Cyber Threat Intelligence або що там за «стіною»

Нині вже замало просто захищатися: треба превентивно оцінювати, що саме може загрожувати вашій організації.

Кіберзлочинний світ завершує перехід до моделі Threat-as-a-Service та активно надає свої послуги для гравців усіх поточних війн та конфліктів. DDOS-атаки замовляють на сайтах (**рис. 1**) у три кліки «як піцу додому»; новітні віруси, які обходять типові антивірусні продукти, можна придбати в даркнеті; настає нова епоха інфостілерів, які полюють за обліковими записами. Очікується, що збитки, пов'язані з кіберзлочинністю, вже у 2025 році досягнуть $10,5 трлн. У 2024 році було виявлено понад 30 000 нових вразливостей безпеки, що становить зростання на 17% порівняно з попереднім роком. Інфраструктура IT та ІБ ускладнюється, а брак відповідних компетенцій та фахівців виходить на новий рівень.

Організації продовжують накопичувати рішення інформаційної безпеки з надією, що ці системи зможуть створити непроникну та незнищенну стіну для кіберзлочинців, але такий підхід є реактивним та застарілим. Сучасні загрози вимагають проактивного підходу та постійного аналізу того, що коїться ззовні периметру організації, тому CTI-рішення стають не забаганкою, а потребою для ефективної протидії загрозам та пов'язаним з ними ризикам.

Що таке CTI (Cyber Threat Intelligence) або кіберрозвідка

Cyber Threat Intelligence — це клас рішень, які надають інформацію про зовнішні загрози для організацій. Типово рішення CTI є модульними і дозволяють проаналізувати багато різних аспектів безпеки, здійснюючи зокрема:

- моніторинг Dark Web;
- аналіз зовнішньої поверхні атаки;
- захист бренду;
- аналіз кіберінцидентів постачальників;

та інше.

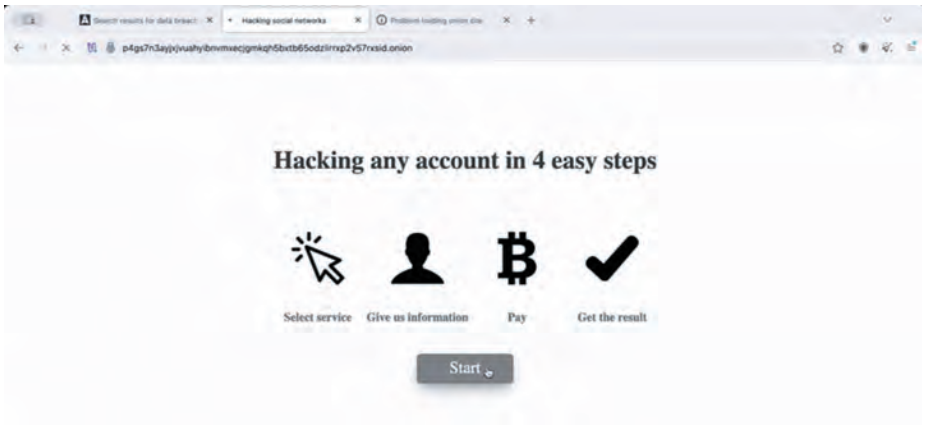

Рис. 1. Сторінка-візард для зламу облікових записів в форматі «обери і отримай»

Ідея подібних систем полягає в тому, щоб подивитися на «стіну безпеки» ззовні очима злочинця: які системи видно назовні? Які є вразливості на периметрі? Чи продаються облікові записи організації в Dark Web?

Використовуючи CTI, організації можуть подивитися на свою безпеку з обох боків та відповідно проаналізувати недоліки, вразливості та загрози.

Окрім облікових записів та вразливостей периметра, типовими об'єктами аналізу CTI є потенційні фішингові домени, сертифікати та ключі, приватні адреси пошти, номери карт та рахунків, використання логотипів організації, підроблені мобільні застосунки та багато іншого. Щоденні знахідки системи передаються на відпрацювання фахівцям безпеки у вигляді алертів або інцидентів.

