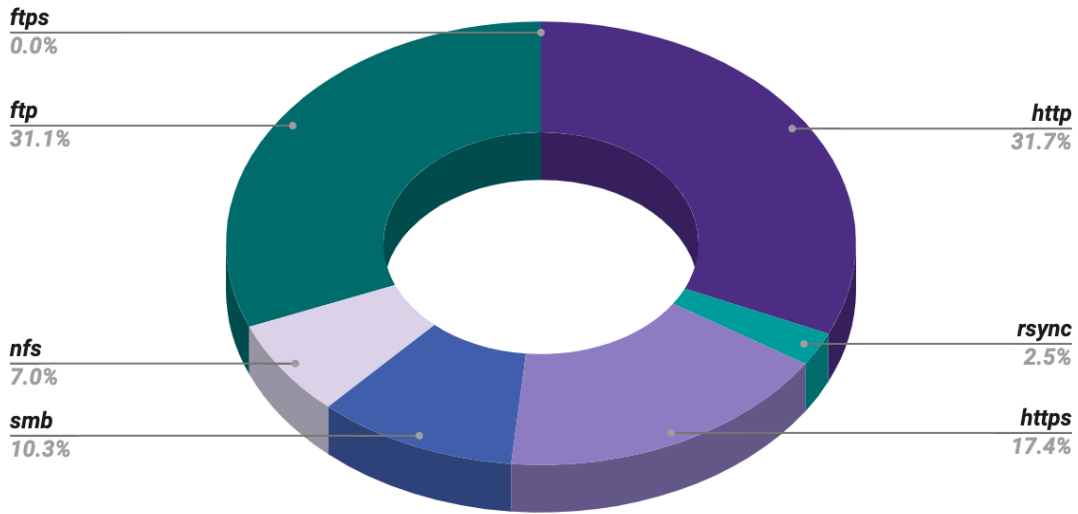
# 70,111,869,863

Number of unique files detected in Dec 2022

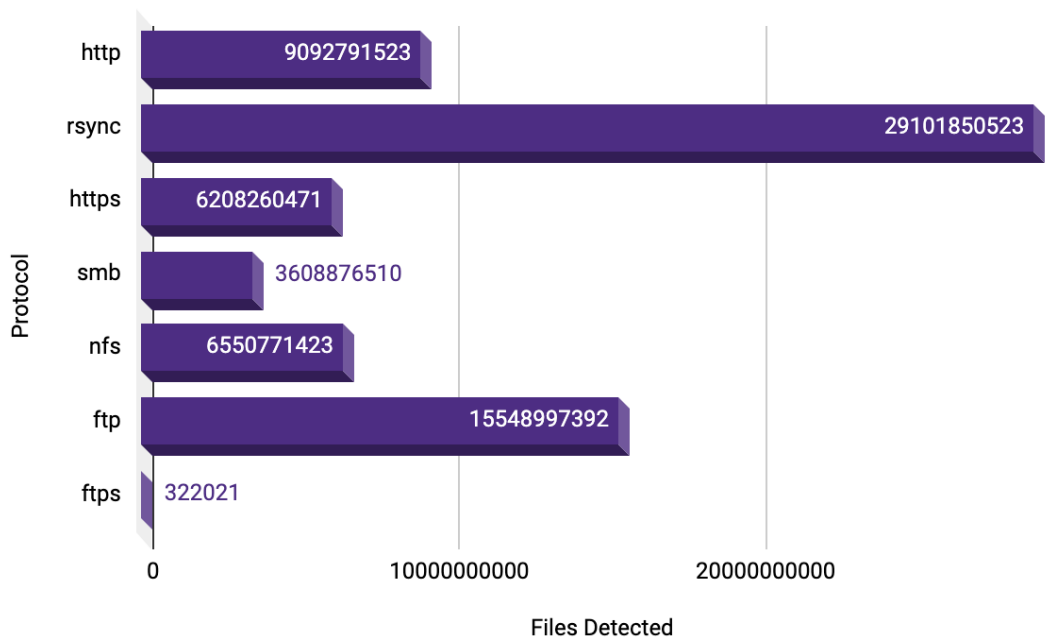
Freely accessible – no authentication required, no security

Look again at the time period: These 70 billion files were found within 498,976 unique open servers in a 31-day period in 2022. We could give you the yearly data but we'd be talking in the incomprehensible quadrillions. These are individual servers with unique IP addresses only counted once, even though CybelAngel scans the entire 4.3 billion IPv4 space within 24 hours and can detect any changes or new devices every day until they are properly secured or removed.

The charts below show the server and file detections by protocol for December 2022:



Unique server detections by protocol, Dec 2022

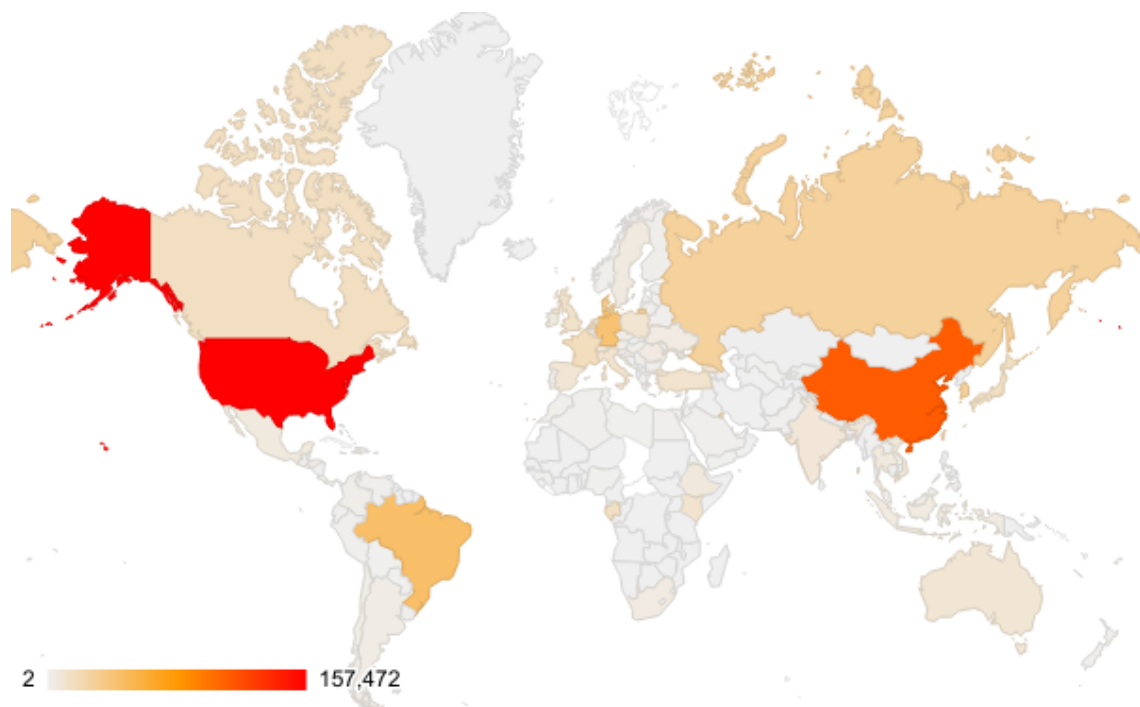


Files detected by protocol, Dec 2022



Not only is the data being exposed from a variety of protocols, it even happens with protocols that include “secure” in the protocol name!

Where is this data coming from? The heat map below shows the locations of these servers, with the darkest colors indicating the countries with the most detections.



*File server detections by country, Nov-Dec 2022*

The results may be surprising, as it is natural to presume that more-developed countries will be more secure. However, a more stable infrastructure means more data centers, which leads to a greater number of exposed assets. What we can derive from this chart is that even though the *internet and information* are controlled in certain countries, *data* is not only seen but unsecured.

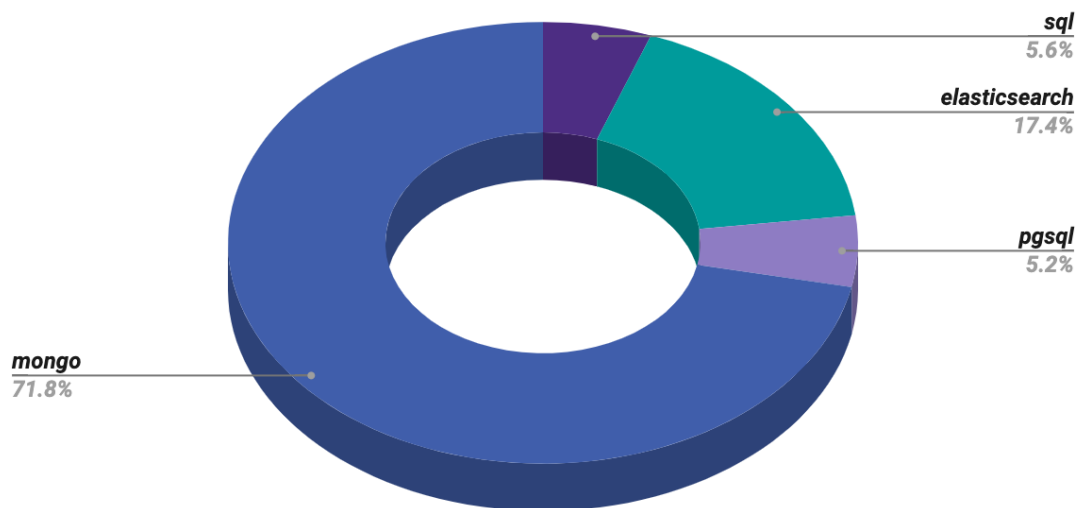
## 4.2. Databases

We know databases because they are the versatile backbone of data storage and correlation. They are also tables full of trouble. CybelAngel detected just under 740K open databases in 2022.

# 740,000

Open databases

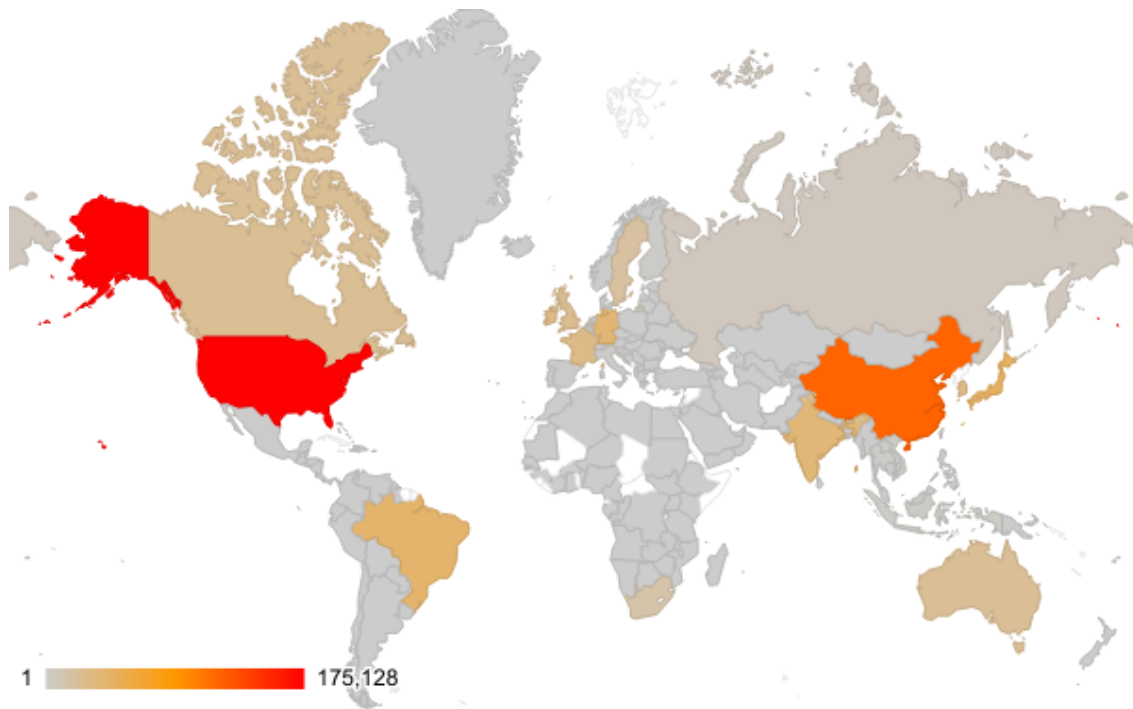
Note that this is the just number of *containers*. The average database has 10 tabs containing thousands of cells of data. Every line, every tab, every cell and every macro in each of these databases is open and available to be exploited by anyone who can find it. Worried? You should be: if it is valuable to you, imagine what it is worth to others.



