Цифровий детектив: розслідування кіберінцидентів

Про те, як криміналісти допомагають покращувати кіберзахист

Цифрова криміналістика (digital forensics) — це напрям кіберзахисту, який дає відповіді про те, хто, коли, яким чином і навіщо спричинив той чи інший інцидент безпеки. Результати розслідувань можуть використовуватись у суді і як докази для регуляторних органів, проте насамперед вони важливі для самих компаній, оскільки дозволяють зрозуміти обсяг і причини проблем і відповідно вдосконалити захист. Цифрові криміналісти співпрацюють з командами реагування на інциденти, через що ці напрями мають об'єднану назву — DFIR.

Для розслідувань використовують як спеціалізовані інструменти, так і системи кіберзахисту, які збирають і візуалізують дані, на кшталт SOAR та XDR. Є компанії, які надають послуги цифрової криміналістики. «МтБ» розбирався, як це працює.

Цифрова криміналістика

Взагалі під цифровою криміналістикою розуміють, власне, криміналістику — тобто збирання доказів злочинів, у цьому разі методами IT. Вона використовується для розслідування як кіберзлочинів на кшталт крадіжок даних або облікових записів, так і цілком фізичних злочинів: убивств, пограбувань тощо, а також злочинів фінансових і здирництва. Інакше кажучи, слідчі вилучають комп'ютери або мобільні телефони і шукають там докази.

Американська компанія BlueVoyant, яка працює у сфері кібербезпеки, так визначає напрямки цифрової криміналістики.

Криміналістичне дослідження комп'ютерів *(Computer Forensics)* — пошук доказів на комп'ютерах і в цифрових

системах зберігання даних. Передбачає дослідження даних задля виявлення, збереження, аналізу і презентації фактів і оцінок на базі дослідженої інформації. Тут використовуються приблизно такі ж прийоми і технології, що й для відновлення даних, але з залученням додаткових практик і процедур, які забезпечують документальну фіксацію доказів.

Криміналістичне дослідження мобільних пристроїв *(Mobile Device Forensics)* — передбачає отримання цифрових доказів з будь-якого пристрою, який має внутрішню пам'ять і функції зв'язку: наприклад, мобільних телефонів, кишенькових комп'ютерів PDA (якщо вони ще залишились в ужитку), планшетів і GPS-обладнання.

Криміналістичне дослідження мереж *(Network Forensics)* — тут за допомогою мережевих аналізаторів і реєстраторів вивчається активність у мережі зв'язку. Мережеві дані дуже динамічні, плинні і зникають після передавання. Тому криміналістичне дослідження мереж часто є проактивним (випереджальним) процесом.

Криміналістичний аналіз даних *(Forensic Data Analysis)* — це дослідження структурованих даних у прикладних системах і базах даних у контексті фінансових злочинів. Відбувається пошук і аналіз патернів шахрайських дій.

Криміналістичний аналіз баз даних *(Database Forensics)* — передбачає аналіз випадків доступу до баз даних і внесення змін. Наприклад, таким чином можна виявляти транзакції з ознаками злочинних дій або верифікувати дії конкретного користувача.

Процес криміналістичного дослідження складається з кількох етапів. На першому вилучаються фізичні носії доказів (комп'ютери, телефони тощо), при цьому задля збереження інформації її можна скопіювати. Далі експерти визначають, чи працювати з «живою» чи «мертвою» системою: наприклад, можна увімкнути ноутбук або вилучити жорсткий диск і підключити до лабораторного комп'ютера. Після чого ідентифікують інформацію, яка має стосунок до розслідування (наприклад, судовий ордер може обмежувати коло даних, які досліджуються).

На етапі власне аналізу потрібно дістати відповіді на питання: хто створив дані, хто їх редагував, як ці дані було створено і коли всі ці події сталися. Окрім того, дослідники визначають, який саме стосунок ця інформація має до справи. На останньому етапі отримані результати викладаються у зрозумілому для посполитих форматі, щоб їх могли прочитати зацікавлені сторони.

До методів комп'ютерної криміналістики належать: зворотна стеганографія (аналіз файлів зображень на предмет захованих у них даних); стохастичний аналіз (реконструкція активності, яка не залишає цифрових артефактів — наприклад, зламів, спричинених інсайдерами); аналіз за багатьма джерелами (зіставлення інформації з кількох комп'ютерів з метою виявлення аномалій); аналіз працюючого пристрою (видобування плинних даних, які зберігаються в оперативній пам'яті або кеші); відновлення видалених файлів.

