Journal of Applied and Advanced Research. Proceedings of the Conference on “Recent Trend of Teaching Methods in Education”. 2018: 3 (Suppl.1) 2018 Phoenix Research Publishers p. 33-35

URL: https://www.researchgate.net/publication/325086709

2. Jozsef Poor, Peter Sasvari, Zsigmond Szalay, Istvan Peto, Norbert Gyurian, Csilla Judit Suhajda, Ferenc Zsigri The implementation and management of e-learning in companies – the state of e-learning in Hungary based on empirical research Journal of engineering management and competitiveness (JEMC) vol. 10, No.1, 2020, 3-14

URL: https://www.academia.edu/79968618

УДК 004.77

TALAN MYKYTA ANDRIIOVYCH

a fourth-year cadet of faculty No.4

Kharkiv National University of Internal Affairs,

SAZANOVA LARYSA SERHIIVNA

scientific adviser

senior lecturer of the department of foreign language of faculty No.4

Kharkiv National University of Internal Affairs

GOOGLE DORKS AS A RESOURSE FOR CRIME INVESTIGATION

Nowadays, the question of finding criminals is very acute, especially if it's a cybercrime. Searching for criminals on the Internet is a very complex and difficult task. But every action done on the Internet leaves its mark. These marks can be used to find information that can help solve a crime. Within OSINT, we can use Google Dorks.

Google Dorks is an information search technique using Google operators (Advanced Search Operators). Google search operators are special characters and queries that extend the capabilities of plain text searches. With the help of Google Dorks, you can perform a variety of OSINT and cyber security tasks, identify potential vulnerabilities of sites and applications, find, and prevent data leaks, reveal hidden information that was indexed by robots and entered the Search Engine Result Page.

Google Dorks is actively used by Pentesters, reverse engineers, researchers and analysts of the IT sphere for the purpose of auditing and identifying security "holes" in systems and electronic resources [1].

Google Dorks allows you to collect quite large amounts of information: people search (names and surnames, nicknames), search for information in social networks, metadata and log files, e-mails, files, and documents (pdf, doc, txt, sql, mp3, jpeg, avi, etc.), web pages (URL), web services and servers, network Devices (IoT), administrative parts of electronic resources and applications (admin panels), vulnerabilities in electronic resources and systems.

Tasks that Google Dorks helps to solve: search for official, administrative, confidential, technically faulty web pages, login and authorization forms that are freely accessible and create security risks, search for vulnerable URLs to includes, injections, traversals, fuzzing, etc., search for official, confidential, user files and folders that are publicly accessible and create security risks, search for any information leaks, databases, usernames and accesses that are publicly available and compromise the system [2].

Google is a fast and effective way of collecting various information on the Internet, accumulating data/facts from open sources (OSINT). In fact, Google Dorks can act as a manual search scanner and parser for cybersecurity audits and OSINT investigations, which is very useful in law enforcement.

“Indeed, the right tool can determine whether you harvest the right information. It follows that the more tools you have in your portfolio, the more flexible your OSINT capabilities are likely to be” [3, p.1].

References

1. Useful Google Dorks for Open-Source Intelligence Investigations . URL: https://www.maltego.com

2. What is OSINT? URL: https://www.linkedin.com/pulse

3. Aleksandra Bielska, Noa Rebecca Kurz, Yves Baumgartner, Vytenis Benetis) Open-source intelligence tools and resources handbook 2020 URL: https://i-intelligence.eu/uploads/public-documents/OSINT_Handbook_2020.pdf