ОРГАНІЗАЦІЯ І БЕЗПЕКА

ЛІС І ЗВІРІ

Невидимий звір на стежці

Безпека починається не з паролів і не із софту, а з моменту, коли світ вирішує перевірити тебе на стійкість.

Одного ранку перевірка прийшла одразу з трьох боків. Спершу сповіщення: «Ваш банківський рахунок заблоковано заради безпеки. Зверніться в підтримку». Не встиг я підняти голову, як DevOps пише: «Артем, на сайт летить DDoS. Підключаю Cloudflare».

А потім — дзвінок із незнайомого номера. Голос з іншого кінця дротів хрипів від люті: «На*** ти розсилаєш дані про ППО? На допиті не був? Скоро будеш!» Я стояв, стискаючи телефон, який здавався гарячим, ніби він увібрав у себе всю злість, яку світ двома натисканнями кнопки відправив на мою адресу. Я заплющив очі. День тільки почався.

За три дні до цього ми опублікували звіт про завод з виробництва «Шахедів» в Алабузі: деталі цехів, маршрути поставок, відповідальні особи, технічні креслення. Ми влучили в болючу точку, і ворог вирішив відповісти. Відповів так, як відповідає завжди — брудно, голосно, без фантазії.

У чатах військових, на пошті держструктур і журналістів з'явився файл — карта Києва із «позначеними» позиціями ППО та датою майбутнього удару. Підпис: «Аналітична група Molfar». Ворожа підробка. Груба, але

майстерно змонтована. Ідеальний інструмент для провокації.

Ми попросили файл для аналізу. Фальсифікація була якісною, але з одним фатальним проколом: офіцер ФСБ, який робив документ, просто ввів у Google «логотип Molfar» і скачав перший результат — логотип гуцульської пивоварні. Так нас врятувала пляшка пива.

Швидкість і безпека рідко співіснують мирно. У розвідці кожен крок — це завжди стежка, де поруч з тобою йде невидимий звір. Треба дивитися під ноги.

Темний ліс

Розвідка починається не з пошуку, не з джерела й навіть не з інструмента. Вона починається з питання. І від того, наскільки правильно це питання сформульоване, залежить усе: чи буде ваша робота точним ударом, чи безцільним копирсанням у хаотичних масивах даних. Але перше правильне питання завжди одне: «Як вижити?»

Безпека — це протокол, і будь-яка серйозна розвідувальна робота починається саме з нього. У комерційній розвідці цей протокол простіший, у військовій — ставки вищі, помилки смертельні. Чим глибше ваше розслідування і чим більше людей до нього залучено, тим вища ймовірність, що хтось помітить ваш рух. І далеко не всі зустрічі з вами будуть дружніми. Поки ви збираєте докази, хтось інший може збирати їх про вас.

Приготуйтеся: у якийсь момент хтось обов'язково спробує знищити сліди.

У 2024 році Molfar опублікували розслідування про росіян, які осквернили пам'ятник Володимиру Великому в Лондоні. Ідентифікація почалася з дрібниць: стоп-кадр з краваткою з рідкісним візерунком, годинник, рюкзак, зріст, хода, геолокаційні натяки в соцмережах.

Далі — граф зв'язків: спільні події, родина, компанії у британських реєстрах. Уже за кілька годин після публікації сторінки зникли, відео видалили, профілі «підчистили». Але копії, хронологія та локальні архіви перетворили цю спробу приховати сліди лише на доказ провини.

Це типова реакція викритого злочинця.

Розслідування Molfar

Подібне відбувається і глобально. У 2024 році російські хакери атакували сервери української прокуратури та навіть Міжнародного кримінального суду — намагаючись стерти або підмінити докази воєнних злочинів. Це вже не просто злочин, це — спроба переписати реальність.

War On The Roks: Росія нищить цифрові докази злочинів

Уявіть всесвіт як темний ліс. Кожна цивілізація в ньому — озброєний мисливець, що ховається між деревами, намагаючись не видати себе жодним звуком. Контакт — потенційно смертельний. Ти не знаєш мотивів іншого, не знаєш рівня загрози. Безпечний варіант лише один — мовчати й ховатися. Якщо ти першим побачив когось — іноді логіка підказує знищити його заради самозбереження. Це і є теорія темного лісу (Dark Forest Theory) — пояснення, чому ми досі не чуємо сигналів від інших цивілізацій. Тепер уявіть, що інтернет — це той самий космос. Майже безмежний. Мільярди «цивілізацій»: користувачів, серверів, систем, ботів. І кожна дія — пост, запит, порт,

метадані — це сигнал у темряву. Чим більше сигналів, тим більше шансів привернути увагу хижаків: зловмисників, ворожих агенцій, конкурентів.