Цифрова криміналістика і реагування

Цифрова криміналістика має інший вимір: виявлення та розслідування інцидентів кібербезпеки в організаціях. Вона є складовою процесу реагування на інциденти і використовується для виявлення причин цих інцидентів, знешкодження загроз, а також підготовки доказів для правоохоронних органів і захисту в суді.

Для цього з'явився окремий напрям кіберзахисту — цифрова криміналістика і реагування на інциденти (Digital Forensics and Incident Response — DFIR). Він доповнює загальну стратегію кіберзахисту, дає змогу швидко отримувати інформацію, необхідну для відбиття атаки, і забезпечує послідовний процес розслідування інцидентів.

Як зазначає компанія IBM, об'єднання двох напрямів забезпечує низку переваг. Якщо обидві команди не взаємодіють, вони можуть заважати одна одній. Захисники у процесі нейтралізації загрози можуть мимоволі знищити або видозмінити докази, тоді як розслідування може затримати вирішення проблеми. У процесі DFIR обидві дії відбуваються одночасно: в ході реагування на інцидент збирають і зберігають докази. А по завершенні нейтралізації загрози відбувається «розбір польотів» на основі накопиченої інформації, що дозволяє реконструювати усю хронологію подій, встановити обсяг шкоди і визначитися, як можна в майбутньому захиститися від подібних атак.

Це забезпечує більш ефективне запобігання загрозам, оскільки дає змогу краще розуміти кібератаки, створювати ефективніші плейбуки реагування і зупиняти атаки ще до їх початку. Окрім того, криміналістика допомагає з процесом «полювання на загрози» (Threat hunting), оскільки виявляє ознаки раніше не відомих загроз. А оскільки криміналістичні дослідження більш ретельні, ніж стандартні розслідування інцидентів, групи DFIR здатні виявляти приховані зловмисні програми і пошкодження, які інакше залишаються непоміченими. Це забезпечує більш якісне відновлення після атак.

З боку криміналістики DFIR гарантує, що не буде (або майже не буде) втрачено жодних доказів. Наприклад, у стандартному процесі реагування на загрозу фахівці з безпеки можуть вимкнути заражений пристрій, тим самим обнуливши його RAM-пам'ять і стерши докази. Окрім того, фахівці DFIR, навчені процесу документування збору доказів, забезпечують результати, які можна використовувати для позовів проти кіберзлочинців, у страхових справах і в аудиті після витоків даних.

Рекомендації NIST

Як працює цифрова криміналістика у цьому випадку? Американський Національний інститут стандартів

Рис. 1. Процес цифрової криміналістики згідно з NIST

і технологій (NIST) у керівництві від 2006 року визначає відповідні процедури. Вони ті ж самі, що і в загальній цифровій криміналістиці, але орієнтовані на пошук кіберзагроз (**рис. 1**).

По-перше, автори додають, що аналітикам можуть виявитися потрібними джерела інформації, які знаходяться поза їхнім контролем, що може мати свої складнощі. Наприклад, для отримання даних від інтернет-провайдера може знадобитись судовий ордер, доступ до персональних пристроїв співробітника залежить від політики компанії, а обстежити комп'ютер вдома у працівника буде ще складніше.

З іншого боку, організації можуть збирати дані проактивно. Наприклад, операційну систему можна налаштувати на запис певних подій, таких як входи користувачів. Важливою функцією є використання централізованих лог-серверів, куди різні системи та застосунки скидають логи подій для зберігання, що також уберігає від несанкціонованого втручання в ці журнали з метою перешкоджання розслідуванню. Автори навіть пропонують заходи з моніторингу поведінки користувачів, на кшталт запису натискань клавіш, хоча це вже може бути втручанням у приватне життя.

Перш ніж приступати до отримання даних, аналітикам варто розробити порядок їх отримання, що залежить від цінності потенційних джерел даних, волатильності даних і зусиль (часу, коштів), необхідних для їх отримання. Якщо інформацію не зібрано наперед різними інструментами безпеки, здійснюється копіювання волатильних даних спеціальними інструментами, дуплікація джерел неволатильних даних і вилучення носіїв.