Open databases by protocol for 2022

Of the database protocols scanned by CybelAngel in 2022, MongoDB was by far the most frequently detected, accounting for 71.8% of open databases. Detection of open databases is a result of the setup and use of databases including misconfiguration and failure to include user authentication. CybelAngel detected over 525K open Mongo databases alone in 2022.

This heat map below demonstrates where we detected open databases across the world and the saturation by country.



*Open databases by country, Nov-Dec 2022*

The United States had by far the most open databases with over 175K detected in 2022 but no country was spared. Even the Isle of Man had one open database detected by CybelAngel. The scanners used by CybelAngel have no language, alphabet or geographical limitations.

### **4.3. Ransomed Servers**

If CybelAngel can find it, others can too—hackers, competition, nation-states and people you just don't want to see your information. Some of them will give it back...for a price.

ATTENTION!

Don't worry, you can return all your files!  
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.  
The only method of recovering files is to purchase decrypt tool and unique key for you.  
This software will decrypt all your encrypted files.  
What guarantees you have?  
You can send one of your encrypted file from your PC and we decrypt it for free.  
But we can decrypt only 1 file for free. File must not contain valuable information.  
You can get and look video overview decrypt tool:  
<https://we.tl/t-V2fE396VPW>  
Price of private key and decrypt software is \$980.  
Discount 50% available if you contact us first 72 hours, that's price for you is \$490.  
Please note that you'll never restore your data without payment.  
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

To get this software you need write on our e-mail:  
[helpteam@mail.ch](mailto:helpteam@mail.ch)

Reserve e-mail address to contact us:  
[helpmanager@airmail.cc](mailto:helpmanager@airmail.cc)

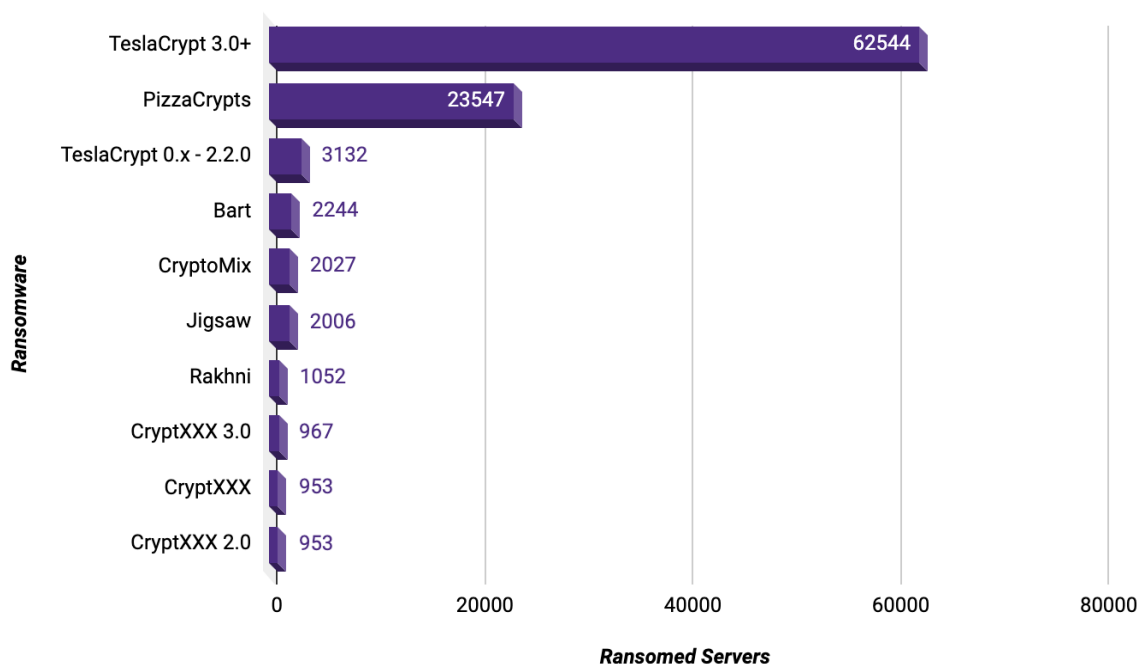
Your personal ID:  
121dvhgCeQS9z0ZE9AvEcn034DNsTYPXPmbcPhmBrQ2bS4znn

*Ransomware message present in the server*

CybelAngel's technology scans for the file extensions that are the leading causes of data leaks. Besides being unsecured via bad/misconfigured protocols, CybelAngel detected 116K ransomed servers online during December 2022 alone. Of these ransomed servers, 198 different types of ransomware were found.

**116,000**

Ransomed servers detected in December 2022



*Top 10 ransomware types, Dec 2022*

The bottom line with ransomware is that you've lost control of your data. Data security is formulated around the "CIA triad": confidentiality, integrity and availability. If a cybercriminal has your data, its availability has already been compromised and it is no longer confidential. This naturally means that the data's integrity can no longer be guaranteed. From a data security perspective, you've lost everything because once cybercriminals have your data, they can make copies and sell it even after you paid the ransom.

Here's what many companies overlook: Your data can be ransomed without your knowledge. You share critical business and security data with your "trusted" partners, suppliers and vendors—if their data is ransomed it may also include your data. You may have a data protection clause in your contracts but the simple fact is, if they don't tell you, you won't know.



## 4.4. The Cloud

If we aren't putting data in databases, we are storing it in the cloud. These amazing services have reduced the cost of storage and increased the ability to share...and the ability to overshare. With technology and advancements of ease come the inability to configure properly or track as an asset, which makes you vulnerable to hackers.

CybelAngel scans for data that is available and unsecured in the cloud. The outcomes can be looked at in two categories:

1. Personal cloud drives
2. Enterprise storage

Personal cloud drives include Google Cloud Drive, OneDrive and Dropbox. Individuals or small businesses may use email-related storage or other free services to store important data, spreadsheets, pictures, presentations and other critical data.

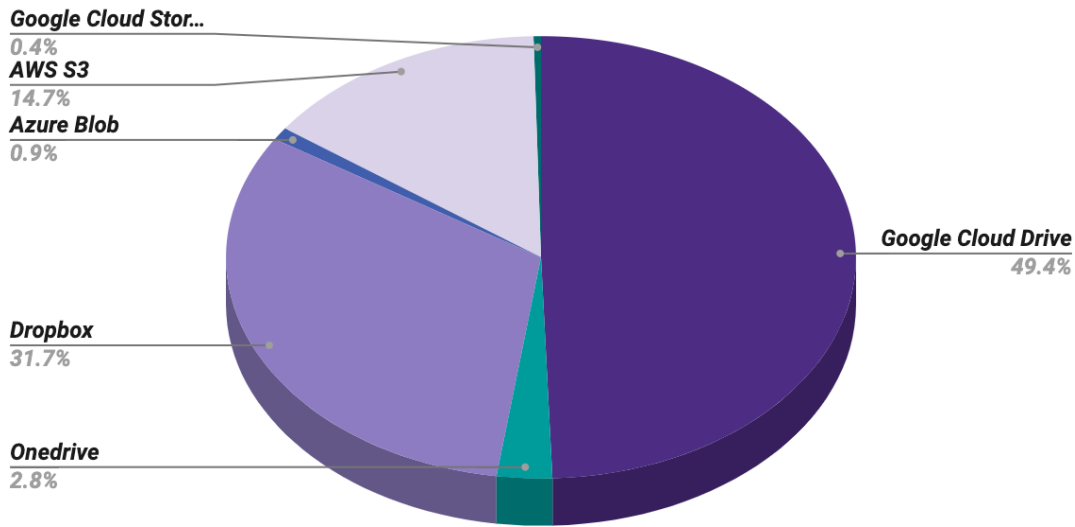
As much as security professionals may advise against it, the ugly truth is that people scrape business-critical data from work, clients and past employment and store it on these types of services. CybelAngel finds these overshared, unprotected and misconfigured at an alarming rate.

The second category of cloud exposures CybelAngel detects is enterprise storage. This is used by a company for both cloud services and for infrastructure purposes.

# 1.4M

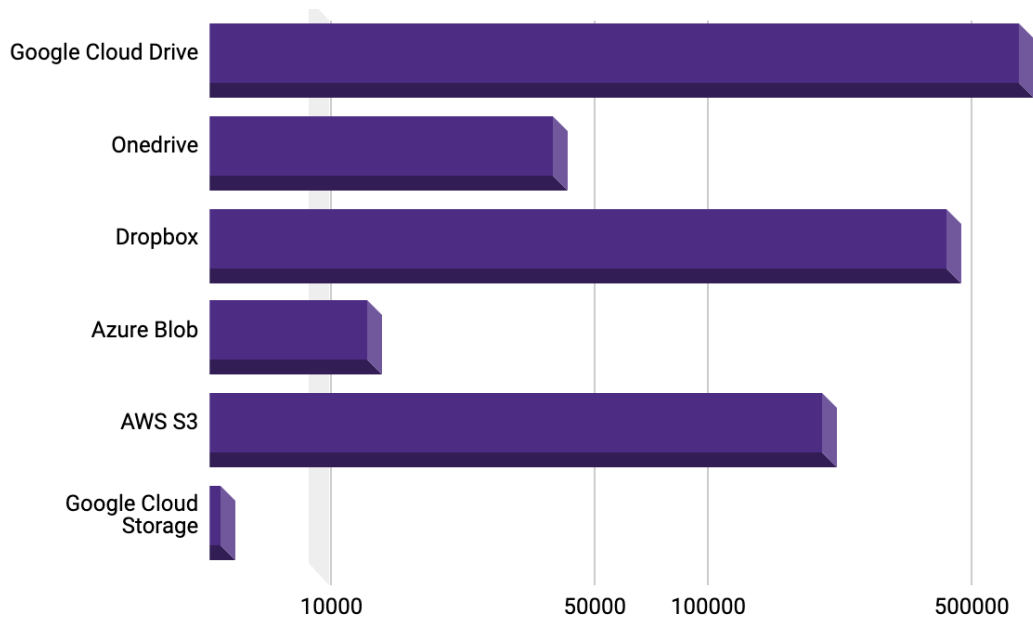
Misconfigured cloud devices

In 2022, CybelAngel detected 1.4 million misconfigured cloud devices, leaving the contents available for exploitation. The graph on page 20 breaks this number down over the industry leaders in cloud storage.