Також рішення CTI надають загальну інформацію про стан загроз за країнами та секторами економіки, мають бази з описом хакерських угруповань, можуть надавати індикатори компрометації (IOC) для SIEM-систем, повідомляють про кампанії з фішингу або вірусні епідемії, також дають статистику найбільш використовуваних вразливостей та проводять загальний аналіз ризиків для постачальників.

Cyber Threat Intelligence надається за моделлю SaaS та не потребує взагалі ніякої наземної інфраструктури, це одне з тих рішень, які дуже легко тестувати і завдяки яким можна за

короткий термін отримати великий обсяг корисної інформації.

Допомога з пріоритезацією вразливостей

Рішення CTI можуть надавати додаткову інформацію щодо вразливостей, виявлених на периметральних системах. Оскільки CTI мають власні дослідницькі лабораторії та постійно аналізують події в інтернеті, вони можуть додати суттєвий контекст для знайдених вразливостей: як часто використовується конкретна вразливість? Чи є угруповання, які використовують цю вразливість? Чи працюють вони в нашій країні? Аналізуючи дані, деякі системи CTI мають власну градацію для вразливостей та відповідно підвищують чи знижують показник критичності відповідно до поточних обставин, що дозволяє більш ефективно планувати роботу.

Після визначення того, які угруповання використовують певну вразливість, CTI надає відповідні IOC, притаманні цим угрупованням, які одразу потрапляють в SIEM. Таким чином, ми проактивно готуємо нашу інфраструктуру до можливих атак.

Але тільки боротьба з вразливостями не вирішує всіх проблем: при замовленні атаки на організацію одним з перших кроків буде прогулянка Dark Web'ом з метою отримання логіна та пароля легітимного користувача з компанії-жертви.

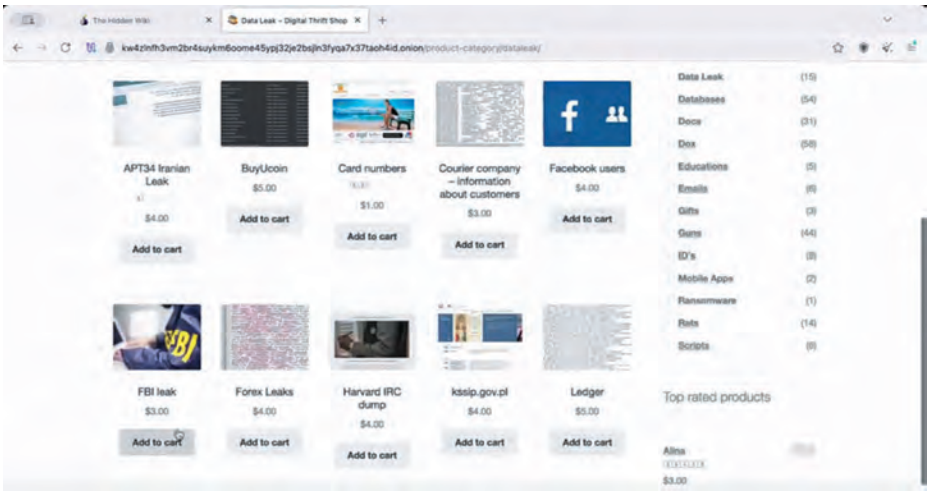

Рис. 2. Різне на продаж... від кредитних карт до витоків з ЦРУ

Прогулянка по «хакерському базару»

Маркетплейси в Dark Web'і є повними аналогами відкритих торгівельних майданчиків, але все ж мають певні відмінності. Дістатися до них можна тільки використовуючи Onion-браузери, такі як Tor, які надають повну анонімність користувачу — ну і, звісно, ніхто не побачить серед продавців реальних людей, все побудовано так щоб товари та послуги надавалися за моделлю повної анонімності. На «закритих ринках» можна придбати фактично що завгодно, чого не можна дістати легально у відкритому світі (**рис. 2**). Dark Web не є місцем тільки для хакерів: там поширена торгівля зброєю, наркотиками, компроматом тощо. До речі, в багатьох країнах використання таких браузерів, як Tor, миттєво привертає увагу провайдерів інтернету, тому всі експерименти слід проводити тільки через VPN. Одним з найбільших «базарів» є Russian Marketplace, де продаються викрадені облікові дані і ще багато чого «цікавого» — і, звісно під час війни продаж облікових даних організацій з України вийшов на новий рівень. В продажу сотні тисяч акаунтів з організацій усіх секторів і розмірів; велика «увага» приділяється державному сектору та критичній інфраструктурі, також багато облікових записів соціальних мереж та публічних поштових сервісів. Між іншим, послуга зламу соціального профілю або пошти коштує до $50, що говорить в першу чергу про те, що для людей з відповідним досвідом це достатньо легко і серед них велика конкуренція (**рис. 3**).

