DOI: 10.2507/31st.daaam.proceedings.024

CROATIAN BANK SECURITY ANALYSIS BY PUBLICLY AVAILABLE DATA

Ena Matvej, Zlatan Morić & Silvio Papić

This Publication has to be referred as: Matvej, E[na]; Moric, Z[latan] & Papic, S[ilvio] (2020). Croatian Bank Security Analysis by Publicly Available Data, Proceedings of the 31st DAAAM International Symposium, pp.0184-0188, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-29-7, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/31st.daaam.proceedings.024

Abstract

No system is perfect, especially given the factor of human error. Banks' IT systems are interesting to potential attackers because of the magnitude of potential damage to customer data, reputation, and banks' finances. All the bank employees' data could be used as a potential vector of attack which represents major security risks that must not be neglected. In this paper, it is analyzed how many publicly available sensitive information about 10 major banks that are active in the Republic of Croatia is possible to collect by using simple and free tools to see if there are any potential security risks for these banks. The paper begins with the introduction of tools and methods used in gathering information. All gathered data is then compared to see which of the banks are most exposed to potential attackers. The subject of system security has been analyzed many times. Some papers describe penetration testing, social engineering in case of attack, data gathering tools, but this paper incorporates all before mentioned theories and provides concrete data gathering results on which the level of risk is determined and suggestions for preventive measures.

Keywords: bank security; reconnaissance; data confidentiality; OSINT

1. Introduction

Today it is normal for most of us to have at least one social media account. From an IT security perspective, this fact can be used to gather important and potentially sensitive information that could be used for launching an attack against the infrastructure of companies whose employees are present on social media. Although social media presence does not seem to be a security issue for most people it is surprising how many information is available publicly and could be used against an individual or the company for which individual works for. Using only publicly available information collected through different free and simple tools an attacker can do some inciteful reconnaissance to learn about his potential target. Ordinary photographs of a pet dog with a dog's name could be a security issue because a lot of employees are using their pet names as a password or part of their password. This kind of information collecting using publicly available sources like newspapers, Internet, books, blogs, social media, etc. is known as Open-source intelligence (OSINT) and as we are publishing more and more personal data online, it is becoming security paramount to take this into account when devising companies security strategies. This is the case all around the world as well as in Croatia. One special type of companies that are of particular interest to attackers are banks and other financial organizations.

In this paper, the authors are trying to determine how much publically available sensitive data is there among the ten biggest banks in Croatia to see if there is a reason for concern. Because of a large number of customer databases and of course potential financial damage. Banks also have a large number of employees so there is a good chance that some of them if not most of them are using the Internet and social media in their private lives. Also, there is a chance that employees are a part of some online community that has something to do with their actual job in the bank which is a useful channel to learn about more sensitive information about the banks' infrastructure, procedures, personnel, and business in general. If one can find out who are these employees and what are their interests they become very susceptible to different social engineering attacks like phishing attacks [1] and revealing more sensitive information. This digital footprint is what attackers will try to use to extract useful information and use this information in the attack on the banks' infrastructure to cause damage or to steal data.

Because of this and many other forms of cyber-crime companies are investing more and more resources trying to tackle this challenge by investing in infrastructure, procedures, developing methods and methodologies [2], and employees' education as the most important part of preventing this kind of data collecting effort by the attackers. Also, governments are trying to legally tackle this issue with different rules and regulations as well as technological solutions to protect the online identity of their citizens from malicious individuals [3]. This paper is a report of short research and analysis of the top ten Croatian banks using six criteria to see what kind and amount of sensitive data is publicly available without using any complex tools and privileges or illegal action. For this purpose, different data collecting tools are used which are publicly available and easy to use. This availability and ease of use mean that anyone could do this sort of research and analysis, and one can only imagine what is possible by using sophisticated tools and actions that are illegal which is not a problem for people with bad intentions and a high level of knowledge and skill.

