UDC 004.415.53 DOI: 10.26565/2519-2310-2022-1-02

A CONCISE OVERVIEW OF THE SPECIFIC FEATURES OF USING EXPLOYTS

Bogdanova Elizaveta, Pavlova Larysa, Pohorila Karina

V.N. Karazin National University, Kharkiv, 61022, Ukraine
xa12850323@student.karazin.ua, l.v.pavlova@karazin.ua, karina.pogorelka@gmail.com

Received: on June 2022. Accepted: on July 2022.

Abstract: *The issue of exploiting the software vulnerabilities is considered in the article. Particular attention has been paid to the two aspects of the practical usage of exploits, as an attack tool and as a means of testing protected information systems. It is stressed that integrating exploits into a single exploit-kit, increases the efficiency of searching for existing vulnerabilities of the modern information systems. The scheme of the exploit kit operation in the target information system is presented. Analysis of the known incidents related to the use of exploits, al-lows us to assert the existence of a relationship between the degree of popularity of a software product or device, and the probability of the exploits being created. The extreme importance of the timely release of security patches as an effective means of preventing the usage of identified software vulnerabilities is emphasized. Releasing security patches is a basic element of possible defensive reactions when dealing with such issues.*

Keywords*: exploits; software vulnerabilities; security patches; information security.*

1. Introduction

Over the past 20 years the exploits have remained one of the most serious problems in the field of information security [1]. Moreover, this problem equally concerns software developers and developers of security solutions, as well as employees of information security departments of companies and organizations. At the same time, among specialists there is ambiguity in determining the actual role and place of exploits, especially in deciding whether an exploit can independently harm an information system (ISs) and/or its information resources, or whether it should be considered as a tool (means) for penetrating and then launching another malicious code.

Taking into account the rapid informatization of all spheres of modern society and its critical dependence on the implementation of network technologies, providing information security for modern ISs and online services is of an absolute priority. This is due to the constant evolution of tools, techniques and technologies used by attackers in the course of searching for and exploiting various software vulnerabilities and security settings of ISs software and hardware. Exploits are one of the tools used to overcome the security measures of attacked ISs. They were most popular over the past decade, but are still considered by attackers as an effective «precision» tool for penetrating modern ISs *(Wanna Cryptor virus attack).* At the same time, exploits are becoming more sophisticated, taking into account the peculiarities of both the attacked resource and its security system.

2. Main part

Software is created by humans, and it is known that «*errare humanum est»*. As a result, even the rigorous testing of newly developed software does not eliminate the possibility of vulnerabilities in a created program code. Moreover, one cannot exclude the threat of deliberate introduction of certain vulnerabilities into created software products. The motivation for introducing vulnerabilities can vary widely from the insider's desire to cause reputational damage to the company to the pursuit of personal gain by trying to peddle those vulnerabilities on special online resources. In any case a user exploiting an existing vulnerability (*including a deliberate attacker*) is potentially able to control the target IP and/or gain unauthorized access to sensitive data.

Using an existing vulnerability of a system program, an application or an online service, the exploit allows for subsequent unauthorized actions [2]. At the same time, the direct destructive im-

pact on the compromised device and/or the target ISs and data is typically carried out by other malicious programs at the later stages of the attack. For example, having gained access to an ISs, an attacker can firstly modify their access rights, and then change the operation parameters of network devices and/or install their own software, which, in any case, should be considered as unauthorized interference with the operation of the system (*device*) [3].

Generally, exploits being a subspecies of malware can be not only a separate application, but a small fragment of program code or a set of commands as well [4]. In addition, for the purposes of penetration testing, exploits can be grouped into the set, a so-called exploit kit. Such kits are effective for preliminary monitoring of devices in the target ISs selected for attacking (*a gateway between the wireless and wired segments of the victim's corporate network, for example*), or monitoring of the entire ISs for various vulnerabilities in the used software. Such network reconnaissance being "successful" [5], the attacker uploads the main "body" of the malicious code (*keylogger*) and starts its phased deployment on a compromised resource.

