Telefónica Tech

Airlines Companies Security Analysis using OSINT

February 14, 2022

Index

1. Executive Summary 3
2. Methodology 4

2. 1. Shodan and Censys 5
2. 2. Spyse 6
2. 3. Intelligence X 7
2. 4. DuckDuckGo & TOR Browser 8
2. 5. Kali Linux Tools 8

3. Regions of the world 10

3. 1. America 10
3. 2. Europe 12
3. 3. APAC 14
3. 4. Africa 15
3. 5. Middle East 17

4. Conclusions and Recommendations 19

4. 1. CVEs and risks comparison 19
4. 2. Main domains hosted comparison 19
4. 3. Data leaks found 20
4. 4. SSL/TLS servers comparison 20
4. 5. Darkweb findings 21

5. Summary 23
6. Telefónica Tech's DRP service 24
7. Collaborators 27
8. Appendix 28

Telefónica Tech

1. Executive Summary

Recently, the number of news reporting **cybersecurity incidents** involving airlines companies worldwide has increased; websites are going down by DDoS attacks, potential data losses, and stolen passengers' details. These news claim that **cybercriminals are targeting airlines** more and more often.

On November the 22nd, 2021, the news[1] published that the Iranian airline **Mahan** had been a victim of an attack provoking its website to go offline and in the alleged theft of their private data. Earlier this year, on May the 3rd, another news[2] about airlines' cybersecurity being compromised was published: an attack had taken place in which hundreds of thousands of **Star Alliance**[3] passengers' details were stolen.

Cyberattacks may cost airlines companies a **large sum of money**, not only because of the interruption of their services, but also for **non-compliance fines** related to the different **data protection laws**. One example of this situation can be observed in a news[4] published in 2018, when **British Airlines** had to face a fine of **$229 million** after suffering a cyberattack.

This document contains the results of an investigation regarding these matters. The main objective was to determine the extent to which airlines are somehow **unprotected** and how much data could be gathered just by performing a **general recognition** and **collecting** only **public information** without intrusion tests being performed.

This report is also based on a **private report** back in 2017, for a world-known airline company, containing the results regarding the **fraudulent sale/purchase of flight and hotel bookings** from the point of view of criminal gangs, cybercriminals, and other actors in the illegal markets of the Deep web. This investigation was mainly focused on the flight illegal bookings methods, although the same techniques, types of buyers, and sellers were applicable to hotel bookings and car rentals (often there are packages "Flight + Hotel + Car", offered by legal travel agencies).

After conducting the study, it could be said that airlines companies in all regions (which will be clarified later on) seem to have potential **security issues** and that anyone could gather valuable data about them in a few clicks. This fact manifests companies' urge to implement and incorporate **Digital Risk Protection** measures that help monitor threats.

Telefónica Tech's DRP service **prevents, identifies**, and **mitigates** a wide variety of threats due to its broad range of tools and qualified analysts that help to protect companies' **valuable data and reputation.** This service takes care of companies' risks in big four categories and its operation will be detailed afterwards.

- **Brand and reputation:** unauthorized use of brand, suspicious domains, offensive content, counterfeit, and digital identity monitoring.
- **Business disruption:** data exposure, hacktivism, activism, breach of security controls, CVEs and security bulletins and credential theft.
- **Online fraud:** phishing and pharming, malware, carding and suspicious mobile apps.
- **Mobile Channel Risks:** proactive discovery, vulnerability assessment and suspicious mobile apps.

1 Hackers hit Iran's Mahan airline, claim confidential data theft (bleepingcomputer.com)
2 Airline data hack: hundreds of thousands of Star Alliance passengers' details stolen | Air transport | The Guardian
3 Home - Star Alliance
4 British Airways Hit With Record Fine Following 2018 Cyberattack (forbes.com)

2. Methodology

This research aims to determine what kind of information is **publicly available** on the Internet and how much can be gathered without advancing further in the cybersecurity kill chain. To achieve this goal, all kinds of data were collected from the **ten most important** airlines in five different regions of the world and presented the results by comparing those territories.

There are a lot of powerful OSINT tools, but since the research was not targeting any specific airline company and the number of targets was high, the investigation considered mostly the **free public search engines** and did not consider many of those tools that actively collect information. All data has been obtained just by performing a first **general recognition** using **off-the-shelf** tools and methods to analyze how much information may be obtained without extensive knowledge in the field.

If the goal was to perform a more thorough study and address a specific target, a wider range of tools allowing to collect more types of data could have been used. While using a search engine, the user must bear in mind that **the scan might not be carried out in real-time** and that the data provided may have changed since the day the scan was performed.

2.1. Shodan and Censys

Shodan[1] and **Censys**[2] are two IoT search engines that scan Internet-facing systems finding open ports and services that listen on them. They can be used to identify **old and vulnerable versions** of some operating systems and protocols as well as some devices with poor security configurations that could be accessed remotely.

This research shows which ports have the main domains of the airlines' websites open. Censys allows to search in three modes: IPv4 Hosts, Websites and Certificates. As web-security-based research, the information was searched using the **Websites** mode, and the obtained data was complemented with the IPv4 Hosts one.

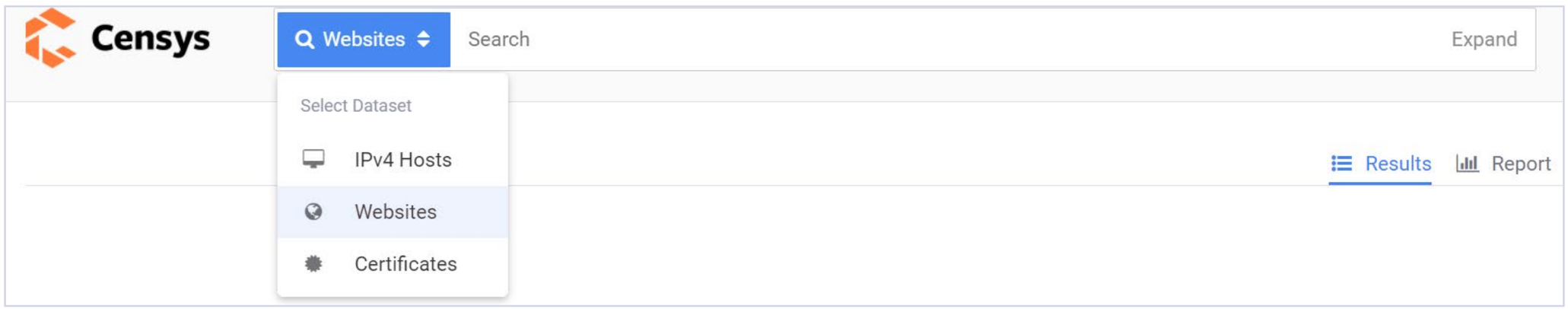


Figure 1. Censys modes

Search filters can be used to help find more useful information. Searching with the Websites mode and filtering by domain, IPv4 addresses on which the web's main domains are hosted can be found, their open ports and the protocols that are being used with their supported versions.

Figure 2. Censys example

Shodan works similarly, and its main potential is the powerful search filters it has. In this case, it was enough to search for the IP addresses that host the main domains of the targeted websites. **Shodan** shows data in a similar way to **Censys**: it shows the address' open ports, protocols, and versions and also provides information like geolocation, the ISP, and the ASN.

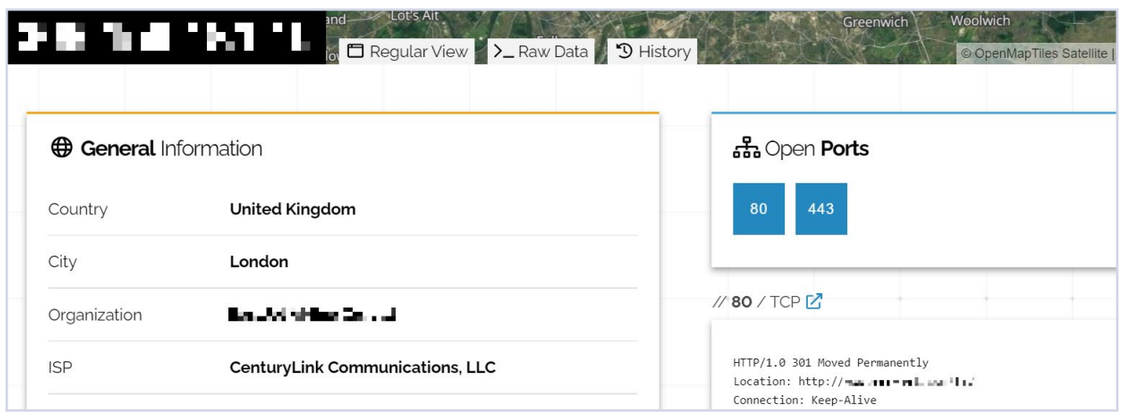


Figure 3. Shodan example

1 Shodan Search Engine
2 Home - Censys

2.2. Spyse

Spyse[3] is a cybersecurity-based search engine that offers the possibility to search data related to a domain name, an IP address, an SSL/TLS certificate, an organization, specific technology, and even particular CVEs. Spyse finds any Internet asset by digital **fingerprints** and has a large database from where it extracts the requested data during a user's search. This reduces a lot the scan time and allows you to gather some very useful information without the need to use many different services for each type of data.

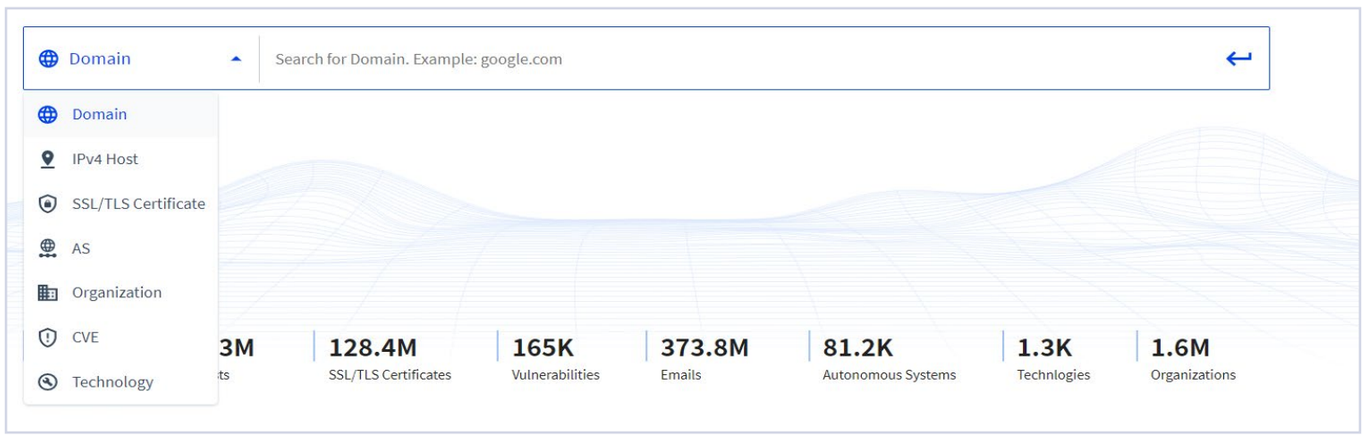


Figure 4. Spyse modes

Spyse has been one of the main sources of information during this investigation due to the large amount of details it provides. Many useful data about the airlines' domains and subdomains have been gathered, especially the number of potential CVEs that may exist.

This website **catalogs the security level** depending on the number of potential CVEs found and gives the domain a **risk score** accordingly. These scores have later been used to make one of the final comparisons between the regions. The four possible categories are *low*, *medium*, *severe* and *critical*.

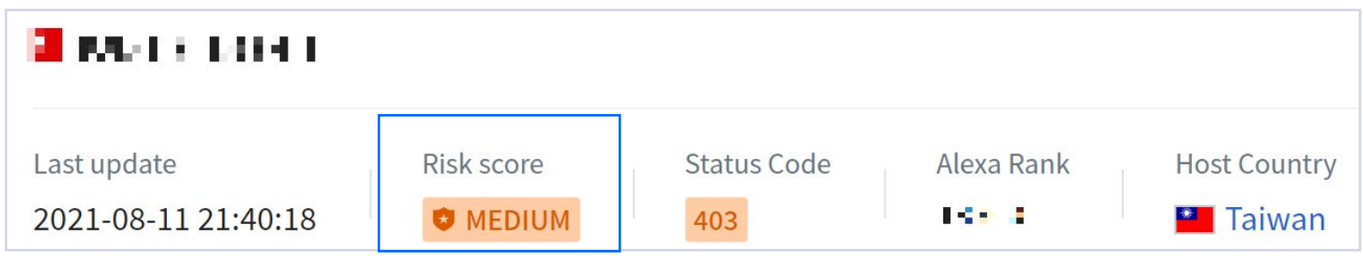


Figure 5. Spyse example

Spyse also gives some useful **snapshots** such as DNS records, the status of the SSL/TLS certificate, WHOIS data, and the organization or company to which the domain belongs. The only inconvenient is that since Spyse focuses on reducing the scanning time, these snapshots correspond to different days and **some data could be obsolete**, for example, the SSL/TLS certificate status.

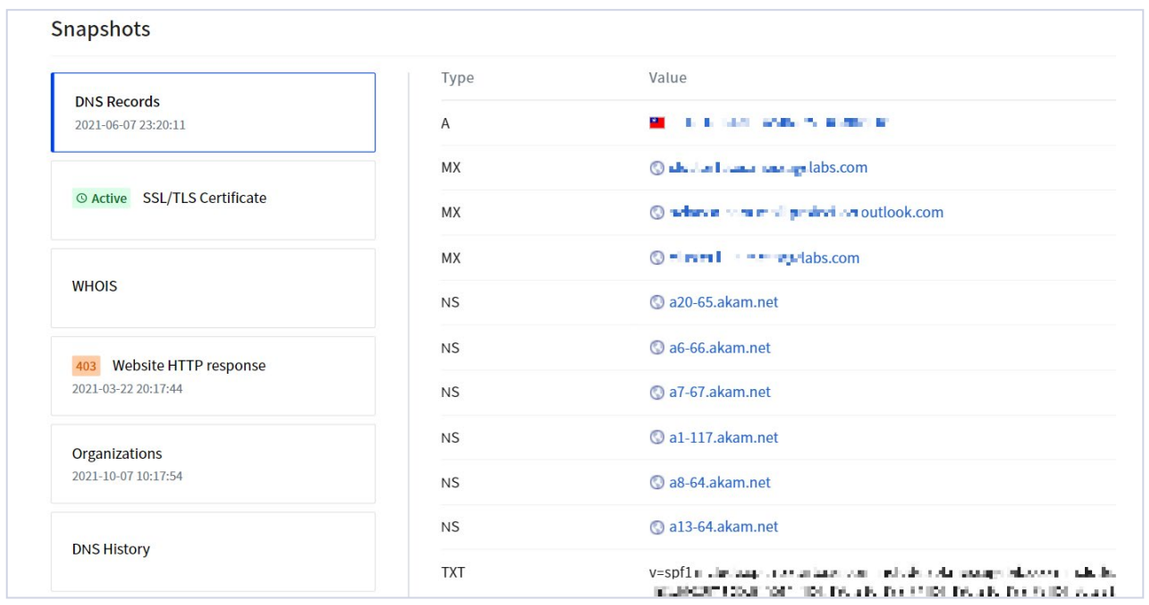


Figure 6. Spyse snapshots

3 Spyse — Internet Assets Search Engine

One of the last things that can be seen on Spyse is the specific number of potential CVEs their scan has detected and why it has given a certain security risk level.