Cloud drive detections, 2022

Almost 50% of all open cloud devices detected are Google Cloud Drives (personal). It isn't that the technology is bad, it's that non-enterprise users typically don't understand how to secure and configure it properly. This is the typical negligence example which, left unchecked, can lead to exposures and malicious activity like ransomware, exploitation or monetization of critical data.



Exposed cloud drives, 2022

Of the exposed and open enterprise services, AWS - S3 devices or buckets are by far the most detected as being open and accessible to attackers. CybelAngel detected over 218K open AWS S3 storage devices.

What can we infer from this? The raw detection numbers could be a direct correlation to their respective market shares, i.e., cloud services that are more popular are detected more frequently simply because they are more abundant, not necessarily that they are less secure. Without concrete market share figures, we can speculate that paid Google Cloud Service may come with more security features and protection versus the free version—you get what you pay for and what you use. The other side of the coin is AWS also has security features, but they may not be as user friendly or may have less secure default settings, which lead to more misconfigurations by users.

However, the main point is that any enterprise-level cloud storage device and services will contain more sensitive and company-linked data that should not be left open. Any exposure derived from enterprise products has a higher criticality and great risk of attack and exploitation of content, based on the sensitivity and value of the drive.

## 4.5. Credentials

Hackers are determined, but they are also creatures of habit and will always leverage the tried-and-tested methods. Why? Because they work. Credentials, exploits, vulnerabilities and open and unsecured devices are the hacker's playground, gateways to information they can use for their own gain.

One of the most proven ways to gain access is by using exposed credentials. Hackers may be able to get in via brute force, but it takes a lot of time and effort. Employees credentials that are publicly exposed on the open, deep or dark web expedite the process: It's easy to open a lock when you have the key.

Scanning for emails associated with CybelAngel's clients in 2022, we found 50% of them came with an unhashed password. We also see that many of the exposed emails in different breaches either share the same password or a close variation of another exposed password. Although NIST password guidelines released in 2022 indicated that password rotation and forced changes are not necessary practices, the data and behavior suggest otherwise.

Despite the valiant efforts of organizations to implement password policies to prevent password attacks, passwords will inherently always be at risk of being stolen from negligent employees. Policies alone are not enough; employees must be trained on proper cybersecurity hygiene and this training must be continually reinforced.

## 4.6. Code Sharing

Codeshare sites are another hunting ground for hackers and a CISO's source of nightmares. Github alone boasts they have 94 million users who share code, development and ideas. CybelAngel finds this is also where they overshare, cut & paste and place critical code, API keys and credentials by mistake, leaving the door open to an easier attack via more access at a deeper level. This increases the global attack surface and is another data source that can be used to breach a company.

- Number of repositories detected: **5,517,239**
- Number of repo authors detected: **3,146,964**

These numbers are a representative example of findings to our clients in 2022 and the number of coders mentioning their companies and projects on Github alone. Filtering through this amount of data to detect your own critical data, even with open-source tools, is virtually impossible without outside help.

## 4.7. Dark Web

Hackers love to share and sell information on the deep and dark web. The dark web is a group of websites that cannot be reached without specific software that, if configured properly, will allow for anonymity while using. Some of these criminal sites are even available through the internet.

CybelAngel provides visibility into each step of the kill chain to identify exposures and vulnerabilities on the open web before a malicious actor can take advantage of them. In all the areas we've discussed so far, data is vulnerable but not necessarily compromised yet. The dark web represents the end of the kill chain / lifecycle of a data exposure—malicious actors have compromised systems and stolen credentials along with other sensitive information and posted it on the dark web (mostly for sale), to be leveraged by other malicious actors to cause damage to an organization.

In order to provide comprehensive coverage, we also look into the deep and dark web to provide insight into what has been compromised so that the customer can quarantine the affected areas and have a smoother incident response process.

Below are the number of detections that we have found in 2022 for deep and dark web marketplaces and forums. These represent holes in security that were acted upon, which could have been prevented with continuous EASM.

- Total detections: **6,862,324**
- Total number of sources scanned: **7,204**

Top 10 Deep and Dark Web Sources		
Source	Count	% of overall detections
genesis7sntjrdbt.onion	1,268,450	18.48%
<a href="#">cracked.to</a>	1,124,785	16.39%
rusmarkethgwhfbn.onion	1,082,802	15.78%
<a href="#">www.reddit.com</a>	759,111	11.06%
<a href="#">t.me</a>	453,207	6.60%
<a href="#">www.nulled.to</a>	365,965	5.33%
<a href="#">breached.co</a>	151,085	2.20%
<a href="#">gab.com</a>	108,669	1.58%
dreadditevelidot.onion	99,117	1.44%
<a href="#">wwh-club.net</a>	90,804	1.32%

This data also tells us there is a lot of noise, chatter and garbage on the deep and dark web. Just focusing in on the Genesis and Russian Markets, which are outright criminal forums, over 2.35 million detections were found of stolen credentials and other datasets for sale, some legitimate, some used and others useless. It's essential that you know whether your data is on the dark web but trying to manually scan, scrape and analyze the data on your own is extremely time-consuming and labor-intensive. This is an area where it's best to engage an expert to do the heavy lifting so that your security teams can focus on the right priorities.

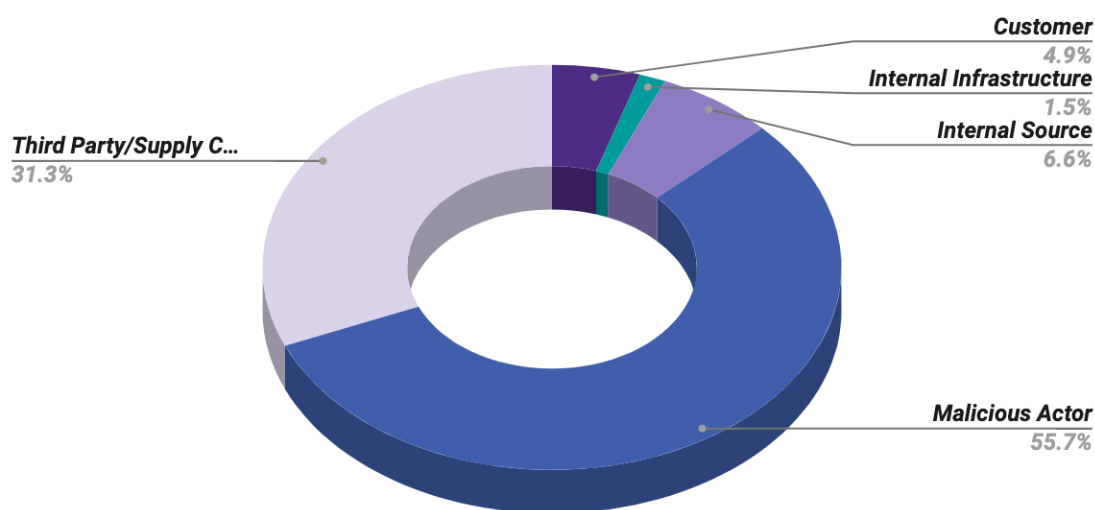


## 5. The Exposure Landscape

Research in this section is based on aggregated data from all CybelAngel clients in 2022. Although the data is from our clients only, CybelAngel clients represent a good cross-section of all industries and can be considered a random sample of sufficient size (statistically speaking) to extrapolate to the market as a whole.

CybelAngel's research shows that 87% of all threats detected are from third-party or malicious actors. While slightly biased (coming from a company that specializes in external detection), it means most customers are doing all the right things in securing their own perimeter from the inside. Otherwise, we would be finding more exposures coming from first-party sources (our scanners find exposures on your servers just the same as we would on a third party's).

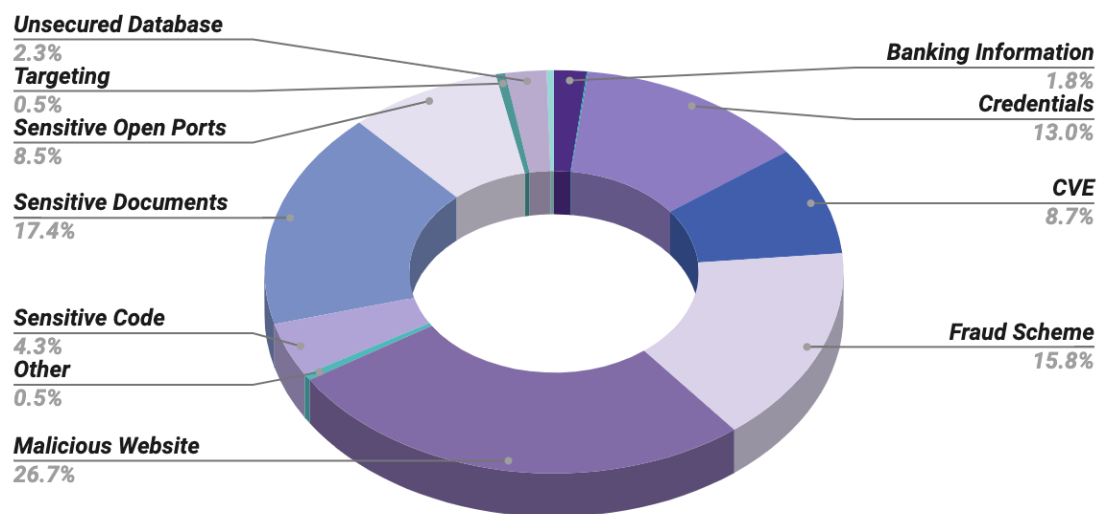
Nevertheless, we still report on a large number of malicious activities, meaning too many threats are discovered after the fact when they could have been eliminated proactively. We see this primarily due to bad actors using domains as an attack vector—CybelAngel can detect look-alike domains early and monitor for malicious activity during the lifecycle of the domain, giving our clients the ability to block and react earlier to attacks.



Source of threats

## 5.1. The External Attack Surface

Think of the external attack surface as a set of doors and keys: Doors are internet-facing assets such as servers, applications, APIs, domains, IoT devices, cloud buckets, etc. Keys are credentials (often weak passwords or stolen login information obtained via phishing attacks or purchased on the dark web), public APIs and vulnerabilities like misconfigured access points or services that basically leave your doors unlocked.



*Threats identified*

If we break down this visual, this is what comprises the external attack surface:

- Unsecured and available data to exploit
- PII, PHI and banking data
- Sensitive open ports to critical services
- Assets with critical and known vulnerabilities and exploits
- Sensitive code exposed
- Credentials exposed in the dark web, being stolen via malware, in code repositories and left in open databases, ripe for the picking
- Malicious websites fooling your clients, partners, supply chain, employees and the public

Even though databases represent a small percentage of the reports CybelAngel sends, the severity of the findings average higher than a typical alert, mainly due to the volume found within databases but also the value of the data inside.

