Telefónica

TREND REPORT_

The Biggest Data Leaks of the Second Third of 2016

28.10.2016

CYBER SECURED BY ElevenPaths

elevenpaths.com

Index

Executive summary

If the rise of major leaked databases had already been significant during the first four months of 2016, the systematic publication of incidents throughout the second four months not only maintained the trend seen until then but multiplied the number of exposed accounts. In addition, the high profile of the affected platforms made it evident that not even major companies are safe from an incident of these characteristics and that the possibilities of controlling the spread after such an incident are limited once the security leak has been consummated.

A significant part of the information that was made public during this period, linked to services of renowned prestige, was from more than three years ago. Although these platforms have recently taken measures forcing all their users to change their access passwords, the fact that the information remained valid until its open publication is in and of itself significant. Furthermore, even if the information had no longer been valid on the affected platform, obsolete information is still a matter of interest for an attacker because it can be reused for the preparation of more sophisticated phishing attacks or for attempting to adjust the identification processes criteria on other platforms where said accounts are being used.

In these second four months, up to 34 of the more than 303 identified information leaks correspond to incidents catalogues as critical (with risk levels greater than 8), motivated by both the volume of the credentials exposed as well as the content of the information itself. The health industry has once again been the most affected party, receiving a significant number of incidents due to the existing legal imperative in some countries regarding the preventative announcement of leaks from the moment their existence is ascertained. However, incidents linked to social networks, forums, and online gaming platforms are those that have, in absolute terms, exposed the greatest number of user records.

Regarding the nature of the information, although most of the credentials are hashed (approximately 1.02 billion), worth mentioning is the fact that this period allowed the identification of nearly 113 million clear text passwords. The emails potentially exposed in this period exceed 1.14 billion, making up a powerful ratio of candidate accounts that can be used for fraudulent purposes.

The motivations of the attackers during these four months can be consolidated as the cybercriminal interest seen in past editions of this report. The direct offer of these leaks in underground markets that are only available through Tor goes hand in hand with other potential uses already seen in the past, uses linked to extortion practices that could be adapted to different objectives such as corporate accounts or profiles related to minors.

In this sense, the existence of information leak publications has given rise to a large number of monitoring and leaked credential alert services. Although some platforms offer affected users the possibility of hiding the information leak from third parties, the simple fact of consulting an undetermined number of corporate accounts, for example, is already a risk in and of itself because it exposes a first list of possible users of an organization to extraneous third parties.

1.Introduction

October 2013 marked an inflection point in terms of information leaks. A massive leak of Adobe users that month served to open up more than 150 million records, and lay the foundations for what we have been seeing in 2014, and especially in 2015 [1] regarding the important security breaches that have been occurring. In this sense, during the first four months of 2016 we were able to see a confirmation of the trends that indicated the rise of large information leaks in 2015, with a systematic increase of the volume of exposed credentials during those first four months of the year. Considering the consulted sources of information and the various leaks that have already been made public, the volume of potentially exposed user records exceeded 330 million records up through the April abril 2016 [2, p. 2].

In that period, we cannot state that the attacks were mostly motivated by hacktivist purposes; on the contrary, they were able to be related to other cybercriminal practices aimed at the monetization of leaks by either selling them or through extortion. According to sector, the security breaches affected organizations that work in different fields, with special focus in the field of institutions related to health and education. In exceptional cases, an important volume of records (nearly 200 million) of an electoral nature were identified during the first four months of the year, records that included detailed information about Philippine, Mexican, and Turkish citizens. As we shall see in this update, this trend has not continued in the second four months of the year.

1.1.Scope

The scope of this document is the compilation of the information leaks that occurred throughout the second four months of 2016, between May 1 and August 31, 2016. The information leaks mentioned in this document come from open sources exclusively, by either having been published in free access platforms or by having been referenced in different specialized media.

1.2.Goals

The goal of this document is to put the security risks that stem from major leaks of credentials that could affect both individual and corporate users, into context in order to identify the trends that have motivated their appearance, and to follow-up the implications that these, and other similar trends, may have by having been published throughout the second four months of 2016.

1.3.Methodology

For the purposes of this report, the incidents will be classified into different categories according to the attackers' motives. These categories are the following:

- Cybercrime. General cybercriminal motivations. These are usually reflected by incidents in which the author or authors have an economic or lucrative motivation and try to benefit from the leak through its sale, by using it as a showcase for other capabilities, or as a result of successful, or unsuccessful, cyberextortion.
- Cyberwar. An act of war in which state figures are allegedly implicated. These incidents include attacks against military infrastructures during times of peace, or critical attacks against military or civilian infrastructures during times of war.

- Hacktivism. Security incidents against technological assets in which the authors express activist motivations of any type. A short list of motivations includes political vindications, transparency, the fight against corruption, feminism, the fight against racism, alignment against social or labour movements, etc.
- Others. Other incidents related to cybersecurity that are not directly dependent on hacktivist activities or associated to cyberwar or cybercrime.

Another characteristic element of each leak is the typology of the attacker who causes is. The different natures of these typologies can lead to a more effective exploitation of the recovered information depending on the sophistication of the attack techniques used, on the one hand, and the interests of those affected, on the other. For these purposes, the following possibilities are considered:

- State-sponsored. Actions sponsored by states or other related international agencies.
- Malicious insider. Actions materialized by individuals from within an organization or by personnel that is no longer a part of it, but did them in the past.
- Malicious outsider. Actions carried out by external individuals with no association to the affected organization.
- Stolen device. Incidents related to potential information leaks as a consequence of stolen devices.
- Lost device. Potential incidents related to information present in devices whose loss has been reported.

The company's area of influence, considering the headquarters for those cases where the platform has a global presence or a regional character or when specifying the location of the affected technological asset is not possible, has been taken into account in order to establish the country affected by each leak. In any event, other relevant methodological aspects that have been considered for the creation of this document, as well as the evaluation criteria followed in relation to the severity level or its typology, are detailed in the ***Annex A. Methodological annex***.

2.General approach and context

The second four months of 2016 were especially prolific in terms of the leak of personal information. The 302 information leaks identified by ElevenPaths in this period have led to more than 1.345 billion records being exposed online, implying a significant increase in comparison to the same period of 2016 [2, p. 2] and especially in comparison to the trends also observed in 2015 [1, p. 3]. The increase in the amount of leaked information exposed in Figure 1 is not only due to an increase in the number of incidents, but also because of the public exposure of important security breaches heretofore unknown. Worth mentioning is the fact that most of the contents included in this calculation correspond to leaks that have been made public during these months despite the fact that the data included in them was, in some case, more than four years old, like Linkedin [3], Dropbox [4] or even seven or eight years old, like in the case of Myspace [5].

