Cisco 2018
Річний звіт з кібербезпеки

Зміст

Основні положення

Що було б, якби засоби захисту могли бачити майбутнє? Якби вони знали, що насувається атака, вони могли б її зупинити. Або принаймні пом'якшити її вплив і допомогти забезпечити безпеку об'єктів, які потребують найбільшого захисту. Гарна новина: засоби захисту вже вміють розпізнавати потенційні загрози. Є багато характерних, і до того ж очевидних ознак, які вказують на існування загроз.

Зловмисники та гравці, за якими стоять держави, вже мають необхідні знання й інструменти, щоб зруйнувати критично важливу інфраструктуру і паралізувати життя цілих регіонів. Але коли з'являються новини про руйнівні кібератаки, такі як, наприклад, трапилися в Україні чи інших країнах світу, деякі фахівці з безпеки можуть спочатку подумати:

«Ринкове/регіональне/технологічне середовище нашої компанії не було ціллю, отже, напевно, ми не знаходимося в зоні ризику».

Однак, відкидаючи те, що здається далеким і чужим, або дозволяючи собі відволікатися на хаос щоденних дрібних сутичок зі зловмисниками, спеціалісти з безпеки припиняють/втрачають можливість розпізнавати швидкість та масштаби накопичення та вдосконалення зловмисниками їхньої кіберзброї.

Упродовж багатьох років компанія Cisco попереджала спеціалістів з безпеки про зростання рівня кіберзлочинності в усьому світі. У цьому річному звіті з інформаційної безпеки ми представляємо дані та аналіз, проведений дослідниками загроз компанії Cisco та нашими технологічними партнерами щодо поведінки зловмисників за результатами спостережень протягом останніх 12–18 місяців. Значна кількість тем, розглянутих у звіті, зосереджені на трьох основних питаннях:

1. **Зловмисники доводять шкідливе програмне забезпечення до безпрецедентних рівнів досконалості та впливу.**

   Еволюція шкідливого програмного забезпечення (стор. 6) була однією з найпомітніших подій у контексті атак 2017 року. Поява мережних програм-здирників (ransomware), що вимагають викупу в криптовалюті, усуває потребу залучення людини до запуску ransomware-кампаній. А для деяких зловмисників нагородою є не викуп, а знищення систем і даних, що підтверджує шкідлива програма Nyetya, яка не залишала слідів своєї активності та маскувалася під програму-здирника (див. стор. 6). Шкідливі програми, що здатні поширюватися самостійно, є небезпечними і, за словами дослідників загроз з компанії Cisco, потенційно можуть «покласти» Інтернет.

2. **Зловмисники дедалі більш вправно уникають виявлення та застосовують в якості зброї хмарні сервіси й інші технології, які зазвичай використовуються в легальних цілях.**

   Додатково до створення загроз, які можуть **уникати так званих «пісочниць»** (виділених середовищ для безпечного запуску комп'ютерних програм) (стор. 22), зловмисники дедалі більше **використовують шифрування з метою уникнення виявлення** (стор. 9). Шифрування призначене для підвищення рівня безпеки, але воно також надає зловмисникам потужний інструмент для приховування каналів керування зловмисним кодом (C2), що надає їм більше часу для роботи та заподіяння шкоди.

   Кіберзлочинці також використовують **канали керування, що працюють на основі легальних інтернет-сервісів,** таких як Google, Dropbox та GitHub (див. стор. 24). Дані практики роблять виявлення трафіку зловмисного програмного забезпечення майже неможливим.

   Крім того, щоб отримати максимальну віддачу від своїх інвестицій, багато зловмисників **запускають декілька кампаній з одного домену** (стор. 26). Вони також повторно використовують ресурси інфраструктури, такі як адреси електронної пошти реєстрантів, номери в автономній системі (ASN) та сервери імен.

