Cyber Intelligence – Using Profiling

Alexandru Ciprian Angheluș[1], Oana Buzianu[2],

Mircea Constantin Șcheau[3]

[1]Prodefence, Romania, contact@prodefence.ro

[2]Wintech, Romania, oana.buzianu@wintechconsulting.ro

[3]University of Craiova, Romania, mircea.scheau@edu.ucv.ro

1. A potential definition of profiling

One approach for such a definition presents profiling as a way to collect from various sources, obtain, deduce, or predict information about groups or individuals. Such knowledge can be exploited to make decisions that can be later automated.

Profiling can structure public and private information with different degrees of precision, including those that are highly sensitive, like personal data/ information. Therefore, the data collected about a person's behavior can be used to generate/ predict new information about the "real" identity, attributes, interests or "probable" personality of the target subject.

In a world where some actions are constantly monitored, profiling raises serious questions and calls for urgent answers about privacy when private information can be deduced from larger or smaller seemingly trivial data sets.

How do we ensure that profiling (and the decisions it generates) is legal, fair and non-discriminatory?

How can data subjects exercise their rights (especially the right to object to, or oppose automated decision-making) if the processing itself is nontransparent?

Integration algorithms could be extremely complex and can deliver different results, depending on the expectations and interests of analysts. Building on Machine Learning capabilities, profiling automates such inferences and predictions by expanding databases such as location and contacts.

For example, if someone visits a website that presents serious health issues and then calls their surgeon, we can assume that he is thinking of going to a health service soon. Building on Machine Learning capabilities, profiling automates such inferences and predictions by relying on expanding databases such as location and contacts.

Anyone who has access to large amounts of Internet traffic can create Internet usage profiles for every visible user profile on the Internet, all they have to do is "just" collect cookies, super cookies IPs, the fingerprint the browser referrers and all of the types of identifying indicators (e.g. target detection identifiers or presence events), which on their own have very little meaning, but once you have association and links between them you start to build a detailed profile of an Internet user.

The Internet browsing allows understanding of your political affiliations, your religious beliefs, your sexual orientation, friends, family, colleagues (etc.) and build this detailed profile. And this is possible only if the traffic passes through equipment that attackers can control, or that they own. If you'd have already given away your identity at some point in the past and that has been stored in a surveillance database on all of these associations, or groups of hackers, cross-references would allow your identification almost instantly (for example the association between your browser and X number of IP addresses).

A person from outside your approved group gets to know your preferences and adapt quickly to manipulate you, completely ignoring the concepts related to autonomy and ethics.

Some encryption techniques do actually prevent most of this uncontrolled dissemination of information at national and international level, intensifying efforts to adapt legislation both in respect for individual rights and on other technical means of mass surveillance, with the role of maintaining national security and protection of citizens.

2. Relevance of profiling in the cyber-intelligence context

Structured information about a cyber-entity, independent groups or economically and logistically supported units, can provide answers regarding the individual's personality, the activity, the manner of operation and the motive behind the actions. Such fingerprints allow the development of countermeasures, adapted to the required situations.

Cyber-attacks can be classified according to several criteria, the diversity of technical resources facilitating the intersection or parallel development of several aggressions from different areas. There are cases in which a cyber-attack is a portal or launch pad for other totally different attacks, the multitude of scenarios and the negative effects reflected on the victims being theoretically limited only by imagination.

The risk of deficit for danger/impact awareness (e.g. “What should it take for me?” or “Why me, because I am not interested?”) can generate an impressive number of cascading problems, directly and through contamination, if the element of interconnectivity is a web page that contains an aggregate amount of data about the individual.

For example, the attacker can send messages to acquaintances, customers, employees or partners of a company under different pretexts:

- Sending infected visible, attached or hidden files;
- Fraud attempts;
- Illegal requests for personal data;
- Phishing attempts etc.