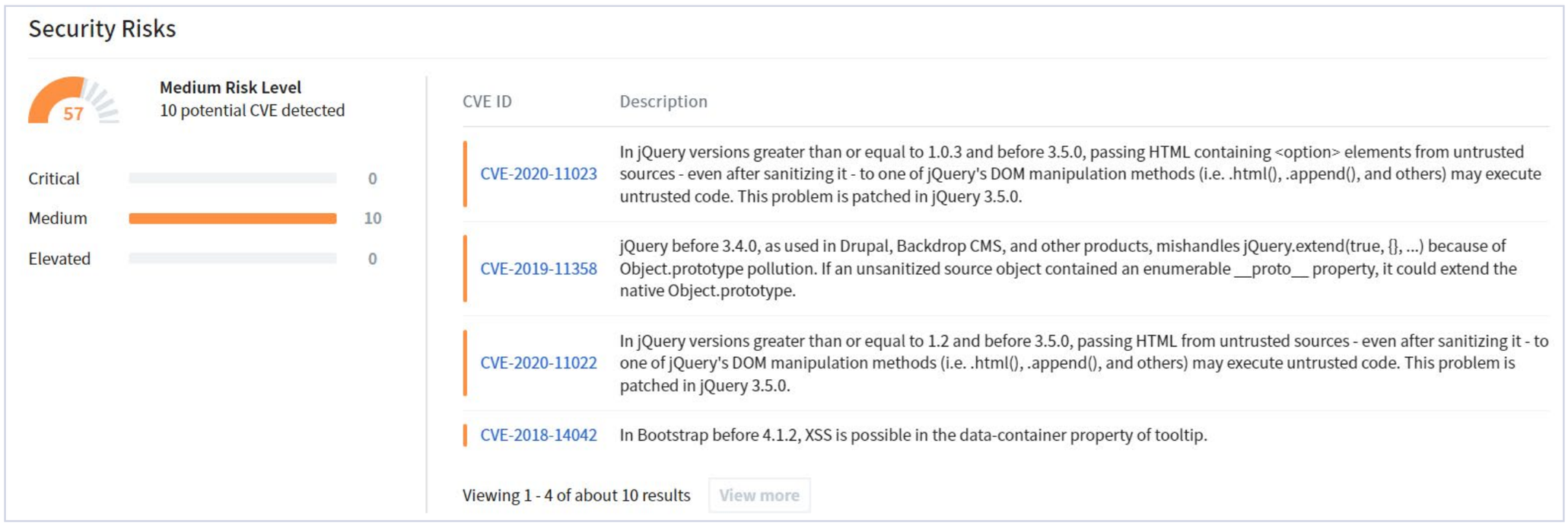


Figure 7. Spyse CVEs

2.3. Intelligence X

Intelligence X[4] is a search engine and **data archive**. It searches the public web, private data leaks, Tor and I2P given a domain, email, IP addresses and more. Intelligence X claims to make accessible the **deepest parts** of the Internet with a few clicks and it searches billions of selectors in milliseconds.

Intelligence X collects many types of data and allows the user to filter the results per **data source** and per **file type**.

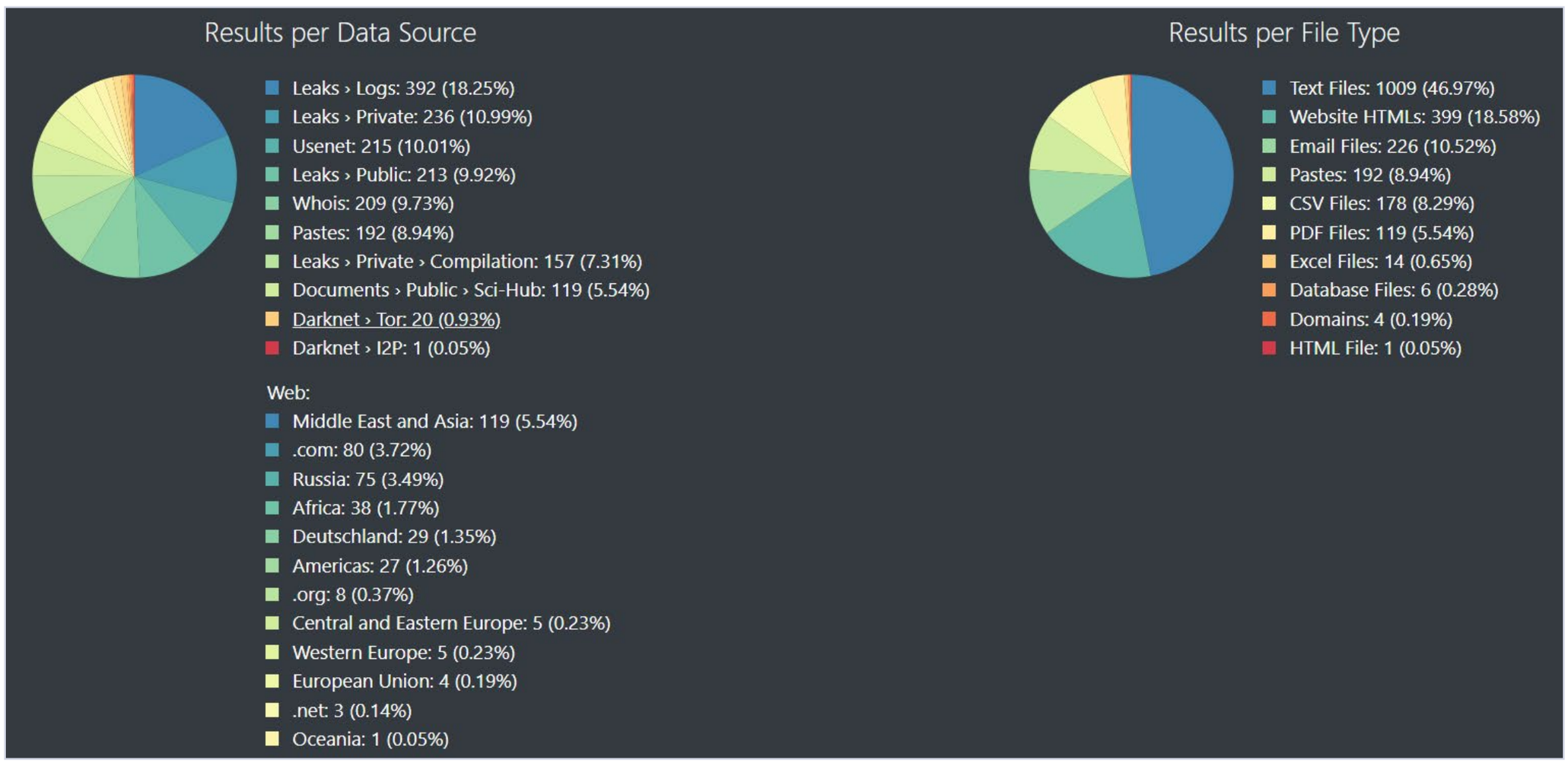


Figure 8. Intelligence X contents

[4] Intelligence X

The amount and variety of interesting data that can be found depends on how well the user searches and many **credentials**, interesting **databases** files, **excel** files, and even some **carding** examples were found.

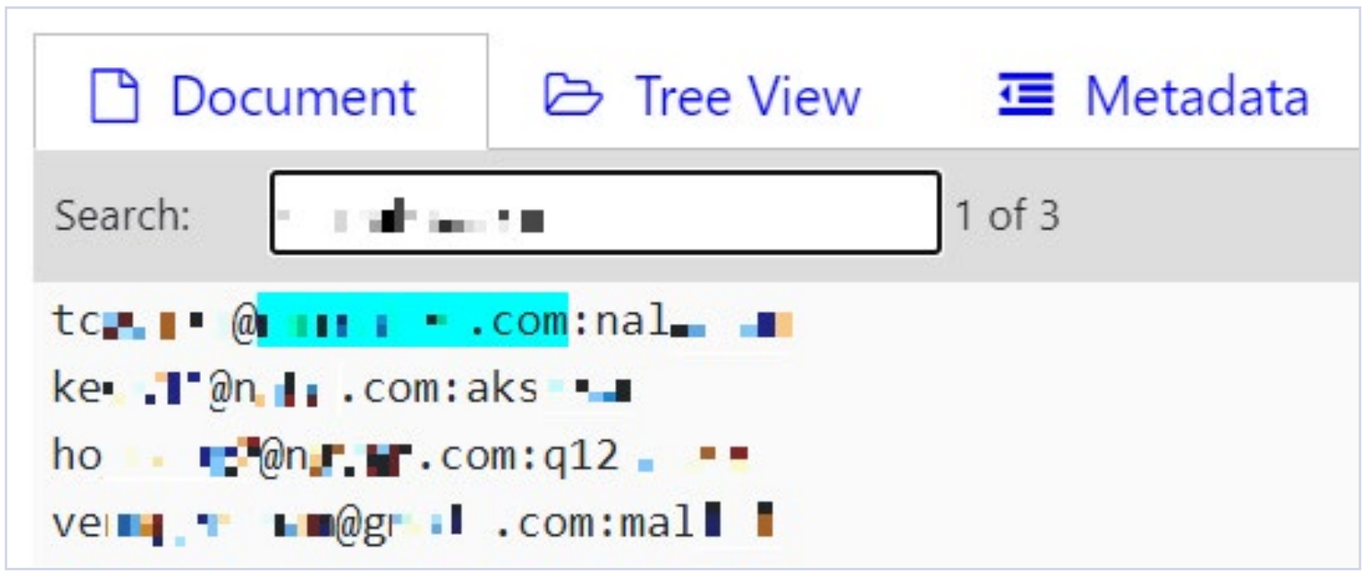


Figure 9. Intelligence X leaked credentials

2.4. DuckDuckGo & TOR Browser

DuckDuckGo[5] is a search engine like Google that delivers more relevant results while enhancing privacy by not collecting any personal data. It is the default search engine **TOR Browser**[6] uses, and it allows to search on the **Deep Web** in a more secured manner.

Deep Web was accessed to see if there were flight tickets, gift cards and other things related on sale. To do so, the most common **Dark Markets** were searched for these kinds of offers.

2.5. Kali Linux Tools

Kali Linux[7] has a large variety of **penetration testing and OSINT powerful tools**[8] that help in data gathering and reconnaissance. Although this is out of search engine group, there are some websites that collect information about the SSL/TLS servers on a specific domain in a very similar way to **SsIscan**[9] and **Sslyze**[10] tools. Both were used to test the security level of these servers, allowing to make another comparison between the regions.

Both tools work in a very similar way and show valuable data that can complement the results of each other. These two tools complemented can be a **powerful source** of information while performing data gathering.

SsIscan shows the results in a very **graphic way** that helps visualizing them better. It provides information about protocols, supported fallback, supported server cipher, TLS renegotiation and more.

5 DuckDuckGo — Simplified privacy.
6 Tor Project | Anonymity Online
7 Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution
8 Kali Tools | Kali Linux Tools
9 sslscan | Kali Linux Tools
10 sslyze | Kali Linux Tools

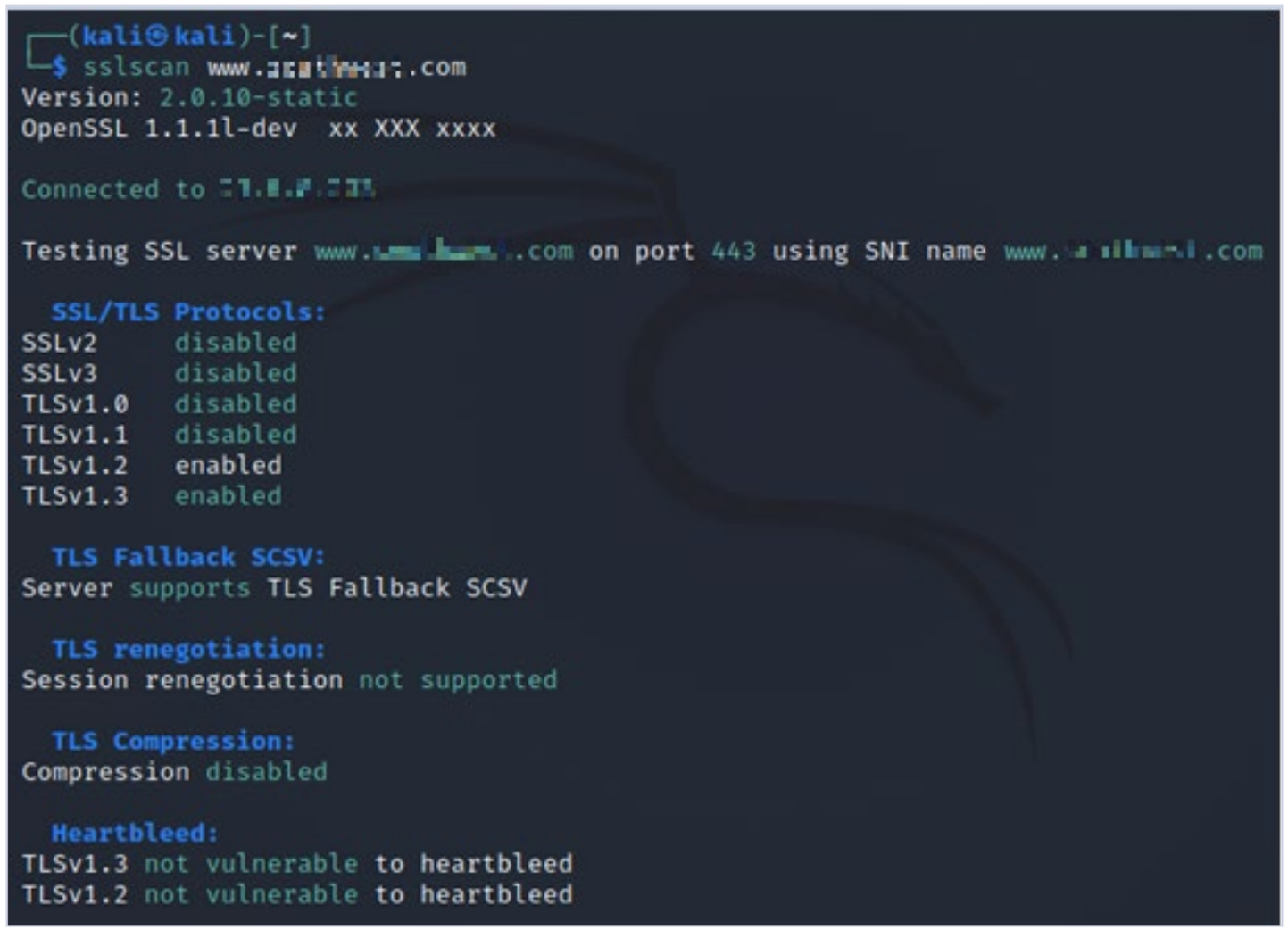


Figure 10. Sslscan example

Sslyze collects the same data, but it also supplies information about specific attacks that can be performed against the server. Here are some examples:

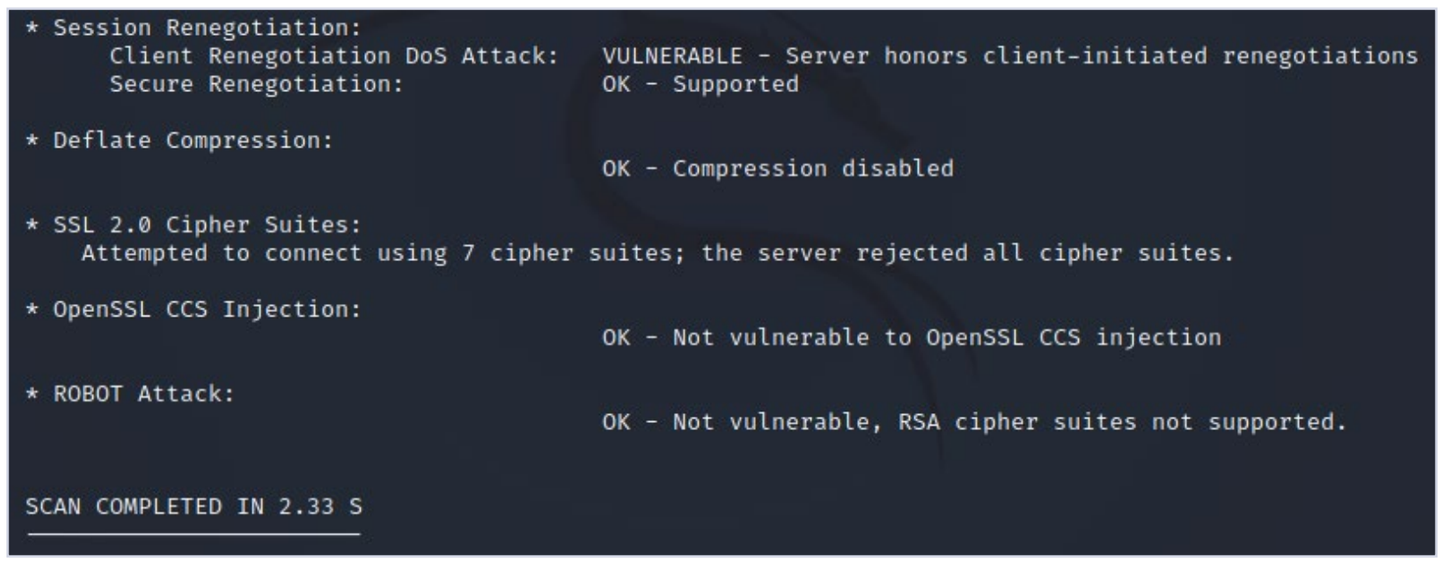


Figure 11. Sslyze example

3. Regions of the world

To carry out this study, five regions of the world were chosen and a comparison among them was performed. These five regions are: **America**, **Europe**, **APAC**, **Africa**, and **Middle East**. These regions were chosen because the number of airlines on each can be considered balanced between them, even so, the study could have been carried out considering other regions and will be qualified later in some cases. The ten airlines chosen for each area have been selected after conducting research and obtaining the ones that are apparently **most renowned**.