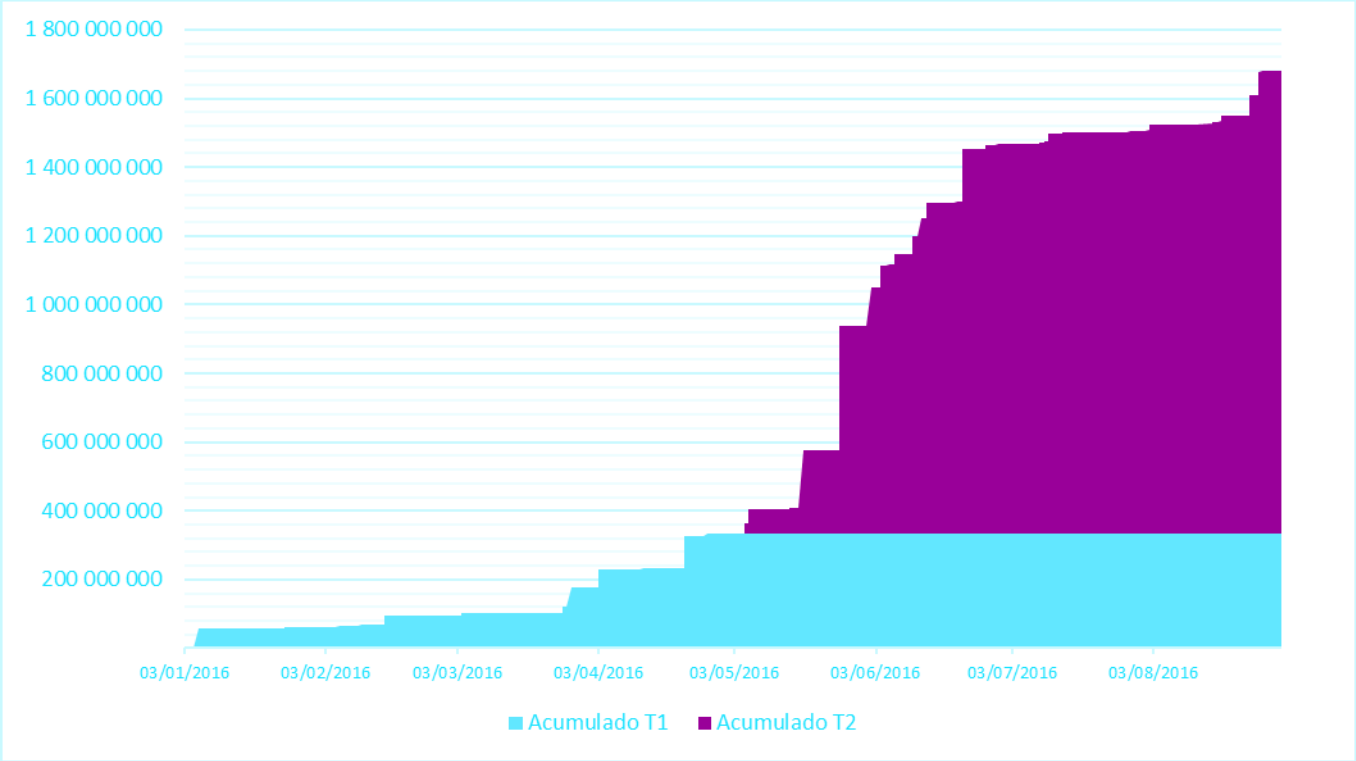

Figure 1. Evolution of the volume of leaked credentials throughout the second four months of 2016. Source: prepared by the authors.

In order to have the elements that enable us to make a comparison between the severity levels of the information leaks that have taken place in the second four months, the application of the unified risk criteria of the ***Annex A. Methodological annex*** also used in the first period reveals the publication of 34 critical level leaks above level 8 (see Figure 2) resulting in a 300% increase compared to those identified in the first period of the year [2]. Among those that have had the most media repercussion are the leaks that affected Myspace [5], Linkedin [3], Badoo [6], Neopets [7] or iMesh [8] with maximum risk, and others such as Dropbox [4], Tumblr [9], Zoosk or R2Games [10] which also exceed a risk of 9.5.

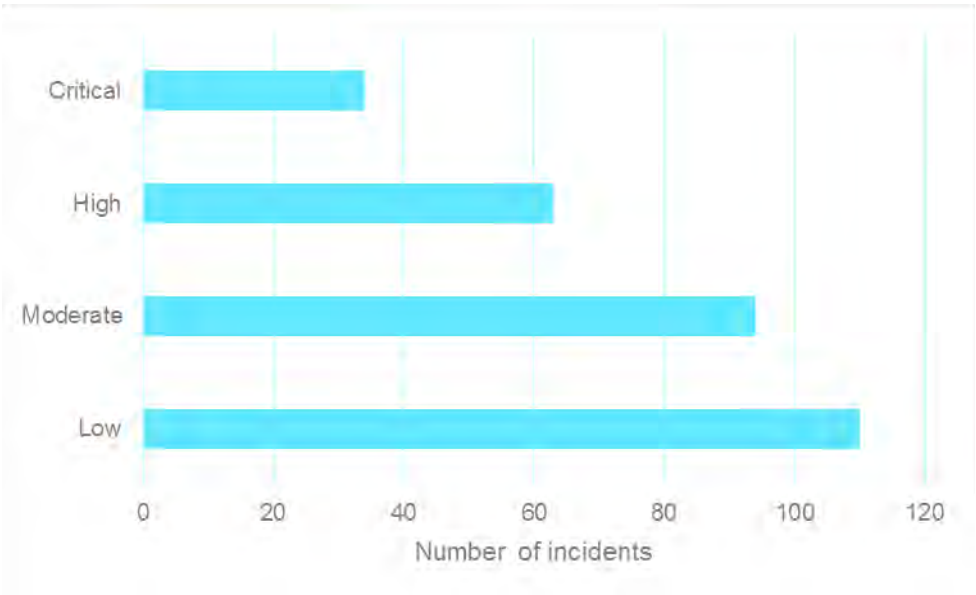

Figure 2. Risk levels of the identified leaks identified in the second four months of 2016. Source: prepared by the authors.

As for the motivations of the authors for carrying out each one of the attacks, worth mentioning is an increase in cybercriminal motivations in this field as seen in the Figure 3, much higher than *hacktivist* interests which represent just over 7.5% of the total. The nature of the attacked sectors, and the existing possibilities for monetizing the obtained information, are elements that facilitate the criminal use of the information either through the direct sale of the databases or through other channels. In any case, both reasons account for the great majority of the attacks that have taken place in this period of time within the scope of the leaks of information leaks.