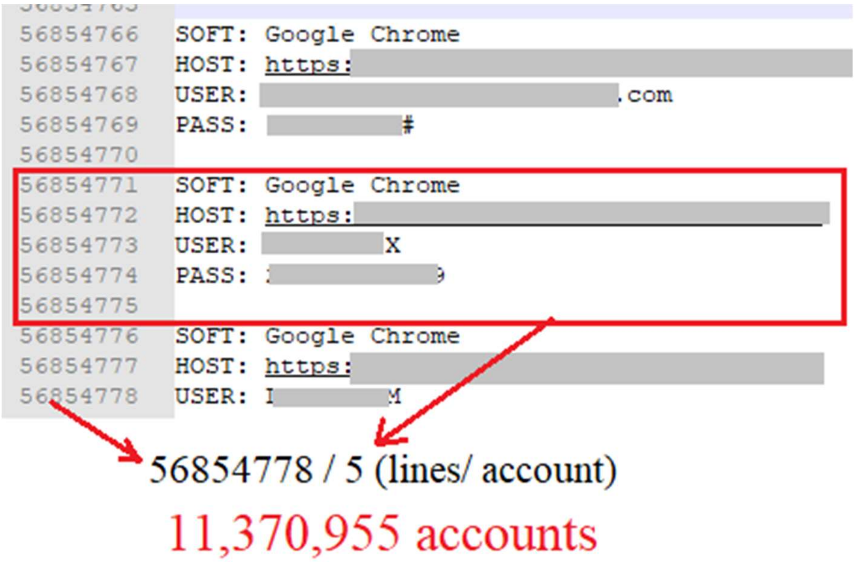
The study is based on cyber aggression aimed at leaked information from non-proprietary devices and a list of over eleven million compromised accounts, initially sold on the Darkweb and then made public.

List content:

c:\users\administrator\desktop\country + IP

SOFTWARE: BrowserX
HOST: https://www.domain.
USER: User
PASS: Password

registering at least 5 accounts for each victim.



```
56854766   SOFT: Google Chrome
56854767   HOST: https:[redacted]
56854768   USER: [redacted].com
56854769   PASS: [redacted]#
56854770
56854771   SOFT: Google Chrome
56854772   HOST: https:[redacted]
56854773   USER: [redacted]X
56854774   PASS: [redacted]
56854775
56854776   SOFT: Google Chrome
56854777   HOST: https:[redacted]
56854778   USER: [redacted]
```

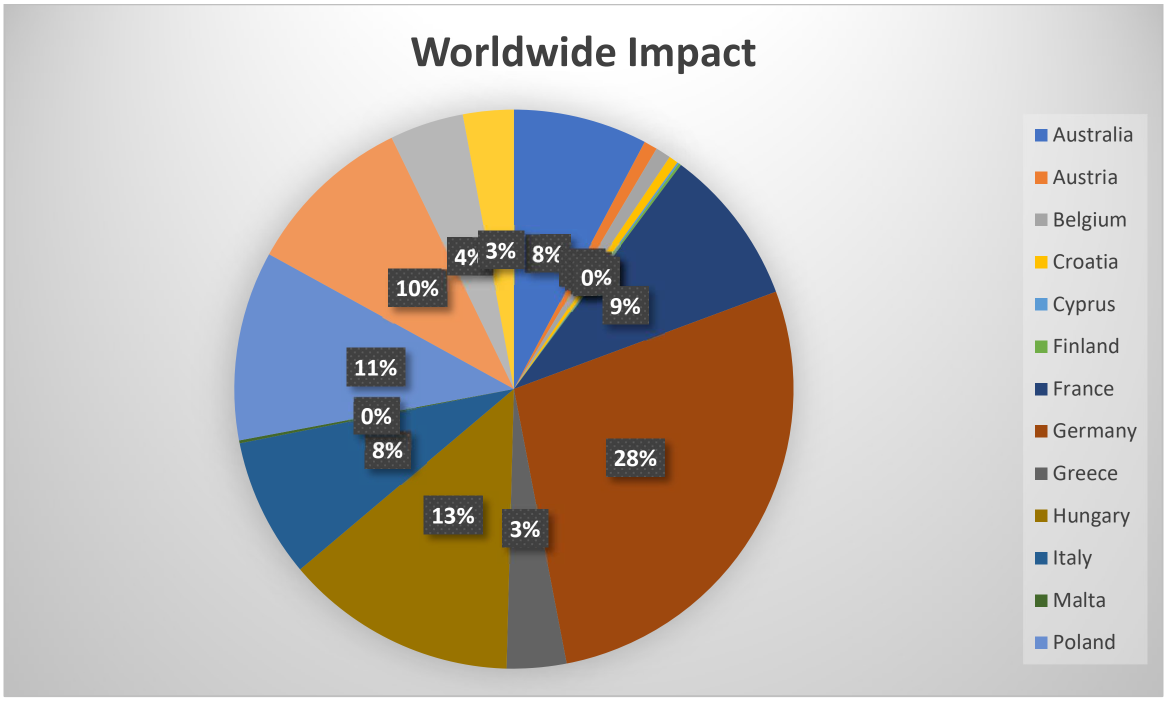
56854778 / 5 (lines/ account)