Since a large amount of data from the ten airlines in each region has been collected, just **two examples** of each are going to be shown. One of the examples will be from an airline that could be considered **safer** in terms of cybersecurity, and the other one from an airline that may have some **cybersecurity issues**. Even so, the totality of them is going to be used later for the comparisons.

Any names or private information about the airlines will not be provided. Any data that could identify them has been censored.

3.1. America

Since airlines have been chosen based on their popularity and the number of passengers traveling with them, most of the ten American airlines have turned out to be in **North America**. Even so, some instances from Latam have been used too.

Out of the ten airlines analyzed, the main domains of seven of them were rated as **low risk** by Spyse, nevertheless, **only two of them** had all their subdomains with the same rating, the other five had some issues and potential CVEs associated with the software of the servers where some subdomains are hosted. Some of them had **potential critical CVEs** and worked with sensitive data. The other three out of the ten airlines were rated as **medium**, **severe** and **critical** respectively. Also, five of them have their main domains hosted out of America.

The next images belong to one of the two potentially "true-low" risk American airlines rated by Spyse (the ones which have **all** their subdomains apparently secured).

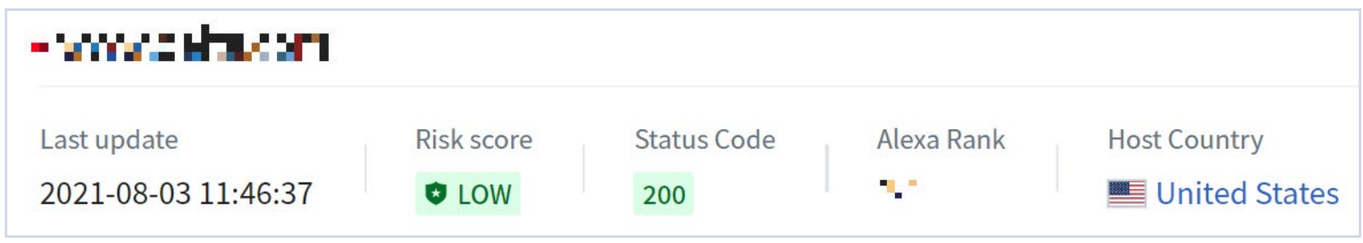


Figure 12. Low risk rated American airline

On the other hand, here is the critical rated airline and its potential CVEs, which, if they are all right, they could **pose a great risk** to the security of the web.

Figure 13. Critical risk rated American airline

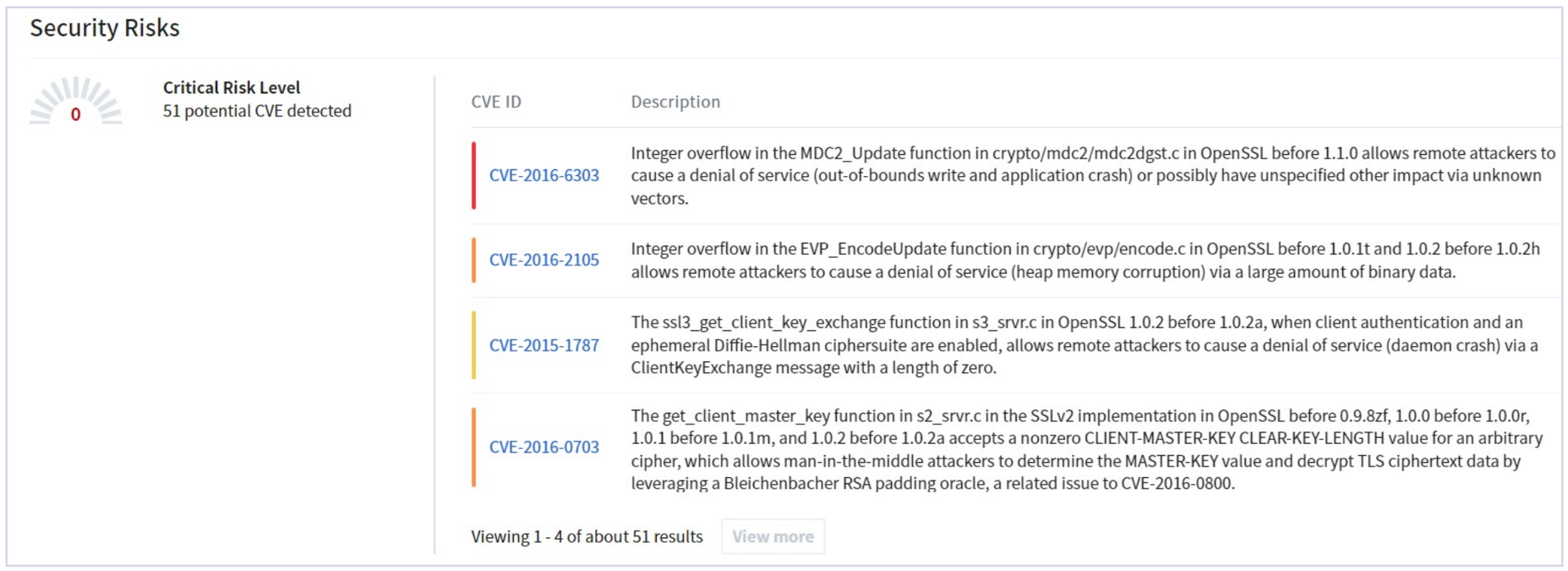


Figure 14. American airline potential CVEs

In all cases, including airlines for which no potential CVEs had been found, **leaked credentials** have been obtained using Intelligence X. Intelligence X contains files that collect many gathered credentials and, looking for the names of the airlines or the extensions of their mails, they are very easy to find.

Intelligence X also contains other kinds of sensitive data documents. Searching for an airline, a private **credit card statement** was found due to a system of points and rewards the airline offers.

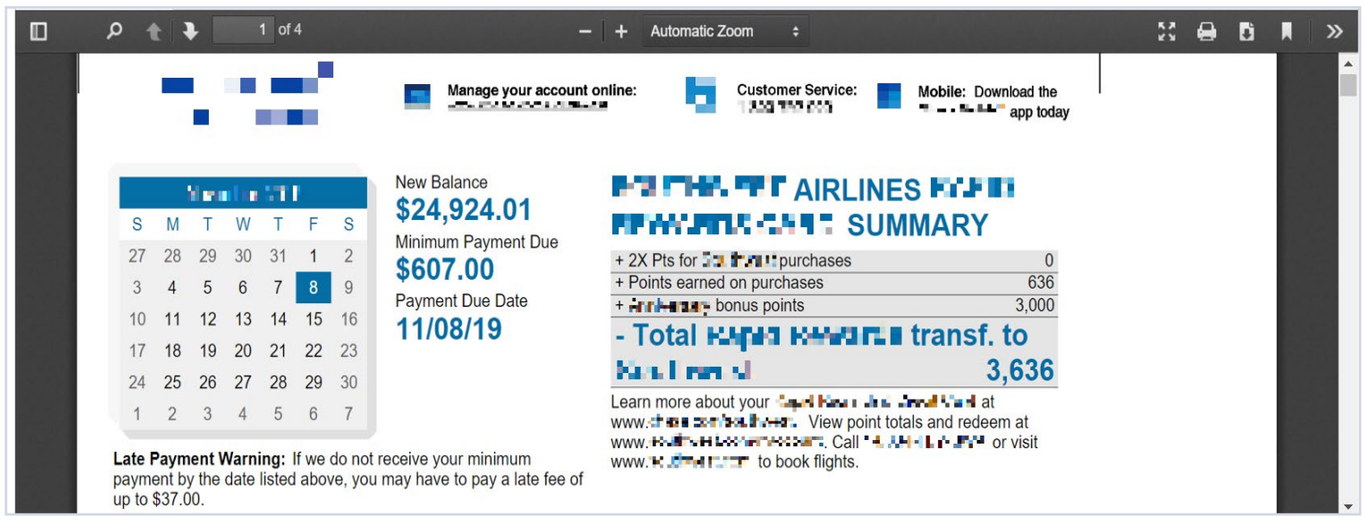


Figure 15. Found credit card statement [1/3]

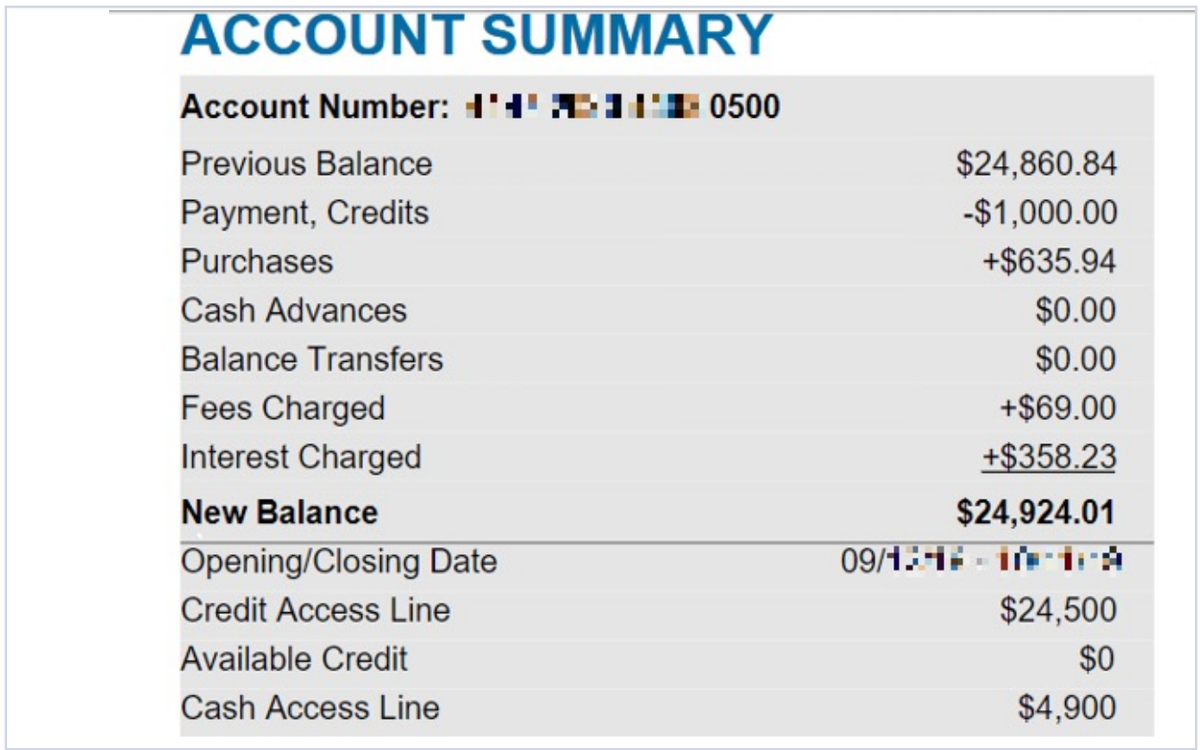


Figure 16. Found credit card statement [2/3]

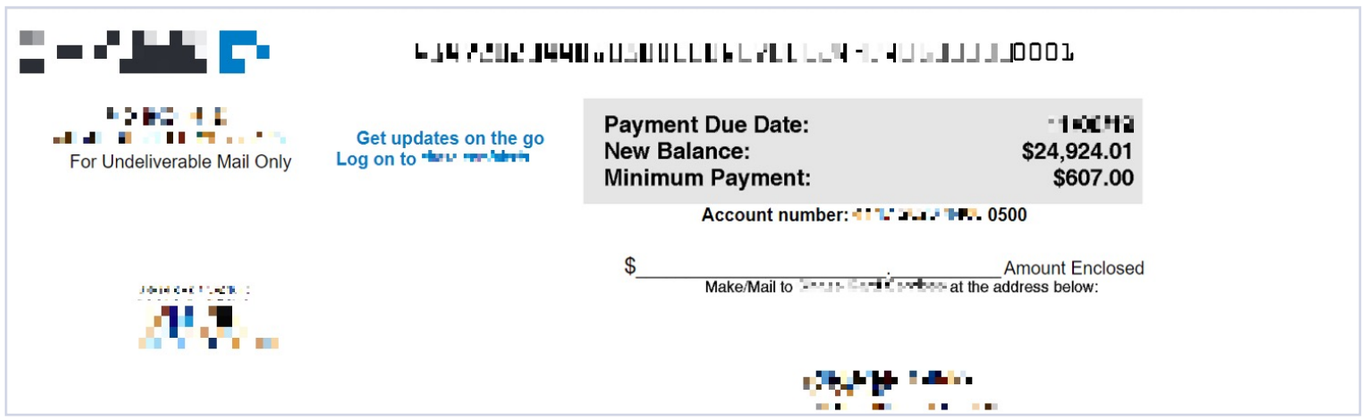


Figure 17. Found credit card statement [3/3]

During the research on the Deep Web, it was also found that in some darknet markets **flights**, **gift cards** and **airlines' accounts** were being sold. All the found offers were from various American airlines and any sale from other regions was found. A possible reason for this may be that the purchase method in America may require fewer steps than in other regions like for example Europe, where **two-factor (or even three) authentication** is required for the user to make a purchase through SMS confirmation and card of coordinates.