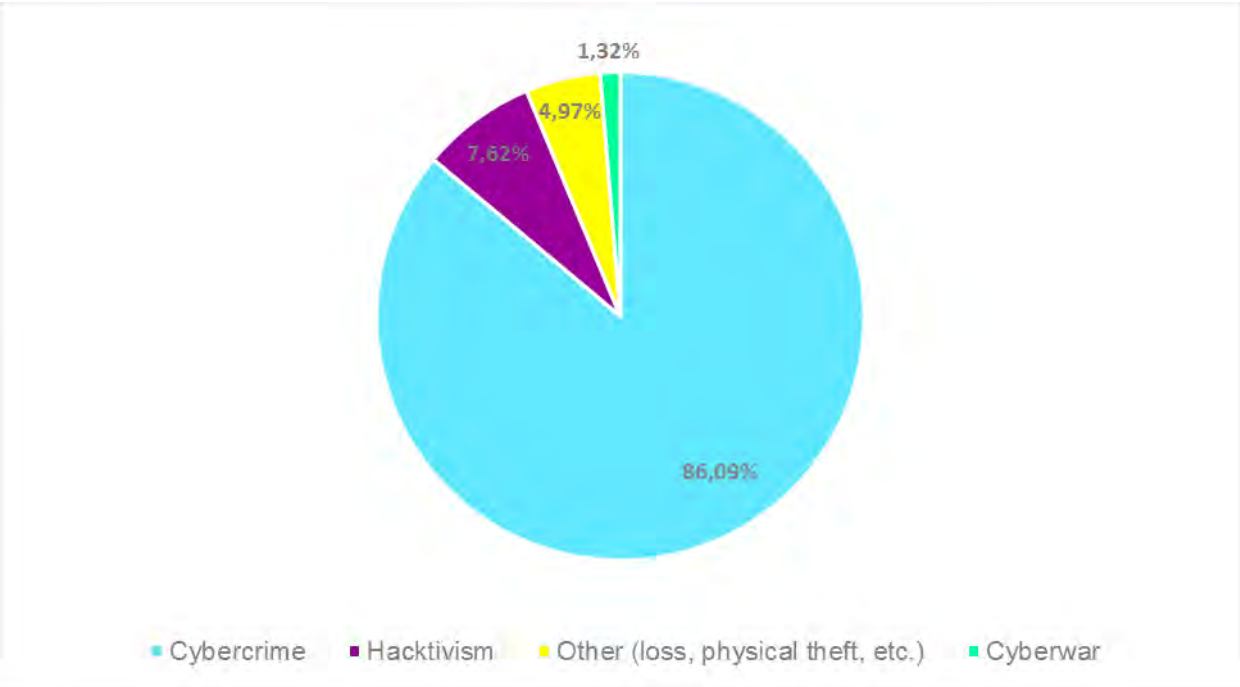

Figure 3. Motivations for the attacks carried out in the second four months of 2016. Source: prepared by the authors.

3.Types of affected platforms

Following the method of prior editions of this document, this section will approach the typologies of the affected platforms from two points of view: through the number of individual incidents identified, on the one hand, and through the volume of leaked credentials and records, on the other hand.

3.1.Per number of incidents

Many sectors have been the subject of cybersecurity incidents linked to the leak of large databases throughout this period. As seen in the Figure 4, a very important part of the incidents were linked to the health industry, followed by the entertainment industry, social networks, and the government sector as the most popular areas. The vast majority of the motivations respond to cybercriminal interests of different natures, among which is the sale of the extracted information in underground markets.

If one had to establish the characteristics of the average incident linked to the exfiltration of data in these months, said average incident would correspond to a cybercriminal incident linked to the health industry in the United States. As we shall later see, this model does not have to be the sector with the most relevant incidents (barely one of the 110 identified incidents linked to the health industry is of a critical nature).

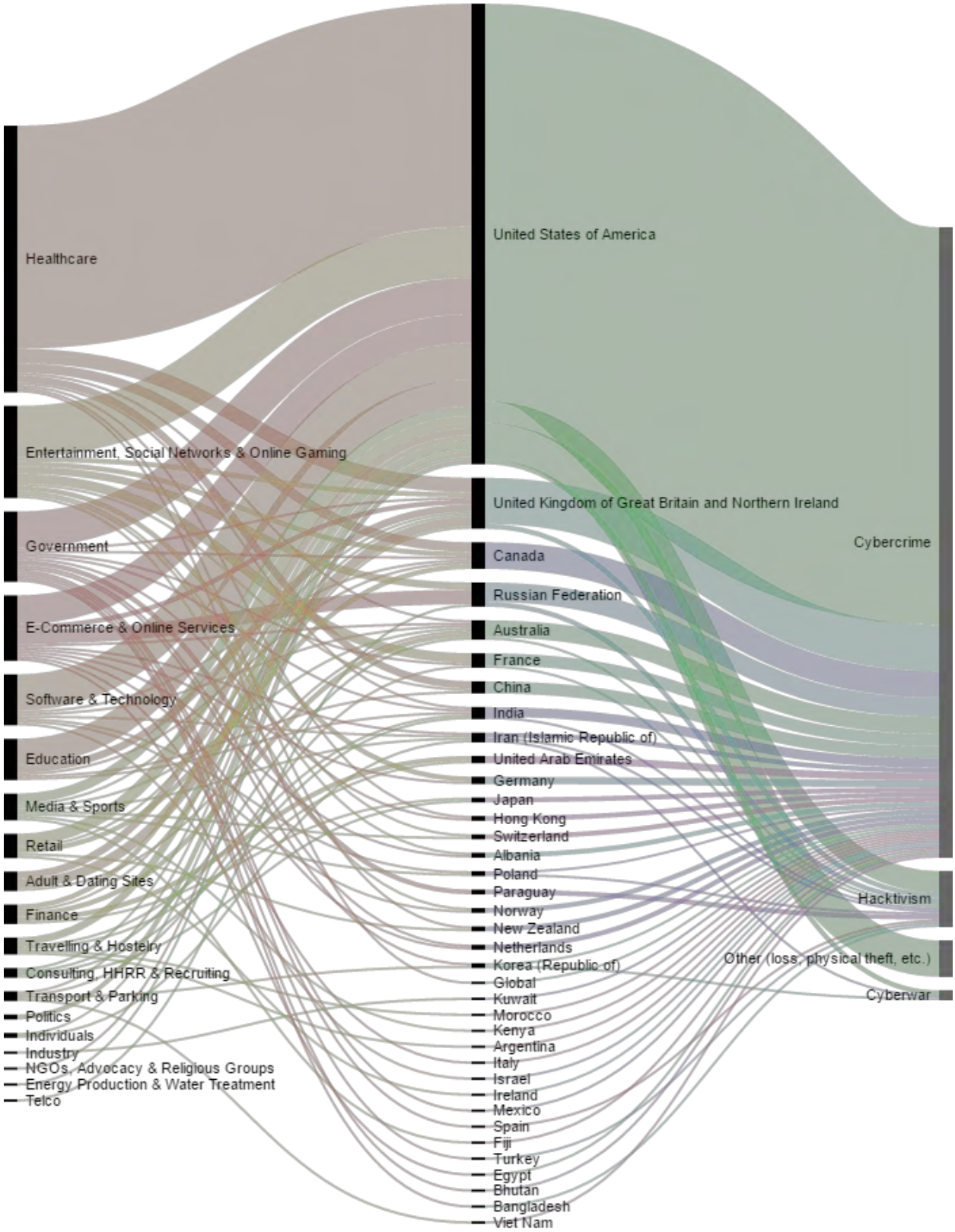

Figure 4. Incidents consummated during the second four months of 2016 grouped by sector, country, and motivation. *Source: prepared by the authors.*

If we look at who the most prolific authors were during this period, the fundamental reference is Peace o peace_of_mind [11] confirming its position during this period as one of the reference accounts in terms of the publication of databases of credentials. After offering some databases with the greatest media impact in marketplaces, this cyberidentity has become a media icon for the publication of these databases that, although old and which appear through private channels a short period of time later, have allowed the user to monetize its actions. However, the real affiliation of this profile is not clear, nor is its link to another profile that goes under the name Tess88 and that has also been privately supplying these databases to other sources.

Some of the authors that have leaked information are known from other previously published reports. Profiles such as SonnySpooks, 0x2Taylor, Ghost Squad Hackers, or bRpsd are also well-known accounts in the field of the public filtration of information leaks. In any case, the identification of many of these profiles as publishers of the information leak does not necessarily imply that said profiles are the original leakers, this considering that they may simply be accounts that echo the leaks after obtaining them through other means in specialized forums and IRC channels, or Jabber rooms. In the Table I we can see that most of the incidents have not been able to be conclusively attributed to any account.

Table I. Recognized authorship for incidents in the first four months of 2016. Source: prepared by the authors.