As we sought out patterns related to sectors or industries, we broke down our client base into the following sectors:

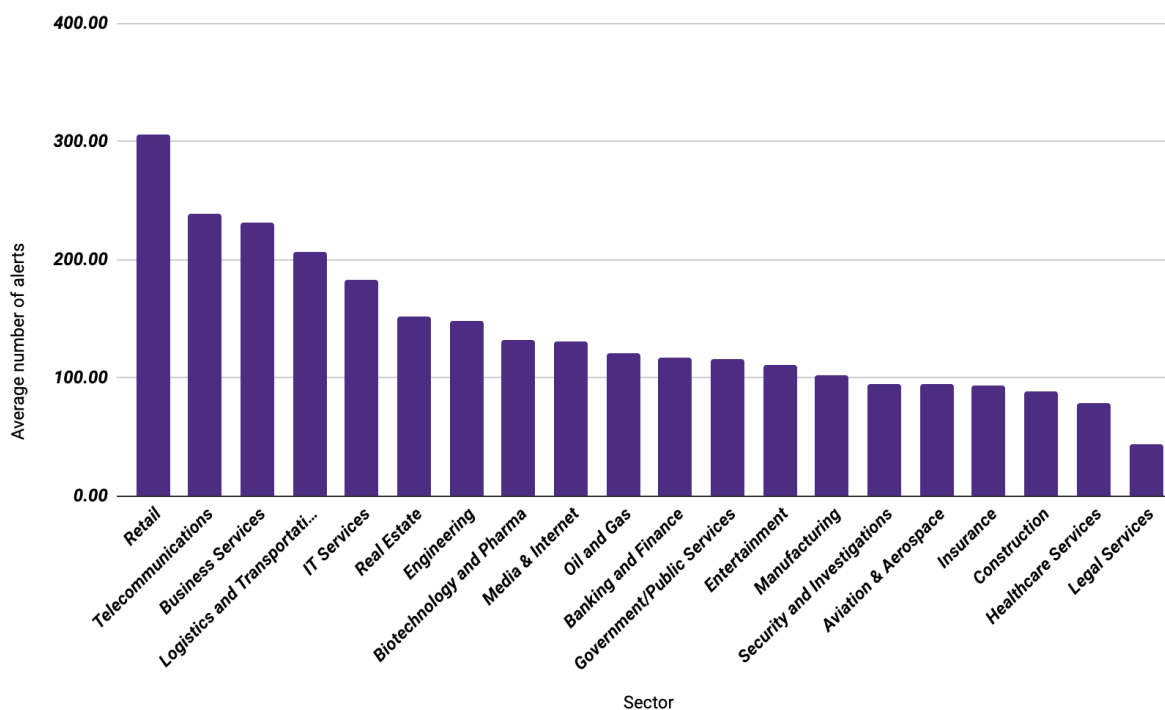
- Aviation & Aerospace
- Banking & Finance
- Biotechnology & Pharma
- Business services
- Construction
- Engineering
- Entertainment
- Government/Public Services
- Healthcare services
- Insurance
- IT services
- Legal services
- Logistics & Transportation
- Manufacturing
- Media & Internet
- Oil & Gas
- Real estate
- Retail
- Security & Investigations
- Telecommunications

Let's examine more granular data around types of alerts and attacks detected as sent to CybelAngel customers in 2022.

## 5.2. Risk Areas by Industry

In this section, we take a closer look at different risk areas such as exposed assets, data leaks, stolen credentials and malicious domains and how these impact various industries.

### 5.2.1. Average number of critical alerts



Top three:

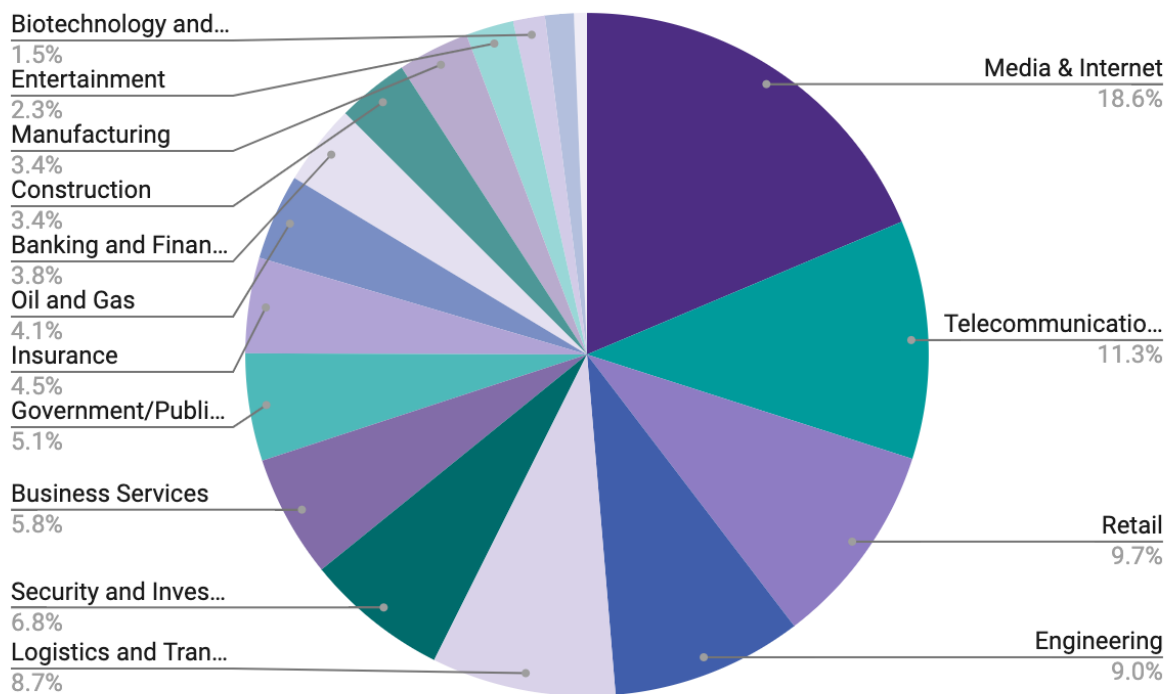
1. Retail  
Telecommunications
2. Business Services

What made these industries top the chart:

- **Retail:** Retail had a disproportionately high number of malicious domains and many vulnerabilities detected in their assets.
- **Telecommunications:** Telecommunications ranked quite high in many of the risk areas we examined—open ports, unsecured databases, sensitive documents, leaked credentials and dark web activity.
- **Business Services:** Business Services were overrepresented in dark web activity and the number of malicious domains.

The average number of critical alerts can be thought of as an “overall score” as to which industries are most at risk. It represents the overall risk better than the raw number of alerts since it also takes into account the severity of alerts. However, it does not tell the full story, which is why we follow this with a deeper dive into different risk areas that could generate an alert.

### 5.2.2. Relative percentage of assets with vulnerabilities detected

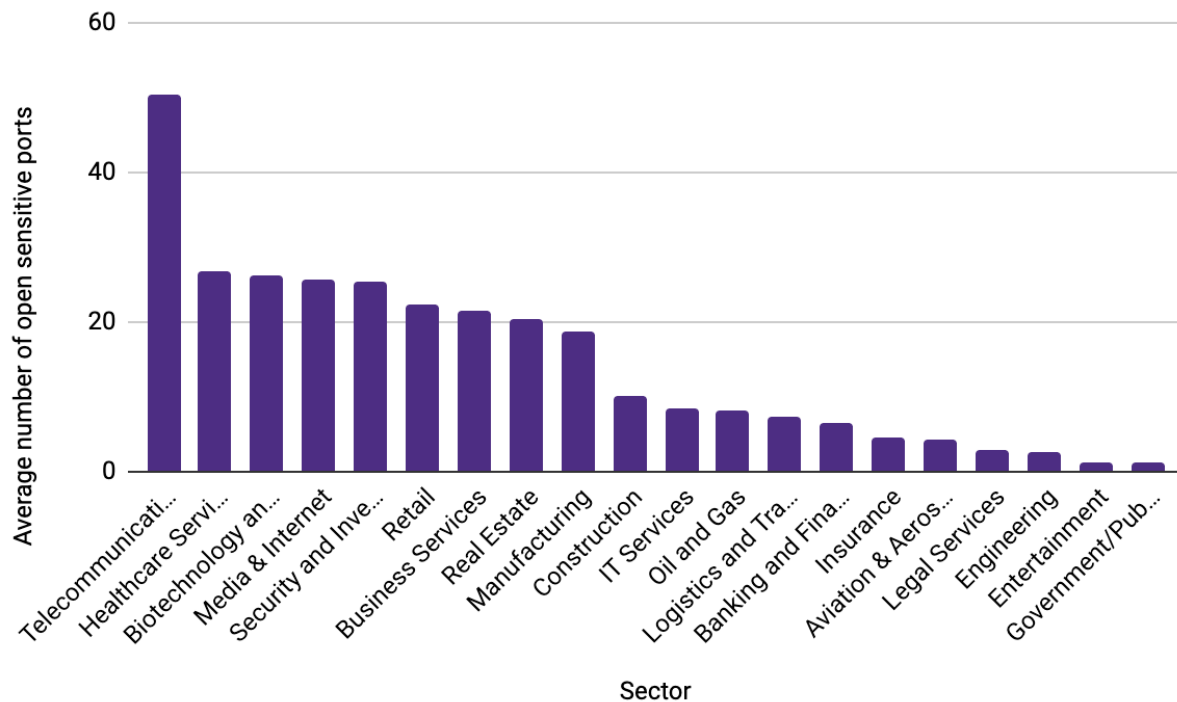


Top three:

1. Media & Internet
2. Telecommunications
3. Retail

These industries all have a huge number of digital assets. They are frequently enterprise-level companies with a large number of employees and widespread use of personal devices on corporate networks, which means increased shadow IT and assets. They are also industries with a huge supply chain of distributors, partners and vendors, which typically results in a higher risk of exposure by third parties.

### 5.2.3. Average number of open ports



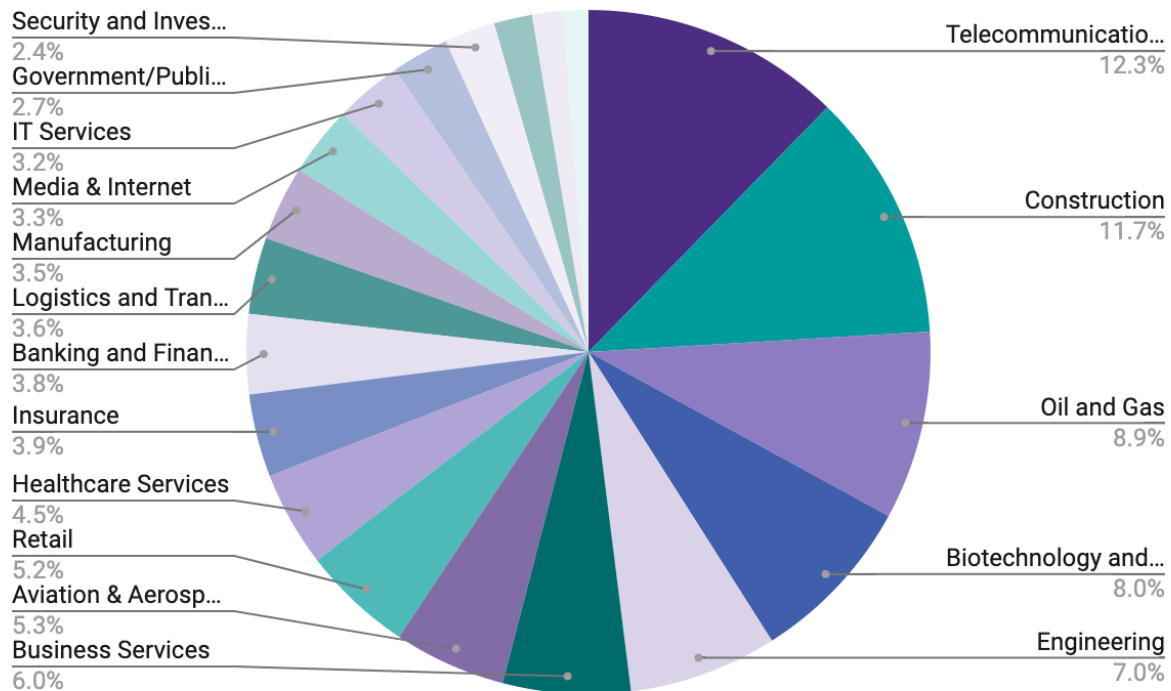
Top three:

1. Telecommunications
2. Healthcare
3. Biotechnology

These industries have a greater number of OT and IoT devices, which have less-common ports, protocols and configurations compared to typical business networks. Typical security processes might not be effective or miss detections as they are coming from a broad network. It can be easier to map the attack surface from the outside-in versus from within looking out.