3. **Зловмисники використовують прогалини в системі безпеки, значна кількість яких пов'язана з розширенням Інтернету речей (Internet of Things, IoT) та застосуванням хмарних сервісів.**

   Спеціалісти із захисту швидкими темпами впроваджують IoT-пристрої, проте звертають мало уваги на безпеку цих систем. **Незахищені та неконтрольовані IoT-пристрої** надають зловмисникам можливість проникати в мережі (стор. 34). Згідно з результатами дослідження, організації, що мають IoT-пристрої, які є незахищеними від атак, також, здається, **не мотивовані прискорювати усунення наслідків атак** (стор. 42). Гірше за те, ці організації, ймовірно, мають набагато вразливіші IoT-пристрої у своїх IT-середовищах, про які вони навіть не знають.

Тим часом разом з Інтернетом речей **розширюється використання бот-мереж на базі IoT,** які стають досконалішими й більш автоматизованими. У міру їхнього зростання зловмисники використовують їх для запуску більш просунутих розподілених атак типу «відмова в обслуговуванні» (DDoS) (стор. 31).

Зловмисники також використовують на свою користь той факт, що команди служб безпеки **мають певні труднощі із захистом як IoT, так і хмарних середовищ.** Однією з причин є відсутність чіткого розуміння стосовно того, хто саме несе відповідальність за захист таких середовищ (див. стор. 42).

Рекомендації для спеціалістів із захисту

Коли зловмисники неминуче вдарять по їхніх організаціях, чи будуть готові до цього системи захисту? І як швидко вони зможуть відновити роботу? Результати проведеного **Cisco Порівняльного дослідження рішень безпеки за 2018 рік** (Security Capabilities Benchmark Study), яке містить приклади роботи з питаннями безпеки від більш ніж 3600 респондентів з 26 країн, демонструють, що спеціалістам із захисту необхідно вирішувати велику кількість проблем (стор. 46).

Навіть у такому випадку спеціалісти із захисту дізнаються, що здійснення стратегічних удосконалень безпеки та дотримання найкращих практик може зменшити сприйнятливість до ризиків уповільнити виконання зловмисниками своїх планів та забезпечити вищий рівень помітності загроз. Їм варто замислитися про наступне:

- Запровадження інструментів «першої лінії захисту», які можуть масштабуватися, наприклад, платформи хмарної інформаційної безпеки.
- Гарантування дотримання корпоративних політик та процедур щодо оновлення програм, систем і пристроїв.
- Сегментація мереж для зменшення впливу від проникнення.
- Запровадження наступного покоління інструментів моніторингу процесів у кінцевих вузлах.
- Своєчасне підключення точних даних аналітики загроз і процесів, що дозволяють включити такі дані до системи моніторингу та обробки подій у сфері безпеки.
- Проведення більш глибокої та розширеної аналітичної роботи.
- Перегляд та відпрацювання процедур реагування на проблеми у сфері безпеки.
- Часте резервування даних та тестування процедур/процесів відновлення, що є надзвичайно важливим у світі шкідливих мережних програм-здирників, які швидко розповсюджуються, та нищівної кіберзброї.
- Аналіз тестування ефективності технологій безпеки третіх сторін з метою зниження ризику атак на ланцюги поставок.
- Проведення перевірок (сканувань) на предмет проблем з безпекою мікрослужб, хмарних служб та систем адміністрування програм.
- Аналіз систем безпеки та вивчення можливості використання аналітики каналів SSL та, якщо можливо, SSL-дешифрування.

Спеціалістам із захисту також варто розглядати можливість застосування передових технологій безпеки, які включають у себе можливості машинного навчання та штучного інтелекту. Зважаючи на те, що шкідливе ПЗ ховає свою комунікацію всередині зашифрованого веб-трафіку, а неавторизовані інсайдери надсилають конфіденційні дані через корпоративні хмарні системи, команди служб безпеки потребують ефективних інструментів для запобігання або виявлення шифрування, що приховує діяльність шкідливих програм.

Про звіт

Річний звіт ***Cisco з інформаційної безпеки за 2018 рік*** представляє останні досягнення індустрії у сфері безпеки, мета яких – допомогти організаціям і користувачам захиститися від атак. Ми також розглядаємо технології та стратегії, які зловмисники використовують для проходження через засоби захисту та уникнення виявлення.

У звіті висвітлено основні результати проведеного **Cisco Порівняльного дослідження рішень безпеки за 2018 рік** (Security Capabilities Benchmark Study), в якому вивчаються засоби безпеки підприємств та їхня думка стосовно готовності їх до захисту від атак.

