УДК 004.056

О. П. Войтович
В. О. Головенько

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ НУЛЬОВОГО ДНЯ

Вінницький національний технічний університет

Анотація
У даній роботі досліджено вразливості та атаки нульового дня, життєвий цикл вразливостей, актуальність та проблематику. Розглянуто характеристику появ вразливостей нульового дня у інформаційних системах.
Ключові слова: Вразливості нульового дня, атаки нульового дня, захист інформації, кіберзлочинці.

Abstract
Zero day vulnerabilities and attacks, as well as vulnerability lifecycle, relevance and perspective are researched in this work. The feature of zero-day vulnerability occurrences in information systems is considered.
Keywords: 0-day vulnerabilities, 0-day attacks, information security, cybercriminals.

У сьогоденні проблема вразливостей нульового дня є досить актуальною та важливою, оскільки чимало відомих компаній стали жертвами кіберзлочинців, які використали саме такі вразливості для атак. Жертвами атак нульового дня можуть стати будь хто: відомі бренди як Microsoft [1], Apple [2] та навіть хмаринні технології Google [3]. Тому постає питання боротьби з вразливостями та атаками нульового дня.

Вразливості класифікуються за місцем їх появи: у апаратному забезпеченні, програмному забезпеченні, інформаційно-комунікаційних системах, веб-ресурсах, а також через персонал [4].

Для розуміння вразливостей нульового дня необхідно розглянути їх життєвий цикл, описаний у (рис. 1) [5]. При виявленні вразливості кіберзлочинці можуть здійснити атаку з її використанням. У цей час «власник вразливості» зазнає збитків від атаки та може навіть не здогадуватися про неї. Після того, як потенційна жертва виявляє атаку та вразливість, вона намагається запобігти збиткам та випускає оновлення з патчем, який зменшить або нейтралізує дію атаки. У той час зловмисник намагається обійти патч для продовження експлуатації вразливості у своїх цілях. Така гонка між атаками та новими патчами може тривати навіть протягом декількох років, поки вразливість не буде повністю нейтралізована.

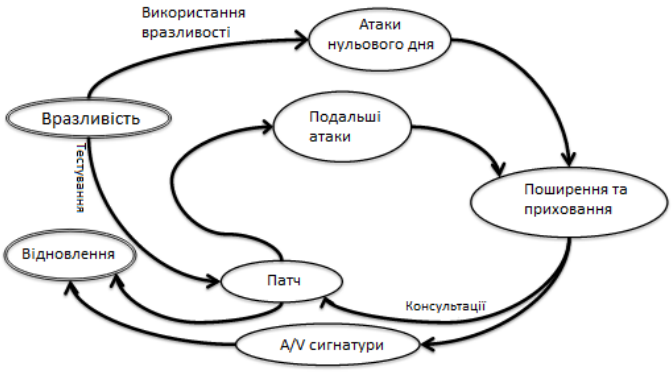

Рисунок 1 – Життєвий цикл вразливості нульового дня

Вразливості нульового дня сприяють розповсюдженню шкідливого коду, що використовується кіберзлочинцями для створення ефективного механізму зараження інформаційних систем [6]. Зрозуміло, що зловмисники проводять атаки на продукти масового використання для ефективності розповсюдження шкідливого програмного забезпечення. Проте вразливості нульового дня можуть використовувати не лише хакери, а й спецслужби у національних інтересах тієї чи іншої країни. Для прикладу, уряд США повідомив, що буде збирати усі звіти вразливостей нульового дня з усіх зареєстрованих на території країни компаній-гігантів, таких як Microsoft, Apple та інші[7].

Атаки нульового дня можуть тривати по-різному [8], від кількох днів і до кількох років. Середня тривалість вразливості нульового дня складає близько 312 днів. За цей час, компанія, на яку була здійснена атака, може втратити до половини свого бюджету. Для прикладу, вразливості CVE-2015-2545 та CVE-2015-2546 були приховані у документах Microsoft Office та дозволяли здійснювати приховані атаки на користувачів [1].