Після цього здійснюється верифікація цілісності отриманих даних, щоб їх можна було використати в суді. Окрім того, в процесі збирання даних потрібно документувати кожен крок, записуючи й інформацію про кожен інструмент, який використовується. Це необхідно, щоб за потреби інші аналітики могли повторити процес. Також потрібно фотографувати зображення, документи, вікна програм і іншу інформацію, яка відображається на екрані. За можливості варто виділити окремого співробітника, який буде займатися всім цим документуванням.

Якщо дослідження проводиться просто під час інциденту, важливо ізолювати відповідні системи для запобігання поширенню загрози. При цьому аналітики можуть співпрацювати з командами реагування і разом приймати рішення щодо, наприклад, вимкнення живлення або від'єднання мережевих кабелів залежно від існуючих процедур і оцінки ризику — так, щоб достатньою мірою зменшити цей ризик і водночас зберегти цілісність доказів. Водночас організація мусить враховувати вартість простою, якщо, наприклад, необхідно на кілька годин відключити критично важливу систему для копіювання образу диска.

Одним з кроків для ізоляції інциденту є обмеження доступу до комп'ютера, щоб ніхто не міг віддалено змінити дані; за потреби можна навіть вимкнути точку доступу Wi-Fi, хоча це не завжди гарантує недоступність бездротової мережі. Але складають список людей, які мають доступ до цього комп'ютера, бо вони можуть надати паролі і підказати, де яка інформація знаходиться.

Після отримання даних відбувається їх перевірка і вилучення релевантної інформації. На цьому етапі може бути потрібно обходити механізми контролю доступу, стиснення і шифрування інформації, а також здійснювати пошук, наприклад, документів і листів, які стосуються конкретної особи.

DFIR-автоматизація

Велику частину роботи розслідувачів беруть на себе технології. По-перше, функцію збирання даних виконують загальні інструменти безпеки, такі як SIEM, SOAR і EDR/XDR.

Наприклад, у SIEM стікаються дані щодо подій в системі (log data), логи мережевого трафіку, а також інформація з інших джерел у мережі організації. Усі ці дані використовуються для виявлення загроз, реагування на інциденти і дій на випередження, а також розроблення протоколів дій проти конкретних загроз. Це багатство інформації є й проблемним місцем, оскільки аналітикам може бути складно в ній розбиратися і швидко виявляти критичні події. XDR дозволяє отримати повну картину подій на кінцевих станціях. Наприклад, Cortex XDR Forensics, додатковий модуль до рішення від Palo Alto Networks, збирає дані з дисків і пам'яті, дозволяє переглядати детальну інформацію про систему, аналізувати конкретну кінцеву точку або шукати артефакти на всіх пристроях (**рис. 2**).

Також існує безліч спеціалізованих інструментів, за допомогою яких команди DFIR можуть розслідувати і зупиняти кіберінциденти. Багато з них створені на базі відкритого коду і доступні безкоштовно, інші є комерційними продуктами. Ось лише деякі з них.

Платформа ***Cyber Triage*** може працювати на ноутбуці, у хмарі або на локальному сервері. Вона використовує для збирання інформації безагентний інструмент, який може працювати у складних середовищах, де неможливе використання агентів. Інтеграція з системами SIEM і EDR дозволяє негайно розпочати збір даних. Платформа сканує виконувані файли, використовуючи понад 40 механізмів виявлення зловмисного ПЗ, збирає десятки типів артефактів, які відповідають різним атакам, ідентифікує і рекомендує ті з них, що релевантні для розслідування. Персонал переглядає ці артефакти і копає глибше залежно від питань, які його цікавлять.