2. OSINT short overview

OSINT or Open Source Intelligence in short is any information or data that is publicly available on the Internet. This also includes Deep Web and Dark Web but also it encompasses information available publicly by other means like newspapers, commercials, job advertisements, counting people in and out of the bank at certain periods of the day or month, or any other form of information that does not require any kind of access rights or permissions. This data, if analyzed properly can revile important information that is supposed to be secret like for example operating systems or equipment that an organization uses or what are critical elements of a particular IT system. All of us are using OSINT every day without even realizing it. We use Facebook, Instagram, Linked-in to learn something about our friends or to check out someone interesting, and so on. But aside this innocent usage of OSINT this kind of information is used also by law enforcement, private investigators, military and secret services but also by hackers and terrorists. One example of using OSINT is when rebels in Ukraine shoot down an aircraft using a surface to air (SAM) missile and posted video about it on the internet [4].

People using this information from social media, car dash cameras, and Google street view found the location of the launch site and evidence of SAM launch site as well as the movement of this weapon system. This is a good example of what is possible if one wants to put some effort and use only freely available information. This is important to keep in mind because in times of crisis one wants to know what is possible to know about the reality of the situation. Using OSINT in a clever way it is possible to indirectly learn all kinds of information that others do not want one to know like for example how many soldiers are in the barracks by knowing how many toilet paper is shipped into barracks and what is the norm per person. As technology develops and more people start using this technology the amount of publically available data will only increase which will become more of a security issue. A short search on the internet can show us how data breaches are becoming numerous and more severe [5] and because users are using the same credential for business accounts that have become a great security concern. Analytical tools are also becoming ever simpler and require less specific skills to be used to extract relevant information. As mentioned earlier average person maybe does not care about their data being publically available or eve wants their data to be visible, but if this behavior is demonstrated for occupation like military pilots or secret service employees, or banks' employees the problem becomes obvious. Imagine a situation where ninety percent of military pilots of some country have publicly available Facebook or Linked-In profiles where they post photographs, activities, and location of their whereabouts it is easy to conclude.

This is very problematic, especially in the case of escalating arms conflict where this kind of personnel is invaluable. One of the major challenges with OSINT is misinformation which is deliberately published to mislead the investigation or to manipulate public opinion. This is maybe an even darker side of technology development regarding information. People are the end recipients of the information whether the information is true or not. If one has the opportunity and skills to present false information as true and people receiving the information do not possess the required critical thinking skills, one can influence critical aspects of society like democratic elections and practically determine the direction of the entire society. One can expect that as more information is available the more risk there is for influencing national policies through the manipulation of the average person without critical-thinking skills. Especially because photos and videos are becoming a dominant source of information for most of the people which by itself without context is not a good source of information. The average internet user does not research to verify the source of the information and with the development of Deepfake technology [6], it will be practically impossible to distinguish fact from fiction, and that is a potentially dangerous situation for the society as a whole [7].

3. About the tools used

Tools that are used in this paper to gather OSINT on Croatian banks are all open source freely available tools that anyone can use. This is an important fact because today it is possible for a person with a basic skill set to do what twenty or thirty years ago only governments could do in the context of information gathering and analysis. And in the same context criminals are catching up with nation-states in hacking capabilities [8]. Just to illustrate how much data is easily accessible through the Internet one can start by using the osintframework.com web page, which is just a tip of an iceberg, where we can find hundreds of OSINT sources which can be used to learn about people, companies, or places to do reconnaissance before potential cyber-attack or any kind of campaign against the target [9]. The main tools and services used in this paper are social platforms LinkedIn and Facebook, Google, archive.org, Wayback Machine (integrated into archive.org), Spiderfoot, Shodan, and Maltego.

Service archive.org [10] is an online library that contains millions of web pages, books, music, movies, and other content. Using the tool Wayback machine which is an integral part of archive.org is possible to browse webpages years back and see the old information contained in snapshots even older than 20 years. Because security was not such a big topic 20 or more years back it is possible to find useful information about the behavior of some companies for example banks and learn how they behave and what kind of employment policies they are using, what type of experts they employ and learn about technologies used etc. In this paper, archive.org and Wayback machines were used to find out information about bank employees so that they could be investigated further.

Bank's current web page is also very useful because of all the names and contacts of employees which can then be researched further by looking at their social media accounts like Facebook, Twitter, LinkedIn to learn about expertise, political views, or any other characteristics that might be useful later. By learning only about the expertise of the person we can learn about technologies used in the bank system. In this paper, employees' names were additionally researched using Facebook, LinkedIn, Google, and Maltego. An especially useful tool was LinkedIn where the names of other employees were found with their skillsets and other useful information.