Частина I:
Ландшафт атак

Частина I: Ландшафт атак

Зловмисники роблять шкідливе програмне забезпечення з безпрецедентним рівнем складності та впливу. Зростаюча кількість та різноманітність шкідливих програм підсилюють хаос у ландшафті атак, підриваючи зусилля щодо захисту від загроз.

РОЗВИТОК ШКІДЛИВИХ ПРОГРАМ

Один з найважливіших проривів у ландшафті атак 2017 року полягав у розвитку програм-здирників. Поява мережних програм-здирників усуває потребу в наявності людського елемента під час запуску зловмисних кампаній. Причому в деяких випадках винагородою є не викуп, а руйнування систем і даних. Ми очікуємо побачити більше цієї активності наступного року.

Вони вже там: у 2018 році захисники мають підготуватися до нових мережних загроз, які розповсюджуються самостійно

2017 року програми-здирники вийшли на новий рівень, хоча це й було досить очікувано. Після кампанії SamSam у березні 2016[1] року – першої масштабної атаки, яка використовувала мережний вектор для програми-здирника, видаляючи таким чином користувача з процесу зараження, дослідники загроз компанії Cisco знали, що через деякий час учасники загрози знайдуть спосіб автоматизувати цю техніку. Зловмисники могли б зробити свої шкідливі програми ще більш потужними, поєднуючи їх з «черв'якоподібними» функціями з метою приведення до масштабних збитків.

Розвиток шкідливих програм був стрімким. У травні 2017 року комп'ютерний вірус WannaCry з'явився та поширювався, як пожежа, по всьому Інтернету[2]. Для поширення він скористався вразливістю безпеки Microsoft Windows під назвою EternalBlue, інформація про яку витікла від групи хакерів Shadow Brokers у середині квітня 2017 року.

WannaCry заробив більше $143 тисяч через платежі біткойнами на момент, коли кошти з гаманців були виведені в готівку. З огляду на хронологію подій та розрахувавши зростання вартості біткойнів, які було початково сплачено в гаманці на суму в розмірі $93,531, за оцінками дослідників загроз Cisco в якості викупу було здійснено приблизно 312 платежів. Для порівняння, набір з експлуатації вразливостей Angler (у період його активності) заробляв близько $100 млн на рік – як глобальний бізнес.

WannaCry не відслідковував шкоду для постраждалих користувачів та платежі, що були здійснені ними. Кількість користувачів, які отримали ключі для дешифрування після здійснення платежу, також невідома. (WannaCry все ще розповсюджується, а користувачі продовжують платити викуп – а дарма). Через дуже низьку продуктивність WannaCry як програми-здирника уряд США і багато дослідників у галузі безпеки вважають, що компонент викупу є ефективним засобом для приховування дійсної мети WannaCry – стирання даних.

Nyetya (також відомий як NotPetya) з'явився у червні 2017 року[3]. Ця шкідлива програма для стирання даних також маскується під здирника та застосовує вразливість віддаленого виконання коду під назвою EternalBlue, а також вразливість віддаленого виконання коду EternalRomance (що також просочився через хакерську групу Shadow Brokers) та інші вектори, що включають збирання облікових даних, не пов'язаних із випуском Shadow Brokers[4]. Nyetya було розгорнуто через системи оновлення для пакета податкового програмного забезпечення, який використовують понад 80 % компаній в Україні та який встановлений на більш ніж 1 млн

1 *SamSam: The Doctor Will See You, After He Pays the Ransom,* блог Cisco Talos, березень 2016 року: blog.talosintelligence.com/2016/03/samsam-ransomware.html.
2 *Player 3 Has Entered the Game: Say Hello to 'WannaCry,'* блог Cisco Talos, травень 2017 року: blog.talosintelligence.com/2017/05/wannacry.html.
3 *New Ransomware Variant 'Nyetya' Compromises Systems Worldwide,* блог Cisco Talos, червень 2017: blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.
4 *Ibid*

комп'ютерів[5]. Українська кіберполіція підтвердила, що від цієї атаки постраждало більше двох тисяч українських компаній[6].