### 5.2.4. Relative percentage of unsecured databases

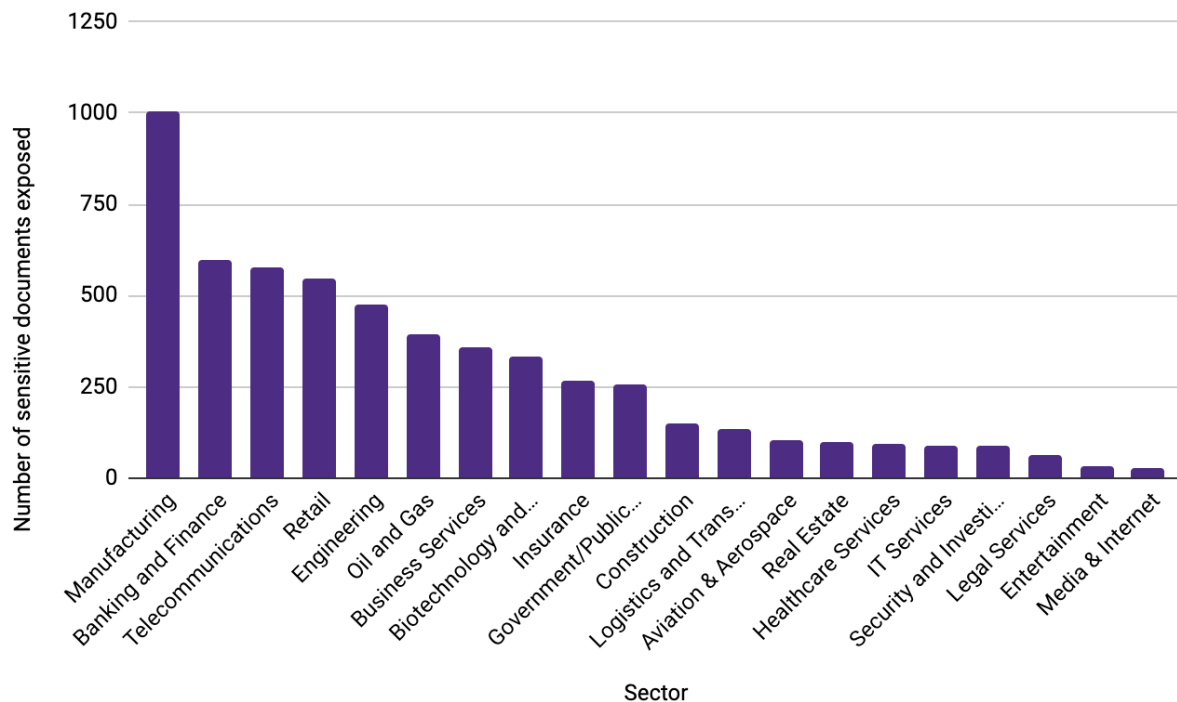


Top three:

1. Telecommunications
2. Construction
3. Oil & Gas

These are traditional industries in the midst of rapid digital transformation across vast global networks. They are typically less mature in security practices compared to digitally native industries. They have a large and complex supply chain, which comes with a high risk of third-party exposures.

### 5.2.5. Average number of sensitive documents exposed



Top three:

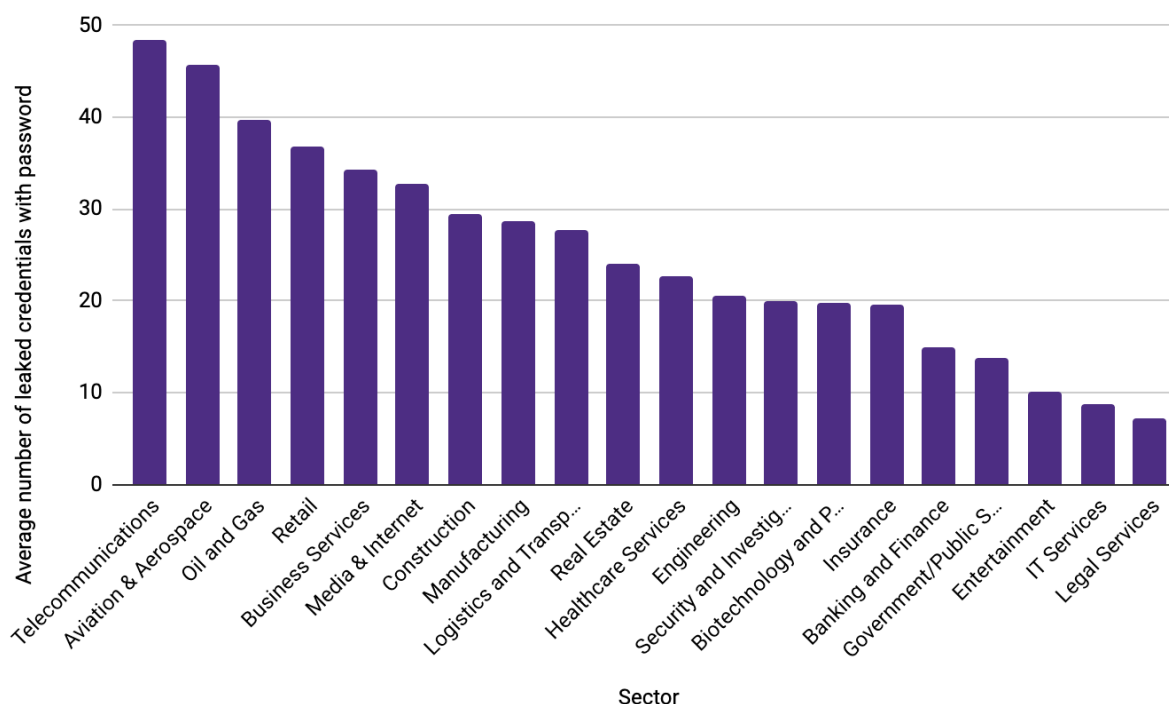
1. Manufacturing
2. Banking & Finance
3. Telecommunications

Manufacturing and Telecommunications are both industries with vast and complex supply chains. As the number of players in the ecosystem increases, so does the risk of third-party exposures, especially if not all entities within the system have mature security practices or strong security postures.

Banking & Finance are typically thought of as cybersecure, and they are, but they are still a high-value target due to the lucrative information they possess. And with sheer volume of transactions, all digital and online, there is almost no escaping accidental exposures even if you somehow managed to eliminate all intentional and malicious attacks.

### 5.2.6. Average number of leaked credentials with passwords

Leaked credentials are credentials that were found in open/unsecured databases and file servers.



Top three:

1. Telecommunications
2. Aviation
3. Oil & Gas

As we've discussed previously, when traditional industries undergo rapid digital transformation, there are often gaps in their security. It takes time to modernize and retrofit legacy systems that were not designed from the ground up with cybersecurity in mind. Many of these critical systems cannot be simply taken offline or replaced without serious disruptions to, not just the company itself, but also the wider economy.

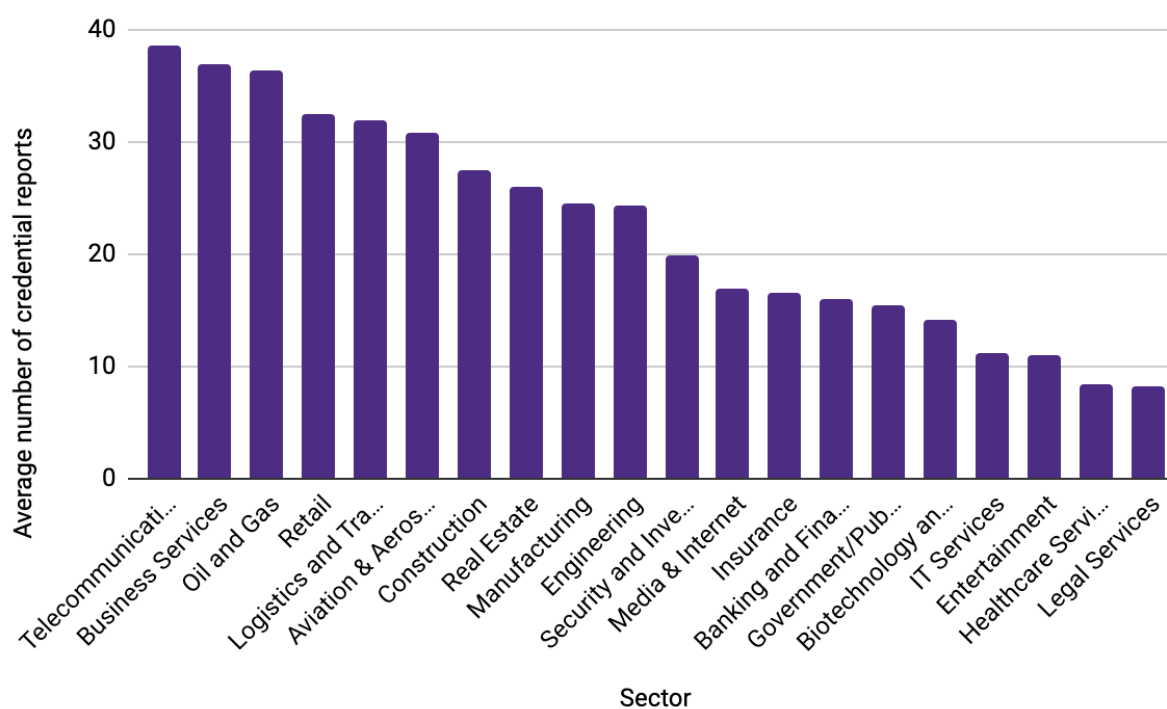
What is especially concerning about seeing these particular industries top the chart for leaked credentials is that they are all critical infrastructure sectors that are vital to the

functioning of the global economy. If the right credentials end up in the wrong hands, nation-state actors could gain unauthorized access to sabotage these critical choke points, causing wide-ranging and debilitating effects on international economic security.

We felt that this deserved more analysis, so we looked at credentials from another angle: Credentials that were leaked could be accidental and may not be inherently malicious, but which credentials do malicious actors think are worth paying for?

### 5.2.7. Dark web credential activity

Alerts that included credentials and passwords being sold or exposed on dark web forums. Each alert could include multiple credentials and passwords being sold as a bundle.