У жовтневому релізі 2024 року розробники додали функції виявлення ексфільтрації даних і використання сторонніх USB-пристроїв (**рис. 3**), обробку

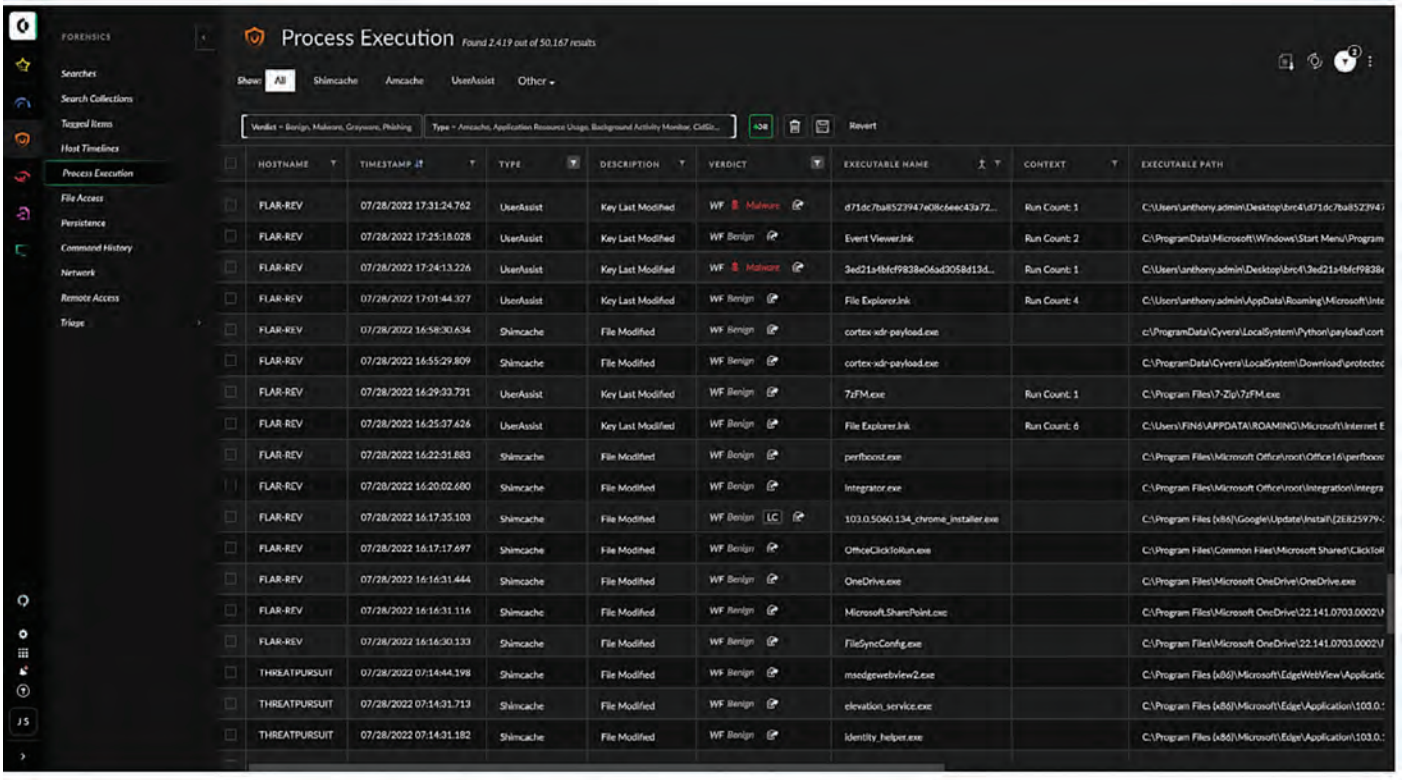


Рис. 2. Доступ до інформації в Cortex XDR Forensics (джерело: Palo Alto Networks)

образів на сервері і новий інструмент валідації результатів. Серед замовників Cyber Triage — NATO, Deloitte, FBR і армія США.

SIFT Workstation — це набір інструментів, початково створений Робом Лі (не плутати з відомим військовим аналітиком) з SANS Institute (абревіатура розшифровується як SANS Investigative Forensics Toolkit). За твердженням розробників, він не поступається жодному сучасному пакету інструментів для розслідування і реагування і доводить, що потужні можливості реагування на інциденти і глибоких криміналістичних досліджень можна отримати, використовуючи передові інструменти на базі відкритих джерел, які знаходяться у вільному доступі і часто оновлюються.

SIFT має функції для аналізу файлових систем, мереж, пам'яті та ін. Додатково можна інсталювати інструмент REMnux для реверсивного аналізу зловмисного ПЗ. SIFT використовує національна прокуратура Бразилії, зокрема через бюджетні обмеження.