11,370,955 accounts

3. Target considerations

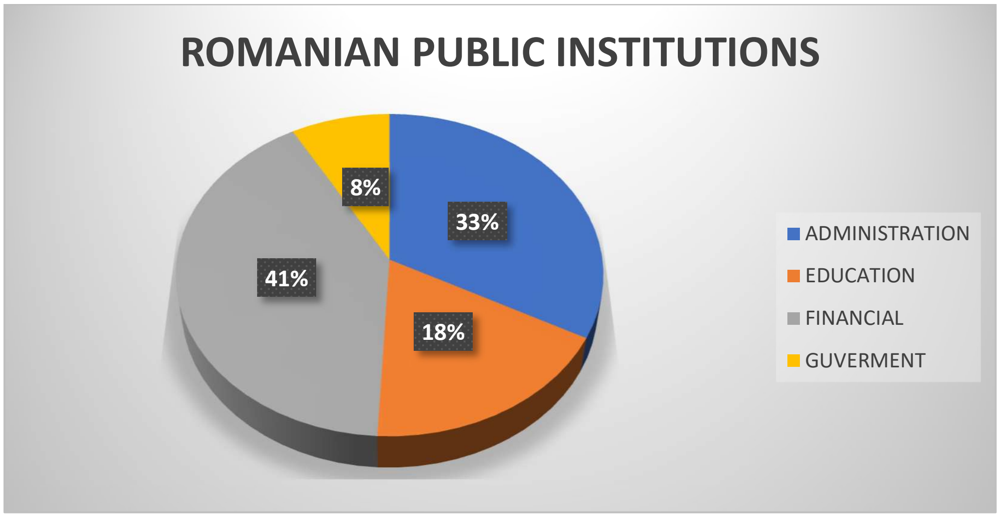
Attackers exploit malicious files (e.g.: stealer, keylogger, rat, botnet, ransomware, etc.) inserted in applications considered "fashionable", eagerly desired by enthusiasts (e.g.: crack for software or games, license generators, fake hacking applications, etc.) or attached to emails (e.g.: Emotet) with exciting topics. We will focus only on these types, because otherwise the analysis would become particularly complex.

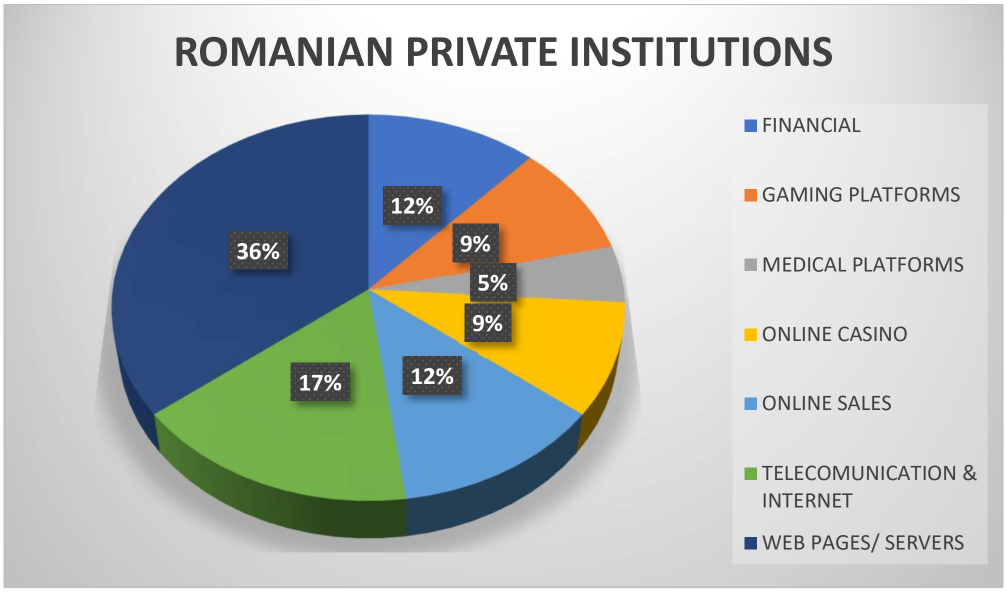
The victims are located in different geographical areas, which confirms the wide distribution, diversity and intensity of the campaigns.