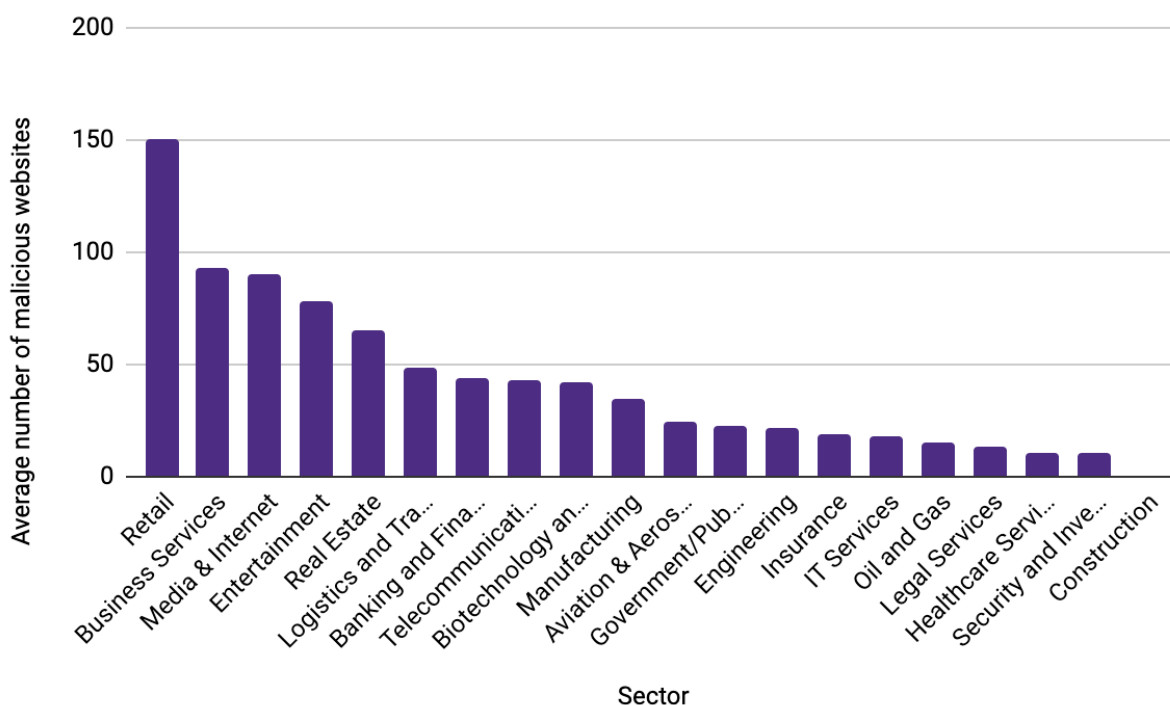
Top three:

1. Telecommunications
2. Business Services
3. Oil & Gas

The charts are fairly similar to the previous section, with telecommunications and oil & gas remaining in their respective spots. What is interesting is that compared to leaked credentials, business services credentials are now ranked as one of the most available for sale on the dark web. There can be several reasons:

- Access to these systems themselves are seen as valuable, whether it is for potential profit or malice
- The data in these industries are worth more and therefore credentials that allow access to the data are worth more
- The nature of the business, many of which we have discussed: more employees, more customers, larger supply chain; all of which increase risk and prevalence of fraud

### 5.2.8. Average number of malicious sites



Top three:

1. Retail
2. Business Services
3. Media & Internet

It is no surprise that the chart toppers here are all consumer brands with the most recognized names. These industries have the most digital presence and the most direct-to-consumer interactions. This is why cybercriminals often hijack these brands for phishing attacks. These companies have to be vigilant about protecting the reputation and goodwill they have spent millions (even billions) of dollars building up, or it can easily be eroded if their name is used to perpetuate fraud or becomes associated with criminal activities.



## 6. Conclusion

We've presented a 30,000-foot view of the exposure landscape in 2022 and dissected some of the risk areas by industry. Now that we are done analyzing the past, we can use this information to predict what we can expect looking forward.

### 6.1. Trends for 2023

#### *6.1.1. Proliferation of Information Stealers*

Information-stealing malware is becoming one of the most popular vectors for cyberattacks. From our monitoring of credential leaks and dark web marketplace activity, we predict an increase of important corporate credentials being stolen by malware designed specifically for this purpose, potentially exposing sensitive and proprietary data.

#### *6.1.2. Increase of shadow IT, including OT and IoT*

Most companies invest a lot of resources to protect their known assets but shadow assets are, by definition, a blind spot and are therefore unprotected and extremely vulnerable. The number of unsecured, internet-facing operational technology (OT) and Internet of Things (IoT) devices is also growing, and especially attractive to attackers. With the number of internet connected assets growing by day, the risk of something flying under the radar of security teams is only going to keep increasing.

#### *6.1.3. Increase in unsecured/misconfigured clouds*

Cloud adoption is ramping up at an incredible pace, with applications and workflows moving to the cloud to support our new "work from anywhere" lifestyle. Unfortunately, this complicated multi-cloud environment is now part of your external attack surface and even if you secured everything under your purview, there is still the risk of a leak or breach from a third party in your supply chain or partner ecosystem.

## 6.2. Recommendations for 2023

Our recommendations boil down to one thing: **Adopt a preemptive security strategy.**

The days of passive or reactive security are gone. Today's threats cannot be found by waiting for detections from endpoints or alerts from inside your security perimeter. Security teams need to be on the constant lookout for early indicators and address them before they even become problems.

To do this effectively, you need full visibility of your extended external attack surface, which not only includes your known assets, but also shadow assets of your employees and assets belonging to your partners, vendors, suppliers or other third parties. Taking an outside-in view, like an attacker would, allows you to spot any weaknesses in your security and remediate them before they can be exploited.

*Looking for more personalized recommendations?  
Contact CybelAngel for a complimentary [External Exposure Scan](#).*

## 7. About CybelAngel


CybelAngel is a leader in external attack surface management (EASM) solutions. We protect our customers with an extensive and continuous ‘outside-in’ search of an organization’s internet-facing attack surface to discover exposed and unknown assets, produce a living map of online infrastructure, and uncover hidden vulnerabilities and threats. CybelAngel analysts then contextualize the most critical findings based upon business severity and perceived risk. This unique combination of machine and human intelligence leads to the highest signal-to-noise ratio on the market, leaving IT and Security teams free to focus on core business operations.

### CYBELANGEL PROFILE

Founded	Customers	Employees	Analysts	Engineers	Gartner® Peer Insight	ROI per Forrester®
2013	170+	175	40	60	4.8/5	359%

Paris | Boston | London | Dubai | New York City

**A leading vendor recognized by:**



No endorsement is expressed or implied.

“

CybelAngel is best of breed for [detecting] leaked data that can be accessed outside the enterprise perimeter, such as public cloud environments or connected storage devices.

*Elizabeth Kim, Ruggero Contu*  
*Competitive Landscape: Digital Risk Protection Services*

”

## 8. Appendix: Sample Findings

Think of the external attack surface as everything you can't see or control but you rely on every day to do your job, conduct business or do your day-to-day activities. Do you see or control the revenue tools you use, the bank that does your payroll and bills, the infrastructure of the applications you are using right now on your devices or the way other businesses are interacting with your systems and data on a daily basis? Of course not, yet they have a significant impact on your operations.

The external attack surface enables your managed perimeter to be breached, and it happens with the (typically unwitting) help of your employees, partners, vendors, contractors and others via your trusted relationships. To regain control, you need to be aware of what your attack surface looks like so you can prioritize your limited security resources to stop attacks before they happen and stop leaks before they become breaches. **EASM is about being proactive rather than reactive.**

As part of our EASM solution, CybelAngel focuses on addressing threats across five key areas:

1. Asset Discovery & Monitoring
2. Data Breach Prevention
3. Account Takeover Prevention
4. Dark Web Monitoring
5. Domain Protection

In this appendix, we've gathered examples of real-world findings across these areas. All findings have been anonymized to protect the affected customers.

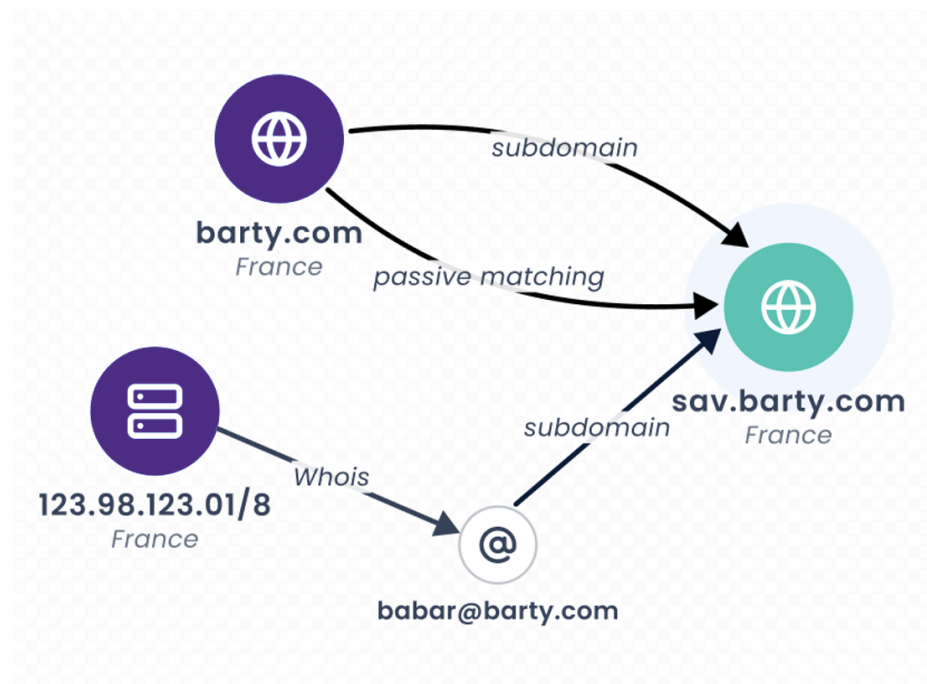
### 8.1. Asset Discovery & Monitoring

**Protecting organizations against shadow IT risks.**

CybelAngel identifies decommissioned cloud instances, unmonitored domains and rogue assets through its external asset inventory tool. This allows for a visual assessment of connected assets as seen externally without deployed agents. Besides knowing your inventory, CybelAngel discovers new potential threats coming from known CVEs, internet-facing critical ports left open and expired SSL certificates.

In 2022, we alerted our clients to vulnerabilities associated with externally detected assets, noted in sections [5.2.2](#) and [5.2.3](#), awareness of the vulnerabilities and open ports is vital to our customers overall, as you cannot protect what you don't know exists. Having an inventory of hosts and subdomains with associated issues is essential in today's dynamic environments and growing attack surface.

