Scientific and Practical Cyber Security Journal (SPCSJ) 5(1): 35-39 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

USING OPEN SOURCE INTELLIGENCE (OSINT) AS ONE OF THE EFFECTIVE AND LEGITIMATE WAYS TO AVOID THREATS TO THE CORPORATION

Oleksii Kuchmai, Tetiana Shelest

Taras Shevchenko National University of Kyiv, 24 B. Gavrilishyna St., Faculty of Information Technology, Kiev, 02000, Ukraine

ABSTRACT: Open source intelligence (OSINT) is an intelligence discipline that includes the search, selection and collection of intelligence from publicly available sources, as well as its analysis. In the intelligence community, the term "open information source" refers to the public availability of a source (as opposed to secret and restricted sources), but it is not related to the notion of "just a source of information" (English open source information; OSIF), which means any information in the media space.

KEYWORDS: *Cyber Intelligence, OSINT, Cybercrime, Threats, Company, Security*

Introduction

The current OSINT regulatory framework is based on the Directive of the Director of National Intelligence (2006) ICD 301 "National Plan for Intelligence Based on Open Sources". It defines the following strategic objectives of ROII: - the principle of "first step" - OSINT should be the "first step" for all intelligence disciplines and precede intelligence and intelligence by technical means; - reliance on specially trained groups of experts in the field of ROII, training in methods of obtaining open information and implementation of ROII technologies in all intelligence processes; - global coverage of information sources; - a single architecture of means, forms and methods of ROII; - the use of the principle of skunkworks, ie the introduction to solve certain problems of "breakthrough", highly intelligent methods of obtaining information with a minimum of bureaucratic red tape and restrictions. air force "[1].

Regulatory framework

The law enforcement OSINT community applies open-source intelligence to crime prediction, prevention, investigation, and prosecution, including terrorism. Search through social media and DarkNet plays a significant role in their work, and so does connection analysis [2]. With the sheer volume of content traffic transiting across the internet through social media platforms, law enforcement would be remiss to ignore social media accounts as a resource for discovering evidence potentially relevant to a variety of criminal investigations.

Private corporate security services are also eager to apply OSINT tools. They conduct individual checks: their own employees, top-management, employees, executive officers and shareholders of their contractors. 'Know Your Customer' (KYC) mode is on here. Is this an off-shore company or not? Who is the real owner? Hasn`t it been into any dark business? Knowing this is crucial before execution of any major deal.[3]

To check affiliation of individuals or entities - this is the main goal, as it is expressed usually. Economic security services monitor internal deals for hidden interest. For instance, if a procurement manager enters into transactions with entities belonging to his or her family members. Transaction services department runs check-ups before each merger or acquisition: whether a firm acquired is run by criminals. Thus, major companies endeavor to minimize reputational risks for the company, as for the shareholders. Each serious firm usually has its own list of reliable and non-advisable counter agents. In any case, management always has to know, who stands behind this or that entity[4].

Interesting cases of application of OSINT in insurance business have already come into our knowledge. They correlate to a company's personal data analysis, as so as to business analytics. A huge federal company notices that in one separate region payments for one separate insurance product have increased significantly.

Affiliation checks through social media of the company's region branch employees has shown that one of the managers had been insuring his or her friends and family in order to register insured accidents and payments afterwards. Such knowledge is still not an evidence of the person's guilt, but it sure is a matter for internal investigation.

HR departments [8] employ OSINT for running check-ups of actual or possible employees of their companies. Do they post any negative data on the company in their social media? Or maybe they disclose confidential information? Sometimes it happens not out of malice but accidentally [5].

Some public organizations perform constant monitoring of threats, including terrorist threats. For example, one Jewish studies organization form the USA uses Social Links for this exact purpose. They fear attacks or incidents during their events, so they perform such monitoring in order to prevent them.

A whole other group of goals is reached through OSINT: risk assessment, when information is collected in order to make a decision [10]. Due diligence procedure can be performed by a bank or by a consulting company, when the main goal is to run a complex assessment of the asset value. In such cases reputation, connections and beneficiaries' financial position matter.

Such check-ups, as so as affiliation search between employees and contractors, have been performed as far as business goes [8]. The matter is - how fast and how efficient, and how precise they may be. Internet, especially social media, gives us huge volume of data for analysis, but collecting data by hand would be too difficult, too long and too inefficient.

The main bonus of the OSINT tools is possibility to find and check all the necessary information with software. For example, a Social Links product requires one hour to gather such an amount of data from open sources, which a skilled worker would collect by hand in a week.

With Social Links you can mine data from 50+ socials, databases and use 700+ search methods empowered with Face Recognition and search by Geo-coordinates [13]. You will get unique searches in 30+ DarkNet forums and marketplaces without authorization by Phrase, PGP Key, Alias, also, you can get analytics by Products and Locations (shipping from/to).

Small businesses also arguably have the most to lose from being hit with a damaging cyber-attack. A recent report revealed that businesses with less than 500 employees lose on average $2.5 million per attack. Losing this amount of money in a cyber breach is devastating to small businesses, and that's not to mention the reputational damage that comes from being hit by a cyber-attack.

For these reasons, small businesses need to be aware of the threats and how to stop them. This article will cover the top 5 security threats facing businesses, and how organizations can protect themselves against them.[14]

1) Phishing Attacks

The biggest, most damaging and most widespread threat facing small businesses are phishing attacks. Phishing accounts for 90% of all breaches that organizations face, they've grown 65% over the last year, and they account for over $12 billion in business losses. Phishing attacks occur when an attacker pretends to be a trusted contact, and entices a user to click a malicious link, download a malicious file, or give them access to sensitive information, account details or credentials.