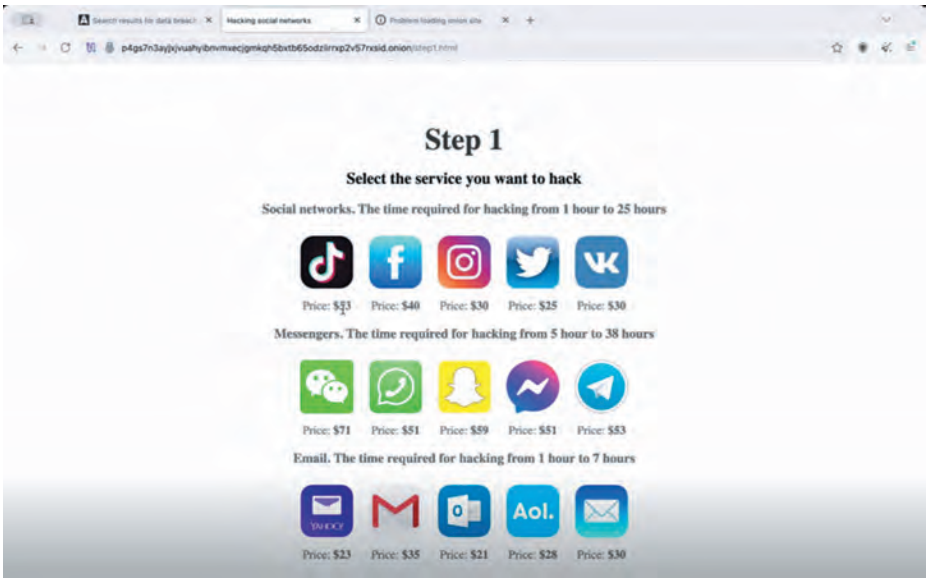

Рис. 3. Вартість зламу облікових записів у Dark Web'і

Як маркетплейси гарантують прозорість угод

Якщо всі продавці анонімні, то яким чином можна проконтролювати, що послуга або товар будуть якісними? Для цього передбачено купівлю через посередників. Спеціальні «арбітри» долучаються до угоди і контролюють виконання її умов з обох боків, утримуючи перерахування криптовалюти виконавцю, поки замовник не отримає узгоджений результат. Таким чином, кошти перераховуються на «нейтральний» гаманець, і виконавець розуміє, що кошти для нього зарезервовані, водночас замовник може отримати товар або послугу та подивитись на результат (наприклад, перевірити недоступність сайту у разі купівлі DDOS-атаки або провести тестове інфікування купленим вірусом), не

переймаючись тим, що йому запропонували щось неробоче. Окрім того, арбітр слідкує за можливим порушенням правил ексклюзивності: наприклад, після викупу облікового запису він не має з'являтися знову в продажу. За порушення угод виконавцями сам маркетплейс накладає на них санкції аж до повного блокування.

Яким чином облікові записи потрапляють на маркетплейс

Є декілька способів отримання облікових записів від користувачів.

1. Фішинг. З розвитком ШІ фішинг переживає швидке зростання завдяки автоматизації створення індивідуалізованих листів та роботі з невеликими групами потенційних жертв для зниження ризику виявлення. Після публічного запуску ChatGPT у 2022 році кількість фішингових інцидентів зросла на 4151%.