GRR Rapid Response — ця система для реагування на інциденти сфокусована на віддаленій криміналістиці в реальному часі. Систему було створено, щоб дати змогу аналітикам швидко класифікувати атаки і здійснювати віддалений аналіз. Розробники відштовхувались від трьох сценаріїв: «Джо помітив щось дивне і перевіряє свою машину (p.s. Джо на вихідних у Камбоджі і виходить через 3G)»; «Візьміть 25 машин для криміналістичного аналізу (p.s. вони на 5 континентах і жодна не з Windows)»; «Скажіть мені, чи не скомпрометована ця машина (p.s. а заразом перевірте всі 100 тис. — тобто "прочешіть" увесь парк)».

Система складається з python-клієнта, який встановлюється в цільових системах, і серверної інфраструктури, також на python, яка керує клієнтами і забезпечує графічний інтерфейс користувача.

Bulk_extractor — це інструмент, який сканує образ диска, файл або директорію і видобуває корисну інформацію без парсингу файлової системи. Результат можна аналізувати

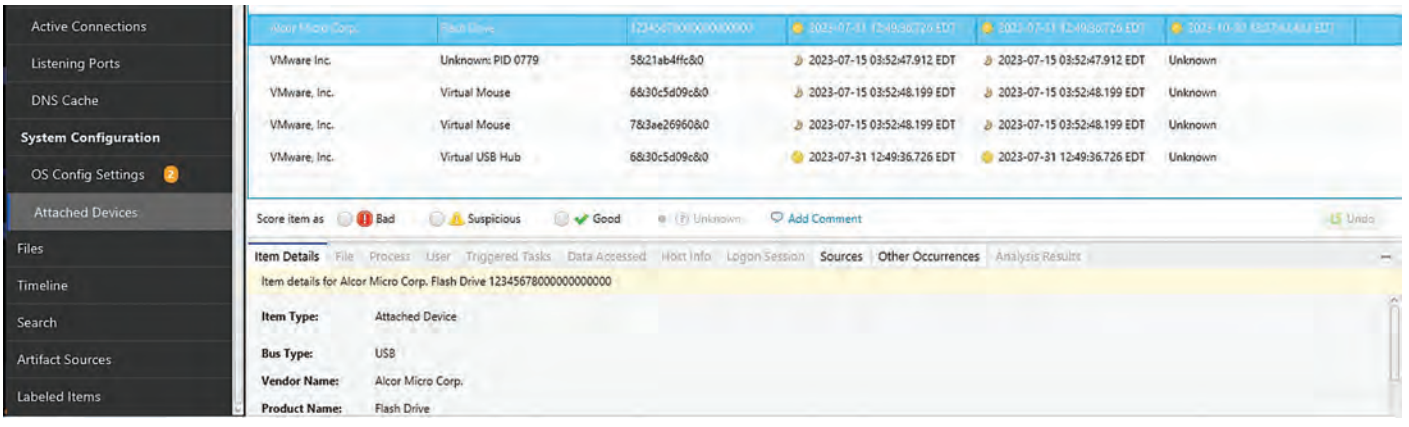


Рис. 3. Детекція підключень USB-пристроїв у Cyber Triage

іншими інструментами. Оскільки bulk_extractor ігнорує файлову систему, він може обробляти різні ділянки диска паралельно, розподіляючи їх між ядрами процесора. Іншою перевагою такого підходу є те, що програма здатна обробляти будь-які цифрові носії, як-от жорсткі диски і SSD, оптичні диски, мобільні телефони тощо. Також існують додаткові програми для подальшої обробки даних. Наприклад, можна створити образ диска, дати комп'ютеру попрацювати деякий час, повторити процедуру і порівняти два образи — так можна зрозуміти дії користувача за цей проміжок.

The Volatility Framework — платформа, створена неприбутковою організацією Volatility Foundation і призначена для видобування даних з енергозалежної пам'яті для криміналістичної експертизи.

Криміналістика як сервіс

Оскільки криміналістичні дослідження вочевидь потребують спеціалізованих інструментів, а головне — навченого персоналу, для бізнесів вони можуть бути дорогим задоволенням. Тому логічним чином з'явилися компанії, які пропонують такі операції як послугу.

Gartner у своєму ринковому путівникові за червень 2024 року вказує, що організації, які надають послуги Managed Detection and Response (MDR), також можуть додатково пропонувати DFIR. Деякі з них встановлюють на кінцевих точках замовника свої агенти, інші обходяться без агентів, а треті потребують наявності у клієнта якогось рішення EDR.