Перед появою саморозповсюдної програми-здирника шкідливе програмне забезпечення розповсюджувалось трьома способами: приховане завантаження, електронна пошта або через фізичні носії, такі як, наприклад, заражені пристрої пам'яті USB. Усі способи передбачали певну взаємодію з людиною для зараження пристрою або системи. Ураховуючи застосування зловмисниками таких нових векторів, усе що потрібно для запуску мережної кампанії програми-здирника, – це активна робоча станція, на яку не було встановлено необхідні оновлення.

Спеціалісти з безпеки можуть вважати черв'яка старим типом загрози, оскільки кількість червоподібних CVE із Загального переліку вразливостей та загроз (Common Vulnerabilities and Exposures) знизилась із покращанням базового рівня безпеки продуктів. Проте, на думку дослідників з компанії Cisco, саморозповсюдне шкідливе програмне забезпечення є не просто актуальною загрозою, але також має потенціал «покласти» Інтернет. WannaCry та Nyetya – це лише проба того, що може бути, тому спеціалісти із захисту повинні знаходитись у повній бойовій готовності.

WannaCry та Nyetya могли б бути попереджені або їхній влив міг бути суттєво знижений, якби більша кількість організацій застосовувала найкращі практики базової безпеки. А саме такі, як виправлення вразливостей, запровадження відповідних процесів і політик для реагування на інциденти, а також використання мережної сегментації.

Для отримання додаткових порад щодо боротьби із загрозою автоматизованих мережних червоподібних програм-здирників читайте розділ ***«Назад до основ: захист від черв'яків в епоху програм-здирників»*** у блозі Cisco Talos.

Слабкі місця безпеки: ланцюг поставок

Кампанія Nyetya також була атакою через ланцюг поставок – однією з тих багатьох, які спостерігали дослідники Cisco у 2017 році. Одна з причин успіху Nyetya в зараженні такої кількості машин з такою швидкістю – що користувачі не сприймали автоматичне оновлення програмного забезпечення як ризик для безпеки. А в деяких випадках навіть не розуміли, що вони отримують шкідливі оновлення.

Інша атака через ланцюг поставок відбулась у вересні 2017 року. В ній були задіяні сервери завантаження, що використовуються виробником для поширення легітимного пакета програмного забезпечення, відомого як CCleaner[7]. Бінарні коди CCleaner, що містили троянський бекдор, були підписані з використанням дійсного сертифіката. Це створило в користувачів хибну впевненість у тому, що програмне забезпечення, яке вони використовують, було безпечним. Зловмисники, які стояли за цією атакою, були націлені на великі технологічні компанії, в яких використовувалось програмне забезпечення як на законних підставах, так і в якості тіньових IT-ресурсів.

Схоже, що атаки через ланцюги поставок зростають як у контексті швидкості, так і в контексті складності. Вони можуть впливати на комп'ютери у величезному масштабі та можуть зберігатися протягом місяців чи навіть років. Спеціалісти із захисту повинні знати про потенційний ризик використання програмного чи апаратного забезпечення від організацій, які не мають відповідальної позиції щодо безпеки. Шукайте постачальників, які видають CVE, здатні швидко впоратись із загрозами та постійно намагаються гарантувати, що їхні системи збирання не мають вразливих місць. Крім того, користувачі повинні виділяти час на сканування нового програмного забезпечення перед його завантаженням для гарантування того, що воно не містить шкідливих програм.

Мережна сегментація програмного забезпечення, яке не підкріплене засобами комплексної безпеки, може сприяти обмеженню шкоди внаслідок атак через ланцюг постачання, запобігаючи її поширенню на всю організацію.

5 *Ukraine scrambles to contain new cyber threat after 'NotPetya' attack,* автори Jack Stubbs та Matthias Williams, Reuters, липень 2017 року: reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.
6 *The MeDoc Connection,* блог Cisco Talos, липень 2017 року: blog.talosintelligence.com/2017/07/the-medoc-connection.html.
7 *CCleaner Command and Control Causes Concern,* блог Cisco Talos, вересень 2017 року: blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

Чому достовірність має важливе значення в звітах про дослідження щодо загроз?