2. InfoStealers: тип шкідливого ПЗ, який спеціально створений для викрадення даних з пристроїв.

- Протягом 2023–2024 років було скомпрометовано майже 26 млн пристроїв на Windows, з яких понад 9 млн — у 2024 році.
- Торік інфостілери викрали приблизно 2,1 млрд облікових даних, що становить понад 60% усіх викрадених даних за цей період.
- Приблизно 2,3 млн банківських карт були викладені в даркнеті через зараження інфостілерами у 2023–2024 роках.
- При потраплянні на кінцевий пристрій інфостілер, окрім іншого, «патрає» браузери та виймає звідти всі збережені облікові записи.

Скарги на Dark Web Monitoring

При тестуванні рішень CTI часто чую від фахівців замовника, що CTI надає нерелевантні дані, а виявлені в Dark Web'і облікові записи вже давно видалені, паролі змінені, і взагалі цього користувача було звільнено «три роки тому», тож нема сенсу купувати систему. Розберімося, чому так відбувається. Системи класу CTI не можуть гарантувати релевантність даних, тому що не можуть її перевірити. На маркетплейсах кожен продавець може продавати все що захоче, CTI, своєю чергою, може тільки шукати відповідні облікові записи або інші артефакти, які стосуються організації або належать до певного домену, в форматі «чи є згадка на маркетплейсі, чи немає».

Розгляньмо ситуацію: продається архів з обліковими записами в кількості 1000 штук і в ньому є одна обліковка нашого домену. Продавець викладає новий лот та надає в описі до нього список доменів, обліковки з яких у нього є. Відповідно проаналізувати, коли обліковий запис було отримано, неможливо... може, вчора, а може, пару років тому. CTI-система покаже, що з'явився новий лот на продаж облікових записів поточною датою з обліковкою у відповідному домені, але перевірити, наскільки вона стара, немає змоги. Отже, CTI показує, що є певний ризик, але його рівень визначити неможливо.

Тепер розберімо ситуацію з точки зору компанії-жертви. Для деяких організацій наявність в Dark Web'і облікових записів півріччної давнини не становить суттєвої загрози, бо за цей проміжок часу паролі вже змінилися декілька разів, і на додачу використовується двофакторна автентифікація; для інших же — може бути ситуація, коли політики зміни паролів немає або вона не виконується, тож ризики максимальні. Рішення CTI ніяк не може перевірити налаштування ваших сервісів, а відтак не може надати й інформацію про релевантність.

Оскільки інформаційна безпека — це процес, важливо постійно слідкувати за виявленими обліковими записами та реагувати на подібні інциденти. В рішеннях CTI типово є функція Take Down, тобто замовник рішення може запросити викуп знайденого облікового запису з залученням фахівців виробника CTI. Такий сервіс, наприклад, у одного з вендорів коштує $10 за обліковий запис, і запит робиться в один клік. З точки зору ризиків $10 це не так багато, навіть якщо ми придбаємо «старий» обліковий запис.

Деякі кейси з практики

За допомогою CTI-рішень було знайдено:

- API-ключі, які були зашиті в мобільному застосунку;
- обліковий запис адміністративного рівня, який був скомпрометований, бо в базах Dark Net виявилося декілька облікових записів одного користувача до різних сервісів, зокрема особистих (ігровий портал, магазин техніки), відповідно такий збіг можливий тільки якщо машину було інфіковано;
- декілька покинутих серверів, які мали доступ ззовні, але про них забули і не оновлювали більше п'яти років.

Висновки

Світ кіберзагроз стрімко змінюється — атаки стають дешевшими, швидшими та більш персоналізованими. У той час як організації продовжують інвестувати в «традиційні» засоби захисту, кіберзлочинці вже давно адаптувались до нових умов і активно використовують усі можливості для компрометації компаній. У таких умовах Cyber Threat Intelligence — це не опція, а необхідність, яка дозволяє діяти на випередження, виявляти загрози ще до того, як вони спричинять інциденти, і зменшувати ризики, які неможливо побачити зсередини.

CTI не дає ідеальних відповідей, але пропонує критично важливий контекст, без якого організація сліпа до значної частини загроз. Правильно інтегроване CTI-рішення дозволяє побудувати більш стійку та адаптивну стратегію захисту, де ключовим стає не лише реагування, а й передбачення.

Олексій ЗАЙОНЧКОВСЬКИЙ,
архітектор рішень інформаційної безпеки та IT, компанія «Проспера»,
oz@it-prospera.com