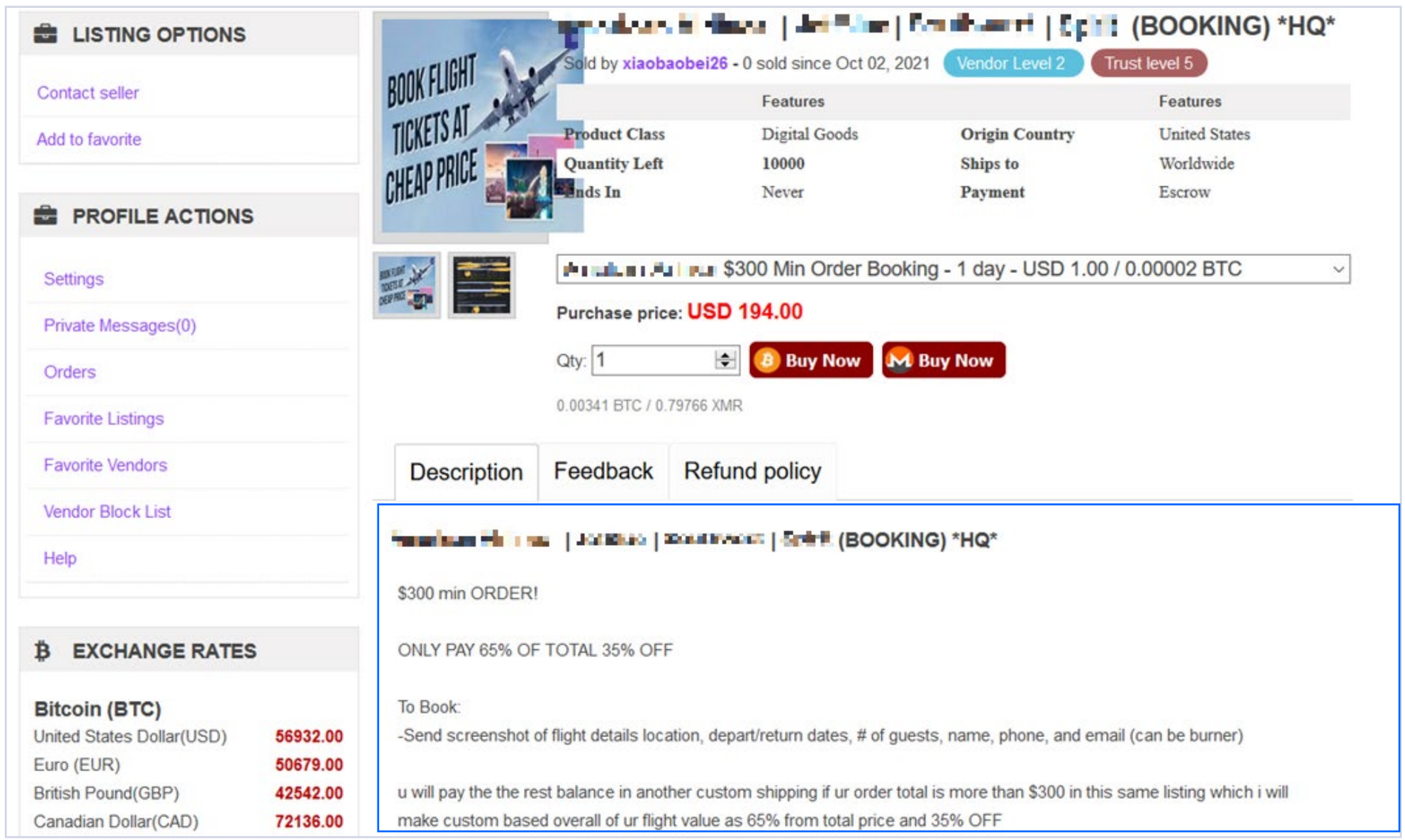


Figure 18. Offer example

Regarding the analysis of the SSL/TLS servers, only two of them could be considered somewhat worse than the others. The two of them because of supporting **deprecated versions TLSv1.0** and **TLSv1.1**.

3.2. Europe

Of the ten European airlines analyzed, **six** of them were rated as **low** by Spyse. Only one of them did not have potentially insecure subdomains. Two of the other three airlines were rated as **medium** and **severe** respectively. The remaining airline had not been analyzed by Spyse yet, and since it would require performing a vulnerability scanner against the airline in order to analyze it, **it will not be taken into account** for the comparisons.

In Europe and America, the ratio of domains hosted inside or outside the region is 50-50%. In this case, the airline that seems to not have potential CVEs on its website has its main domain hosted in **Germany**.

Here is the example of the airline rated as **SEVERE** by Spyse and four of its twenty-five potential CVEs.

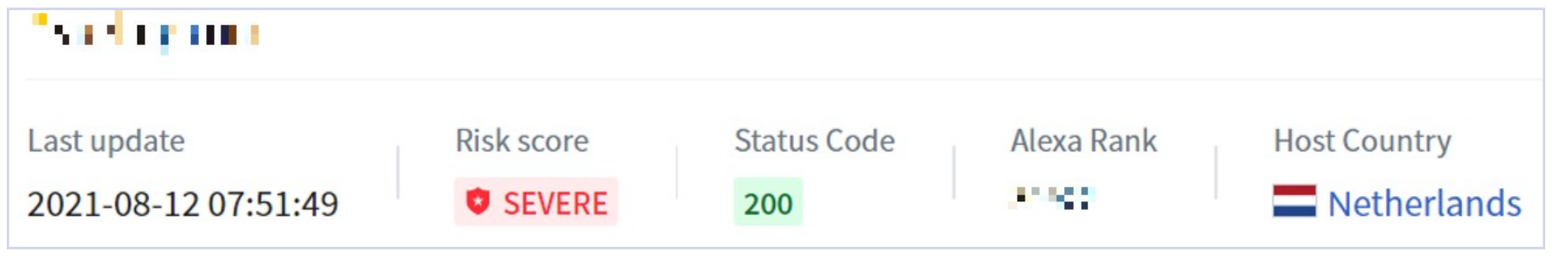


Figure 19. Severe risk rated European airline

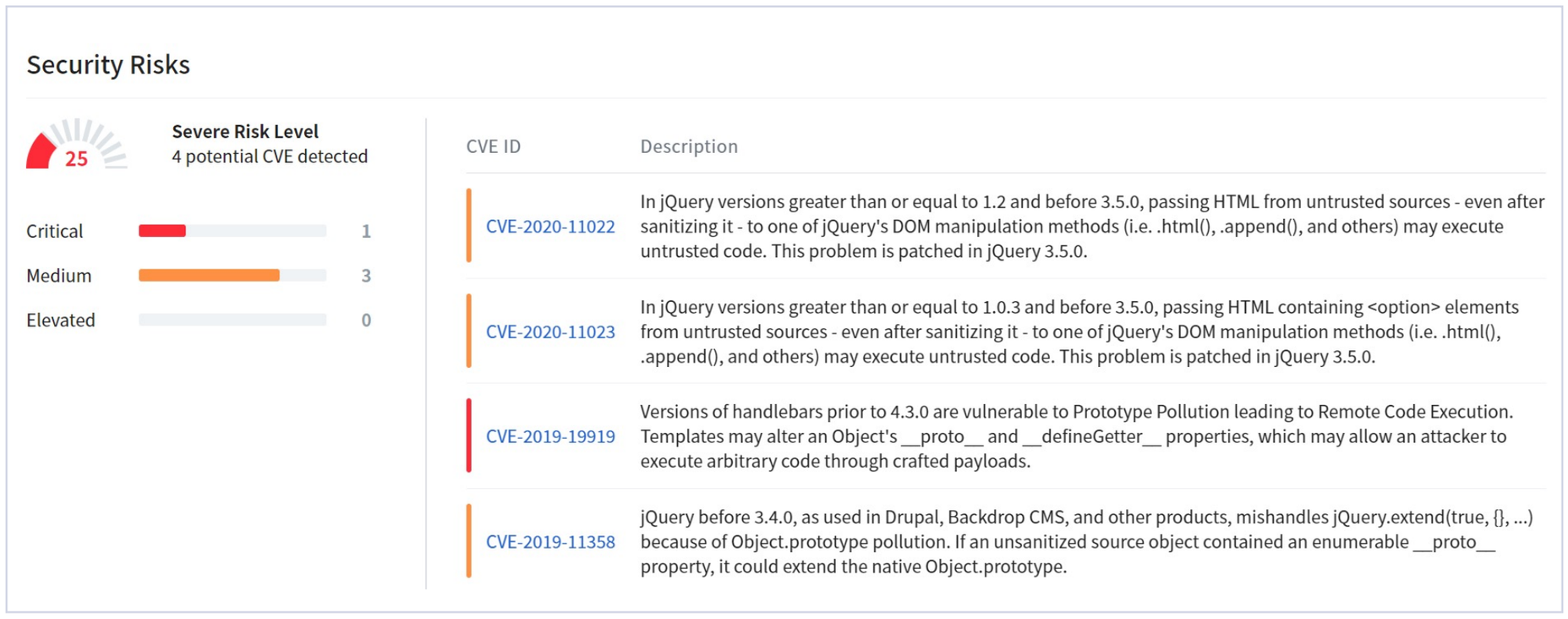


Figure 20. European airline potential CVEs

On the other hand, here is the best rated airline. Although the risk associated to all its subdomains as well as the main one was rated as **LOW**, some **logging credentials** were found with Intelligence X.

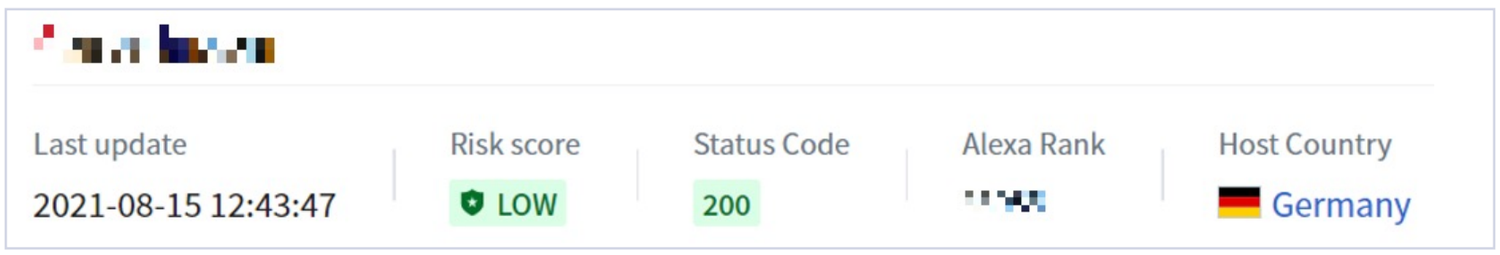


Figure 21. Low risk rated European airline

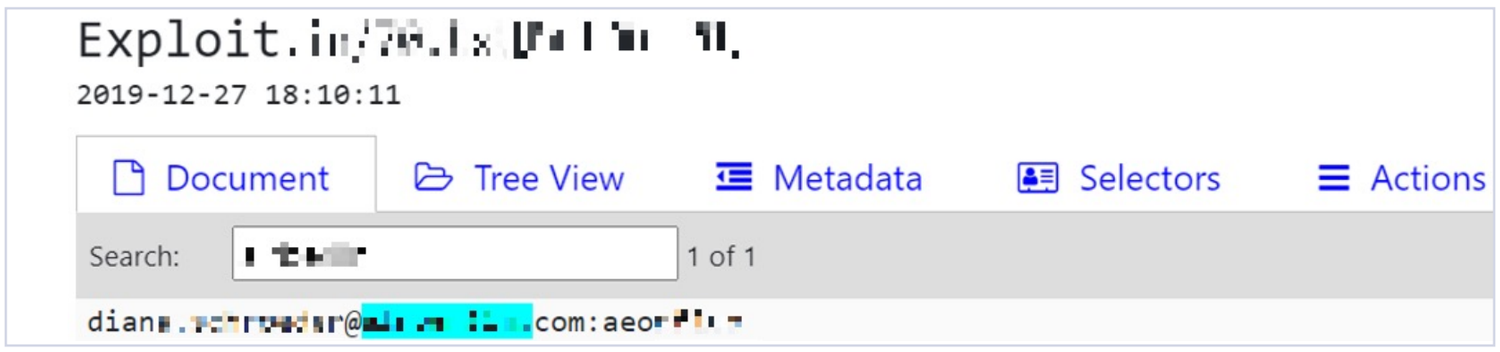


Figure 22. European leaked credentials

In Europe, the totality of airlines has a quite good quality SSL/TLS servers and no airline supports deprecated or insecure versions. In fact, half of them deployed **HSTS** on their server and use safe and powerful **cipher suites**.

3.3. APAC

As for the ten selected APAC airlines, all of them are rated as **low** by Spyse. Even though this might seem like an indicator that they are all safe, the reality is that **only two of them** have all their subdomains with the same rating. Several of these airlines have major security issues in important web pages as **loggings** and **booking forms**. Subdomains susceptible to attacks such as **APIs** or **test pages** have also been found, one of them having up to **eighty-eight** potential **CVEs** found.

