АНАЛІЗ ПРИЧИН ЗРОСТАННЯ ЧАСУ ПЕРЕБУВАННЯ ЗЛОВМИСНИКА В МЕРЕЖІ

Леонова А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Протягом останнього десятиліття скорочення часу перебування зловмисника в мережі (Dwell Time) вважалося ключовим показником ефективності кіберзахисту. Однак сучасні кіберінциденти демонструють зміну цієї тенденції: за даними Mandiant, у 2024 році глобальний медіанний показник зріс з 10 до 11 днів – вперше з 2010 року [1]. Це свідчить про адаптацію зловмисників і їхню здатність довше залишатися непоміченими в інформаційних системах.

Метою дослідження є ідентифікація та аналіз основних чинників, які зумовили збільшення часу перебування зловмисника в корпоративних мережах, на основі даних провідних наукових звітів у сфері кібербезпеки.

Однією із ключових причин є ускладнення початкових векторів проникнення. За даними Mandiant, експлуатація вразливостей залишається провідним способом компрометації, становлячи 33% випадків [1]. Зокрема, експлуатація невиправлених вразливостей дозволяє обходити традиційні механізми захисту та залишатися непоміченими на початкових етапах атаки, що створює передумови для подальшого закріплення в мережі.

Значну роль відіграють атаки на периферійні мережеві пристрої. За даними Verizon DBIR 2025, використання вразливостей у VPN та інших периферійних пристроях зросло майже у вісім разів [2]. Такі пристрої часто не інтегровані в централізований моніторинг, що ускладнює своєчасне виявлення.

Крім того, патерн «System Intrusion», який включає переміщення та ескалацію привілеїв, фіксується у 53% витоків даних [2], що сприяє збільшенню часу перебування зловмисника в мережі.

Зміна мотивації атак також впливає на тривалість перебування зловмисника. За даними Mandiant, кількість інцидентів зі шпигунською метою зросла на 163%, що орієнтує атаки на тривале приховане перебування в системі [1]. Водночас у випадках ransomware середній час перебування становить близько 6 днів, що свідчить про швидке завершення фінальної стадії атаки [1]. У 57% випадків організації дізнаються про компрометацію із зовнішніх джерел, що підкреслює обмеженість внутрішнього моніторингу [1].

Важливим чинником є зростання ролі сторонніх організацій. За даними Verizon DBIR, частка інцидентів за їх участю зросла з 15% до 30% [2]. Використання довірених каналів дозволяє зловмисникам маскувати активність і ускладнює її виявлення, що подовжує час перебування в мережі.

Отримані результати свідчать про неефективність традиційних підходів до кіберзахисту, орієнтованих на периметр мережі. Зростання часу перебування зловмисника до 11 днів зумовлене експлуатацією вразливостей, компрометацією облікових даних та залежністю від сторонніх сервісів. Значна

частина інцидентів виявляється зовнішніми джерелами, що підтверджує обмеженість внутрішнього моніторингу.

Необхідно забезпечити своєчасне усунення вразливостей, зокрема у VPN та мережевих пристроях, що може зменшити ризик початкового проникнення на 30-40%. Доцільно впровадити апаратну автентифікацію (FIDO2) та принцип тимчасового доступу (just-in-time), що знижує ймовірність компрометації облікових даних до 50%. Важливо обмежити збереження паролів і розмежувати робочі та особисті облікові записи. Підвищення ефективності виявлення можливе через інтеграцію журналів подій у системи SIEM та UEBA, що дозволяє скоротити час виявлення інцидентів до 30% [3].

Доцільним є перехід до моделі Zero Trust, що знижує ризик несанкціонованого доступу до 40% [4]. Регулярне проведення Red Teaming дозволяє виявляти до 60% критичних вразливостей до їх експлуатації. У сфері освіти необхідно змістити акцент на практичний аналіз інцидентів. Важливо також запровадити обов'язкові вимоги кібербезпеки для сторонніх організацій, що дозволяє зменшити ризики ланцюгових атак до-30%.

Практичні дослідження [5] показують, що навіть базове налаштування міжмережевих екранів і HTTPS-шифрування не забезпечує виявлення складних атак, які використовують легітимні облікові дані або приховані канали. Це свідчить про обмеженість ізольованого застосування засобів захисту, таких як фаєрволи, VPN чи антивіруси. Ефективний захист можливий лише за умови їх інтеграції в єдину адаптивну систему з можливостями поведінкового аналізу та виявлення аномалій.

Отже, зростання часу перебування зловмисника в системі є результатом складної взаємодії технічних, організаційних і поведінкових чинників: ускладнення векторів атак (периферійні пристрої), збільшення ролі сторонніх постачальників, поширення компрометації через infostealer malware, а також недостатня інтеграція засобів моніторингу. Зниження цього показника можливо лише за умови переходу до динамічних моделей захисту, що передбачають безперервний моніторинг, адаптацію політик безпеки та контроль доступу в режимі реального часу.

Список літератури

1. Mandiant M-Trends 2025 Report. Google Cloud Security. 2025. 94 p.
2. 2025 Data Breach Investigations Report. Verizon Business. 2025. 116 p.
3. Москвін, К., Сєвєрінов, О., Сидоренко, З., Балагура, Д., & Литвин, А. (2025). Дослідження впливу інтеграції засобів кіберзахисту на захищеність ІТ-інфраструктури організації. Вісник ХНТУ, 2(2 (93)), 246-255.
4. Moskvin K., Sievierinov O. Zero Trust Architecture in Corporate Cybersecurity Systems // Computer and information systems and technologies : Seventh International Scientific and Technical Conference, 2024. – Kharkiv : NURE, 2024. – p. 54-55.
5. Євтушенко Д. С. Порівняльний аналіз методів захисту інформації у мережах: кваліфікаційна робота магістра: спец. 172 «Електронні комунікації та радіотехніка» / Д. С. Євтушенко; ХНУРЕ. Харків, 2025. 58 с.