SECTION 2. COMPUTER SYSTEMS AND NETWORKS, CYBERSECURITY / КОМП'ЮТЕРНІ СИСТЕМИ І МЕРЕЖІ, КІБЕРБЕЗПЕКА

Валерій Лахно
д.т.н., професор
кафедра комп'ютерних систем, мереж та кібербезпеки НУБіП України, Київ, Україна
ORCID ID 0000-0001-9695-4543
lva964@nubip.edu.ua

Байдур О.В.
Аспірант

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ КІБЕРЗАХИСТУ ЗБРОЙНИХ СИЛ УКРАЇНИ

Сучасна нормативна база Збройних Сил України та Міністерства оборони України за напрямом організації кіберзахисту базується на засадах, що в світових фахових виданнях отримали назву "моделі Замку" (Castle model) [1]. Організація захисту інформаційно-комунікаційних систем покладається на "внутрішній" довірений периметр, що відокремлюється від "зовнішнього". Тобто те, що відбувається ззовні, вважається потенційно шкідливим або небезпечним, а внутрішні процеси мають певний рівень довіри за замовчуванням. В світовій практиці критика "Моделі Замку" особливо посилилися після виходу на початку 2011 року статті науковців корпорації Lockheed Martin [2], що встановила відповідність між моделлю структури атаки "F2T2EA" армії США, що також має назву "ланцюжок знищення" (kill chain), та діями кіберзлочинців. Це спричинило активізацію досліджень і згодом формування альтернативних підходів до організації кіберзахисту. Алгоритм дії кіберзлочинців відповідно до "ланцюжка знищення" визначається як послідовність таких дій:

1. Розвідка. Дослідження, ідентифікація та вибір цілей, часто представлених у вигляді сканування веб-сайтів Інтернету.

2. Створення зброї — поєднання троянської програми віддаленого доступу з експлойтом у доступне корисне навантаження, як правило, за допомогою автоматизованого інструменту (зброї).

3. Доставка - Передача зброї в цільове середовище.

4. Експлуатація - після того, як зброя доставлена жертві, експлуатація запускає код зловмисника.

5. Встановлення. Встановлення троянської програми віддаленого доступу або бекдора в систему-жертву дозволяє зловмиснику отримати стійкий доступ у атаковане середовище.

6. Командування та керування (C2) – зазвичай скомпрометовані хости повинні передати вихідні сигнали на сервер контролера Інтернету, щоб встановити канал C2. .

7. Дії щодо цілей - Лише тепер, після проходження перших шести фаз, зловмисники можуть вживати заходів для досягнення своїх початкових цілей.

Накопичення і систематизація знань щодо послідовності дій кіберзлочинців призвели до розуміння, що на етапах 1 (розвідка) та 2 (створення зброї) ланцюжка знищення завадити кіберзлочинцю неможливо, при цьому вірогідність того, що кіберзлочинець може успішно виконати наступні етапи ланцюжка, завжди більша за нуль. Критика "моделі Замку" та викриття багатьох успішних кібератак, що довгий час залишалися поза увагою фахівців з кібербезпеки, призвели до створення нової моделі кібербезпеки, що отримала назву "Модель нульової довіри" (Zero trust model) [3]. Ця критика актуальна і для підходів, що використовувалися в Міністерстві оборони України та Збройних Силах України до 2022 року. Вразливі місця "моделі Замку" проявили себе з початком відкритої фази агресії російської федерації.

Сучасна практика організації кіберзахисту інформаційно-комунікаційних систем Збройних Сил України формувалася у відриві від вимог діючих нормативних актів на тлі постійного протистояння агресивним діям вмотивованих російською федерацією кіберзлочинців. Досвід активного протистояння висококваліфікованим кіберзлочинцям підтвердив, що акцент при побудові кіберзахисту виключно на периметрі мереж не є ефективним та призводить до значних обмежень для користувачів, збільшує час розгортання складових інформаційних систем та підключення їх користувачів [4]. Ці обмеження часто можуть критично знижувати мобільність бойових підрозділів та збільшувати час відновлення зв'язку і функціонування бойових інформаційних сервісів в разі фізичного знищення обладнання або успішної кібероперації ворога. Особливості організації кіберзахисту під час ведення активних бойових дій дуже подібні до тих, які призвели до виникнення моделі нульової довіри, а саме:

- під час активних бойових дій існує висока вірогідність захоплення або втрати обладнання, що забезпечує підключення та роботу з інформаційними сервісами, тому перший принцип моделі нульової довіри — "не довіряйте — перевіряйте" стає особливо актуальним;
- другий принцип нульової довіри, а саме — використання найменш привілейованого доступу дозволяє значно зменшити втрати та загрози у випадку фізичної втрати обладнання;
- постійно припускати попущення також є природнім в динамічних умовах реальної війни. Ворог весь час прикладає максимум зусиль для пошуку вразливостей і нанесення максимальної шкоди.

Тріада CIA (конфіденційність, цілісність, доступність) працює інакше на оперативно-тактичному рівні в умовах ведення війни. Конфіденційність на тактичному рівні важлива на короткій дистанції, швидкоплинні дані реального бою роблять інформацію тактичного рівні не актуальною вже за декілька годин. Цілісність даних інколи простіше забезпечити не залучаючи сучасних IT-технологій. Паперовий конверт, в деяких випадках, може бути надійнішим способом збереження таємної інформації, ніж сучасна інформаційна система, а доступність (своєчасність) інформації відіграє роль набагато більшу, ніж це є у системах не бойового призначення. Все це призводить до необхідності створення унікальної, відмінної від поширених корпоративних практик, моделі кіберзахисту для Збройних Сил України, яка має включити в себе використання кращих практик, що довели свою ефективність в бойових умовах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Christian Leuprecht, David B. Skillicorn, Victoria E. Tait. Beyond the Castle Model of cyber-risk and cyber-security, 2016. - Режим доступу: https://doi.org/10.1016/j.giq.2016.01.012

2. Eric M. Hutchins, Michael J. Clopperty, Rohan M. Amin, Lockheed Martin Corporation Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2011. - Режим доступу: https://www.researchgate.net/publication/266038451_Intelligence-Driven_Computer_Network_Defense_Informed_by_Analysis_of_Adversary_Campaigns_and_Intrusion_Kill_Chains

3. Executive Order on Improving the Nation's Cybersecurity May 12, 2021 № 14028. - Режим доступу: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

4. https://www.armyupress.army.mil [Електронний ресурс] Lt. Gen. Milford Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol, The Graveyard of Command Posts What Chornobaivka Should Teach Us about Command and Control in Large-Scale Combat Operations. - Режим доступу: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MJ-23/Gen-Beagle/beagle-slider-arrol-command-posts-UA.pdf

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE

NATIONAL UNIVERSITY OF LIFE AND ENVIRONMENTAL SCIENCES OF UKRAINE

FACULTY OF INFORMATION TECHNOLOGY

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

PROCEEDINGS

МАТЕРІАЛИ

XI International scientific conference

XI Міжнародної науково-практичної конференції

GLOBAL AND REGIONAL PROBLEMS OF INFORMATIZATION IN SOCIETY AND NATURE USING '2023

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 November 2023

Kyiv, NULES of Ukraine

15-16 листопада 2023 року

Київ, НУБіП України

Kyiv 2023

Київ 2023

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

МАТЕРІАЛИ

XI Міжнародної науково-практичної конференції

ГЛОБАЛЬНІ ТА РЕГІОНАЛЬНІ ПРОБЛЕМИ ІНФОРМАТИЗАЦІЇ В СУСПІЛЬСТВІ І ПРИРОДОКОРИСТУВАННІ '2023

15-16 листопада 2023 року

Київ, НУБіП України

Київ 2023

УДК 004

Рекомендовано до друку вченою радою факультету інформаційних технологій Національного університету біоресурсів і природокористування України (протокол № 4 від 20.11.2023)

Укладач: к.е.н., доцент Харченко В.В.

Збірник матеріалів XI Міжнародної науково-практичної конференції "Глобальні та регіональні проблеми інформатизації в суспільстві і природокористуванні '2023", 15-16 листопада 2023 року, НУБіП України, К. НУБіП України, 2023. 117 с.

Відповідальність за зміст публікацій несуть автори.