Усі організації, що надають інформацію про загрози своїм клієнтам чи широкому загалу через будь-який канал, повинні використовувати рекомендації, які допоможуть забезпечити точність їхніх звітів. Навіть якщо не всі факти є зрозумілими, організації все одно можуть повідомити те, що вони знають, але уникати здогадок. Краще бути правим, ніж першим.

Наприклад, коли в травні 2017 року розгорнулась атака WannaCry, у професійному середовищі з питань безпеки панувала певна збентеженість щодо того, яким чином програма-здирник проникала в системи. Велика кількість організацій як у державному, так і в приватному секторі повідомляли, що атака виникла внаслідок фішингової кампанії та відкриття шкідливих вкладень з повідомлень електронної пошти. Проте, мережна загроза по суті полягала у виявленні та зараженні вразливих загальнодоступних портів серверу Microsoft Windows Server Message Block (SMB).

Дослідники загроз з компанії Cisco швидко повідомили спільноті спеціалістів з безпеки про те, що електронні листи, які, на їхню думку, пов'язані з кампанією WannaCry, були швидше спам-повідомленнями від бота Necurs, які поширювали програму-здирника Jaff. Минуло декілька днів до того, як спільнота погодилася, що підозрілі листи містили Jaff, а не WannaCry. І протягом усього цього часу користувачі використовували інформацію, яка не могла допомогти їм уникнути впливу стрімкої кампанії WannaCry.

Відчуття хаосу, яке панувало після поширення кампанії WannaCry, нагадує про те, що спільнота із безпеки повинна уникати повідомлення неточних фактів щодо походження та характеру кібератак. В перші години кампанії відчуття необхідності невідкладного реагування з метою оперативної зупинки зловмисників та захисту користувачів може легко призвести до оприлюднення, особливо в соціальних мережах, інформації, яка може вводити її користувачів в оману та не дати їм можливості захистити свої системи.

Для отримання більш детальної інформації із цього питання рекомендуємо Вам переглянути статтю **«Про поширення сумнівів»** у блозі Cisco Talos.

ЗАШИФРОВАНИЙ ЗЛОВМИСНИЙ ВЕБ-ТРАФІК

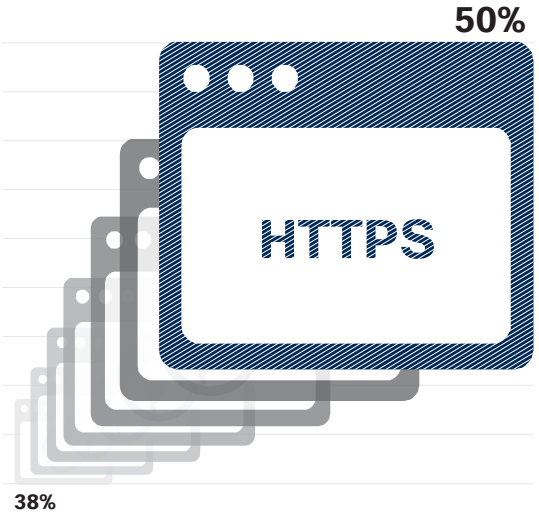
Постійно зростаючий обсяг зашифрованого веб-трафіку, як легального, так і зловмисного, створює ще більше проблем і плутанини в намаганні ідентифікувати та відстежувати потенційні загрози. Шифрування призначене для підвищення рівня безпеки, але воно також забезпечує зловмисникам потужний інструмент, який приховує діяльність каналів керування зловмисним кодом (C2), надаючи їм більше часу для заподіяння шкоди. Дослідники загроз з компанії Cisco очікують, що зловмисники збільшать застосування шифрування у 2018 році. Щоб не відставати, спеціалістам із захисту доведеться використовувати більший рівень автоматизації та більш вдосконалені інструменти, такі як машинне навчання й штучний інтелект, для підвищення потенціалу попередження, виявлення та відновлення після загроз.