Spiderfoot [11] is another simple tool that was used in this paper and the main usage of this tool is for the automation of the OSINT process. To automate OSINT, Spiderfoot queries over 100 public information sources and processes all the intelligence data from domain names, email addresses, names, IP addresses, DNS servers, and much more to find connections between the data. For example, if we want to learn about a certain bank's web page Spiderfoot will discover IP addresses, emails in this domain, phone numbers, physical addresses, open server ports, operating system versions, leaked passwords from email accounts if there are any, and other information.

Shodan [12] is a search engine for finding Internet-connected devices, unlike Google which is optimized for finding web sites and documents on the Internet. Maltego [13] is a software used for open-source intelligence and forensic which focuses on providing a library of transforms for the discovery of data from open sources and visualizing the information suitable for link analysis and data mining.

These tools used in this paper, although available to anyone are also used by the police, military, intelligence agencies, different companies as well as hackers and criminals [14].

4. Methodology

In this research and analysis of available OSINT for the ten biggest Croatian banks combination of previously mentioned tools was used. The first tool that was used was archive.org to find as much as possible information about employees like names and email addresses which then were used on LinkedIn to learn about their competencies and skillset as well as their affiliation with a bank and other banks employees.

Spiderfoot and Shodan were used to find information about technologies used on web servers and Maltego was used to learn about the DNS structure of the bank's infrastructure and email addresses of the employees that were compromised. For comparison of the banks, six criteria were used. Every criterium represents potentially useful information about the bank and the total quantity of gathered information was compared. One could say that the more available information could correlate to lower Cyber Security efforts on part of the bank.

Criteriums are as follows:

- Criterium 1: Information published by employees on social media, blogs, and forums
- Criterium 2: Information from job adds (current and archived)
- Criterium 3: Information about web servers
- Criterium 4: Information about email addresses that were compromised
- Criterium 5: Information about applications on web servers
- Criterium 6: Technologies used on web servers

5. Results

In this chapter, results are presented in the table per each of the criteria stated before for all ten banks. In table 1, banks are ordered based on the total number of sensitive information found going from lowest to highest. It is important to note that this number by itself does not give the real incite in the cybersecurity of the specific bank. To have this information, further analysis should be conducted based on the size of the bank, the number of employees, services offered, etc. nevertheless these numbers could be used as an input that could point in the direction of critical elements that could easily be tackled to make banks system more secure.

These findings also can suggest that there is a lack of adhering to procedures and security policies that banks must have which in turn can suggest that there is a need for more employee's education on the importance of cybersecurity. Better education and strict security policies would greatly improve many incidents related to compromised email addresses and leaked passwords. It is also interesting to note that things like technologies used on web servers and versions of operating systems, although easily attainable, could become critical if it turns out that a certain version of an application or operating system has a flaw that could be exploited for an attack. To decrease the possible risk of exploiting flawed systems, regular patching of applications and the system itself is highly recommended. Many comparisons could be done, and different speculations could be constructed from this data. For example, if we compare Croatia bank and Sberbank, both banks have no information about job positions but there is a significant difference in compromised email accounts.

One could speculate that there is a difference in the level of cybersecurity education between employees of these two banks and attackers could try to use this for some kind of social engineering attacks which are becoming more elaborate and more frequent [15]. On the other hand in the case of Sberbank, there is information about job positions and the kind of tasks their employees are expected to do which could be used to learn more about the IT system itself, while in the case of Croatia bank there is no such information. Of course, this would require in-depth research and analysis using more expensive and sophisticated tools and skills.