Author	Number of incidents
anon	11
SonnySpooks	8
Peace	8
bRpsd	4
0x2Taylor	4
ElSurveillance	3
Scrub	3
mitm3r	3
Pravy Sector	2
Sonny	2
Ghost Squad Hackers	2
imtolame	2
Other actors (one incident per perpetrator)	40
Incidents whose authors remained unidentified	213

In any case, even though authorship has not be claimed in all cases it has been fairly diverse, even when the actions have been linked to hacktivist movements. Similar to what occurred in the first four months of

2016, the origins of the identified security breaches are, to a significant degree, linked to external actors as can be seen in the Figure 5.

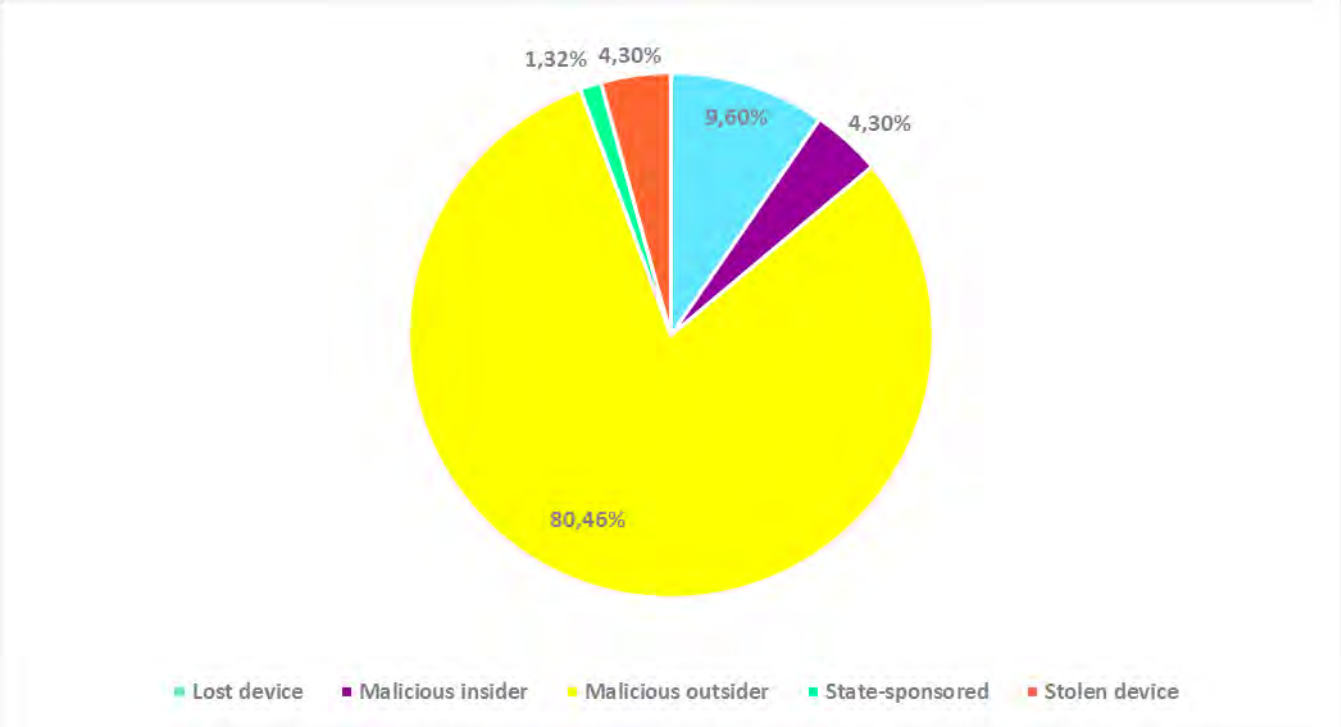

Figure 5. Origins of the attack leaks in the second four months of 2016. *Source: prepared by the authors.*

3.2.Per volume of credentials

During the previous four months, the health industry was one of the most affected sectors, followed by the education industry and government agencies; when taken together, these three areas totalled more than half of the leaked user records. Although they are still an important number of the total incidents that have taken place during the period, as seen in the Figure 4, the proportion of leaked user credentials is not maintained mainly because of the magnitude of the filtered leaks in the field of social networks.

The diversity of the affected industries was reduced during this period. The publication of a large number of databases linked to social networks and videogame platforms (MySpace, Twitter, and Tumblr are good examples), have cornered a large part of the exposed credentials, followed by others that also appear in a recurring manner among the most affected: electronic commerce platforms, government websites, and platforms for adult platforms and those linked to dating sites. The fact that the organisms in many countries linked to the health industry are legally forced to report possible security incidents they may be aware of leads to a large number of low criticality preventive reports for the loss of equipment and intrusion alerts.

Figure 6. Volume of leaked credentials per sector during the second four months of 2016. *Source: prepared by the authors.*

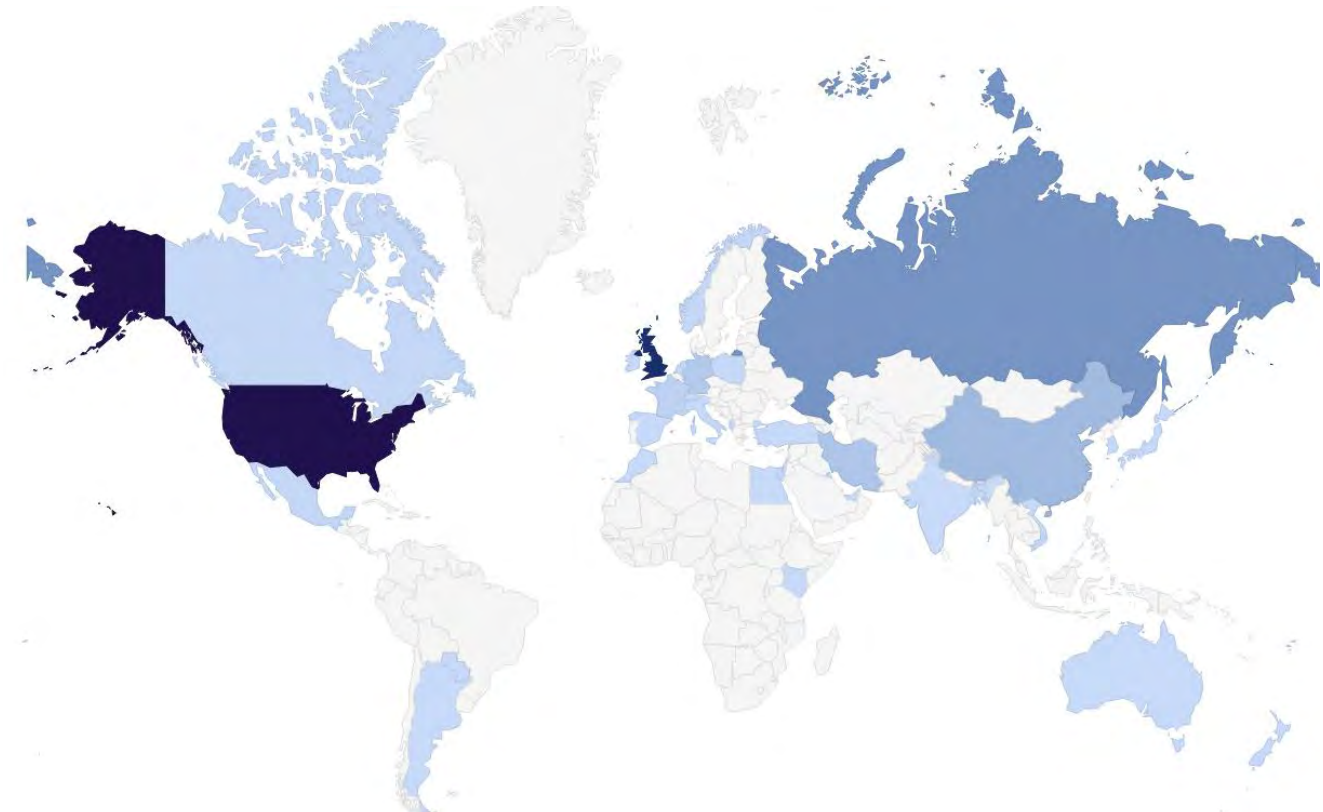

Figure 7. Volume of credentials leaked per country of the affected platform. *Source: prepared by the authors.*