Проте необхідно пам'ятати, що після оприлюднення вразливості нульового дня та її «повної нейтралізації», атаки можуть продовжуватися ще деякий час. У наступних патчах знову може бути щілина, що відкриває шлях до вразливості нульового дня, тому зазвичай хакери спостерігають за інформаційною системою навіть після оприлюднення вразливості та виходу фінального патча [5].

Виявлення атак нульового дня швидше за зловмисника наразі є однією з найбільших проблем, оскільки не можна чекати, поки хакери продадуть цю вразливість іншим, як це робить Dark-Web Market [9].

Платформа Microsoft Windows, а також мобільні платформи Android, iOS стали найголовнішою мішенню для кібер-атак протягом останніх років, тому чимало провідних компаній з інформаційної безпеки розробляють спеціалізоване програмне забезпечення саме для них, в тому числі таке, що дозволяє виявити або захиститись від вразливостей нульового дня. Також серед найбільшої кількості здійснених атак нульового для є програмне забезпечення, базоване на мові програмування Java-Script [1]. За статистикою лідером за кількістю жертв атак нульового дня став браузер Internet Explorer [10].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Kindlund D. Recent zero-day exploits and vulnerabilities. // Kindlund D., Pidathala V. [Електронний ресурс]. – Режим доступу до ресурсу: https://www.fireeye.com/current-threats/recent-zero-day-attacks.html - назва з екрану.
2. Ducklin P. Secret Apple iPhone zero-day exploit earns $1000000. [Електронний ресурс]. – Режим доступу до ресурсу : https://nakedsecurity.sophos.com/2015/11/03/secret-apple-iphone-zero-day-exploit-earns-1000000-well-maybe/ - назва з екрану.
3. Knaddison G. J. Cloudy with the chance of zero day [Електронний ресурс]. – Режим доступу до ресурсу : http://crackingdrupal.com/blog/greggles/cloudy-chance-zero-day - назва з екрану.
4. ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008
5. Leyla B. Before we knew it: an empirical study of zero-day attacks in the real world. // Bilge, L., Dumitras, T. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 833-844) [Електронний ресурс]. – Режим доступу до ресурсу : http://dl.acm.org/citation.cfm?id=2382284 – назва з екрану.
6. PC Tools What is zero-day vulnerability? [Електронний ресурс]. – Режим доступу до ресурсу : http://www.pctools.com/security-news/zero-day-vulnerability/ - назва з екрану.
7. Антипов А. Правительство США будет эксплуатировать уязвимости нулевого дня [Електронний ресурс]. – Режим доступу до ресурсу : http://www.securitylab.ru/news/473324.php - назва з екрану.
8. Jones G. How to find zero-day vulnerabilities [Електронний ресурс]. – Режим доступу до ресурсу : http://www.slideshare.net/secfigo/owasp-session-feb-2012 - назва з екрану.
9. Greenber A. New Dark-Web Market Is Selling Zero-Day Exploits to Hackers [Електронний ресурс]. – Режим доступу до ресурсу : http://www.wired.com/2015/04/therealdeal-zero-day-exploits/ - назва з екрану.
10. IlyinY. Уязвимость нулевого дня в IE [Електронний ресурс]. – Режим доступу до ресурсу : https://business.kaspersky.ru/0day-ie-windows-xp/1700/ - назва з екрану.

Головенько Віталій Олександрович, студент, Вінницький національний технічний університет, м. Вінниця, факультет інформаційних технологій та комп'ютерної інженерії, 1БС-14б, torvald124@gmail.com

Войтович Олеся Петрівна, к.т.н., доцент, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Holovenko Vitaliy Oleksandovych, student, Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, 1BS-14b, torvald124@gmail.com

Voitovych Olesya Petrivna, Ph.D. docent, docent of Vinnytsia National Technical University, Vinnytsia, Faculty for Information Technologies and Computer Engineering, chair of information security.