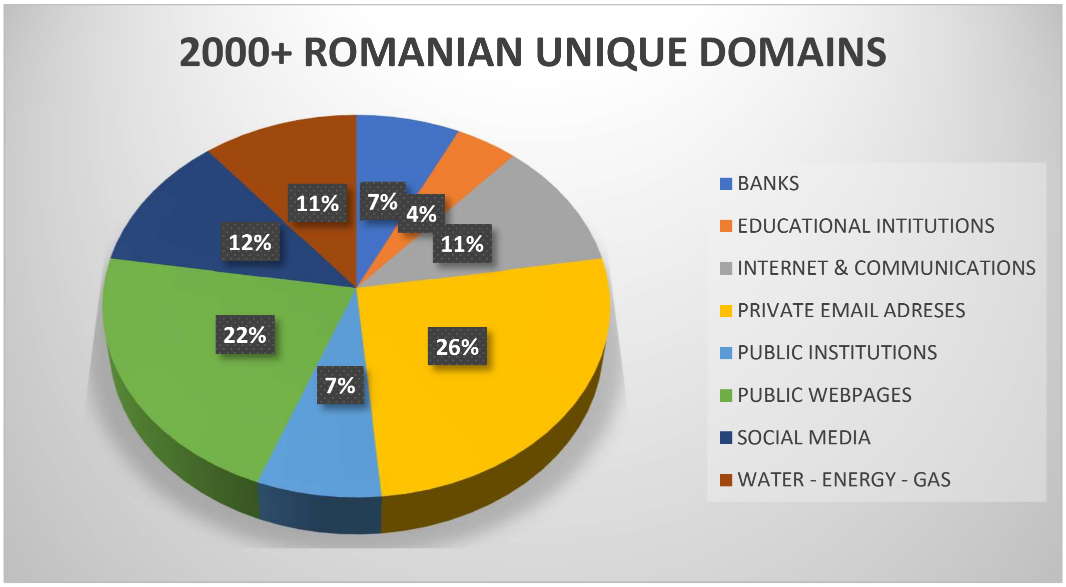


The list of personal and professional accounts of the target victims belongs to both the institutional and the private domain. The main areas affected:

- Public institutions;
- Government bodies;
- Banking companies;
- Energy & Gas;
- Social media platforms;
- Online sales platforms;
- Servers & Web Pages;
- Email accounts, etc.


ROMANIAN PUBLIC INSTITUTIONS
8%
33%
41%
18%
ADMINISTRATION
EDUCATION
FINANCIAL
GUVERMENT


ROMANIAN PRIVATE INSTITUTIONS
12%
36%
9%
5%
9%
12%
17%
FINANCIAL
GAMING PLATFORMS
MEDICAL PLATFORMS
ONLINE CASINO
ONLINE SALES
TELECOMUNICATION & INTERNET
WEB PAGES/ SERVERS



4. “Adrian” profiling

The issue of personal data and the danger to which we are exposed due to the collection about information activities, location, political orientation, family, name, address, telephone, etc. are constantly discussed. Sometimes, institutions, companies, social platforms, media are considered guilty, because data is used or sold through them, with the subsequent commercial, marketing, political, propaganda purposes etc..

We will introduce in the analysis below a lower degree of risk in order to illustrate the main steps taken for the use of profiles in cyber intelligence.

Many of the attacks have in common the HUMAN, especially if he/she activates in the attacker's area of interest. External compromise is much easier to implement if it is facilitated by an internal vulnerability.

Identifying the interests and the devices owned are necessary steps to create access points. If a victim does not have the necessary permissions in a system, the aggressor can use it as a way to access a target with more rights, the scenarios staged proving its effectiveness.