Більша частина клієнтів Molfar – із категорії high net worth. Спілкуючись з ними, я краще зрозумів фразу: «гроші люблять тишу». Вони не хизуються благодійністю чи брендами, ходять у простих кросівках ON і більше пишаються ідеєю, яка змінює індустрію, ніж годинником чи авто.

Один інвестор з активами понад $3 млрд розповідав мені, що вигнав сина з дому за покупку Ferrari «аби похвалитися». І його жарт, що люди після обкладинки Forbes часто втрачають багатство, був не про заздрість — а про безпеку. Він принципово залишався в тіні.

Але бути абсолютно безшумним — майже неможливо. Кожен інструмент, кожен додаток, кожен «безкоштовний» сервіс залишає слід. Багато VPN, які обіцяють анонімність, живуть за ваш рахунок: продають журнали з'єднань, IP, час активності. У темному лісі таке світіння — запрошення на полювання.

Стратегія виживання у цьому середовищі починається з розуміння: вас уже хтось бачить. Саме тому існують canary tokens і honey traps — цифрові пастки, які ставлять ті, хто хоче знати, чи ведуть проти них розслідування. Це може бути фальшивий документ, посилання, фото, API-ключ. Варто комусь відкрити його — і ви отримуєте сигнал: час, IP, user-agent, інколи геолокацію. Це «пісня канарки», що сповіщає про вторгнення.

Сервіс, що створює «цифрові пастки»

Окрім пасток, існують інструменти пасивного моніторингу згадок. Вони щодня перевіряють інтернет-простір на появу імен, назв компаній, брендів чи юросіб. Коли ваші дані з'являються у новій статті, форумі або навіть у PDF, система надсилає попередження. Для юристів чи підприємців це спосіб помітити, що хтось почав цікавитись їхньою справою. Є також сервіси, які моніторять судові реєстри, сповіщаючи, якщо проти вас або вашої компанії подано позов — часто ще до офіційного повідомлення суду.

Ще один рівень захисту — data room. Це контрольований цифровий простір, який використовують під час due diligence або переговорів про злиття й поглинання. Усі документи — контракти, звіти, реєстраційні дані — зберігаються на сервері з багаторівневими правами доступу. Адміністратор бачить, хто відкривав файл, коли, з якої IP-адреси, як довго переглядав. Будь-яке завантаження чи скриншот фіксується. Data room — це і архів, і пастка, і дзеркало: він показує, хто цікавиться вами більше, ніж варто.

Окремі системи працюють на рівні документів: вони дозволяють вставити невидимі трекери у PDF-файли, щоби знати, кому відправлено документ, з яких пристроїв і адрес його відкривали. Такі інструменти, як Digify, DocSend, Vitrium або PDFTrak, застосовують у фінансових, юридичних і розвідувальних структурах. Для відправника це — цифровий відбиток, який не дає документу зникнути безслідно.

А найпростіша, але часто ефективна форма контр-розвідки — IP-logger. Він маскується під зображення або посилання у листі: ви надсилаєте файл, а коли адресат його відкриває, ви отримуєте дані про IP, пристрій, браузер і географію. Звучить дріб'язково, але для аналітика це може бути перший слід, який приведе до того, хто стоїть «по той бік дзеркала».

У темному лісі перемагає не той, хто швидше бігає, а той, кого не видно.

Що допомагає вижити?

1. Zero Trust	Філософія, в якій компрометація — не загроза, а даність. Ворог уже всередині системи. Довіряти — нікому.
2. Регулярна ротація ключів і сесій	Термін життя пароля чи токена — день, тиждень, місяць. Ні секунди більше.
3. Шифрування та out-of-band підтвердження	Зміст захищає шифр, а ідентичність — додатковий канал. Пошта + окремий пароль у Signal. Чат + дзвінок. Два джерела правди.
4. Контроль техніки	Службові пристрої, зашифровані диски, оновлення, MAC-регістри. Будь-який невідомий девайс — під забороною.
5. Двоконтурний Wi-Fi	Внутрішній сегмент — для перевірених пристроїв. Гостьовий — ізольований. Проста межа, що зупиняє більшість загроз.
6. Одноразові пристрої	Телефони без історії, без акаунтів, без IMEI. Канал на одну місію — і в утиль.
7. Цифрове радіомовчання	У проєктах високої чутливості Wi-Fi заборонений. Телефони — у чохлах Фарадея. Ніяких сигналів назовні.

8. Контроль зовнішніх API і бекдорів	Ваш продукт складається з десятків інтеграцій. Достатньо однієї «дірки» в одному постачальнику — і вас немає

Zero Trust нагадує: стін більше немає. Є лише мережа світла в темному лісі. І ваше завдання — не дозволити нікому підмінити це світло.