36. OSINT IN CYBERSECURITY

Kudritskii N.I.

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Subbotkina I.G. – Associate Professor

This paper explores the fundamentals of OSINT, providing an overview of its key concepts, methodologies, applications and provides a description of some basic cybersecurity rules.

Nowadays data is one of the most substantial assets for every business and industry model. It is an essential element required to make or break the security mechanism of any organization's assets, network, or application. Every field is threatened by cyber-attacks, and information is the crucial element that cybercriminals aim at [1].

OSINT stands for open-source intelligence, which refers to legal information about individuals or establishments from public sources [2]. In practice, it means the information available on the Internet. Nevertheless, any public information falls into the category of OSINT: it's presented in books, journals, magazines, newspaper articles, posts on social media or statements in press release.

Open-source intelligence plays a vital role in information collection, which helps everyone, including security professionals, technical specialists, cybercriminals get necessary and essential data and information [3]. It helps to find digital footprints that are publicly accessible in any format, including videos, images, conferences, research papers, webinars. Besides compromised and breached credentials, popular business records and background information, documents and other material are discovered by using OSINT tools. The usage of these means is considered to be a legal activity as long as the person does not break the law or violates the copyrights.

There're three main sources of OSINT [4]:

- Dark Web.
  This source basically breaks the main rules of OSINT, such as diving into information without touching private information. Also, not the everyone can obtain the access to these resources, mainly because they are banned or not accessible from the "white" side of the Internet.
- Search Engines.
  Most people underestimate the power of various search engines. By using special search queries, one can acquire private information about different associations.
- Social Media.
  Recently it has become the most popular decision to gain information. Electronic gadgets are widely used for posting a lot of information to the Internet. There are some risks not to take into consideration some rules of self-security which can be used by hackers.

OSINT has advantages as well as disadvantages, OSINT can be used in both ways. Notably, in ethical hacking, OSINT helps to discover digital footprints in various cybersecurity assessments such as penetration testing, red teaming, social engineering. While utilizing available information, security professionals and certain organizations identify sensitive, exposed information that could allow any ill-intentioned hacker to use and initiate an attack on the critical assets [3]. By doing this, white hat hackers detect some vulnerabilities in security systems. On the other hand, OSINT is the most powerful, popular and legal tool for everyone, who wants to damage your reputation and receive the information which is extremely important. Technically, the goal of any hacker before attacking a system is to receive as much information about a target as possible.

Currently, Open-source intelligence is being used professionally in different kinds of fields. Everyone relies upon publicly available and usable data. Besides cybersecurity experts, OSINT is highly used by a huge group of professionals in the field of law enforcement officers, students and writers, investigators and journalists, military man [2].

References:

1. What is OSINT (Open-Source Intelligence). [Electronic resource] – Mode of access: https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/. *Date of access: 02.03.2024.*

2. An introduction to Open Source Intelligence (OSINT). Varin Khera. – Mode of access: https://cyberprotection-magazine.com/an-introduction-to-open-source-intelligence-osint. *Date of access: 07.03.2024*

3. How OSINT is used in cybersecurity – Part 1. Omar. – Mode of access: https://iosentrix.com/blog/How-OSINT-is-used-in-Cybersecurity-Part-1/. *Date of access: 28.02.2024*

4. 5 Sources of Open Source Intelligence in Cyber Security. Editorial Team. – Mode of access: https://diesec.com/2023/09/5-sources-of-open-source-intelligence-in-cyber-security/. Date of access: 25.02.2024