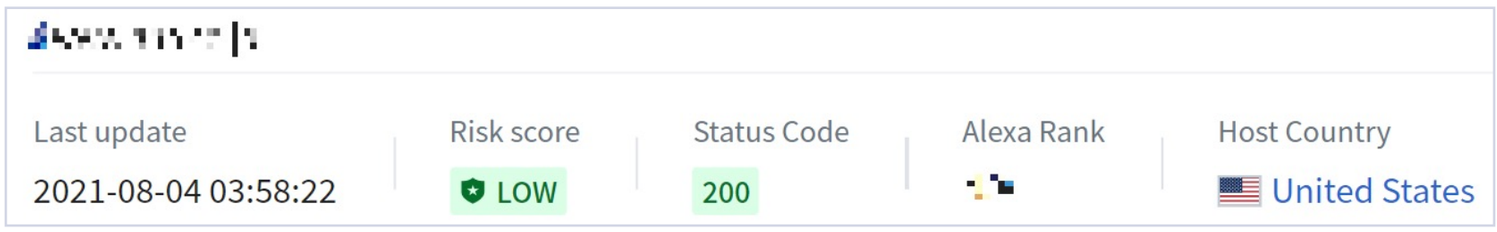


Figure 23. APAC main domain rated as Low

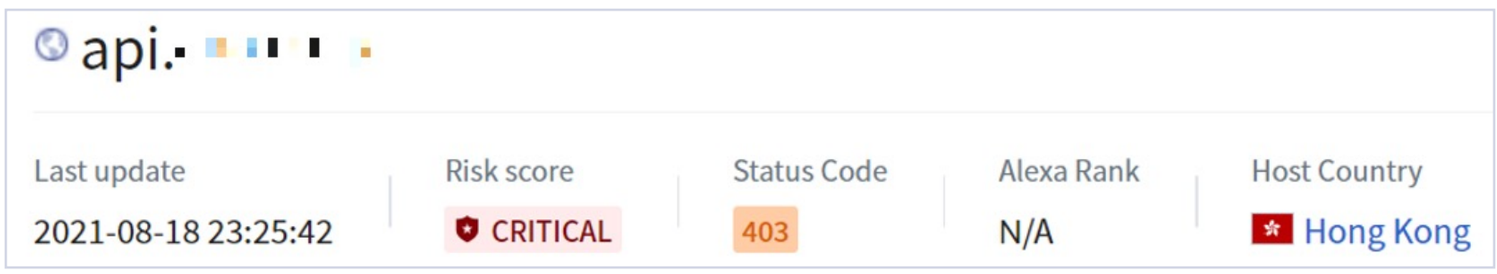


Figure 24. APAC subdomain rated as Critical

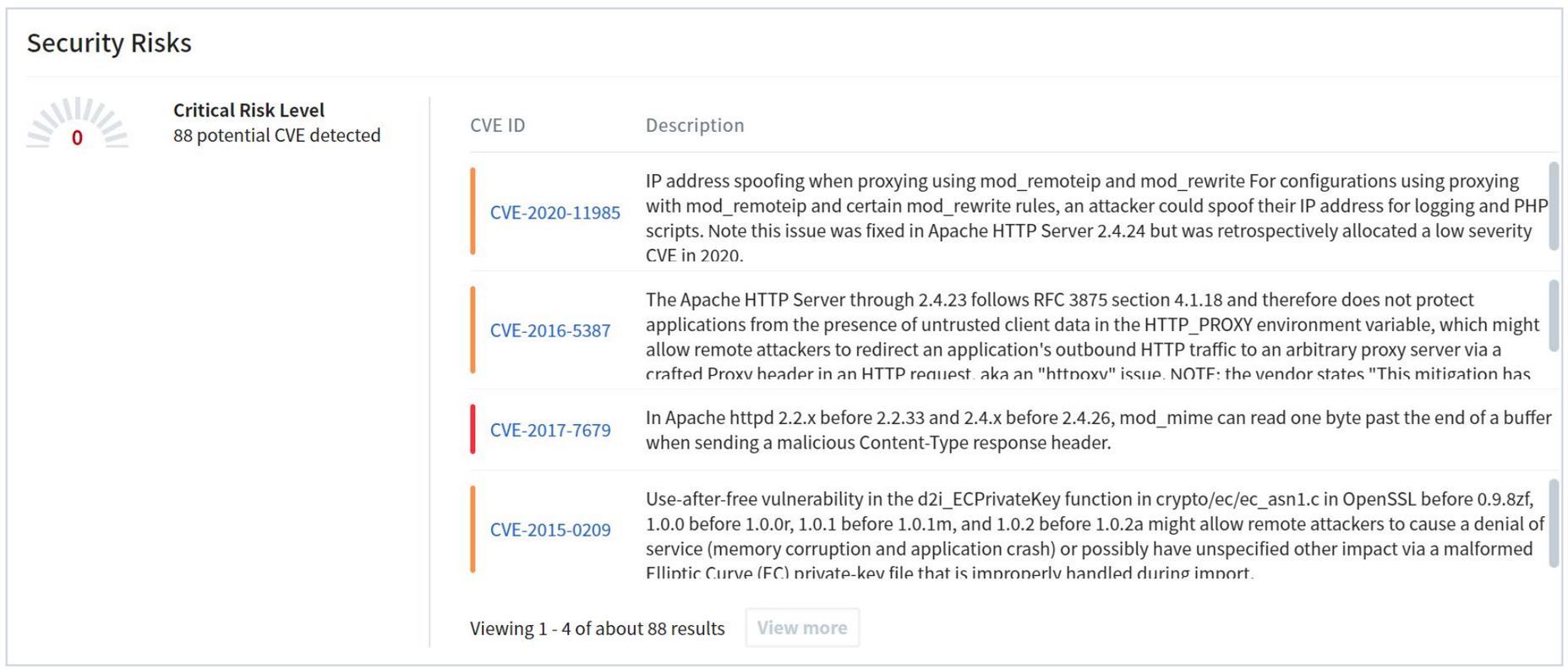


Figure 25. APAC airline potential CVEs

As with the previous regions, **credentials for all the airlines** were obtained with Intelligence X.

Regarding the security of APAC airlines SSL/TLS servers, it could be found that two of them support TLSv1 and TLSv1.2, versions that are now **deprecated** and should not be supported anymore.

3.4. Africa

In Africa, a certain decrease in the level of general security has been observed. In terms of risks, it may be the most vulnerable region.

Only four out of the ten main domains tested were rated as LOW risk by Spyse and only one of them truly has all its subdomains with LOW risk as well. Three airlines were rated as **medium** risk, two as **severe** and the last one as **critical**. Four African airlines have their main domains hosted in African countries, the remaining six have them hosted outside. It should be noted that the four **LOW** rated main domains are, indeed, hosted in **non-African countries**:

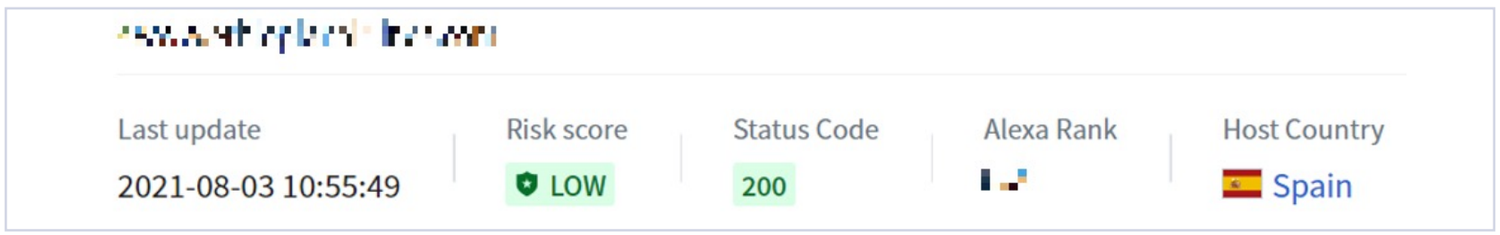


Figure 26. Low risk rated African airline

The worst rated airline (by Spyse's metric) has only three potential CVEs but they are of utmost importance. The three of the possible existing CVEs are known vulnerabilities in IIS 7.5.

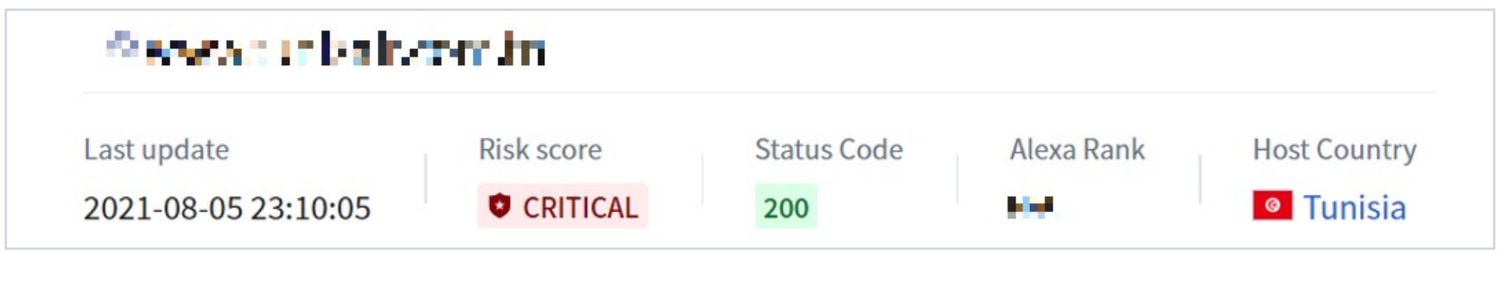


Figure 27. Critical risk rated African airline

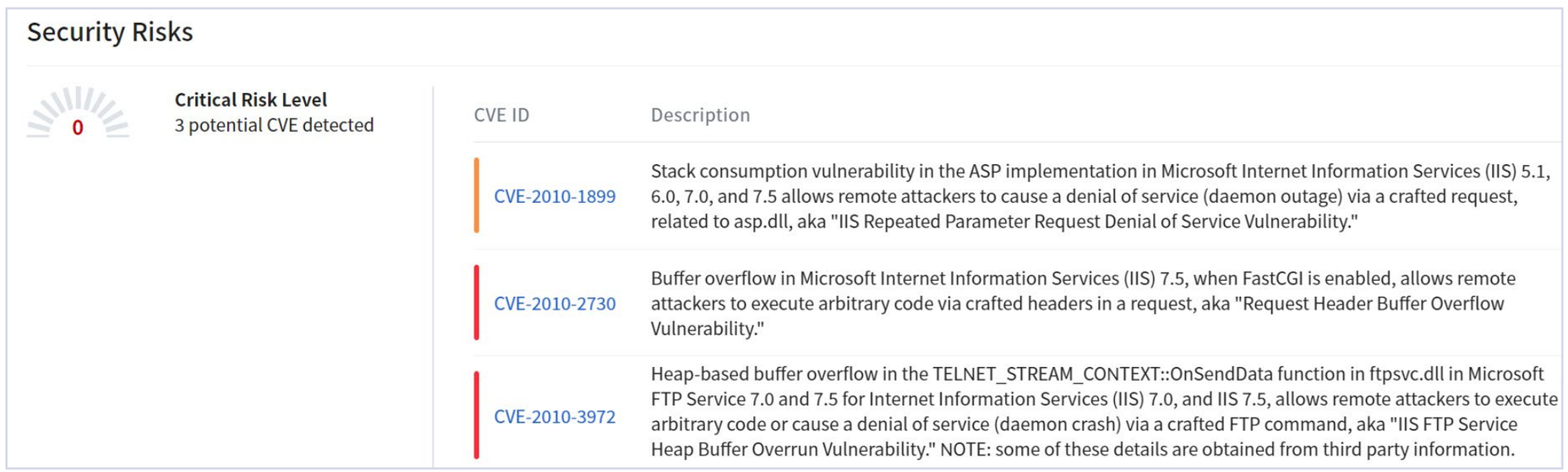


Figure 28. African airline potential CVEs

In Africa, the amount of information gathered with Intelligence X is similar to the amount obtained in the rest of the regions. What in fact does stand out is the **lower security** of their SSL/TLS servers. It was found that all of them support **TLS 1.0** and **TLS 1.2**, and that two of them also give support to **SSL 3 and RC4 cipher**, which makes them vulnerable to **POODLE Attack**. This is an example of an airline susceptible to this attack analyzed with Sslscan:

```
┌──(kali㉿kali)-[~]
└─$ sslscan [redacted].com
Version: 2.0.10-static
OpenSSL 1.1.1l-dev  xx XXX xxxx

Connected to [redacted]

Testing SSL server [redacted].com on port 443 using SNI name [redacted].com

  SSL/TLS Protocols:
SSLv2     disabled
SSLv3     enabled
TLSv1.0   enabled
TLSv1.1   enabled
TLSv1.2   enabled
TLSv1.3   disabled

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.2 not vulnerable to heartbleed
```

Figure 29. African airline Sslscan [1/2]