We start from the premise that our victim will be Adrian, a special employee, appreciated by colleagues and employer! The below aspects are an outline of the main steps that an aggressor/attacker could take and are mentioned here for illustrative purposes in order for the blue team members within organizations to understand the mechanisms used by aggressors/attackers and to implement measures to protect the organization (and the individuals related to the organization from such attacks).

Name: Adrian

Profession: Accountant

Employer: Critical Infrastructure X

An attacker can't do much with this data alone, but if he/she has access to a database like the one mentioned above, the attacker can try to outline a profile.

The attacker will include a series of data from those "found" about Adrian!

SOFT: Browser HOST: https://www.socialmedia_1.com/ USER: adi1991@zahoo1_mail.com PASS: Adri@n!007	SOFT: Browser HOST: https://www.payment_money.com/ USER: adi1991@zahoo1_mail.com PASS: Adri@n!007
SOFT: Browser HOST: https://www.socialmedia_2.com USER: adi1991@zahoo1_mail.com PASS: Adri@n!007	SOFT: Browser HOST: https://192.168.1.0/ USER: Admin PASS: 1234
SOFT: Browser HOST: https://www.zahoo1mail.com USER: adi1991@zahoo1_mail.com PASS: @gent007_ADI SOFT: Browser	SOFT: Browser HOST: https://www.software_top_1.com/ USER: adi1991@zahoo1_mail.com PASS: 12345678

HOST: https://mail. critical_infrastructureX.com USER: adrian.smith@ critical_infrastructureX.com PASS: @gent007_ADI	SOFT: Browser HOST: https://www.personal_page.com/ USER: Admin PASS: Adri@n!007
SOFT: Browser HOST: https://www.socialmedia_2.com/ USER: adi1991@zahoo1_mail.com PASS: Adri@n!007	SOFT: Browser HOST: https://www.socialmedia_1.com/ USER: adi1991@zahoo1_mail.com PASS: Adri@n!007
SOFT: Browser HOST: https://www.sexygirls_00.com/ USER: adi1991@zahoo1_mail.com PASS: 12345678	SOFT: Browser HOST: https://www.phone_line_0.com/ USER: adi1991@zahoo1_mail.com PASS: 12345678
SOFT: Browser HOST: https://www.webcamxxx_1.com/ USER: adi1991@zahoo1_mail.com PASS: 12345678	SOFT: Browser HOST: https://192.168.1.36:3204/ USER: root PASS: root
SOFT: Browser HOST: https://member.university_edu.com/ USER: adrian.smith@university_edu.com PASS: Adri@n!007	SOFT: Browser HOST: https://www.social_dates.com/ USER: adi1991@zahoo1_mail.com PASS: 12345678

The outlined profile looks like the one below:

Name: Adrian Smith

Age: 2021 - adi1991 = 30 years old (+ data from the social media profile)

Personal e-mail: adi1991@zahoo1_mail.com

Professional e-mail: adrian.smith@critical_infrastructureX.com

University e-mail: adrian.smith@university_edu.com

Job: Accountant at Critical Infrastructure

Phone: 074XXXXXXX (exists in social media profiles)

Passwords used: Adri @ n! 007, @ gent007_ADI, 12345678

Activities, family, locations: Visible in social media accounts

More intimate occupations: webcam girls, social dates, etc.

Router access: Probably home, because the accountant does not have access to the router (so it should…)

Device access: Root on a device that can be a storage of personal data, so a lot of information and documents

Software license: Software_top_1.com

Online payment platform access: payment_money.com

As you can see, the attacker begins to collect personal and professional information, then the attacker can diversify sources for additional data about the individual. Basically, if the attacker would want to sell Adrian something, it wouldn't be difficult to identify something "interesting" for Adrian, but he attacker's intentions in this case are not noble. In addition, the set of passwords used can be helpful in the attacker's attempt to compromise accounts that do not appear in the above list. As a result, we will build below some examples of approach and attack scenarios that could be considered by the attacker!

Scenario 1

The attacker could prepare an e-mail for Adrian, he/she could send it to him as coming from the software vendor and could offer him the last improved version, the one which "only" loyal customers receive. The attacker could download the application, attach a virus to it and forward it to Adrian for download.

Or, through the same method, the attacker could send him a confidential "video" from Maria on webcamxxx_1.com.