2) Malware Attacks

Malware is the second big threat facing small businesses. It encompasses a variety of cyber threats such as trojans and viruses. It's a varied term for malicious code that hackers create to gain access to networks, steal data, or destroy data on computers. Malware usually comes from malicious website downloads, spam emails or from connecting to other infected machines or devices.[15]

3) Ransomware

Ransomware is one of the most common cyber-attacks, hitting thousands of businesses every year. They've grown more common recently, as they are one of the most lucrative forms of attacks. Ransomware involves encrypting company data so that it cannot be used or accessed, and then forcing the company to pay a ransom to unlock the data. This leaves businesses with a tough choice – to pay the ransom and potentially lose huge sums of money, or cripple their services with a loss of data [16].

4) Weak Passwords

Another big threat facing small businesses is employees using weak or easily guessed passwords. Many small businesses use multiple cloud based services, that require different accounts. These services often can contain sensitive data and financial information. Using easily guessed passwords, or using the same passwords for multiple accounts, can cause this data to become compromised.

5) Insider Threats

The final major threat facing small businesses is the insider threat. An insider threat is a risk to an organization that is caused by the actions of employees, former employees, business contractors or associates. These actors can access critical data about your company, and they can case harmful effects through greed or malice, or simply through ignorance and carelessness. A 2017 Verizon report found that 25% of breaches in 2017 were caused by insider threats. [17]

This is a growing problem and can put employees and customers at risk, or cause the company financial damage. Within small businesses, insider threats are growing as more employees have access to multiple accounts, that hold more data. Research has found that 62% of employees have reported having access to accounts that they probably didn't need to [18].

Conclusion

There are a range of threats facing small businesses at the moment. The best way for businesses to protect against these threats is to have a comprehensive set of security tools in place, and to utilize Security Awareness Training to ensure that users are aware of security threats and how to prevent them.

REFERENCES

1. McLaughlin, Michael (June 2012). "Using open source intelligence [https://www.usersearch.org software] for cybersecurity intelligence". ComputerWeekly.com. Archived from the original on 2018-06-29.
2. The US Intelligence Community. ASIN 0813349184.
3. Gagnidze, M. Iavich, G. Iashvili, Some Aspects of Post-Quantum Cryptosystems, Abstract book, EURO-ASIA FORUM IN POLITICS ECONOMICS AND BUSINESS – 2016, JULY 21-22, 2016, BELGRADE, SERBIA.
4. "Spy Agencies Turn to Newspapers, NPR, and Wikipedia for Information: The intelligence community is learning to value 'open-source' information". Archived from the original on 2012-04-07. Retrieved 2008-09-15.
5. "As defined in Sec. 931 of Public Law 109-163, entitled, "National Defense Authorization Act for Fiscal Year 2006."". Archived from the original on 2008-11-12.
6. Richelson, Jeffrey T (2015-07-14). The U.S. Intelligence Community. Avalon Publishing. ISBN 9780813349190. Retrieved 15 May 2017.
7. George, edited by Roger Z; Kline, Robert D; Lownethal, Mark M (2005). Intelligence and the national security strategist: enduring issues and challenges. Lanham: Rowman and Littlefield. ISBN 9780742540392.

8. Bornn, D Marshall (9 Jan 2013). "Service members, civilians learn to harness power of 'Open Source' information". www.army.mil. Archived from the original on 9 December 2017.
9. Lowenthal, Mark; Clark, Robert (2015). The Five Disciplines of Intelligence Collection. CQ Press. p. 18.
10. (The Commission on the Intelligence Capabilities). Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction
11. "Reexamining the Distinction Between Open Information and Secrets – Central Intelligence Agency". www.cia.gov. Archived from the original on 2018-06-08. Retrieved 2018-06-29.
12. Hudnall, Ken (2011). "Intelligence Failures". No Safe Haven: Homeland Insecurity. Grave Distractions Publications. ISBN 9781452493923.
13. Kozlenko, M., Lazarovych, I., Tkachuk, V., Vialkova, V. Software Demodulation of Weak Radio Signals using Convolutional Neural Network
    2020 IEEE 7th International Conference on Energy Smart Systems, ESS 2020 - Proceedings, 2020, pp. 339–342
14. Zhengbing Hu, Sergiy Gnatyuk, Tetiana Okhrimenko, Sakhybay Tynymbayev, Maksim Iavich, "High-Speed and Secure PRNG for Cryptographic Applications", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.3, pp.1-10, 2020. DOI: 10.5815/ijcnis.2020.03.01
15. Zh. Hu, V. Kinzeryavyy, M. Iavich et al., "High-Speed Privacy Amplification Method for Deterministic Quantum Cryptography Protocols Using Pairs of Entangled Qutrits", CEUR Workshop Proceedings, vol. 2393, pp. 810-821.
16. Hubskyi, O., Babenko, T., Myrutenko, L., Oksiiuk, O. Detection of sql injection attack using neural networks //Advances in Intelligent Systems and Computing, 2021, 1265 AISC, pp. 277–286
17. Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and practical cyber security journal, 2019
18. Kovalova, Y., Babenko, T., Oksiiuk, O., Myrutenko, L. OPTIMIZATION OF LIFETIME IN WIRELESS MONITORING NETWORKS//International Journal of Computing, 2020, 19(2), pp. 267–272