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA
Accepted  TLSv1.2  128 bits  RC4-SHA
Accepted  TLSv1.2  128 bits  RC4-MD5
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Accepted  TLSv1.1  128 bits  RC4-SHA
Accepted  TLSv1.1  128 bits  RC4-MD5
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  TLSv1.0  128 bits  DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
```

Figure 30. African airline Sslscan [2/2]

3.5. Middle East

One of the airlines in Middle East was rated as **medium**, other one was **critical** and seven of them were **low** (five of them with some of their subdomains with potential CVEs discovered). The remaining airline had not been analyzed yet, and **it will not be considered**. Five of the ten airlines were hosted in Middle East and the other five in other regions outside it.

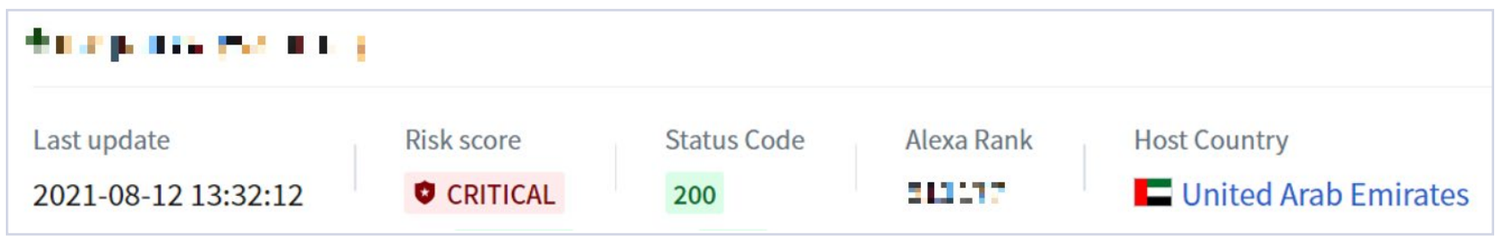


Figure 31. Middle East airline rated as Critical

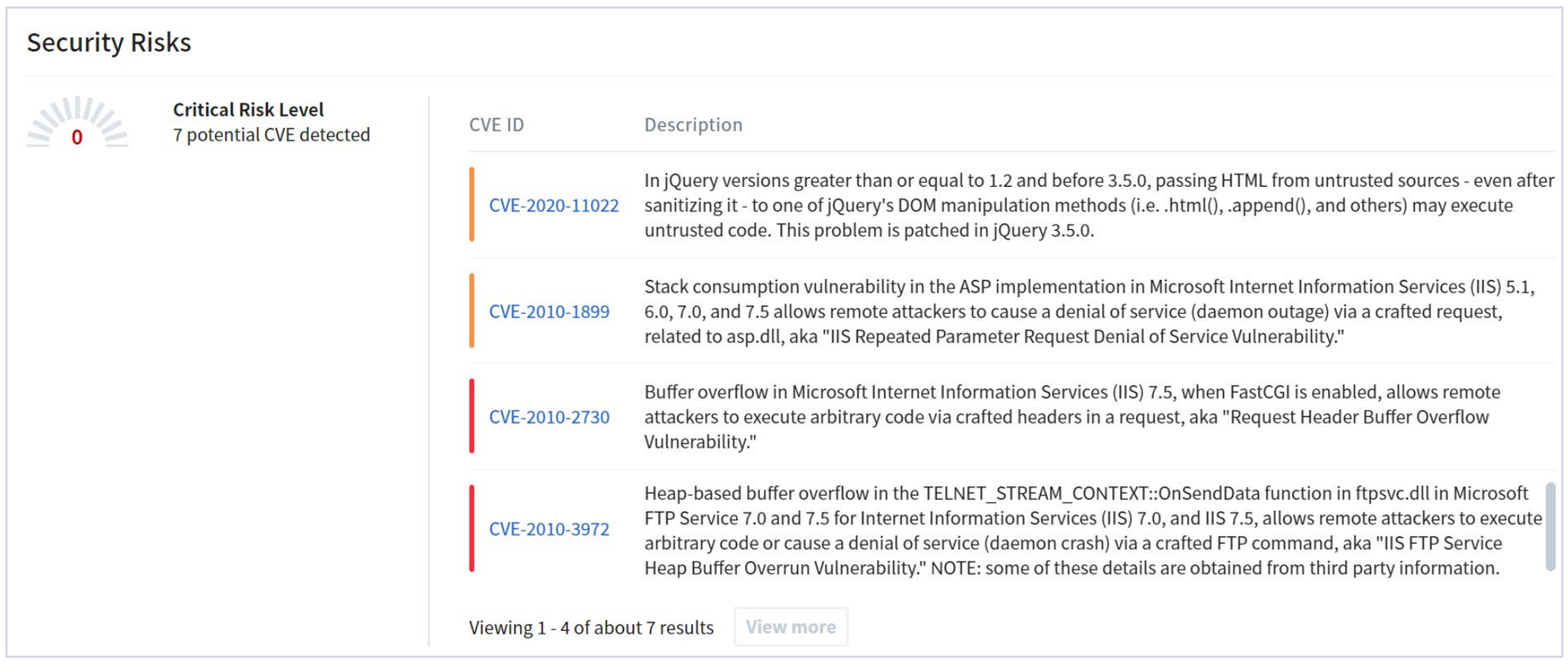


Figure 32. Middle East airline potential CVEs

In Middle East, it was found that there were three airlines with **many open ports** and it draws attention that these airlines belonged to Spyse's **LOW** category.

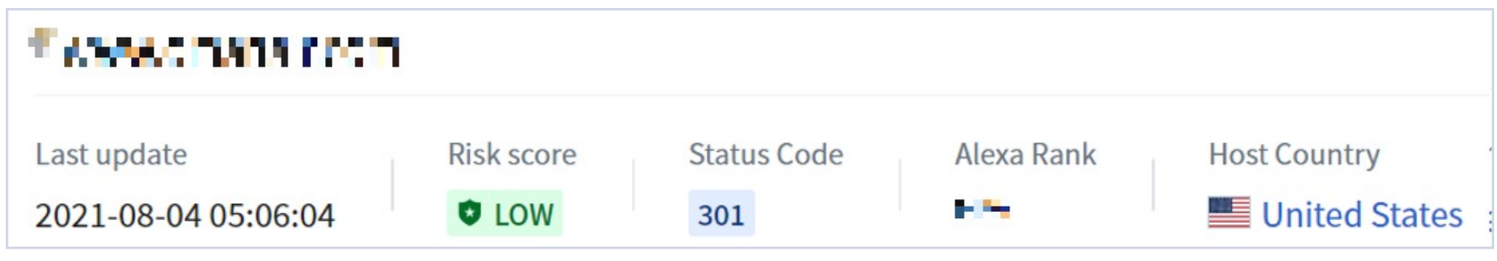


Figure 33. Middle East airline rated as Low

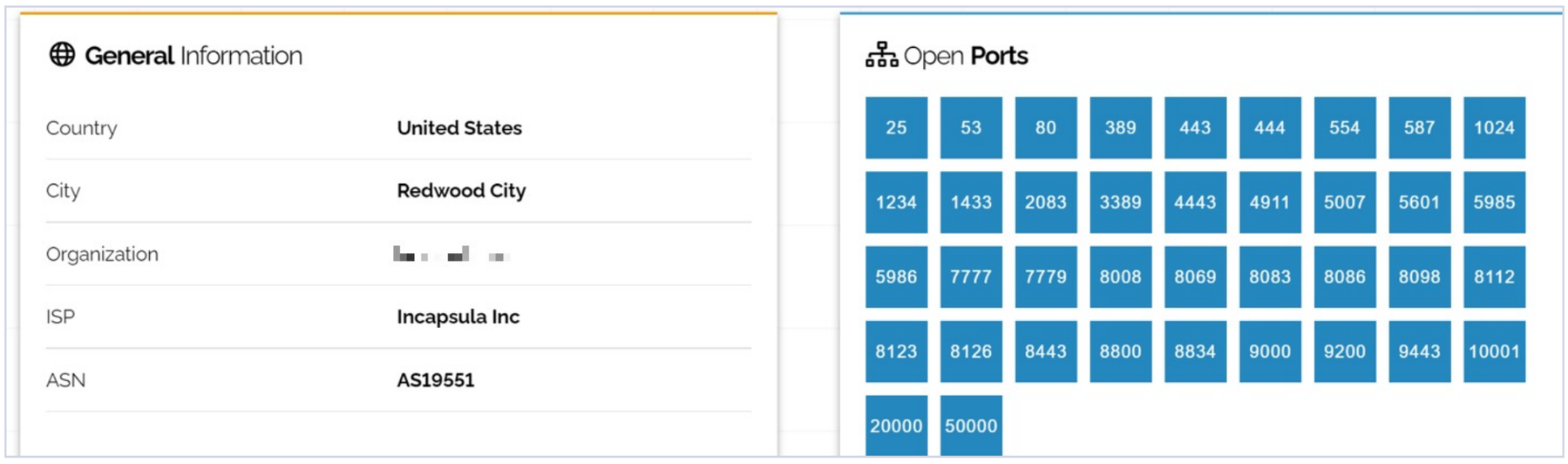


Figure 34. Open ports in Shodan (ME)

In one of them, all the following active protocols could be seen with **Censys** but, more importantly, a **case of carding** that contains the CC number, CVV, name, user, password and more data of an airline's worker was found on Intelligence X.

Protocols	80/HTTP , 443/HTTP , 2052/HTTP , 2053/HTTP , 2082/HTTP , 2083/HTTP , 2086/HTTP , 2087/HTTP , 2095/HTTP , 2096/HTTP , 8080/HTTP , 8443/HTTP , 8880/HTTP

Figure 35. Censys active protocols (ME)

Figure 36. Middle East carding case found

Apart from the case of carding, a high number of credentials was also found as in the previous regions.

Regarding the SSL/TLS server's security, it can be considered that Middle East airlines are very **good rated**. Only one of them supports TLS 1 and TLS 1.1, and most of the airlines integrate **HSTS**.

4. Conclusions and Recommendations

4.1. CVEs and risks comparison

As it has already been seen, at first sight, it may seem that **African** airlines struggle the most when it comes to the security of their websites and that **APAC** airlines might be addressed as the most secure ones. Nevertheless, the **actual number** of web pages that could be categorized as "**true LOW**" (the ones with all their subdomains apparently secured) is very similar among all regions.

Some airlines also have subdomains with descriptive names such as "test" or "API" that can provide helpful information for an attacker to map out a company's attack surface and learn where the potential weaknesses could be.

Every airline should review the security level of its websites and should have in mind the totality of its subdomains while applying security measures.

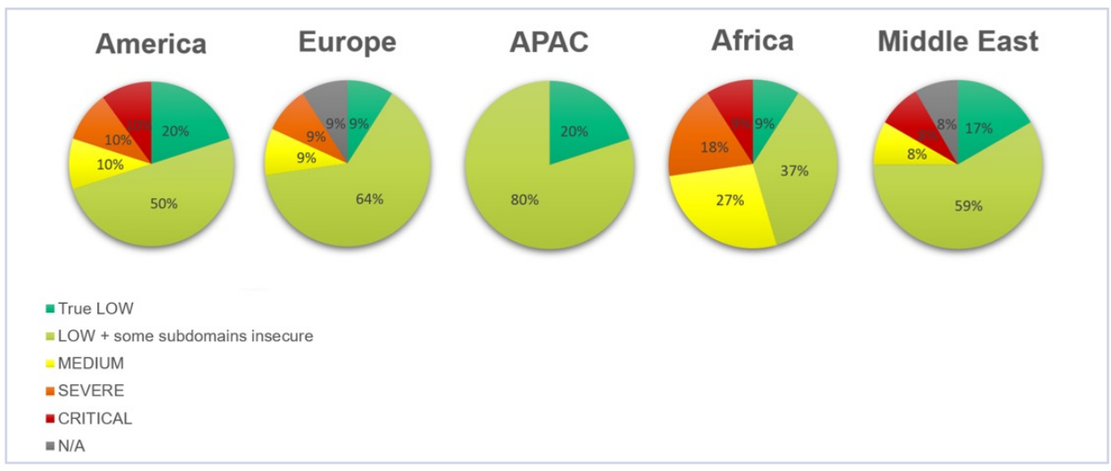


Figure 37. CVEs comparison

4.2. Main domains hosted comparison

Although the main domains were expected to be hosted in their airlines' same region, it does not seem to be the rule. **Data protection policies** should be considered by airlines when deciding where to host their websites as they can change significantly depending on the location.

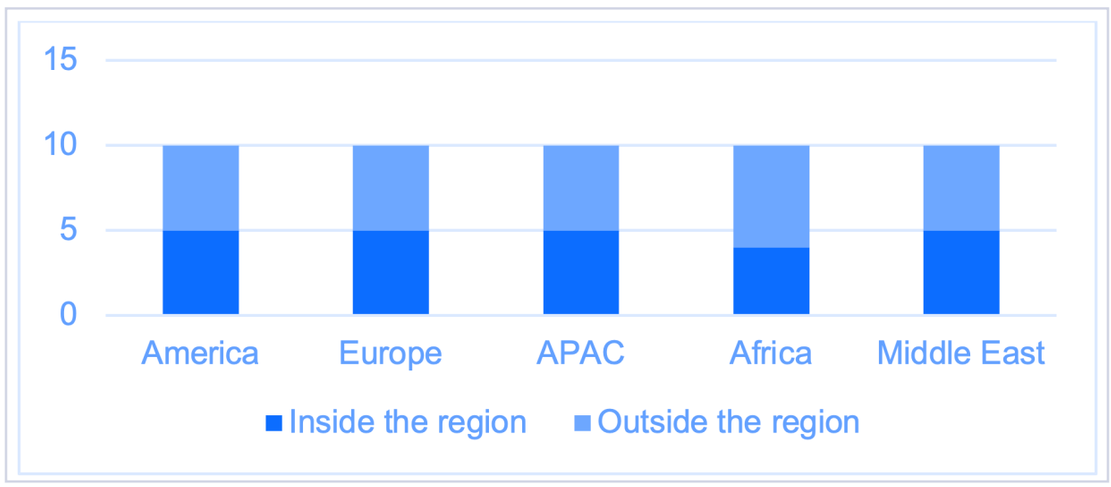


Figure 38. Main domains comparison

4.3. Data leaks found

An interesting amount of **credentials** from almost all the airlines was found. No significant variation has been observed in the quantity of data leaked in the five regions. While potential CVEs found or the quality of their SSL/TLS servers may be useful to tell if they are vulnerable, **leaked files** are an indication that a **certain threat has already materialized**.

Figure 39. Up to 39 credentials found in one file

Airlines should periodically check their possible breaches and take security measures such as a strong password policy. It is strongly recommended to **change the passwords** in the company from time to time so that, in case of a data breach, the passwords do not last long active.

4.4. SSL/TLS servers comparison

In this comparison, **Africa** is the region that stands out. Based on the collected data with Sslscan and Ssslyze, one could say that the security of its SSL/TLS servers is a bit lower than in the other regions. This lower grade has been assigned because of the use of insecure SSL/TLS versions and RC4 cipher that could help materialize a threat and involve direct attacks such as the **Poodle Attack**.

Although it is not reflected in the graph, **Europe** and **Middle East** may have the SSL/TLS servers that have the highest quality. In addition of not supporting insecure versions, they implement **HSTS with long duration** on their servers.

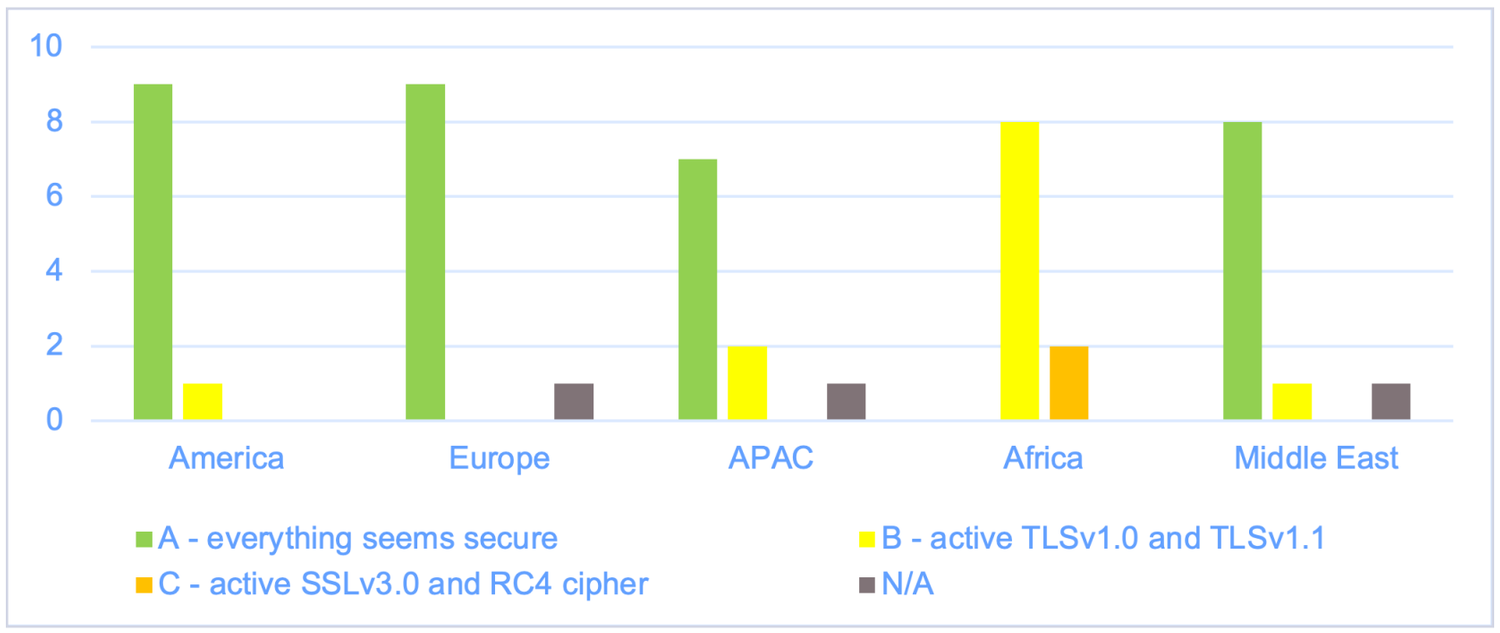


Figure 40. SSL/TLS servers' comparison

The security and quality of the SSL/TLS servers are another very important point to take into account in terms of cybersecurity. Apart from deprecated versions that directly involve security risks like the **Downgrade Attack**, certificates that have expired or are about to expire also leave other doors open such as the possibility of creating another certificate with the same signature and pose as the legitimate service.