Theoretically, even regular updating of existing software does not guarantee complete protection against exploits, because there is always a certain time interval between the discovery of another vulnerability and its elimination (*the release of the so-called software patch*). During this time gap potential intruders can use the so-called zero-day vulnerabilities (*exploits)* [3, 6], which exist due to the fact that software developers in their attempts to eliminate the vulnerabilities of the program code are always "*catching*" up with relatively new techniques and methods of attacking existing software and hardware solutions. Moreover, the strategy chosen by the developer of the compromised software to handle discovered vulnerabilities is extremely important. A responsible developer will not try to hide the discovered vulnerability, but promptly inform the users about the identified threat and form appropriate recommendations for its temporary containment, while expediting the measures for eliminating this problem.

It is important to emphasize that any elements of modern ISs such as application programs, modules of special software, operating system modules (OS) or hardware can be attacked by means of exploits [4]. Since the existence of different exploits implies the unauthorized actions on various compromised objects (*a single PC, ISs, local network device or online service*), it is logical to classify exploits according to the objects being attacked (*targets*) (Fig. 1).

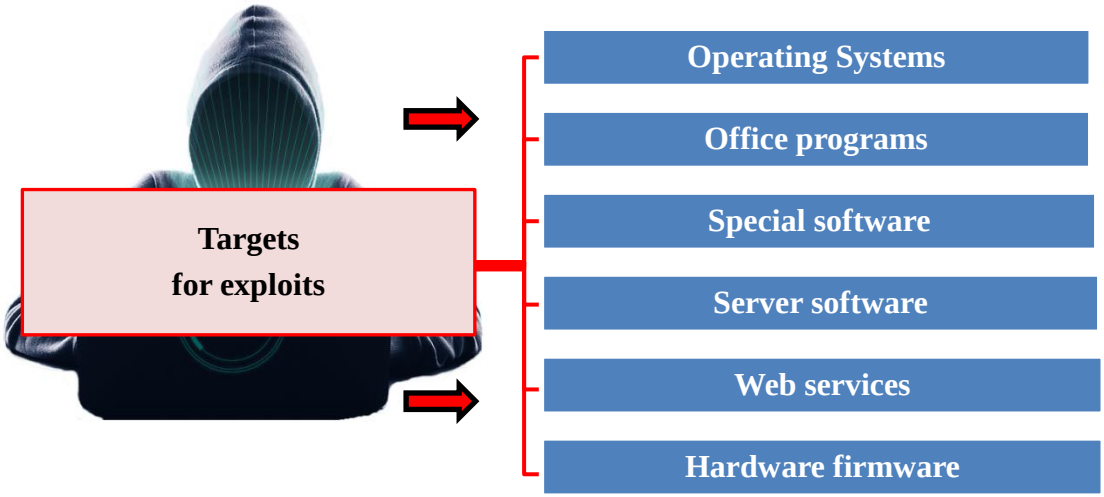

Fig. 1 - Classification of exploits by targets

Analysis of the known incidents related to the use of exploits (*Eternal Blue, for example*), allows us to assert the existence of a relationship between the degree of popularity (*number of uses*) of a software product or device, and the probability of the exploits being created. That is, the wider

the client base of the target being attacked and the higher the expectations for the monetization of a "successful" attack, the higher the probability of creating a corresponding exploit.

There are various ways for exploits to penetrate the target ISs [6-7]: - through an "infected" website, a link in an e-mail, through local access to the system (*see Fig 2*).