Bank	Criterium 1	Criterium 2	Criterium 3	Criterium 4	Criterium 5	Criterium 6	Total
OTP banka	2	1	2	2	1	1	9
Addiko Bank	0	0	3	1	1	6	11
Podravska banka	0	0	3	1	5	2	11
Zagrebačka banka	4	2	2	5	0	0	13
Sberbank	4	0	4	3	0	7	18
Croatia banka	0	0	2	16	0	0	18
Raiffeisen Bank	4	6	2	5	3	2	22
Erste&Steiermärkische Bank	4	3	3	6	3	5	24
Privredna banka Zagreb	3	6	4	7	3	2	25
Hrvatska poštanska banka	3	9	3	39	1	4	59

Table 1. Quantity of gathered information

6. Conclusion

Although this paper shows basic reconnaissance using only OSINT and freely available and simple to use tools it was possible to gain much useful information. It is evident that in the hands of malicious individuals or groups this publicly available and easily attainable information could be used as a starting point for much more sinister steps to gain more sensitive information using sophisticated tools, methods, and skills. Of course, people will continue to use the internet in a private and business context and it is not possible or desirable but one of the most important things is to educate people on the dangers and risks of putting their information on the Internet publicly available. There are many kinds of information that people want to share and it is not possible to know which piece of information will be used in what way by whom. That is exactly why education about Cyber Security and OSINT is mainly focused on the principles that are easily understood and implemented for example do not use the same password for all your accounts.

7. Further research

Based on this paper further research and analysis of Croatian banks' exposure should be done using specialized tools and services carried out with a rigorous methodological approach executed by a team of Cyber Security experts in cooperation with IT Security personnel form banks in question. This approach will give better incite and legitimacy on which concrete steps could be taken to make Croatian banks but also other financial institutions more resilient to cybersecurity threats. Based on this more in-depth research one could make regulatory guidelines to make more uniform practices among banks so that the banking system in Croatia becomes more robust and impervious to various more and more sophisticated cyber-attacks.

8. References

[1] Svoboda, J & Lukas, L (2019). Sources of Threats and Threats in the Cyber Security, Chapter 27 in DAAAM International Scientific Book 2019, pp.321-330, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-24-2, ISSN 1726-9687, Vienna, Austria DOI: 10.2507/daaam.scibook.2019.27

[2] Kafol, C & Bregar, A (2017). Cyber Security – Building a Sustainable Protection, Chapter 07 in DAAAM International Scientific Book 2017, pp.081-090, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-12-9, ISSN 1726-9687, Vienna, Austria DOI: 10.2507/daaam.scibook.2017.07

[3] Zharova, A; Elin, V & Panfilov, P (2018). Technological and Legal Issues of Identifying a Person on the Internet to Ensure Information Security, Proceedings of the 29th DAAAM International Symposium, pp.0471-0478, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978- 3-902734-20-4, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/29th.daaam.proceedings.069

[4] Higgins, E. (2015). MH17 - The Open Source Evidence, Available from: https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/ Accessed: 2020-08-20

[5] McCandless, D.; Evans, Z.; Barton, P.; Starling, S.; & Geere, D. Information is beautiful, IDTheftCentre and media reports, Available from: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ Accessed: 2020-05-31

[6] K. Krombholz, H. Hobel, M. Huber & E. Weippl (2013). Social Engineering Attacks on the Knowledge Worker, Proceedings of the 6th International Conference on Security of Information and Networks, pp. 28-35, Aksaray, Turkey, ACM

[7] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review, Available from: https://timreview.ca/article/1282/ Accessed: 2020-08-19

[8] Vavra, S, (2019). National Security Council cyber chief: Criminals are closing the gap with nation-state hackers, Available from: https://www.cyberscoop.com/cybercriminals-nation-state-tools-grant-schneider/ Accessed: 2020-08-19

[9] Nordin, J. OSINT Framework, Available from: https://osintframework.com/ Accessed on: 2020-08-31

[10] The Internet Archive, Internet archive, Available from: https://archive.org/ Accessed on: 2020-09-01

[11] SM7 Software OÜ, Spiderfoot, SM7 Software OÜ, Available from: https://www.spiderfoot.net/ Accessed on: 2020-09-01

[12] Matherly J. Shodan, Available from: https://www.shodan.io, Accessed on: 2020-09-1

[13] Maltego, Maltego, Available from: https://www.maltego.com, Accessed on: 2020-09-1

[14] Bule G., A Guide To Open Source Intelligence (OSINT), Available from: https://itsec.group/blog-post-osint-guide-part-1.htmle Accessed on: 2020-08-31

[15] Yasin, A; Fatima, R.; Liu, L.; Yasin, A.; & Wang, J (2019). "Contemplating social engineering studies and attack scenarios: A review study", Available from: https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.73. Accessed on: 2020-08-21