The diagram below shows how CybelAngel can use pivoting techniques to discover unknown assets:



The ability to see the associated threats and vulnerabilities is the next step to prevention. The screenshot below shows how these assets are prioritized:

Hosts (753)		Subdomains (1031) <span>?</span>		<a href="#">Export Assets</a>			
Status	IP Address	Threat level	First Seen	Registrar	Organization	Related inputs	Services
To be monitored	203.0.113.60 France	<span style="color: red;">●</span> Critical	Aug 29, 2022	Name.com	Seegal France	2	20
To be monitored	203.0.113.83 France	<span style="color: red;">●</span> Critical	Sep 19, 2022	Name.com	Seegal France	2	2
Discovered	35.187.46.64	<span style="color: red;">●</span> Critical	Sep 14, 2022			3	32
Discovered	192.0.2.7 United States	<span style="color: orange;">●</span> Major	Sep 20, 2022	GoDaddy	Seegal Corporate USA	2	10
Discovered	198.51.100.14 United States	<span style="color: orange;">●</span> Major	Sep 11, 2022	Nameshield	Seegal Corporate USA	2	3
Discovered	198.51.100.191 United States	<span style="color: orange;">●</span> Major	Aug 24, 2022	Nameshield	Seegal Corporate USA	1	1
To be monitored	198.51.100.213 United States	<span style="color: orange;">●</span> Major	Sep 14, 2022	Nameshield	Seegal Corporate USA	2	4
Discovered	192.0.2.128 United States	<span style="color: yellow;">●</span> Moderate	Sep 14, 2022	GoDaddy	Seegal Corporate USA	3	1

We can then drill into a specific asset for additional detail:

**35.187.46.64**

Level: 4/4 Critical

First Seen  
Sep 14, 2022

Registrar

Organization

Services  
32

[Summary](#) [Threats \(32\)](#)

**Top 10 Threats**

4/4 **Vulnerability**

Potential exposition to [CVE-2020-25719](#) on product Samba (CVSS: 9) i

4/4 **Vulnerability**

Potential exposition to [CVE-2020-17049](#) on product Samba (CVSS: 9) i

4/4 **Vulnerability**

Potential exposition to [CVE-2017-7494](#) on product Samba (CVSS: 10) i

4/4 **Vulnerability**

Potential exposition to [CVE-2020-1472](#) on product Samba (CVSS: 9.3) i

**Related inputs**

203.0.113.0/24

198.51.100.0/24

192.0.2.0/24



## 8.2. Data Breach Prevention

### Detecting data leaks before they become data breaches.

The 2022 IBM Cost of a Data Breach report<sup>3</sup> says that the cost of a data breach went up 4.3% in 2022 to USD 9.44 million. On average, it took 207 days to identify a breach and another 70 days to contain it. Clearly, time to awareness is critical.

CybelAngel scans all our sources every 24 hours—that's one day to detect a data *leak*...so it doesn't get the chance to become a data breach. CybelAngel not only has the fastest time to detect but is also the only solution able to match to keywords inside of datasets, making it the most comprehensive and deep scanner available.

### 8.2.1. Healthcare Exposure

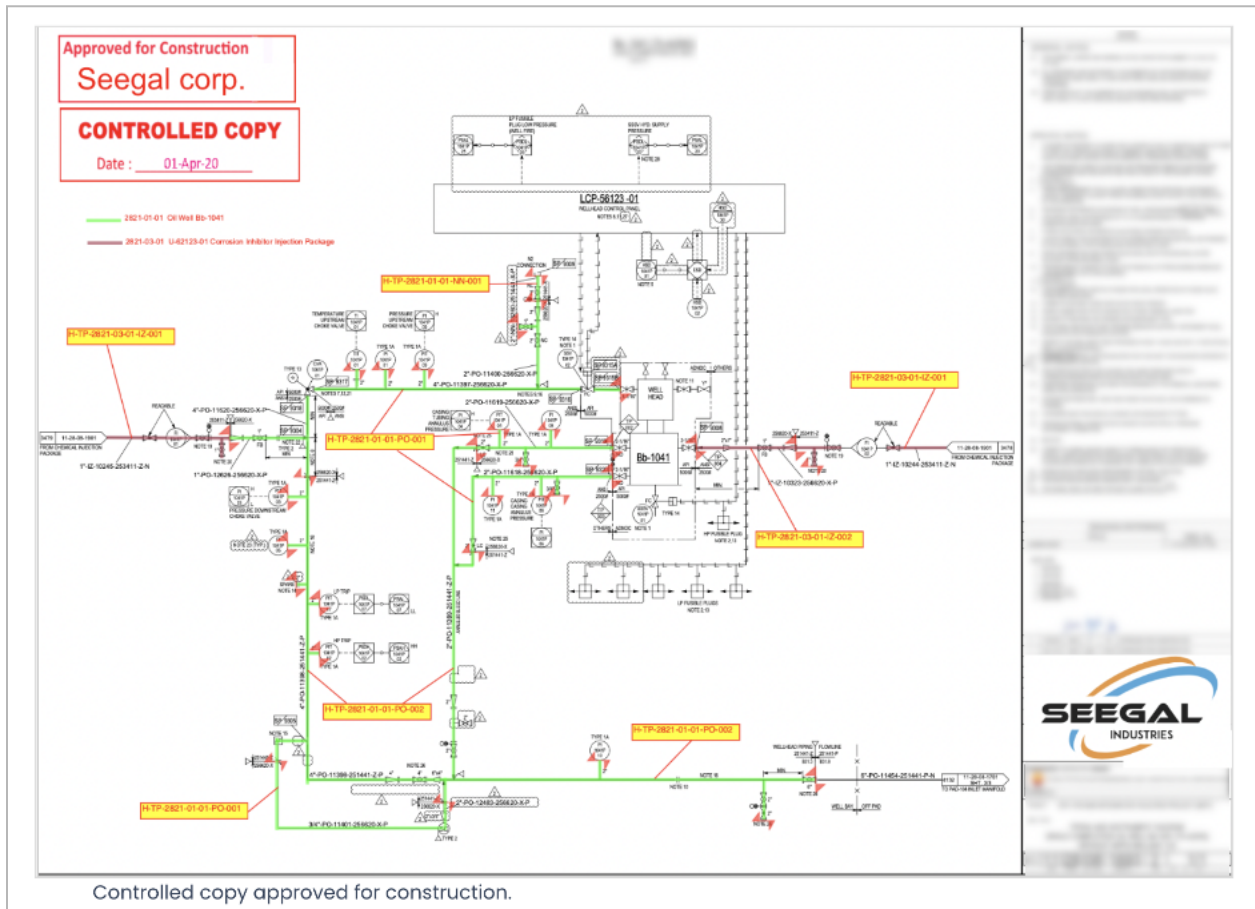
In 2022, CybelAngel alerted a customer in the healthcare services industry to hundreds of patient PHI records being exposed along with details and doctors' reports of the patients' illnesses and diagnoses. The database was found unsecured and belonging to a third-party company that sits between insurance companies and the healthcare systems handling billing and payment.

### 8.2.2. Oil & Gas Exposure

A scan that covered a three-month period for an oil & gas company found more than 170,000 documents on an open FTP server leaking data. The exposure was from a "trusted" third party contracted to undergo the expansion of processing facilities in several Middle Eastern countries. Not only were the construction plans for several facilities exposed but the server included the mechanical instruments, technical drawings and hundreds of signed documents surrounding these projects.

---

<sup>3</sup> [https://www.ibm.com/data\\_breach/codb](https://www.ibm.com/data_breach/codb); report investigates general trends and costs averages and explores ways to mitigate risk



### 8.2.3. Developer Exposure

The following screenshot shows a Github example of exposed API links from a developer. Access information found within the repository included multiple sets of credentials linked to MongoDB, Google Cloud Storage, BigQuery and test and production environments of the developer’s employer.

### Technical details

<b>Main keywords</b>	SEEGAL, seegal.com, seegalindustries.com, test.seegal.com
<b>Category</b>	Code sharing platform
<b>URL</b>	<a href="https://github.com/LuFish3/GER_Engin_useful">https://github.com/LuFish3/GER_Engin_useful</a>
<b>Status</b>	Online (Last check: May 6, 2022)

### Risk overview

Network penetration

Data theft or sabotage

Further data leak

### Detected data sample

Test  
<https://test.seegal.com>  
 Fischerl  
 pw: AZvhDo43d\$5

Production  
<https://prod.seegalindustries.com>  
 Fischerl  
 pw: 56FgTiM^0a

Mongo  
 Login: Fischlu  
 pw: vBdR40)?gT9

GCP Cloud:  
 user: lfischer

## 8.3. Account Takeover Prevention

**Capturing exposed credentials before they are compromised.**

Exposed credentials are the keys that open the doors to your infrastructure. They can be used, reused and monetized over and over again because:

1. Humans reuse the same credentials over and over again.
2. Humans use a variation of the same password over and over again.
3. Credential stuffing starts with old credentials.

Another part of the ATP services is CybelAngel's ability to intercept and alert clients about **infostealers**. An infostealer (information stealer or simply stealer) is a type of malware, usually a Trojan. Its purpose is to collect information on the infected computer. Such information can be but is not limited to:

- Passwords saved in all browsers
- Cookies and history
- Credit card information
- Global information about the computer (OS, hardware, installed software...)
- Software credentials (Telegram, Discord, Steam...)

The information collected by the infostealer is then packaged into an archive, which itself is called a **log**.

With a log—a copy of a user's most precious information—a malicious actor can easily take over full control of the victim's online identity. The passwords can indeed give access from dozens to hundreds of the victim's accounts on any platform: email, gaming, online shopping, social network, entertainment, corporate, etc. In addition, the cookie values can be directly injected in a browser to connect on behalf of the victim, without even entering a password.

#### Detected Data Sample

```
URL: https://seegal.my.salesforce.com/  
Login: martin.fresh@seegal.com  
Password: FreshPrince321  
IP: x.34.56.78
```

```
URL: https://declarants.e-attestations.com/EAttestationsFO/fo/E-Attestations.html  
Login: kathleen.obrian@seegal.com (Sales Director - Ireland)  
Password: MCJeanGabin  
IP: 24.83.x.x
```

#### *Sample of infostealer data detected*

Knowing what credentials are exposed, where and how often is important. As seen from the example below, tracking “when, where and how” can help assess gaps in security, lax employees and other avenues of attack that you may not know about.