When considering the localization of the affected services, practically four out of every five leaked credentials during this period correspond to credentials belonging to platforms located in the United States. Standing out among the remaining affected countries are the United Kingdom (country which had the leaks that affected Fling and Badoo), and Russia (especially pointed out for the leaks linked to Mail.ru). In any case, the fact that the distribution of the affected accounts does not necessarily correspond to this information has to be taken into account because the allocation does not obey criteria linked to the geolocation of the exposed users but rather the origin of each platform itself.

4.Nature of the leaked information

Following the trend marked in the first four months of 2016, the information of the greatest interest for cybercriminals is that which offers the possibility of being exploited directly. Even so, the sensitivity of said information will be marked by the profile of the affected sites and by the nature of the data itself, data that could also be used for practices associated to spear phishing or the cyberextortion of specific objectives linked to dating sites or even against minors in blackmail events linked to sextortion [12, p. 9].

4.1.Passwords: the main objective

As is normally the case, one of the aspects that garners the most media attention of a leak, besides the leak of personal information, is the publication of passwords together with the rest of the personal information identified in the database. When the results are compared to those of the first four months of 2016 [2, p. 14], we can see that a significant part of the leaked databases have exposed hashed passwords in their different formats.

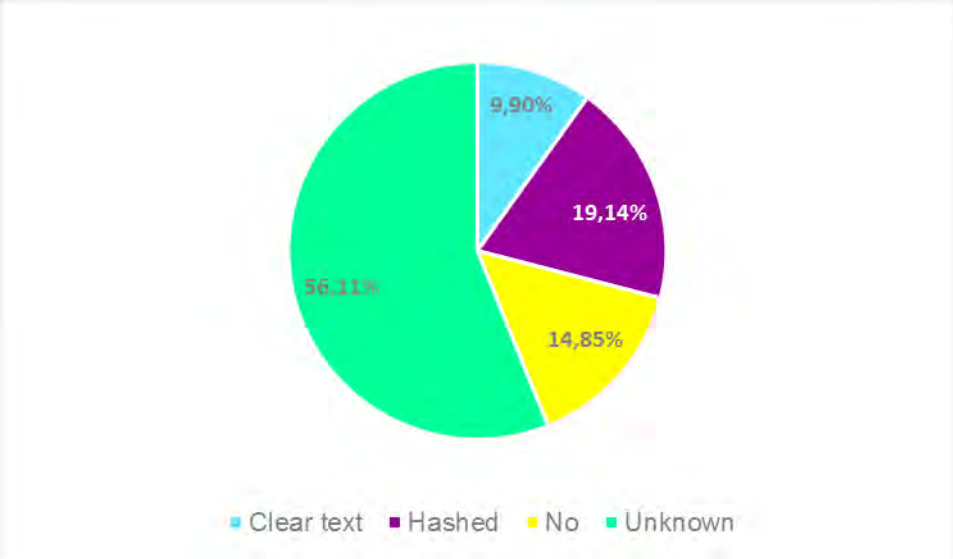

Figure 8. Password formats identified in the incidents registered in this period. *Source: prepared by the authors.*

However, despite the fact that the relationship between the number of incidents in which clear text passwords were leaked and those incidents where the passwords were hashed is practically 2 to 1, the fact that the volume of hashed credentials is greatly superior to that of clear text passwords has been able to be confirmed. This is because the information leaks with more significant volumes correspond to high profile domains that have set minimum security standards (although these standards are often insufficient, such as the storage of the password hash without including any kind of salt), which also implies an a posteriori layer of additional protection for users whose credentials have been exposed.

While clear text passwords barely represented 6.5% of the total in 2015 (although they appeared in 42.6% of all attacks), [1] during the first four months of 2016 these passwords accounted for more than three quarters of all leaked credentials that included passwords [2, p. 16]. During this period, the trend has reversed itself and the proportion is practically 9 to 1 as can be seen in the Figure 9, exceeding 1.14 billion *hashed* credentials and 113 million clear text passwords.

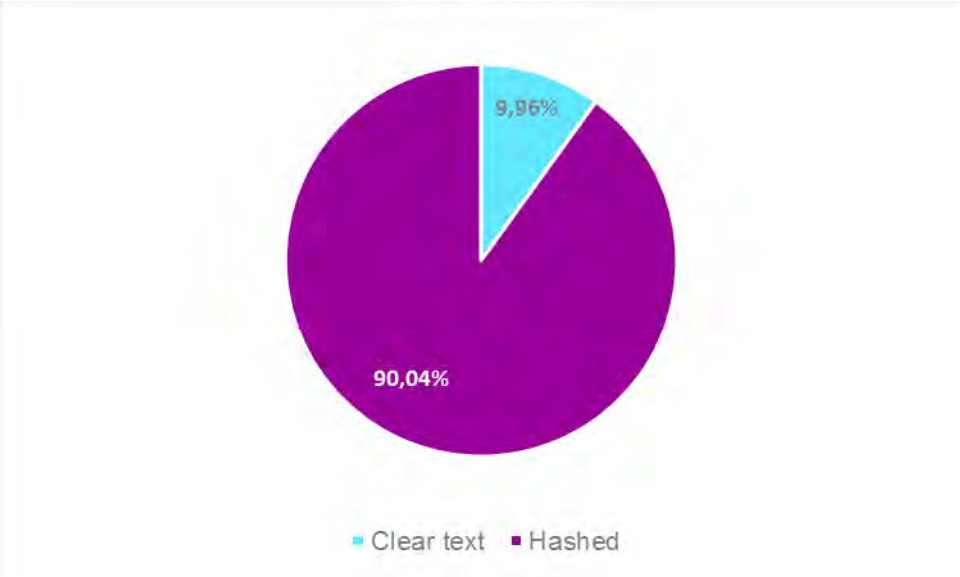

Figure 9. Comparison of leaked passwords that include clear text passwords in comparison to the number of credentials that include hashed passwords in any form. *Source: prepared by the authors.*

Among the motives behind said change in the trend is the high profile of many of the platforms that have been victims of the major information leaks published during these four months. The fact that platforms such as LinkedIn (ranked 14 in the Alexa ranking as of the date of this report's preparation), Dropbox (ranked 73), or MySpace (top 2400), have been implicated has not only caused massive information leaks that have affected millions of users, but has also raised the issue of the existence of some minimum security measures.

Due to how widespread the practice of reusing passwords in different services is, their leak is a problem in and of itself. Throughout these months we have seen different automatic verification processes of exposed credentials in third party assets such as Github [13] using the passwords that have already been exposed in other information leaks as reference.