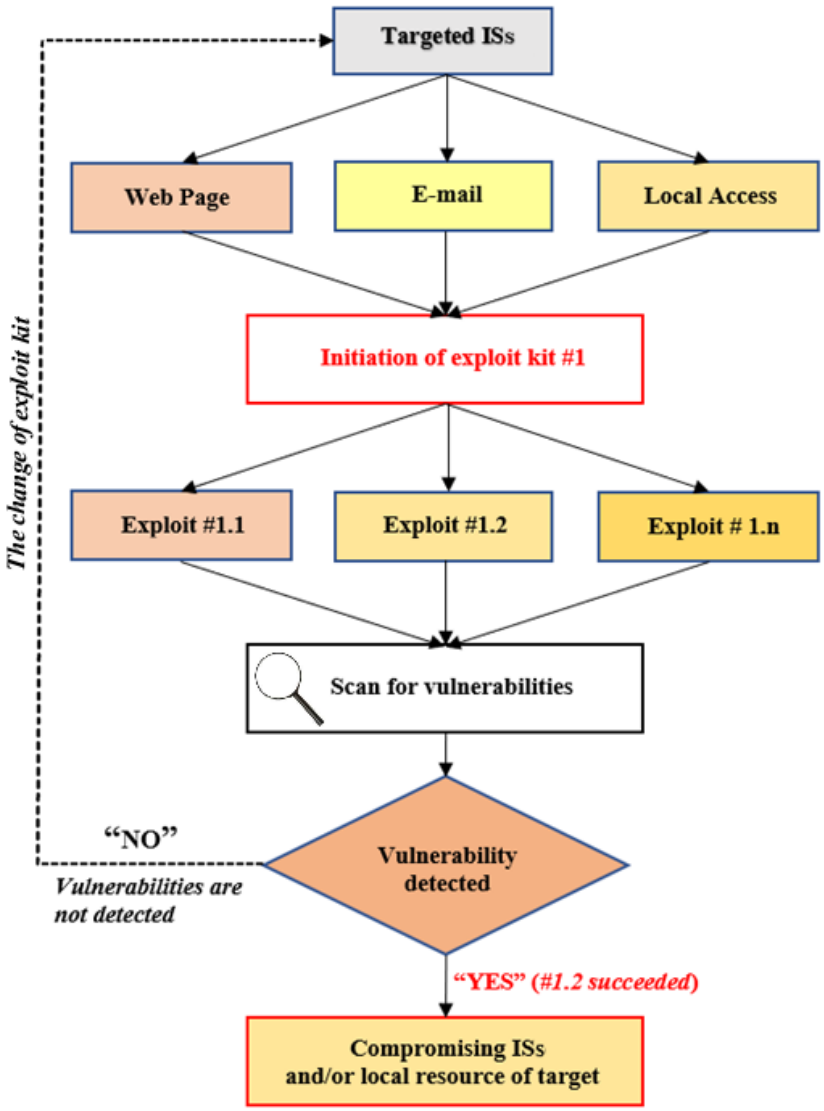

Fig. 2 - The operating principle of exploit kit in the target information system

However, in order for the exploit to start scanning the target ISs or local device for vulnerabilities, the user of the system needs to run the corresponding malicious code (*regardless of the way it has got into the attacked system, see Fig. 2*). Therefore, a local ISs node *(server or computer)*, network hardware (*switch or gateway*), a software utility and/or a process within the attacked IS (*including «cloud» ones*) can be a local/final resource to be attacked. However, it should be noted, that the exploit kit can also be launched from outside. This option is possible within the framework of network reconnaissance of the external perimeter of the attacked system [5]. In this case, the «success» of the exploit kit activation is determined by the presence of gross errors in the functional parameters of the elements of the corporate information security system (*for example, the input (first) firewall or proxy server*) [8].

Obviously, after unauthorized penetration of the ISs, the «*attacker*» acts according to his goals and motives. In other words, usage of exploits can be harmful, i.e., to carry out an attack on the information resources of the victim, as well as beneficial. For example, information security

specialists test their corporate ISs specifically to identify vulnerabilities (the so-called *Pen test - Penetration Testing*), thereby trying to identify existing security problems in advance and determine possible vectors of cyber-attacks on their information resources [9].

Based on the results of external penetration tests and internal activations of exploit kits, information security specialists get an idea of the presence of vulnerabilities in the systems they maintain and creates appropriate exploits for inform developers about vulnerabilities in their product *(including the results of an external information security audit)*. This gives them the opportunity to provide a security patch in advance, before this exploit is released to the public domain. However, there are the certain exceptions, for example, the practice of using exploits as a cyber weapon by special services providing the information security for their states.

3. Conclusions

1. In the most of information security incidents, the use of exploits provides the necessary conditions for the subsequent unauthorized actions in the infrastructure of the attacked target.

2. The wider the client base of the target being attacked and the higher the expectations for the monetization of a *«successful»* attack, the higher the probability of creating a corresponding exploit.

3. The most dangerous are *«zero-day»* exploits, which exclude the time limit of the security services and developers of compromised software from reacting in time. That is why these exploits are the main means of implementing covert attacks and are in steady demand among a certain category of the Internet community.

4. The measures that can potentially mitigate the consequences of attacks which use zero-day vulnerabilities are the usage of layer *NGFW*, *Honeypot* and *IDS* proactive protection tools integrated within a single *XDR*-platform and subjected to regular updates and internal penetration tests (*vulnerability scanners*).