Темна пляма для засобів захисту: зашифрований зловмисний веб-трафік

Дослідники загроз з компанії Cisco повідомляють, що станом на жовтень 2017 року 50% глобального веб-трафіку було зашифровано. Тобто з листопада 2016 року цей обсяг збільшився на 12 пунктів (див. Рисунок 1). Одним з чинників, що призвів до такого зростання, є наявність дешевих або безкоштовних SSL-сертифікатів. Іншим чинником зростання є різке розширення практики Google Chrome маркувати як «не захищені» незашифровані веб-сайти, що обробляють конфіденційну інформацію, як, наприклад, інформацію про кредитні картки клієнтів. Компанії зацікавлені в дотриманні вимог Google щодо шифрування HTTPS, якщо вони не хочуть мати ризик потенційно значного зниження рейтингу пошуку їхньої сторінки в Google.

Із зростанням обсягу зашифрованого глобального веб-трафіку зловмисники, як виявляється, розширюють застосування шифрування в якості інструмента для приховування діяльності каналів керування C2. Дослідники загроз із компанії Cisco спостерігали більш ніж потрійне збільшення зашифрованої мережної комунікації, що використовується аналізованими зразками шкідливих програм протягом 12-місячного періоду (див. Рисунок 2). Наш аналіз понад 400 000 шкідливих бінарних файлів виявив, що близько 70% використовували певне шифрування станом на жовтень 2017 року.

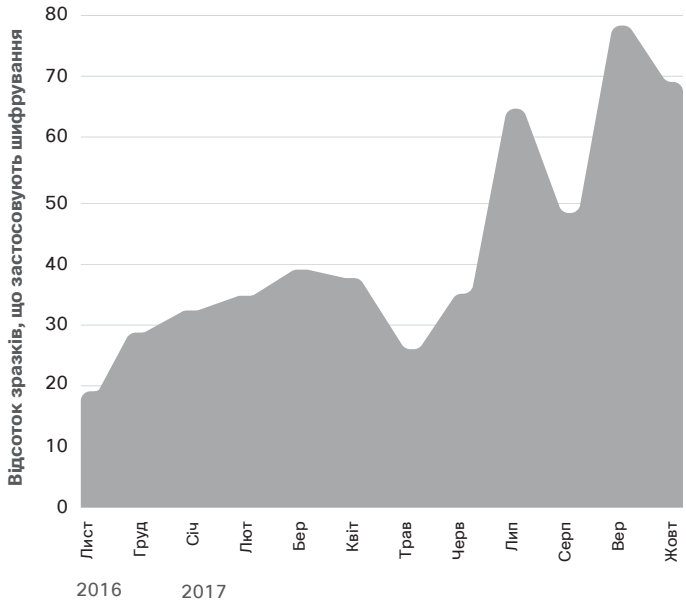
Рисунок 1 Збільшення обсягу зашифрованого глобального веб-трафіку



12-відсоткове зростання Глобального веб-трафіку в період з листопада 2016 по жовтень 2017 року

Джерело: дослідження Cisco щодо безпеки

Рисунок 2 Збільшення обсягу шкідливих бінарних кодів з використанням мережної комунікацій з певним шифруванням



Джерело: дослідження Cisco щодо безпеки

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Застосування машинного навчання до спектру загроз

Ми бачимо, що для подолання недостатньої видимості внаслідок шифрування та для зменшення часу роботи зловмисників більша кількість компаній вивчає можливості використання машинного навчання та штучного інтелекту. Ці сучасні можливості можуть покращити засоби захисту мережної безпеки і з часом навчитися автоматично виявляти незвичні моделі веб-трафіку, що може свідчити про шкідливу активність.

Машинне навчання є корисним для автоматичного виявлення відомих загроз – типів заражень, які були помічені раніше (див. Рисунок 3). Але його реальна цінність, особливо в разі моніторингу зашифрованого веб-трафіку, зумовлена його здатністю виявляти загрози типу «відомі-невідомі» (раніше невідомих варіантів відомих загроз, підсімейств зловмисних програм або пов'язаних з ними нових загроз) та «невідомі-невідомі» (нові мережні шкідливі програми). Технологія може навчитися виявляти незвичні моделі у великих обсягах зашифрованого веб-трафіку й автоматично попереджати команди безпеки про необхідність подальшого дослідження.