Apart from mass verification, the analysis of the leaked clear text passwords can be used as an indicator for disclosing complete passwords or patterns in the generation of said passwords that may be being used in other databases where the information is hashed. The fact of having real relevant samples is a good approach to the generation of ad hoc dictionaries that include complex patterns that would be difficult to generate using brute force, conventional dictionary attacks, or other hybrid approaches.

4.2.The interest for other fields

As occurred in prior editions of this report, the leaks in this period have exposed information of different natures if we consider the characteristics of the exposed fields. As we can see in the Figure 10, among the most repeated fields whose presence has been able to be confirmed are, in the following order, emails, *passwords* (both in clear text and *hashed*), aliases, and full names. There still remain numerous leaks where we can also associate the profiles to postal addresses, IP addresses, and telephone numbers, providing an idea of the realization of the profiling that could be undertaken. Also specially significant is the information linked to highly protected personal information, considering that up to 13 security breaches have

already been identified, breaches that may include information regarding medical records, police information obtained without authorization from the investigated party, and sexual tastes and/or preferences.

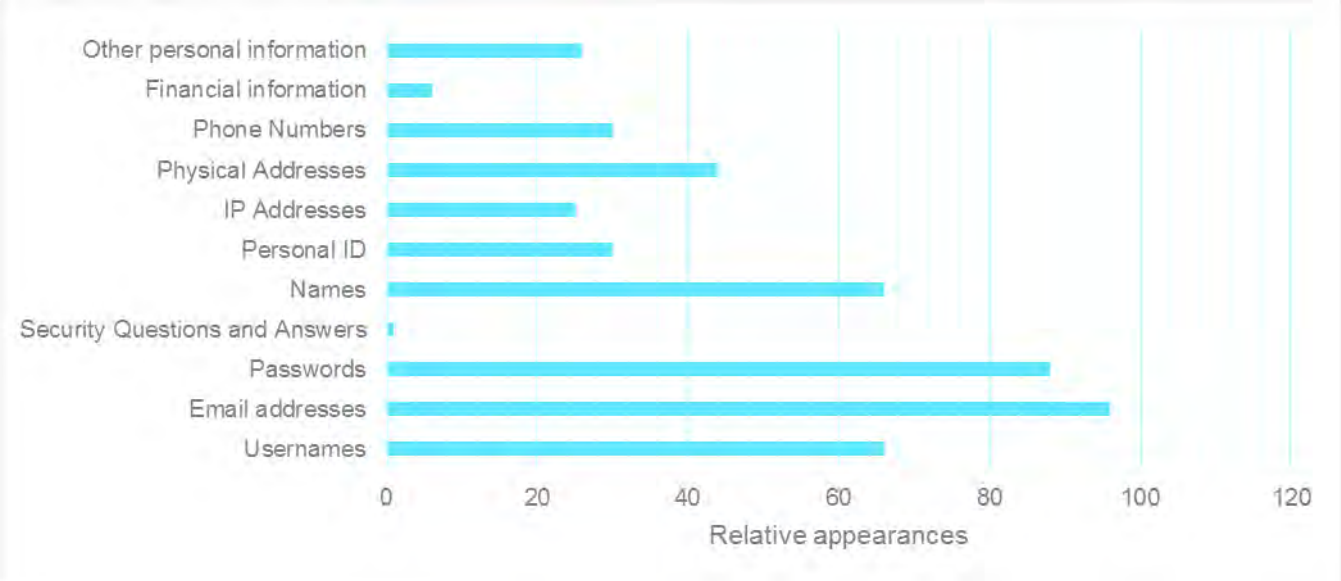

Figure 10. Number of analysed leaks in which each one of the different fields appears.

5.Recommendations

Although the fact that some of the data published is already several years old has been able to be verified, the information obtained in these incidents can also be used to materialize other types of attacks that go beyond each service resetting or not the passwords of the users of that platform. The comfort of reusing the same credentials in different websites therefore implies a real risk even when the passwords are not identical. The fact that these may expose patterns regarding the habitual structure of a user's passwords is a risk factor that has to be considered and put into the context of information leaks that many times imply personal and professional information.

The normal recommendations can be extended to this period. On the one hand, avoid reusing passwords by periodically changing the passwords used. The use of password managers that are responsible for generating complex versions of said passwords is another favourable point considering that the user will need to remember a single highly complex password. Furthermore, the configuration of two-step authentication systems is a desirable additional security measure that will protect the user from unauthorized connection attempts that may access their password one way or another.

Even though both of these measures are headed in the right direction, we can't lose sight of the fact that they will not protect the user in case the platform is compromised. This circumstance, which months ago may have appeared limited to medium or low profile pages, has also been proven to affect platforms such as LinkedIn, Dropbox, or Tumblr. In any case, even in situations where a leak occurs in some of these platforms the use of robust passwords that cannot be linked to the user is a practice that would serve as protection.

From the point of view of the attacker, having access to personal information is an element that can be exploited in different ways of extortion, in the manner already used in dating site platforms. Similarly, the information can also serve to configure phishing attacks with higher probabilities of success using details recovered from the information leaks that expose personal information.

In any case, the volume of leaked information in this period has been exceptional. The practically consecutive leaks of databases linked to high profile platforms has increased the interest towards this type of information leak beyond the media. During this period, the number of services that now offer monitoring and alert services regarding the leak of information linked to both personal and corporate emails has multiplied. By offering these types of services, these platforms are acquiring knowledge regarding the existence of email accounts in multiple services thanks to the queries made by users about their own accounts, knowledge that would, in any other way, be difficult to acquire. Unfortunately, and though some platforms offer the user the possibility of avoiding the query of certain information, the decision to trust, or not, one platform or another, is many times left up to the user.

Bibliography

[1] Eleven Paths, «2015: el año de las fugas de información,» 22 12 2015. [Online]. Available: https://www.elevenpaths.com/es/nuevo-informe-sobre-las-principales-brechas-de-seguridad-2015-el-ano-de-las-fugas-de-informacion/. [Latest access: 27 10 2016].

[2] Eleven Paths, «The Biggest Data Leaks of the First Four Months of 2016,» 01 06 2016. [Online]. Available: https://www.elevenpaths.com/new-report-the-largest-data-leaks-of-the-first-quarter-of-2016/index.html. [Latest access: 27 10 2016].

[3] Eleven Paths, «Linkedin Information Leak,» 30 05 2016. [Online]. Available: https://www.elevenpaths.com/research-report-linkedin-data-leakage/index.html. [Latest access: 27 10 2016].

[4] Eleven Paths, «Dropbox Information Leak,» CyberSecurity Shot, 12 09 2016. [Online]. Available: https://www.elevenpaths.com/dropbox-data-breach/index.html. [Latest access: 27 10 2016].

[5] Eleven Paths, «Myspace Information Leak,» 06 06 2016. [Online]. Available: https://www.elevenpaths.com/investigation-report-myspace-data-leakage/index.html. [Latest access: 27 10 2016].

[6] J. Cox, «Anoher Day, Another Hack: User Accoutns of Dating Site Badoo,» Motherboard, 02 06 2016. [Online]. Available: http://motherboard.vice.com/read/another-day-another-hack-user-accounts-of-dating-site-badoo. [Latest access: 27 10 2016].

[7] Eleven Paths, «Neopets Information Leak,» CyberSecurity Shot, 27 09 2016. [Online]. Available: https://www.elevenpaths.com/wp-content/uploads/2016/09/CyberSecurity_Shot_Neopets_v1_1_EN.pdf. [Latest access: 27 10 2016].