5. Integrating exploits into a single exploit kit increases the efficiency of searching for existing vulnerabilities, which makes it possible to identify several points (*directions*) of penetration into the target infrastructure at once.

6. The practical use of exploits develops along two main vectors, as a means of providing attacks on a compromised resource (*i.e., having a confirmed vulnerability*), and as a means of testing protected infrastructure objects for vulnerabilities (*pentesting*).

7. The main reasons for the emergence of software vulnerabilities should be considered as follows: - insufficient personnel qualification; - failures in following the proper stages of developing and testing of software; - excessive use of IT-outsourcing opportunities; - presence of a corporate insider; - deliberate introduction of hidden functions software and/or logical triggers, as part of the interaction between software manufacturers with representatives of national special services in charge of cybersecurity.

References

[1] Синцов А. (2015). Куда катится безопасность? Хакер, (192), 58-59. Извлечено из: http://surl.li/certn

[2] Мелкозьорова, О., Лєсная, Ю., & Малахов, С. (2022). Особливості забезпечення захисту від НСД в сучасних інформаційних системах. *InterConf,* (97). Retrieved from https://ojs.ukrlogos.in.ua/index.php/interconf/article/view/18428

[3] Касперский Е.В. (2012). Эксплойты, зеродеи, их опасность и её профилактика. Retrieved from: https://eugene.kaspersky.ru/2012/05/25/exploits-and-zerodays-protection/

[4] (2017). Эксплойты, (Exploits). Извлечено из https://www.antimalware.ru/threats/exploits

[5] Рузудженк, С., Погоріла, К., Кохановська, Т., & Малахов, С. (2020). Особливості захисту корпоративних ресурсів за допомогою технології Honeypot. Комп'ютерні науки та кібербезпека, (4), 22-29. Retrieved from: https://doi.org/10.26565/2519-2310-2019-4-03

[6] Daniel Simpson. (2022). Наборы эксплойтов и эксплойтов. Retrieved from: http://surl.li/certr

[7] Закрожевский В. (2010). Лазутчики киберкриминала. Retrieved from: https://securelist.ru/lazutchiki-kiberkriminala/1424/

[8] Джон Маллери, & Джейсон Занн (2007). *Безопасная сеть вашей компании.* (Е. Линдеманн, пер. с англ.). Москва: НТ Пресс.

[9] Nikto: A Practical Website Vulnerability Scanner. (2021). Retrieved from: https://securitytrails.com/blog/nikto-website-vulnerability-scanner

Надійшла: червень 2022. Прийнята: липень 2022.

Автори:
Єлизавета Богданова, студентка факультету комп'ютерних наук (бакалавріат), Харківський національний університет імені В.Н. Каразіна, Україна.
E-mail: xa12850323@student.karazin.ua
Лариса Павлова, ст. викладач кафедри іноземних мов професійного спрямування факультету іноземних мов, Харківський національний університет імені В.Н. Каразіна, Україна.
ORCID ID https://orcid.org/0000-0002-5854-4209
E-mail: l.v.pavlova@karazin.ua
Каріна Погоріла, студентка факультету комп'ютерних наук (магістрат), Харківський національний університет імені В.Н. Каразіна, Україна.
ORCID ID https://orcid.org/0000-0001-8701-2394
E-mail: karina.pogorelka@gmail.com

Короткий огляд специфіки використання експлойтів.

Анотація. Розглянуто проблематику експлуатації вразливостей програмного забезпечення. Звернено увагу на існування двох іпостасей практичного застосування експлойтів: - як інструменту атаки та, як засобу тестування інформаційних систем, що потребують захисту. Наголошується, що об'єднання експлойтів в єдиний експлойт-кіт підвищує ефективність пошуку наявних вразливостей сучасних інформаційних систем. Аналіз відомих інцидентів, пов'язаних з використанням експлойтів, дозволяє стверджувати про існування зв'язку між ступенем популярності програмного продукту або пристрою та ймовірністю створення відповідних експлойтів. Представлено схему роботи експлойт-паку в цільовій інформаційній системі. Підкреслено надзвичайну важливість своєчасного випуску патчів безпеки, як ефективного засобу парірування виявлених уразливостей програмного забезпечення. Звернено увагу на те, що процес випуску патчів безпеки є базовою складовою у спектрі можливих захисних реакцій, при вирішенні подібних проблем.

Ключові слова: експлойт; програмна вразливість; патч безпеки; інформаційна безпека.