Scenario 2

The attacker could read Adrian's messages from the e-mail platforms and he/she could see who he talks to, what his current topics are, his way of sending / receiving documents. After which the attacker could act:

• The attacker could send an infected document to a colleague or boss;

• The attacker could request the login data in the system under a certain pretext on its behalf;

• The attacker could request information from the company that maintains the system, or we ask for certain changes;

• If there is a document location for certain employees, the attacker could exchange the files with some infected ones.

Scenario 3

Depending on what the attacker found on the web cam or dating platforms, the attacker could blackmail him by exposing discussions, photos or videos and try to obtain confidential information about the employing company and specialized software.

In the first stage, Adrian Smith becomes a target with multiple possibilities of exploitation and can help the attacker move to the next level. It has become a path to reach the goal (e.g. partner company).

Nevertheless, in this short description, we did not bring the real danger/impact into question and the possible effects could be devastating. Losses can have a snowball effect and can reach amounts having many zeroes.

5. Critical infrastructure exploitation

Scenario 1

With the help of the victim (or victims), depending on the magnitude of the initial attack, it was possible to access the Institution information system, which was part of the list of critical infrastructures, and this was known from the beginning by the attacker, his target being, we suppose that, earning a consistent financial profit. We said "suppose", because actually, the attack on a critical infrastructure can mask the interests of ideologically motivated entities.

With a good access level to exploit, the attacker will try to compromise any devices or servers connected to the original compromised system.

We will consider as the first version of attack the infection of the systems with ransomware sequences capable of extensive compromise, with the role of delay and even totally cancel any attempt to recover the system by internal employees of the IT department, or by external companies specialized in security and protection. By encrypting servers and damaging or destroying backup archives, among the few options to restart the victim accessible activity are rescues performed on external storage devices, unrelated to the company system, or the online environment. Otherwise, the solution followed by the attackers is to pay the requested amount for decryption.

Of course, this option did not take into account the case where the only interest of the aggressors is to destroy the systems, a situation in which risk indicators can undergo a serious exponential evolution.

Scenario 2

After accessing the system, which also includes the e-mail server of the critical infrastructure, the attacker could take all the necessary measures to maintain it, opening a series of loopholes, then beginning data and information collection. He could try to be as quiet as possible in the actions carried out in the system, not to arouse suspicion. This is the classic approach to industrial espionage.

6. Countermeasures

The answer to the question "What can be done?" is as simple as it is complex: Cyber Education for non-technical users!

Technology and cyber-attacks have increased in the last decade and even if we were quickly overwhelmed by the situation, we continue to be very close to the same level of training - precarious. Emphasis is placed on the training of specialists, but in front of computers there are people (the large masses) who are not aware of the danger behind the extensive use of technology, or who do not have sufficient capacity to integrate into the new paradigm of technology.

We are talking about complex passwords with special characters and thus arises a new question: "What is the difference between a very complex password and 1234?"

The difference is made by a password manager: an application that can save the desired passwords in an encrypted form, or can deliver a browser password also in an encrypted form.

In addition to these, there are the following: 3D Secure systems, double validation systems, etc.

It is strongly recommended to purchase a protection solution, because developers implement a series of patches, updates against compromised soft or hard devices and browsing pages with malicious content.

Further potential preventive measures that can be implemented will be detailed in a separate article subsequently.

It is also recommended to follow the activity of the National Incident Response Center Romania - CERT-RO (https://cert.ro/) and of Cyberint (https://www.sri.ro/cyberint), in order to be able to find out in due time about the new methods of attack, but also prevention methods!

7. Conclusions

Fraud, data theft, malware infection, etc. can be combated by user education, regardless of their position or status in an institution. Specialists can get involved in this process, as long as users perceive this approach as an opportunity and make efforts to adapt to the new requirements, challenges, working conditions, cyber playground, education… which mostly takes place online!

Another aspect is the freedom of communication, the courage to ask, the ability to admit that you do not know, etc. Sometimes we avoid asking for help, believing that it can negatively influence our image, but in fact, the effect is exactly the opposite. We cannot be specialists in everything, but we have the power to collaborate, to bring our contribution in a positive way and therefore, in the fictitious case set out in this article, to save, maybe, Adrian's reputation and job!

And not only his own…