In addition to updating all supported versions and making sure not to use those that could pose a security risk, air companies should **monitor the status of their SSL/TLS servers** to find misconfigurations and issues that could lead to subdomain takeovers or other direct risks that could compromise the security of the company's services.

4.5. Darkweb findings

There are many ways of buying flights and traveling packs for less money than the original sale price set by agencies and airlines. There are some specific **black market travel agencies** dedicated to offering these deals so customers can save up to 70% of what they would have paid at a conventional travel agency. Some of these illegal forums such as Patriarh, Sergik00 or Bantik Travel use **Telegram channels** as a platform for their business and are still active to this day.

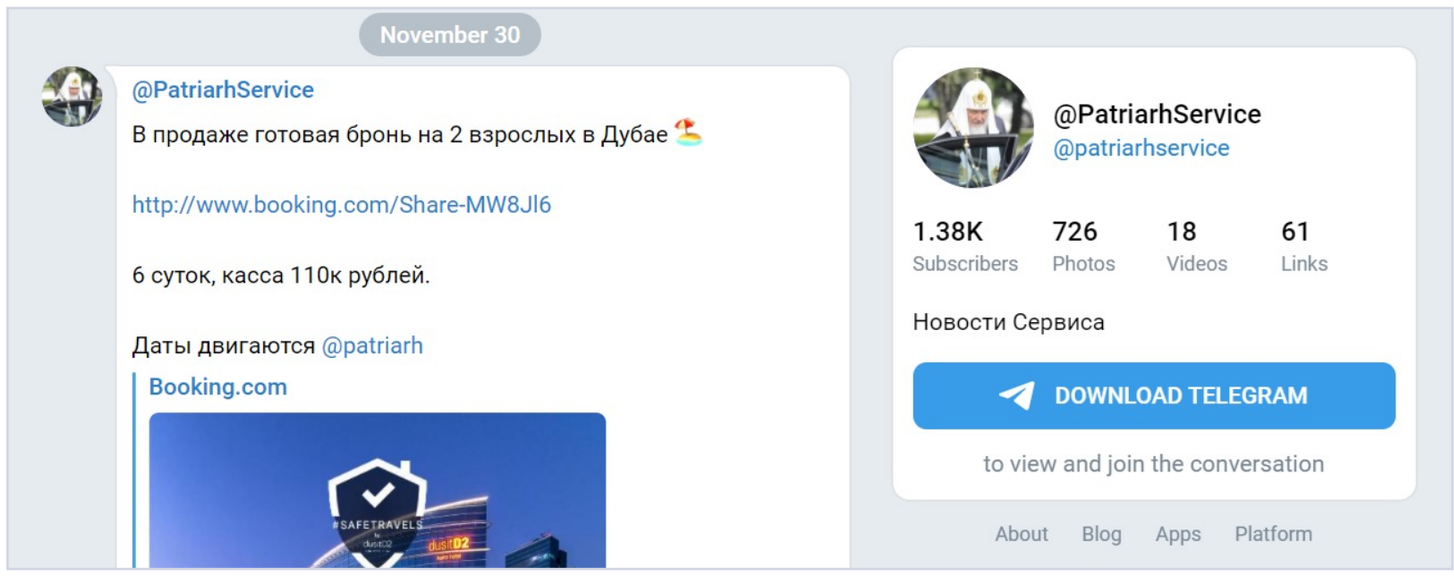


Figure 41. Patriarh's activity on November 30th

As it has already been mentioned, flights at lower price, gift cards and account details were found in some common dark markets as well. The active offers on **common dark markets** belong to **American airlines** and many of them only cover the **USA**. Although it has not been possible to find any offer in common dark markets from these vendors, it was observed that there are some trades that maintain the same format being offered by other sellers.

Figure 42. Travel offers found

Airline user accounts are the most offered trades, where they provide private data like credit card numbers, passwords, and users' addresses. **Back in 2017**, an internal report for an airline was made in which **travel ticketing fraud** was studied. The different methods of theft that cybercriminals use to obtain flights and travel deals were discussed. **Frequent flyer accounts** were already being sold and this method was increasing significantly during 2016-2017. It is no surprise that it is still one of the most popular ones.

This fraud detection takes more time than carding because most users do not check their points account very often. In some places like the USA, it seems not necessary to provide any extra method of authentication and **2FA seem not to be requested**. This may explain why the offers found are condensed in this area.

Although the main vendors and black markets seem to be in constant change, **airlines and travel agencies are still struggling with fraud and illegal sales**.

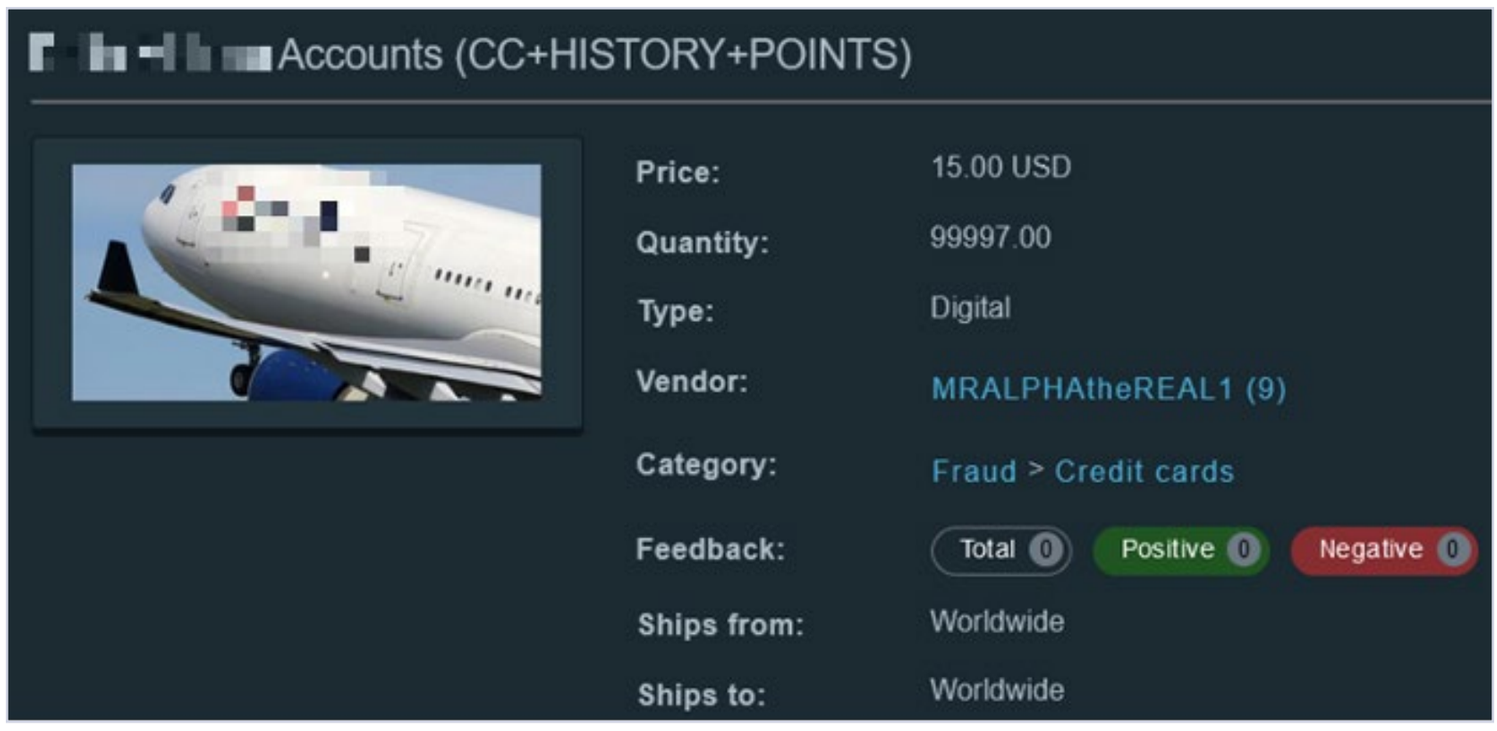


Figure 43. Sale of accounts

5. Summary

After analyzing all the collected information, airlines companies in all regions seem to have potential security issues. Anyone could gather **valuable information** about them in a **few clicks and searches** to perform a more sophisticated targeted attack. It seems that **Europe** and **APAC** could be considered the regions with a highest security maturity level, being **Africa**, the one which may need to improve some of its security measures.

Updated data such as SSL/TLS servers' quality and cipher versions, open ports, and potential CVEs could be a **starting point** in search of **security holes** and **vulnerable applications**. On the other hand, leaked credentials could be the **entry point**.

Suppose anyone wants to attack any of these targets. In that case, a large amount of data and useful information can be obtained in the process of information gathering by using **off-the-shelf** tools and methods. It is **not necessary** to have very extensive knowledge in the field to find useful and sensitive information

It is necessary to spread **awareness** about the scope of cybersecurity in these kinds of services and it is extremely recommended to adopt **Digital Risk Protection** measures or services that help monitor threats.

Telefónica Tech´s DRP service has tools and qualified analysts helping to protect valuable and private data and reputation, preventing, identifying and mitigating a wide variety of threats.

6. Telefónica Tech's DRP service

The Digital Risk Protection service offers a comprehensive solution against external cyberthreats covering the whole process from **early detection** to **final response**. This service takes care of the **detection**, **analysis**, **mitigation** and **resolution** of a wide range of risks and threats divided in four big categories:

- **Brand and reputation**: this category includes unauthorized use of brand, suspicious domains, offensive content, counterfeit and digital identity monitoring.

- **Business disruption**: includes data exposure, hacktivism, activism, breach of security controls, CVEs and security bulletins and credential theft.

- **Online fraud**: phishing and pharming, malware, carding and suspicious mobile apps.

- **Mobile Channel Risks**: includes proactive discovery, vulnerability assessment and suspicious mobile apps.

This 24x7 service helps protect a companies' digital assets by performing an **automated gathering** monitoring the open web, deep web, dark web and specialized feeds, providing a **manual analysis**, **contextualization and recommendations** by a team of experts, and applying countermeasures to **take down** the risk.

The Digital Risk Protection has a **user portal** that helps the client to track the risk to which their organization is exposed, providing a global view of these digital risks. This portal shows the general threats' status as well as a summary of the latest risks and delivered reports. It also offers a **threat list** with the possibility to apply search filters that help find detailed information about any kind of the incidents mentioned above.