[8] Eleven Paths, «iMesh Information Leak,» CyberSecurity Shot, 13 07 2016. [Online]. Available: https://www.elevenpaths.com/wp-content/uploads/2016/08/CyberSecurity_Shot_iMesh_v1_0_EN.pdf. [Latest access: 27 10 2016].

[9] A. Hern, «More than 65m Tumblr emails for sale on the darknet,» 31 05 2016. [Online]. Available: https://www.theguardian.com/technology/2016/may/31/tumblr-emails-for-sale-darknet-65-million-hack-passwords. [Latest access: 27 10 2016].

[10] Eleven Paths, «R2Games Information Leakage,» 19 07 2016. [Online]. Available: https://www.elevenpaths.com/r2games-information-leakage/index.html. [Latest access: 27 10 2016].

[11] Eleven Paths, «peace_of_mind,» CyberSecurity Avatar, 13 06 2016. [Online]. Available: https://www.elevenpaths.com/investigation-report-on-bozkurt-hackers-cyber-identity/index.html. [Latest access: 27 10 2016].

[12] Eleven Paths, «Cyberextortion, a Growing Industry,» Eleven Paths Reports, 25 02 2016. [Online]. Available: https://www.elevenpaths.com/es/nuevo-informe-la-ciberextorsion-una-industria-en-crecimiento. [Latest access: 27 10 2016].

[13] P. Ducklin, «Github hit by massive password guessing attack,» Sophos, 16 06 2016. [Online]. Available: https://nakedsecurity.sophos.com/2016/06/16/github-hit-by-massive-password-guessing-attack/. [Latest access: 27 10 2016].

Annexes

The following is a list of other information that is complementary to the material provided in this report, information that helps to determine the scope of the recovered information as well as the procedures followed for incident evaluation.

5.1.Annex A. Methodological annex

This annex provides details of other complementary information not previously defined in the methodology section regarding the evaluation process for each of the

5.1.1.Risk assessment

Each of the k leaks mentioned has been evaluated according to a formula that establishes an objective risk value for each leak i. The obtained value $R_i(n_i, o_i, d_i, t_i)$ is located on a scale between a minimum of 0 and maximum of 10, and takes into account the volume of leaked credentials, the suspected attackers' motivations, the availability of the leak and the nature of the leaked records. Judgement criteria for a leak i:

- The base $RB_i(n_i)$ risk as a function of the number of credentials n_i relative to the logarithm in base 10 of the number of leaked credentials: $RB_i(n_i) = \log n_i$

- The risk according to the origin o_i of the leak $RO_i(o_i)$, giving a higher score to those actors with greater abilities to carry out compromising activities against the victim. $RO_i(o_i)$ it is assessed as follows:

$$RO_i(o_i) = \begin{cases} 1 & si\ o_i = State-sponsored \\ 0{,}75 & si\ o_i = Malicious\ insiders \\ 0{,}50 & si\ o_i = Malicious\ outsiders \\ 0{,}25 & si\ o_i = Stolen\ device \\ 0 & si\ o_i = Lost\ device \\ 0 & si: o_i = Other \end{cases}$$

- Risk according to the availability of the leak $RD_i(d_i)$, defining those leaks with a broader circulation perimeter as the most severe:

$$RD_i(d_i) = \begin{cases} 1{,}00 & si\ d_i = Available \\ 0{,}50 & si\ d_i = On\ sale \\ 0{,}00 & si\ d_i = Not\ available \end{cases}$$

- Risk according to the type of leaked information $RT_i(t_1, t_2, \ldots t_k)$, with greater weight given to more sensitive information for user identification:

$$RT_i(t_1, t_2, \dots t_k) = \sum_{j=1}^{k} \begin{cases} 0{,}1 & si\ t_i = Usernames \\ 0{,}2 & si\ t_i = Emails \\ 0{,}2 & si\ t_i = Hashed\ passwords \\ 0{,}5 & si\ t_i = Clear\ text\ passwords \\ 0{,}1 & si\ t_i = Sequerity\ questions \\ 0{,}2 & si\ t_i = Names \\ 0{,}2 & si\ t_i = IP\ Addreses \\ 0{,}2 & si\ t_i = Phones \\ 0{,}2 & si\ t_i = Physical\ addresses \\ [0, 0{,}5] & si\ t_i = Financial\ data \\ [0, 0{,}5] & si\ t_i = Other\ personal\ information \end{cases}$$

In cases where not all the available information can be had or it has not been possible to establish it, all the modifiers will be made equal at 0.

$$R_i(n_i, o_i, d_i, t_1, t_2, \dots t_k) = RB_i(n_i) + RO_i(o_i) + RD_i(d_i) + RT_i(t_1, t_2, \dots t_k)$$

5.1.2. Victims' activity sectors

The victims of each of these incidents have been catalogued according to the focus of their main activity based on the following categories:

Sector	Description
Adult & Dating Sites	Dating contact sites, web pages of a pornographic nature or classified as adult pages, except for online games.
Consulting, HR & Recruiting	Companies dedicated to consulting or service provision, as well as HR and recruiting or attracting talent.
E-Commerce & Online Services	Online service provision or e-commerce platforms as sub-categories of the same
Education	Training companies, universities or other initiative institutions.
Energy Production & Water Treatment	Energy production, water treatment and other infrastructure dedicated companies.
Entertainment, Social Networks & Online Gaming	Entertainment, social network and online gaming-related companies
Finance	Financial and investment systems.
Government	Public organisms, including FCSE
Healthcare	Public health, hospitals, clinics and medical treatments.
Individuals	Individuals
Industry	Industrial sector, machine tools.
Media & Sports	Media and sports organisations.

Sector	Description
NGOs & Religious Groups	NGOs, activist groups and religious organisations
Politics & Advocacy groups	Political parties.
Retail	Retail sector.
Software & Technology	Software development and technology equipment companies.
Telco	Telecommunications sector companies.
Transport, Travelling & Hostelry	Public transport, tourism, travel agencies and the hotel business.

Table II. List of sectors for classification of the affected organisation and definition of the types of companies categorised within each sector.

5.2.Annex B. List of information leaks

This annex includes a list of the identified leaks which, for the purposes of this report, are graded as high or critical risk; in other words, with a risk index greater than 6:

DATE	TARGET	SCORE	FILTERED ACCOUNTS	COUNTRY
02/05/2016	remotestaff.com.au	6.90	99 888	Australia
04/05/2016	Kroger/Equifax W-2 Express	6.13	431 000	United States of America
05/05/2016	Neopets	10.00	26 892 897	United States of America
06/05/2016	nulled.io	7.98	599 080	United States of America
06/05/2016	Fling.com	9.41	40 767 652	United Kingdom of Great Britain and Northern Ireland
06/05/2016	Nulled.IO	8.08	599 080	United States of America
07/05/2016	leoprinting.co.uk	6.27	14 958	United Kingdom of Great Britain and Northern Ireland
09/05/2016	Kiddicare	7.40	800 000	United Kingdom of Great Britain and Northern Ireland
11/05/2016	Medical Colleagues of Texas	6.74	68 631	United States of America
13/05/2016	fijilive.com	7.33	106 334	Fiji
15/05/2016	Lookbook.nu	8.24	1 100 000	United States of America
17/05/2016	Linkedin	10.00	167 370 940	United States of America

