1. Law of Ukraine «On Amendments to the Criminal Code of Ukraine to Enhance the Effectiveness of Combatting Cybercrime in a State of War» No. 2149-IX as of March 24, 2022.
2. Law of Ukraine «On the Basic Principles of Cybersecurity in Ukraine» No. 2163-VIII as of October 5, 2017.

УДК 004.056.53
DOI: 10.31733/15-03-2024/2/385-386

Vitalie SPINACHI
Master

Serghei OHRIMENCO
D.Sc. in Economics, Professor

*(Laboratory of Information Security,
Academy of Economic Studies
of Moldova)*

ETHICAL HACKING

«Hacking», as a worldwide phenomenon, has emerged relatively recently, has been widely developed in the conditions of the spread of information and communication technologies and the global Internet, as well as in the development and operation of software for personal computing equipment, systems and networks. This activity is the introduction of deliberate changes to the software to achieve certain (most often, selfish) goals. These unauthorized changes are malicious (i.e. capable of causing significant damage) and can pose a serious threat to individuals, society and the state.

Hacker has a double meaning. Encylopedia.com explains: «During the 1960s, the word 'hacker' grew to prominence describing a person with strong computer skills, an extensive understanding of how computer programs worked, and a driving curiosity about computer systems. Hacking, however, soon became nearly synonymous with illegal activity. While the first incidents of hacking dealt with breaking into phone systems, hackers also began diving into computer systems as technology advanced. During the late 1990s and into the new millennium, hacking became a popular term for the act of breaking in, tampering with, or maliciously destroying private information contained in computer networks»[1].

In order to find and eliminate the introduced changes, which are called vulnerabilities deliberately introduced into the software, software testing is performed, which is a process of research, testing of a software product to check the correspondence between the real behavior of the program and its expected behaviour on a finite set of tests. It should be borne in mind that software developers also make mistakes and, thus, it is necessary to check for errors before the programme is handed over to the customer or implemented as part of an information system. Many experts note the importance, complexity and high cost of testing processes not only for software for personal computers and mobile devices, but also for systems and networks in general.

The composition of the hacker community is quite heterogeneous. Some of them specialise in creating special malware for mobile applications, others create encryption software, etc. And these products are sold and exchanged on closed, illegal markets (Dark Markets).

It should be noted that the «hacker community» directs its efforts to the development of a large number of software abuses, which should be conditionally divided into the following groups by purpose: Espionage, Attack, Destabilization [2]; Attacking Web Applications, Advanced Brute-forcing and Password spraying, File Inclusion Attacks, Authentication and Authorization Abuse, Attacking Custom Protocols, Cross-origin Resource Sharing, Social Engineering Attacks Breaking Containers [3], Injection Attacks, Fuzzing, Dynamic Scanning of REST API, and Web Application [4]. Additional analyses can be gleaned from a set of reports from leading computer firms, including The 2023 Faces of Fraud Research Survey Results Report [5], The 2019 Hacker Report. The Survey and Statistics of the Ethical Hacker Community [6], 7th Annual Hacker-Powered Security Report [7], The Evolution of Online Fraud in 2023 and Best Practices to Plug the Gaps [8].

Summarising the intermediate conclusion, two main groups of interaction among hackers should be distinguished. On the one hand, representatives of the first group see the main purpose of their activity in gaining profit (profit) by making changes to software and selling it to users on a criminal basis. This group is called hackers. The second group unites specialists in searching and fixing vulnerabilities in software for security purposes and they are given several names – anti-hackers, ethical hackers, pentesters, vulnerability hunters, etc.

The statistics of the well-known firm Hacker One, which created the famous Bug Bounty platform that combines computer business and research activities in the field of information security (https://www.hackerone.com), is quite revealing:

- 9 out of 10 hackers are under 35 years old, 8 out of 10 are self-taught, more than 40% of hackers spend more than 20 hours a week searching for vulnerabilities;
- young people aged 18 to 34 (84.1%) form the basis of the platform, 6% are young people aged 13-17, specialists of pre-retirement age make up less than 1%;
- the level of education of participants is characterised by the following data: school students – 30%, undergraduates – 25%, postgraduates – 20%, continuing education – 15%, other forms – about 10%;
- time spent per week searching for vulnerabilities is: from 1 to 10 hours – 35%, from 10 to 20 hours – 15%, from 30 to 40 hours – 10%, more than 40 hours – 15%;
- work experience from 1 to 5 years is the majority – more than 70%, 6 to 10 years is about 20%, 11 to 15 years is 2%, the same number of workers with more than 21 years of experience.

It is of undoubted interest to analyse the main tools used by hackers. They include the following mechanisms (in descending order): XSS – 38%, SQL Injection -13,5%, Fuzzing – 7,5%, Business Logic – 6,4%, Information Gathering -5,8%, SSRF -4,9%, RCE – 3,8%, Enumeration – 3,3%, Reverse Engineering – 3,3%, IDOR – 3,1%, Brute Force – 2,6%, Injection – 2,2%, CSRF – 1,6%, Authentication – 1,5%, XXE – 1,5%, DDoS – 1,3%.

The main efforts of hackers are aimed primarily at hacking websites and this should be recognised as a pattern. Subsequent targets for hacking are the following: technologies that process user data; software interface of applications; software for controlling video cameras, microcalculators, mobile phones, navigators; downloadable software; operating system and platform for mobile devices, etc.

In conclusion, the authors draw attention to the need to develop evaluation models and implementation capabilities for software abuse monetisation processes. An important problem is the study of scenarios of transformation of software threats into financial services, including money laundering.

1. Steven C. Morgan, Connor S. Morgan (2022). Hacker's Movie Guide. The Complete List of Hacker and Cybersecurity Movies. Cybersecurity Ventures. ISBN-13: 978-1-7330157-1-4
2. Buchanan, Ben (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press. ISBN 978-0-674-24601-0
3. Adrian Pruteanu (2019). Becoming the Hacker. The Playbook for Getting Inside the Mind of the Attacker. Packt Publishing. ISBN 978-1-78862-796-2
4. Samir Kumar Rakshit (2022). Ethical Hacker's Penetration Testing Guide. Vulnerability Assessment and Attack Simulation on Web, Mobile, Network Services and Wireless Networks. BPB Online. ISBN 978-93-55512-154
5. The 2023 Faces of Fraud Research Survey Results Report. URL : https://www.bankinfosecurity.com/whitepapers/2023-faces-fraud-research-survey-results-report-w-12630 (access data 04.04.24)
6. The 2019 Hacker Report. The Survey and Statistics of the Ethical Hacker Community. URL : https://www.hackerone.com/ethical-hacker/2019-hacker-report-celebrating-worlds-largest- community-hackers (access date 28.09.23)
7. 7th Annual Hacker-Powered Security Report. URL : https://www.hackerone.com/reports/7th-annual-hacker-powered-security-report (access data 04.03.24)
8. The Evolution of Online Fraud in 2023 and Best Practices to Plug the Gaps. URL : https://www.bankinfosecurity.com/evolution-online-fraud-in-2023-best-practices-to-plug-gaps-a-23094 (access data 04.03.24)