Here are some examples of use showing some of the service's utilities. The bank **Novele Bank** mentioned in the following screenshots is a **fake bank** created by Telefónica Tech to show the operation of the service.

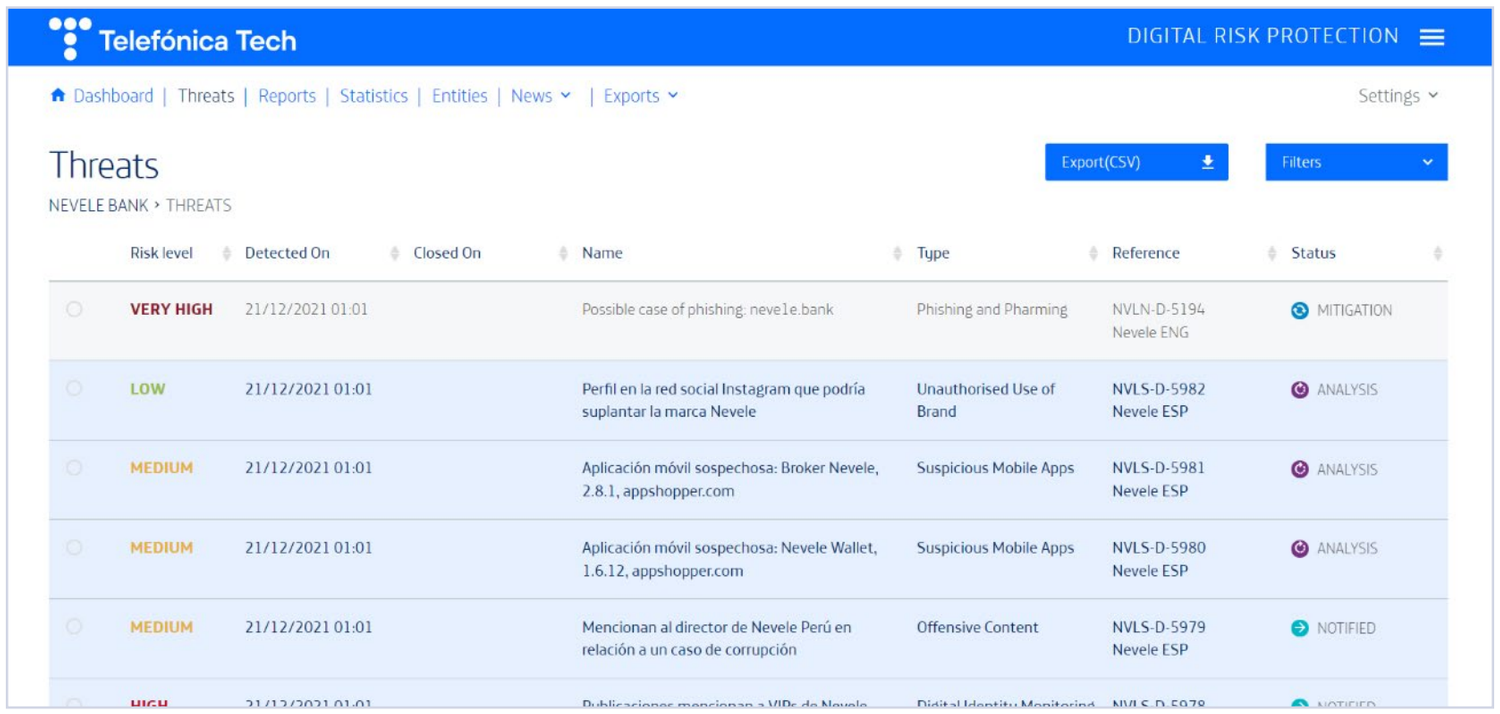


Figure 44. Telefónica Tech´s DRP service

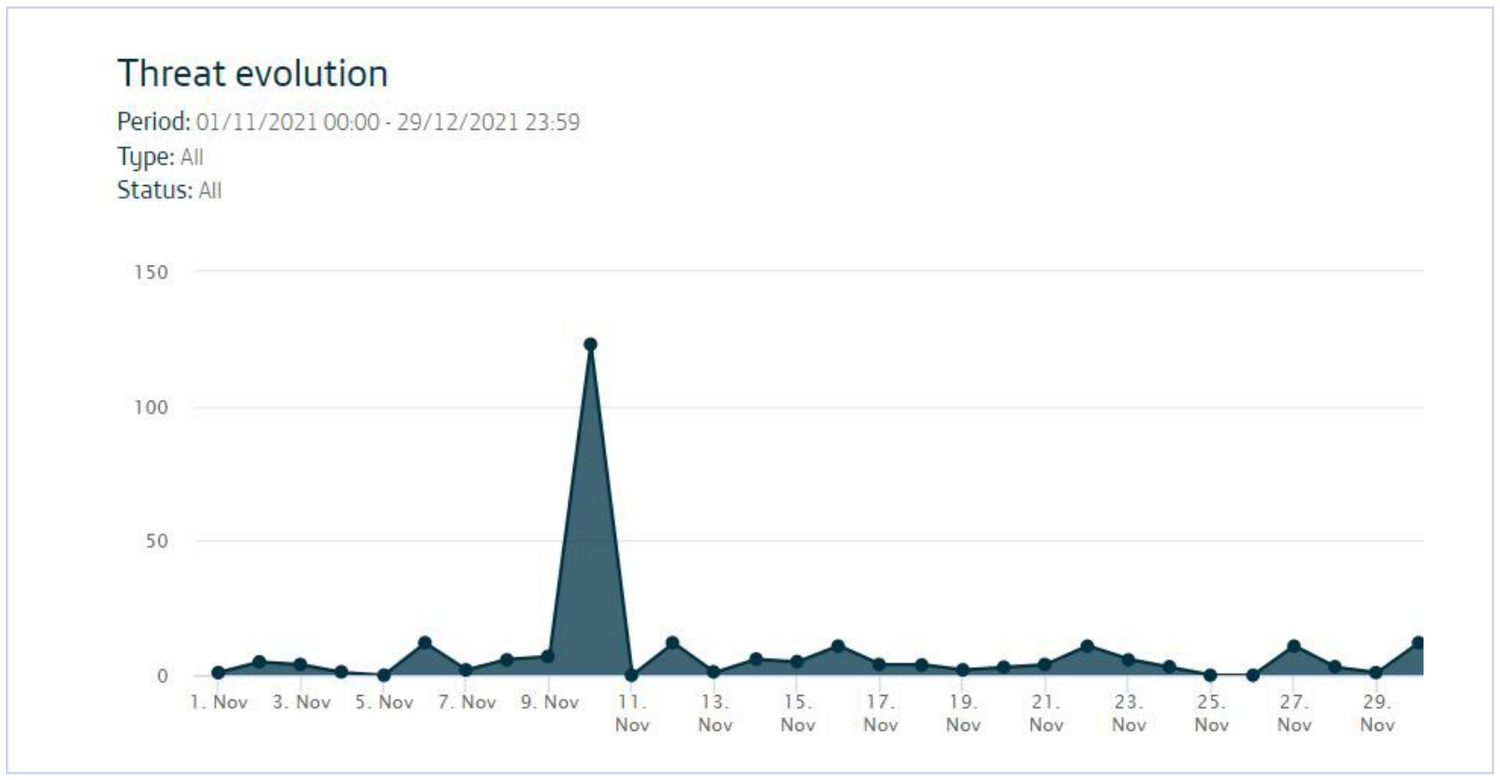


Figure 45. Carding incidents detected in November for one of the airlines companies.

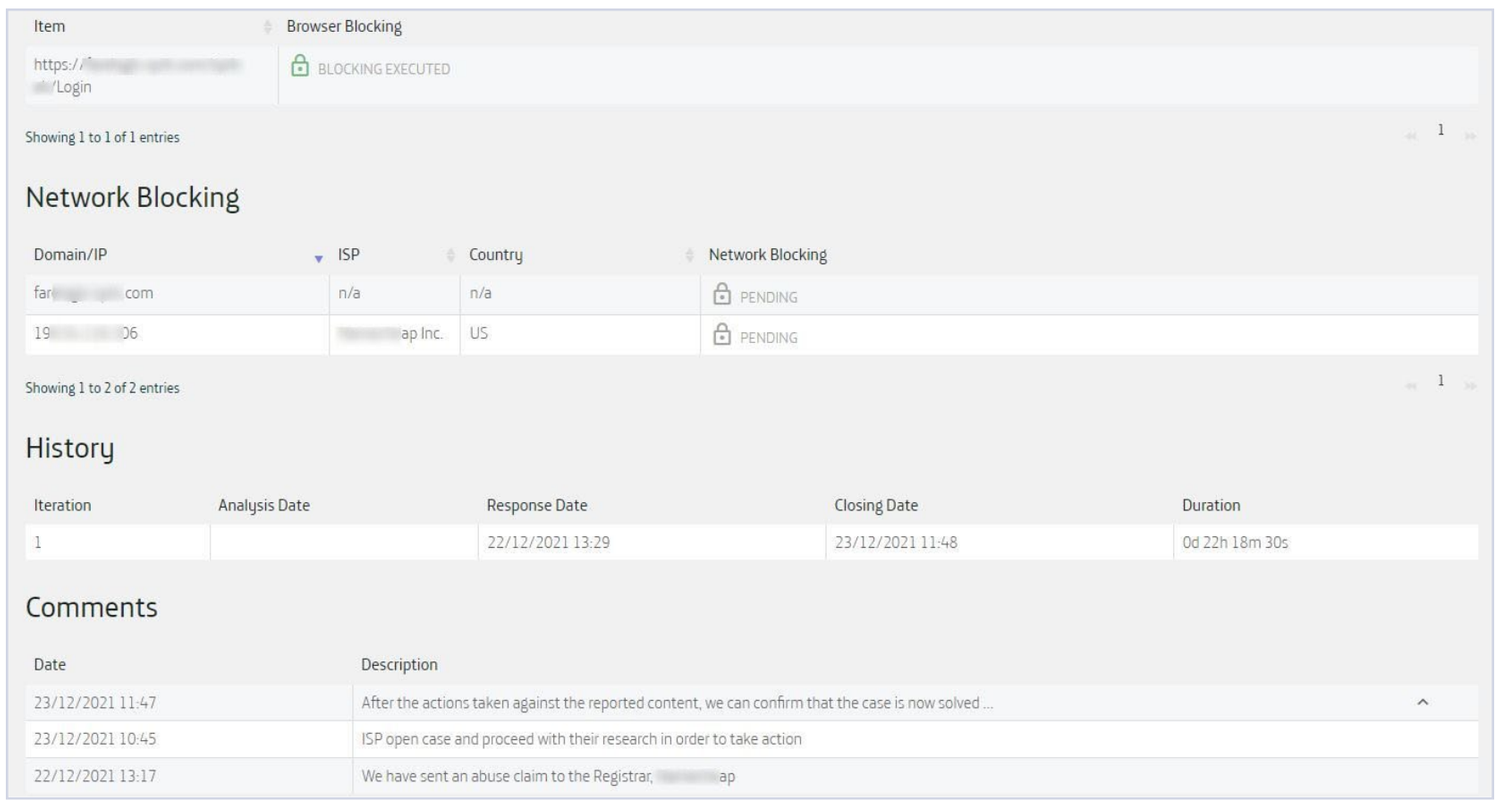


Figure 46. Real Airline phishing case – Mitigation

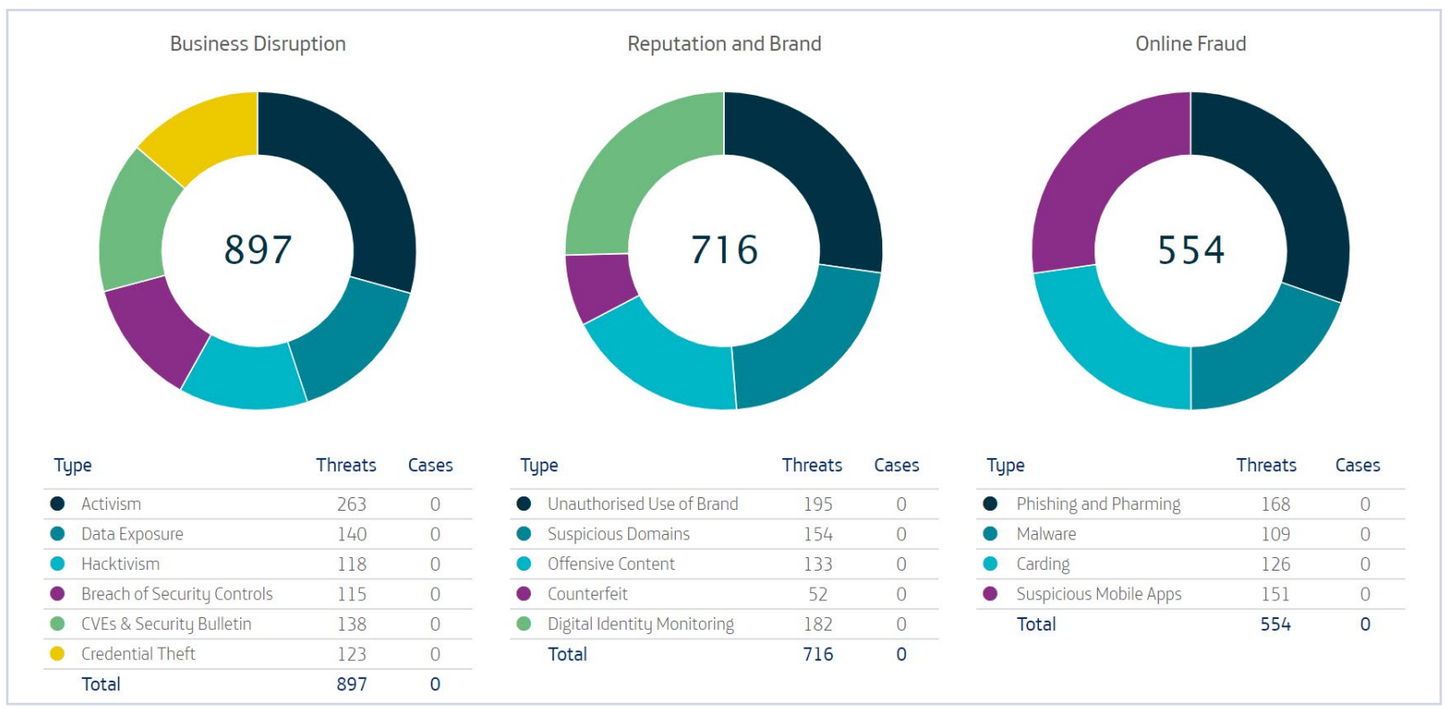


Figure 47. Example of Threat distribution by category (last year period)

Telefónica Tech's DRP service offers to have access to all the information gathered to the detected threats; In case of credentials theft or carding, it lists and shows the number of issues found, but only available to the customers. **Randomly** choosing only one airline of each region, the following number of credentials leaked this year was:

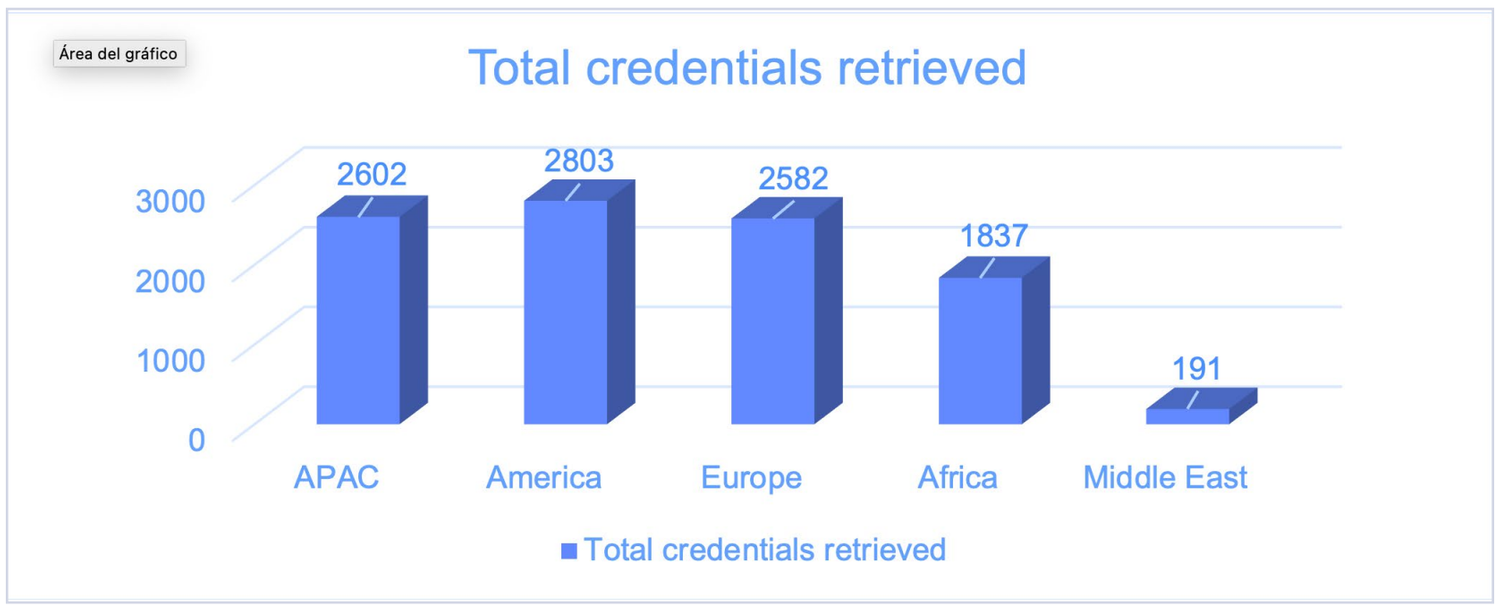


Figure 48. Credentials retrieved with Telefónica Tech's DRP service

The use of this service would help airlines to **increase** their cybersecurity levels and to **prevent**, **detect** and quickly **respond** to any kind of threat due to the constant monitoring of their services and the in-real-time alerts.

→ **VISIT OUR DRP WEBSITE**

7. Collaborators

Telefónica Tech

Lucía López Sánchez

Pablo Cuesta Fernández

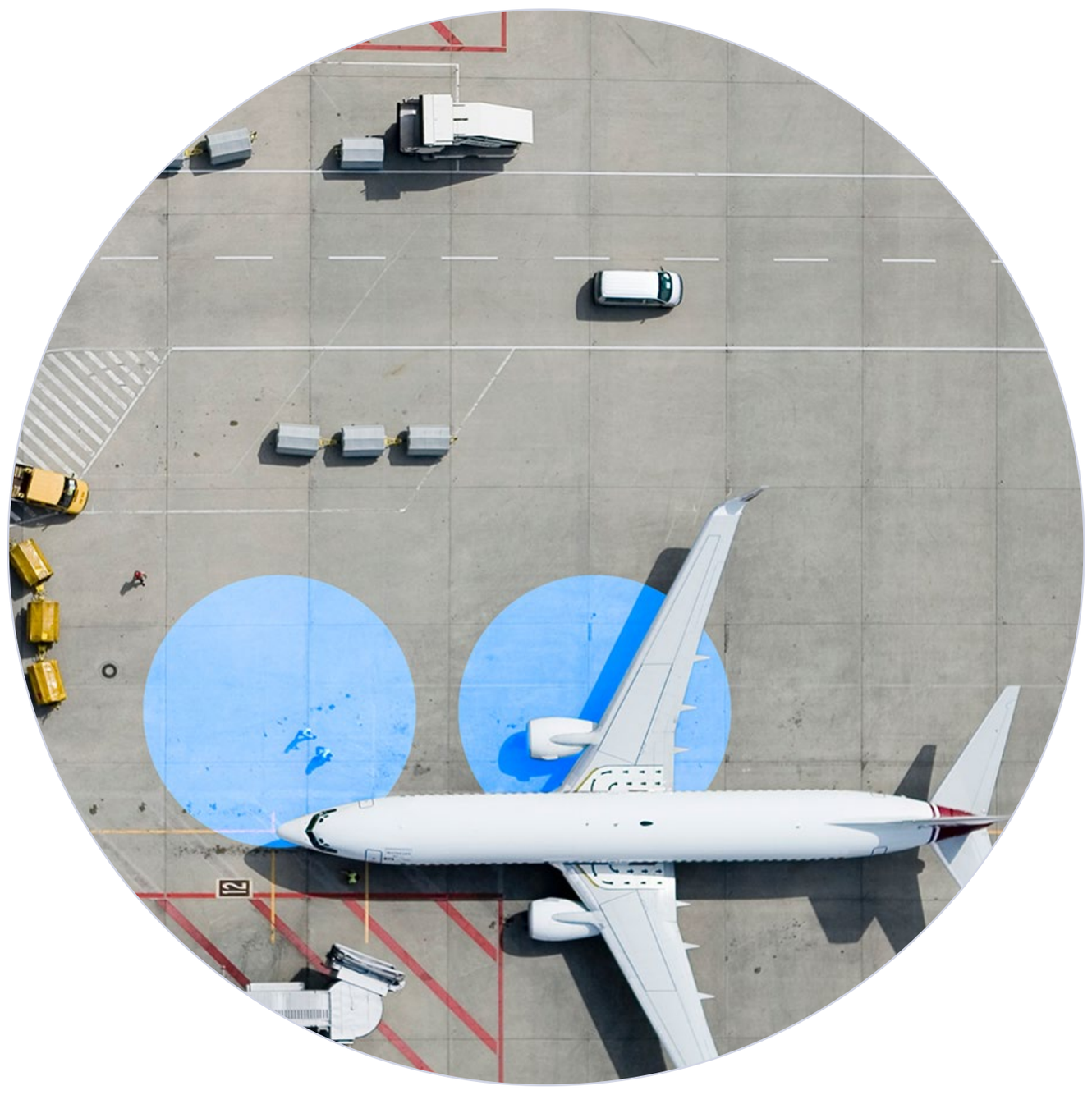
Álvaro Asensio Botanz

Helene Aguirre Mindeguia

Víctor Manuel Salguero Rincón

Ángel Fernández Martín

Sebastián García Saint-Leger



8. Appendix

This appendix contains the **summary** of what was deduced from the **2017 private report** of an investigation regarding the fraudulent sale/purchase of flight and hotel bookings from the point of view of criminal gangs, hackers and other actors in the illegal markets of Deep Web.

- The world of hotel and airline tickets fraud can be divided in **two big areas**: fraud based on the purchase from travel agencies where the payment is made with stolen credit cards or reward points in the case of airlines, and fraud based on more sophisticated methods.

- The common is that fraudsters create advertisements for the black markets providing a description of their services that ask the customers to detail the prices of the flight they want to purchase and tell them if they can satisfy their demand. If so, the vendor tells the final price, and the customer provides data of the travelers. The payment is made through Bitcoins.

- A wide variety of fraud methods are used. The methods described in the report are carding, frequent flyer and hotel reward points, credit line (buy now, pay later), insurance fraud, corporate credits, employee's free tickets, and credential theft for GDS systems (Amadeus, Sabre, Galileo).

- The list of active dark markets and active vendors is in constant change due to the closure of some markets and problems with the law.

- The purchase is easy to make and it is often made by a **third party** who knows how to move through the Deep Web and how to use Bitcoin that resell the ticket. The real customers usually pay this person in real life.

- The main victims of this fraud, besides bank and travel agencies, are airline and Hotel companies, especially for the massive manipulation of the Reward Points programs. Some **recommendations** to improve the security of user accesses are putting in place login systems with strong passwords, using a 2FA, putting in place reputation systems for authentication processes, audit all connections, and audit through offline processes reward points operations between accounts.

telefonicatech.com

→ **CONTACT US**

2022 © Telefónica Cybersecurity & Cloud Tech S.L.U. with Telefónica IoT & Big Data Tech S.A. All right reserved.

The information disclosed in this document is the property of Telefónica Cybersecurity & Cloud Tech, S.L.U. (“Telefónica Tech”) with Telefónica IoT & Big Data Tech S.A. and/or any other entity within Telefónica Group and/or its licensors. Telefónica Tech and/or any Telefonica Group entity or Telefónica Tech’s licensors reserve all patent, copyright and other proprietary rights to this document, including all design, manufacturing, reproduction, use and sales rights thereto, except to the extent said rights are expressly granted to others. The information in this document is subject to change at any time, without notice.

Neither the whole nor any part of the information contained herein may be copied, distributed, adapted or reproduced in any material form except with the prior written consent of Telefónica Tech .

This document is intended only to assist the reader in the use of the product or service described in the document. In consideration of receipt of this document, the recipient agrees to use such information for its own use and not for other use.

Telefónica Tech shall not be liable for any loss or damage arising out from the use of the any information in this document or any error or omission in such information or any incorrect use of the product or service. The use of the product or service described in this document are regulated in accordance with the terms and conditions accepted by the reader.

Telefónica Tech and its trademarks (or any other trademarks owned by Telefonica Group) are registered service marks.