Compromised (178)		Addressed (8)		Export all	
<input type="checkbox"/>	Email	Password	Reported in	Last detected on	
<input type="checkbox"/>	<a href="mailto:joseph.sanchez@seegal.io">joseph.sanchez@seegal.io</a>	+QsMHKzj3Ayr?...	2 incidents	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:kathleen.king@seegal.io">kathleen.king@seegal.io</a>	12345678	2 incidents	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:rebecca.campbell@seegal.io">rebecca.campbell@seegal.io</a>	strongpwlol	1 incident	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:rebecca.clark@seegal.io">rebecca.clark@seegal.io</a>	ren?44	1 incident	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:rebecca.lewis@seegal.io">rebecca.lewis@seegal.io</a>	password99	2 incidents	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:rebecca.young@seegal.io">rebecca.young@seegal.io</a>	hkdNPBULg@5...	2 incidents	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:sharon.king@seegal.io">sharon.king@seegal.io</a>	Italy0!	1 incident	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:thomas.robinson@seegal.io">thomas.robinson@seegal.io</a>	s!8(xz+SuJ2QrE	2 incidents	Jan 21, 2021	⋮
<input type="checkbox"/>	<a href="mailto:amanda.harris@seegal.io">amanda.harris@seegal.io</a>	!vgZEpCYPTsM...	1 incident	Jan 20, 2021	⋮

List of compromised credentials, passwords and how many incidents

Open (2)		In Progress (0)		Resolved (0)		Discarded (0)		All (2)	
<input type="checkbox"/>	Category	Source	Severity	Exposed credentials	Date	ID			
<input type="checkbox"/>	Database	Exposed Database	2/4 Moderate	16 emails	Jan 29, 2021	LDV7N5			
<input type="checkbox"/>	Forum	Dark Web Board	3/4 Major	16 emails	Jan 20, 2021	NZIKQG			

Ability to drill down on the when and where

**Credentials**  
3/4 Major  
Incident report - NZ1KQG  
2021/01/20

**Executive summary**

Detection Date	2021-01-20 08:42 UTC
Potential origin	Malicious actor - Dax3
Volume of detected data	16 Email address(es), 16 Password(s)

**Abstract**  
Our service detected a hacked database that was publicly disclosed recently.

**Technical details**

Main keywords	seegal.io
Category	Forum
Source	Dark Web Board
Status	Online (Last check: 20/01/2021)

**Risk overview**

Spear-phishing   Network penetration   Social engineering

**Detected data sample**

```
rebecca.young@seegal.io:hdNPBLUg@5pWQ]
amanda.harris@seegal.io:3gZ2pCYHrCaMM
joseph.sanche@seegal.io:Qok8H82J3gr78j
shirley.sgh@seegal.io:KxunfU@H9Hv4S1
kimberly.rivera@seegal.io:sunshine3
melissa.clark@seegal.io:R6xLU3rBQ6G7z
joseph.wright@seegal.io:hpDz151w648
shirley.sanche@seegal.io:CnuLAH5v7MjRE9
dorothy.lewis@seegal.io:4D52EaQb1CMq0T
stevan.young@seegal.io:Crack892
daniel.fores@seegal.io:7H8u4R0ZqfE3
anthony.adams@seegal.io:78K0aTYUJFC8t
kathleen.king@seegal.io:12345678
```

Persons named in this alert are believed by the Supplier to be the most likely source of the relevant data leak. The personal information provided represents the Supplier's opinion that the personal named may be worth investigating as a source of leaked information. Consequently, the Supplier shall have no liability whatsoever for the use of the alert by Customer.

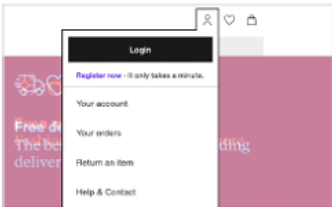
1/2 CONFIDENTIAL - STRICTLY AND EXCLUSIVELY FOR INTERNAL USE

emily.afen@seegal.io:Q3hyye4t1HkP  
sharon.king@seegal.io:8W9@R2D5cKd  
thomas.robinson@seegal.io:8ozr5u3QrE

**Analysis**

On January 20th 2021, the threat actor Dax3 shared 716,888 email addresses from breach retail marketplace. Most of the passwords appear to be hashed, but around 15% of them are displayed in plain text.

**16 Seegal Industries' corporate accounts were impacted.**  
The credentials of Steven Young, the actual CFO of your company, have been compromised.



**Risk assessment**

**Spear-phishing**  
The information referenced in this report could allow hackers to craft spear-phishing emails specifically targeting people related to your organization. These emails will appear particularly authentic, increasing the risk that their malicious content (corrupted file or URL) is opened. Such a scheme could be used to penetrate your network.

**Network penetration**  
The information referenced in this report exposes elements on your IT infrastructure that could be used by malevolent actors to gain access to your internal networks.

**Social engineering**  
The information referenced in this report could be used by a hacker to craft a social engineering attack. This is a manipulation technique whereby an attacker impersonates a third party in order to gain access to confidential information, or to trick them into installing malware.

**Suggestions**

- Invite the concerned employees to change their passwords.
- Raise your employees' awareness to social engineering, phishing and any contact attempt by email that they may receive.
- Warn the employees against any suspicious contact attempt by email they may receive in the upcoming days.

Persons named in this alert are believed by the Supplier to be the most likely source of the relevant data leak. The personal information provided represents the Supplier's opinion that the personal named may be worth investigating as a source of leaked information. Consequently, the Supplier shall have no liability whatsoever for the use of the alert by Customer.

2/2 CONFIDENTIAL - STRICTLY AND EXCLUSIVELY FOR INTERNAL USE

Final report on the incident with intelligence

## 8.4. Dark Web Monitoring

### Shining light in the dark.

As noted in section [5.2.7](#), CybelAngel monitors the dark web for those keys or mentions that allow for access into a company's infrastructure, companies receiving attention on criminal and hacking forums and chatter on channels like Telegram, IRC and Discord. We filter through over 330K deep and dark web posts on a daily basis to look for information and intelligence for our clients.

The example shown below is from a real situation where a Pastebin publication was directed to a server hosted out of Cambodia managed by our client that was distributing









A typical finding from forums/markets on the dark web like Russian and Genesis Markets are the selling of credentials and access. Typically, these can go from \$1.00 up to \$150.00, depending on the uniqueness, timing, age, session information and other data available.

Mask	Country	State / City	Details	Info	Vendor	Blacklist	Price	Action
18.135**** ISP: Amazon Technologies Inc.		England London	OS: Windows 7 Proc: intel Xeon CPU E5-2676 v3 @ 2.40GHz 2.40GHz RAM: 1 GB   sp: -/- Mbit/s	Admin: Yes Paypal: No NAT: -	0###\$ag [platinum]	BL	\$ 4.00	Buy
107.172**** ISP: CoxCrossing		New York Buffalo	OS: Win2016 Proc: intel Xeon CPU E5-2660 0 @ 2.20GHz 2.20GHz RAM: 4 GB   sp: -/- Mbit/s	Admin: Yes Paypal: No NAT: -	0###\$ag [platinum]	BL	\$ 9.00	Buy
24.42**** ISP: Liberty Callcenter of Puerto Rico		Florida Miami	OS: Windows 10 Proc: intel Core i7-10700F 2.90GHz RAM: 16 GB   sp: 109.74 / 108.22 Mbit/s	Admin: Yes Paypal: No NAT: Yes	rd###\$ad [platinum]	BL	\$ 25.00	Buy
192.143**** ISP: simobit.co.za		Eastern Cape Port Elizabeth	OS: Win2008/7 Proc: intel Core i7 7840K RAM: 6 GB   sp: 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ds###\$ok [platinum]	BL	\$ 6.00	Buy
102.182**** ISP: Mweb (Pty) Ltd		Gauteng Sandton	OS: Win2008/7 Proc: intel Core i7 7840K RAM: 6 GB   sp: 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ds###\$ok [platinum]	BL	\$ 6.00	Buy
91.134**** ISP: OVH SAS		Ile-de-France Paris	OS: Win2008/7 Proc: intel Core i7 7840K RAM: 6 GB   sp: 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ds###\$ok [platinum]	BL	\$ 6.00	Buy
196.64**** ISP: Office National des Postes et Telecommunications ONPT Maroc, Telecoms HAM		Casablanca-Settat Casablanca	OS: Win2008/7 Proc: intel Core i7 7840K RAM: 6 GB   sp: 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ds###\$ok [platinum]	BL	\$ 6.00	Buy
198.201**** ISP: Access Online Center		Saxony Falkenstein	OS: Win2008/7 Proc: intel Core i7 7840K RAM: 6 GB   sp: 16.71 / 73.13 Mbit/s	Admin: No Paypal: No NAT: No	ds###\$ok [platinum]	BL	\$ 6.00	Buy
198.12**** ISP: CoxCrossing		Illinois Chicago	OS: Win2016 Proc: intel Xeon CPU E5-2660 0 @ 2.20GHz 2.20GHz RAM: 4 GB   sp: -/- Mbit/s	Admin: Yes Paypal: No NAT: -	0###\$ag [platinum]	BL	\$ 9.00	Buy
198.12**** ISP: CoxCrossing		Texas Dallas	OS: Win2016 Proc: intel Xeon CPU E5-2660 0 @ 2.20GHz 2.20GHz RAM: 4 GB   sp: -/- Mbit/s	Admin: Yes Paypal: No NAT: -	0###\$ag [platinum]	BL	\$ 9.00	Buy

*Data for sale on Russian Market*

RESOURCE NAME / URL	SOURCE	DATASETS	BROWSER	KNOWN	GRABBED / UPDATED
 Netflix https://www.netflix.com "Login": Available After Purchase "Password": Available After Purchase	Any	Any	Any	Any	2021-07-19 17:54:04 2021-07-20 13:59:54
https://my.viagogo.es "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	no	2021-07-19 17:54:04 2021-07-20 13:59:54
https://voyeurhouse.com "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	no	2021-07-19 17:54:04 2021-07-20 13:59:54
https://www.youporn.com "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	no	2021-07-19 17:54:04 2021-07-20 13:59:54
 Google https://accounts.google.com "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	yes	2021-07-19 17:54:04 2021-07-20 13:59:54
 Google https://accounts.google.com "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	yes	2021-07-19 17:54:04 2021-07-20 13:59:54
 Instagram https://www.instagram.com "Login": Available After Purchase "Password": Available After Purchase	Saved Logins	LoginData	firefox	yes	2021-07-19 17:54:04 2021-07-20 13:59:54

*Data for sale on Genesis Market*

## 8.5. Domain Protection

Heavy on cybersquatters, light on your resources.

CybelAngel combines techniques of active and passive searching to protect brands from impersonation on all top-level domains and subdomains. We watch not only the active domains but also those that are dormant, waiting to be used. This allows our clients to focus on the 2% of bad domains and cybersquatting attempts that are actual threats rather than all the noise.

With the increased e-commerce presence with industries like retail, entertainment, and media & internet, it is normal to see a higher-than-average risk involving malicious websites. However, the increase in phishing attacks derived from these sites is increasing every year.

Domain name	Status	Detection date	IP addresses	MX server	Registrant name
segal.com.sa	Monitored	Dec 1, 2022	No ip	5 ALTI.ASPMX.LGO...	إسماعيل والاستشارات القانونية...
blog.deegal.ml	Monitored	Nov 10, 2022	195.20.50.144	No MX	No name
nathan-segal.com	Monitored	Aug 26, 2022	172.67.158.180; 104.2...	0 mail.nathan-seg...	Redacted for Priva...
dan.seegallery.art	Monitored	Mar 16, 2022	44.230.85.241; 52.3...	No MX	No name
seegul.io	Monitored	Feb 1, 2022	No ip	No MX	No name
mail.senegal-ship.com	Monitored	Aug 25, 2021	193.203.239.34	No MX	No name
senegal-taxi.com	Monitored	Jul 26, 2021	No ip	No MX	No name
segal.partners	Monitored	Apr 20, 2021	No ip	No MX	No name
segal.dev	Monitored	Feb 22, 2021	No ip	No MX	REDACTED FOR PRI...

*CybelAngel Watchlist tracking lookalike domains that are parked for potential phishing and other attacks*

## About the Author



Todd Carroll joined CybelAngel in 2019 as the CISO & SVP Global Cyber Operations, bringing with him over 20 years of experience in the U.S. Federal Bureau of Investigation's cyber, counterintelligence and counterterrorism branches. Carroll is instrumental in evangelizing CybelAngel's data leak detection technology throughout North America and is responsible for managing the U.S. cyber operations unit. Prior to joining CybelAngel, Carroll served as the Deputy Special Agent in Charge of the FBI's fourth largest field office, in Chicago, where he oversaw investigations related to cyber and physical security, threat intelligence, risk analysis, compliance, insider threat identification and mitigation strategy.