Саме останній аспект має важливе значення, оскільки нестача кваліфікованого персоналу є перешкодою для вдосконалення засобів захисту безпеки в багатьох організаціях. Це підтверджується результатами Порівняльного дослідження рішень безпеки за 2018 рік, проведеного компанією Cisco (див. на стор. 35). Автоматизація та інтелектуальні засоби, такі як машинне навчання та штучний інтелект, можуть допомогти спеціалістам із захисту компенсувати недоліки в навичках та ресурсах, зробити їх ефективнішими при виявленні та реагуванні як на відомі, так і на нові загрози.

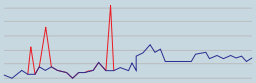
Рисунок 3 Машинне навчання в мережній безпеці: класифікація та систематизація

Відомі-відомі
Виявлення точно відомих виявлених раніше загроз

Відомі-невідомі
Виявлення до цього невідомих версій вже відомих загроз, підсімейств або пов'язаних нових загроз

Невідомі-невідомі
Виявлення шкідливих програм нульового дня, непов'язаних з відомими раніше

Тип загрози – Відповідна техніка виявлення

	Статичні підписи	Динамічні підписи	Поведінкові підписи	Шаблони високого рівня	Неконтрольовані аномалії
Приклади	Конкретне зловмисне доменне ім'я, пов'язане з трояном **server1.39slxu3bw.ru**	Телеметричний шаблон Houdini RAT **regex: .*/i[a-z]-(ready|ri-noy|gnfoh)**	Два ілюстративних знайдених приклади **hxxp://crazyerror.su/b/opt/8681BAE3DB3A2F9D446CD5E3** **hxxp://50.63.147.69:8080/b/req/3D111E6B21F373015C646CA4**	Загальні характеристики підозрілого трафіку 	Очікувані-непояснені та неочікувані 
Що вони роблять	**Ручне визначення, можлива інструментальна допомога** Точне співставлення попередньо заданого символу або числових послідовностей Читабельні для людини визначення	**Ручне визначення, можлива інструментальна допомога** Співставлення попередньо встановлених правил (наприклад, regex – регулярний вираз) Визначення, читабельні для людини	**Застосовується через засоби контрольованого машинного навчання** Співставлення правил, визначених за допомогою машинного навчання, або розпізнавання моделей поведінки, визначених за допомогою машинного навчання, в трансформованому функціональному просторі	**Завдання для напівконтрольованого машинного навчання** Шаблони дуже високого рівня, машинне навчання з метою виявлення узагальненої поведінки	**Автоматичне машинне навчання** Випадки, які істотно відрізняються від усіх відомих звичайних моделей поведінки, де модель відомої поведінки є об'єктом машинного навчання Дистанційні заходи можуть бути дуже абстрактними
Властивості техніки	**Дуже висока точність** **Без узагальнення** Повнота повернення, обмежена точно такими ж самими випадками **Добра можливість пояснення** **Не масштабується** **Вимагає ручного визначення** *Не застосовується до зашифрованих даних без MiTM*	**Дуже висока точність** **Обмежене узагальнення** Повнота повернення обмежена визначеним шаблоном; знаходить варіації, які чітко покриваються шаблоном **Добра можливість пояснення** **Добре не масштабується** **Вимагає ручного визначення** *Не застосовується до зашифрованих даних без MiTM*	**Висока точність** **Узагальнення на основі схожості з відомими шкідливими програмами** Ідеально для виявлення раніше невідомих варіантів/підсімейств відомих загроз **Добра можливість пояснення, більш ускладнена** **Досить добре масштабується** **(Напів-)автоматичне навчання на основі даних** *Застосовується до зашифрованих даних без розшифрування*	**Хороша точність** **Узагальнення на основі загально-прийнятої підозрілої поведінки** Висока повнота повернення, гарна можливість знайти загрозу нульового дня, але при більшій кількості помилкових тривог **Обмежена можливість пояснення** Результати може бути важко віднести до відомих загроз **Добре масштабується** **(Напів-)автоматичне навчання на основі даних** *Застосовується до зашифрованих даних без розшифрування*	**Низька точність** **Узагальнення на основі незвичної поведінки** Найкраща можливість знайти загрозу нульового дня, найвищий ризик помилкових тривог **Складно для пояснення** Результати може бути важко віднести до відомих загроз **Добре масштабується** **Автоматичне навчання на основі даних** *Застосовується до зашифрованих даних без розшифрування*