DATE	TARGET	SCORE	FILTERED ACCOUNTS	COUNTRY
18/05/2016	Mexican Voter Database #2	6.32	2 072 585	Mexico
24/05/2016	raas.com.au	6.30	5 045	Australia
25/05/2016	Stamford Podiatry Group .P.C	6.91	40 491	United States of America
25/05/2016	bitaraf.com	6.66	72 928	Iran (Islamic Republic of)
26/05/2016	MySpace	10.00	359 420 698	United States of America
27/05/2016	PayPalSucks Database 102k	6.51	102 000	United States of America
31/05/2016	umoveindia.com	7.07	18 446	India
02/06/2016	Badoo	10.00	112 005 531	United Kingdom of Great Britain and Northern Ireland
04/06/2016	CiCi's Pizza	6.53	600 000	United States of America
04/06/2016	Tumblr	9.72	65 469 298	United States of America
06/06/2016	uTorrent	6.39	388 000	Albania
07/06/2016	Twitter	9.31	32 000 000	United States of America
08/06/2016	1394store.com	6.51	20 410	United States of America
11/06/2016	zoosk.com	9.72	52 319 612	United States of America
13/06/2016	iMesh	10.00	49 467 477	United States of America
13/06/2016	T Mobile's Czech Subsidiary	6.93	1,500,000	Canada
14/06/2016	Several forums hosted by VerticalScope	9.25	45 000 000	United States of America
21/06/2016	Carbonite	6.68	1,500,000	United States of America
22/06/2016	U.S. Voter/Amazon/Google	8.19	154 000 000	United States of America
25/06/2016	comcast.net	8.67	590 299	United States of America
26/06/2016	Medical Records from three companies in Missouri, Georgia, & Midwest	6.32	655 000	United States of America
27/06/2016	U.S. health insurer	7.47	9 300 000	United States of America

DATE	TARGET	SCORE	FILTERED ACCOUNTS	COUNTRY
28/06/2016	World-Check Database	8.24	2 200 000	United States of America
29/06/2016	Muslim Match	6.68	150 000	United States of America
30/06/2016	crackingforum.com	7.32	660 999	United States of America
04/07/2016	Mac Forums/ HotScripts / Hosting Talk	6.66	1 442 602	United States of America
07/07/2016	www.epilepsymichigan.org personal info	6.09	39 000	United States of America
08/07/2016	Penton Network - 5 databases belonging to the media company Penton	8.46	1 442 602	United States of America
08/07/2016	Amazon	6.62	83 899	United States of America
09/07/2016	NETGEAR router attack - 2731 logins	6.24	2 731	United States of America
09/07/2016	Netia SA	8.48	957 525	Poland
10/07/2016	Dota2	8.28	1 923 972	United States of America
10/07/2016	Prosthetic & Orthotic Care (P&O) Care	6.47	23 565	United States of America
10/07/2016	Shadi.com	8.81	2 035 020	United States of America
11/07/2016	R2Games	9.56	22 695 241	China
12/07/2016	acparadise.com	7.24	55 181	United States of America
12/07/2016	sevendollarclick.com	6.94	109 458	Russian Federation
12/07/2016	fourdollarclick.com	6.56	45 813	Russian Federation
12/07/2016	pingpong.su	6.21	51 814	Russian Federation
13/07/2016	cheapassgamer.com	7.15	444 688	United States of America
14/07/2016	Clash of Kings	7.60	1 597 717	United States of America
14/07/2016	Ubuntu Forums	7.30	2,000,000	United States of America
15/07/2016	PinkDate.co.uk	6.23	67 118	United Kingdom of Great Britain and Northern Ireland
18/07/2016	aha-forums.com	7.75	178 781	Canada
18/07/2016	dealdatabase.com	6.41	81 314	United States of America

DATE	TARGET	SCORE	FILTERED ACCOUNTS	COUNTRY
19/07/2016	Erdogan Email	6.97	294 548	Turkey
20/07/2016	Edaboard	7.66	459 211	United States of America
20/07/2016	avast.com	7.63	423 329	United States of America
22/07/2016	Democratic National Committee (DNC)	6.20	20 000	United States of America
27/07/2016	A group of clinics in Farmington, Missouri	6.86	29 153	United States of America
01/08/2016	Vietnam Airlines	7.71	411 000	Viet Nam
01/08/2016	Yahoo!	6.80	200 000	United States of America
02/08/2016	Banner Health	7.97	3 700 000	United States of America
02/08/2016	Iranian Telegram Users	8.48	15 000 000	Iran (Islamic Republic of)
02/08/2016	parsiva.daba.co.ir	6.42	52 000	Iran (Islamic Republic of)
08/08/2016	RedStation.co.uk Emails	6.40	496 825	United Kingdom of Great Britain and Northern Ireland
12/08/2016	Valley Anesthesiology and Pain Consultants (VAPC)	7.55	882 590	United States of America
16/08/2016	I-Dressup.com	8.94	2 210 703	France
16/08/2016	I-Dressup.com (part 2)	8.74	4 389 297	France
16/08/2016	socialblade.com	6.44	273 086	Canada
18/08/2016	DLH.net (Dirty Little Helper) Main	8.81	3 264 710	Germany
18/08/2016	DLH.net	8.15	9 000 000	Germany
18/08/2016	Leet.cc	8.78	6 084 276	United States of America
22/08/2016	SCAN Health Plan	6.64	87 000	United States of America
22/08/2016	Unreal Engine Forum	7.11	808 000	United States of America
23/08/2016	LateChef.com	7.13	54 221	United States of America
23/08/2016	gragaming.com	6.50	200 000	United States of America
23/08/2016	mylloyd.com	6.69	30 638	Iran (Islamic Republic of)
24/08/2016	GTAGaming.com	7.59	196 742	United States of America

DATE	TARGET	SCORE	FILTERED ACCOUNTS	COUNTRY
24/08/2016	Funcom	6.36	228 000	Norway
24/08/2016	Idaho Department of Fish and Game	7.70	788 064	United States of America
24/08/2016	Kentucky Department of Fish and Wildlife	8.13	2 126 449	United States of America
24/08/2016	cfire.mail.ru (Crossfire)	9.11	12 881 787	Russian Federation
24/08/2016	parapa.mail.ru (Parapa City)	8.96	9 015 764	Russian Federation
24/08/2016	tanks.mail.ru	8.51	3 236 254	Russian Federation
24/08/2016	Oregon Department of Fish and Wildlife	7.88	1 195 204	United States of America
24/08/2016	Three Mail.ru Forums: cfire.mail.ru, parapa.mail.ru, tanks.mail.ru	9.40	25 000 000	Russian Federation
24/08/2016	Washington State Department of Fish & Wildlife	8.19	2 435 452	United States of America
25/08/2016	ExileMod.com	6.92	83 122	United States of America
26/08/2016	Delta-Stresser.xyz	6.02	10 366	Russian Federation
26/08/2016	Dropbox	9.74	68 648 009	United States of America
26/08/2016	Opera Web Browser Sync System	7.03	1 700 000	Norway
27/08/2016	ClixSense.com	9.28	2 424 784	United States of America
30/08/2016	Arizona and Illinois voter database	6.70	200 000	United States of America
30/08/2016	Minecraft World Map (minecraftworldmap.com)	6.05	71 000	United States of America
31/08/2016	The New York State Psychiatric Institute	6.04	21 880	United States of America

About ElevenPaths

At ElevenPaths we believe in the idea of challenging the current state of security, a characteristic which should always be present in technology. We are continually rethinking the relationship between security and people, with the aim of creating innovative products capable of transforming the concept of security and thereby keeping one step ahead of our attackers, who are increasingly present in our digital lives.

Further Information

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com