Загалом Gartner у своїх рейтингах згадує десятки провайдерів DFIR. Криміналістичну експертизу пропонують як частину сервісу кіберзахисту вендори рішень кібербезпеки, як-от IBM X-Force, Check Point Infinity Global Services, Cisco Talos або Palo Alto Unit 42. Також її пропонують глобальні консалтингові фірми, провайдери керованих сервісів безпеки (MSSP) і спеціалізовані «бутікові» фірми з надання послуг безпеки. Найчастіше вони укладають з замовником річні контракти, проте деякі працюють за викликом (від інциденту до інциденту), а ще інші укладають договори без передоплати, але й послуги надають без формального SLA. Цікавим трендом є те, що підписки на послугу DFIR вимагають кіберстрахувальники.

Gartner зазначає, що провайдери DFIR повинні допомагати організаціям, окрім дослідження зловмисної активності, реверсивного аналізу зловмисного ПЗ і допомоги у відновленні також: здійснювати навчання та тренування; вести переговори зі злочинцями (наприклад, стосовно викупу); допомагати з відновленням даних, зокрема знаходити відповідні дешифрувальники і забезпечувати документування процесу; допомагати в судовому процесі, зокрема свідченнями і представництвом в суді; підтримувати особливі сценарії, такі як OT, IoT і мобільні пристрої.

Справді, наприклад, компанія SafeAeon пропонує не лише аналіз мережевого трафіку і пам'яті плюс реагування на інциденти, а й реверсивний аналіз зловмисного ПЗ, відновлення даних з пошкоджених накопичувачів, аналіз фінансових даних для виявлення потенційних фінансових злочинів, збір та аналіз інформації з соціальних мереж. Компанія Trustwave обіцяє допомогу з судовим захистом на випадок витоку даних.

Gartner радить усвідомити, що інциденти кібербезпеки — це ситуації типу «коли це станеться», а не «якщо це станеться», тому організаціям потрібно мати програми реагування і впровадити відповідні процеси, регулярно ті процеси тестувати. Не можна з цим не погодитись.

Василь ТКАЧЕНКО, **МтБ**

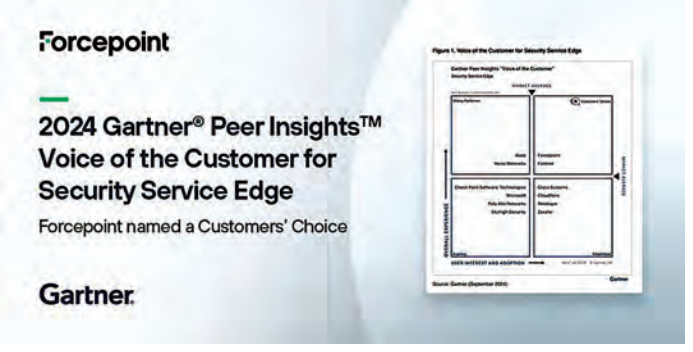
ХРОНІКА

Компанія Forcepoint визнана вибором клієнтів 2024 року в рейтингу Gartner Peer Insights Voice of Customer for Security Service Edge

У звіті Gartner Peer Insights Voice of the Customer від 27 вересня компанія Forcepoint отримала загальний рейтинг 4,7 із 5 на ринку послуг безпеки Security Service Edge (SSE) та 98% готовності рекомендувати її на основі 65 відповідей у Gartner Peer Insights Voice of the Customer станом на 31 липня 2024 року. Виробник рішень також отримав найвищу оцінку у розділі «Можливості продукту».

У звіті Gartner зібрано коментарі реальних користувачів продуктів: «організації використовують *Security Service Edge* як рішення для ефективної роботи гібридних співробітників із цілою низкою хмарних технологій та засобів безпеки».

SSE-рішення Forcepoint ONE, орієнтоване на роботу з даними, унікальним чином поєднує у собі розширений захист від загроз і безпеку даних корпоративного класу зі зручністю використання, що дозволяє підвищити продуктивність роботи співробітників, скоротити операційні витрати, знизити ризики та оптимізувати дотримання нормативних вимог.



За матеріалами компанії Oberig IT, офіційного дистриб'ютора Forcepoint в Україні.