Краща точність та пояснення, простота доказів

Краща повнота повернення, масштабованість, можливість застосування до зашифрованих даних, можливість виявлення вразливостей нульового дня

Техніка співвіднесення

Зверніть увагу: звіти масштабування стосуються часу, необхідного людині для підтримки системи виявлення
Зверніть увагу: ця діаграма є спрощеною ілюстрацією можливостей машинного навчання у сфері безпеки

Джерело: дослідження Cisco щодо безпеки

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

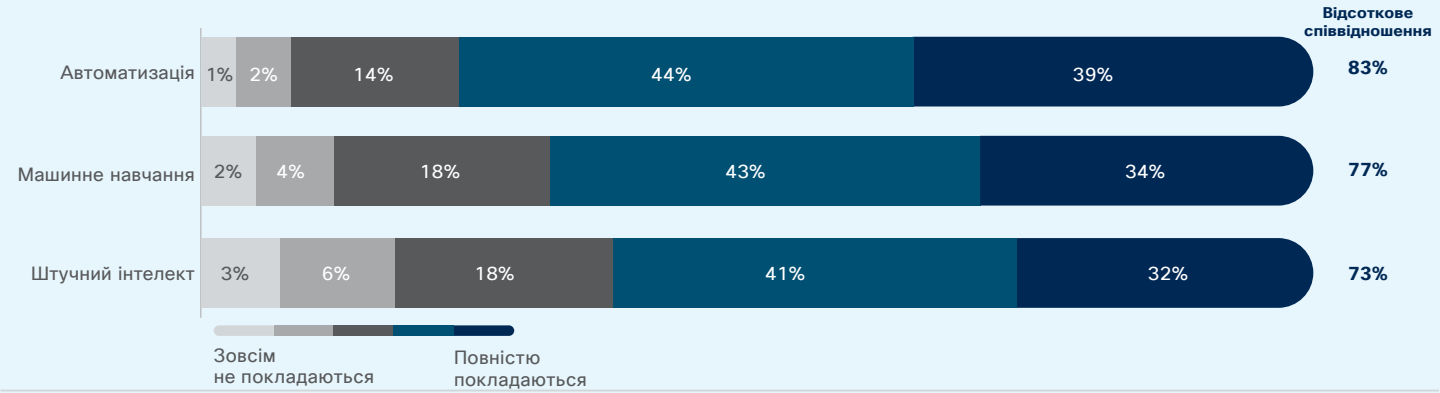
Порівняльне дослідження рішень безпеки за 2018 рік, проведене компанією Cisco: спеціалісти із захисту повідомляють про більшу довіру до автоматизації та штучного інтелекту

Директори з питань інформаційної безпеки (CISO), які були опитані в рамках Порівняльного дослідження рішень безпеки за 2018 рік, проведеного компанією Cisco, повідомляють, що вони бажають використовувати інструменти штучного інтелекту та машинного навчання. Директори вважають, що рівень складності та інтелекту їхньої інфраструктури безпеки постійно зростає. Однак вони також розчаровані кількістю помилкових спрацьовувань, які створюють такі системи, оскільки помилкові виявлення збільшують навантаження на команду безпеки. З часом ці проблеми мають бути вирішені, оскільки технології машинного навчання та штучного інтелекту постійно розвиваються і вчаться розпізнавати, що є нормальною активністю у мережних середовищах, які вони моніторять.

На питання стосовно того, на які автоматизовані технології їхні організації покладаються найбільше, 39% спеціалістів у галузі безпеки заявляють, що повністю покладаються на автоматизацію, у той час як 34% повністю покладаються на машинне навчання, а 32% повідомили, що їхня робота повністю базується на штучному інтелекті (Рисунок 4).

Інструменти аналізу поведінки також вважаються корисними при виявленні зловмисників у мережі; 92% спеціалістів з питань безпеки заявляють, що такі інструменти працюють у діапазоні від «дуже добре» до «надзвичайно добре» (Рисунок 5).

Рисунок 4 Організації сильно покладаються на автоматизацію, машинне навчання та штучний інтелект



Джерело: дослідження Cisco щодо безпеки

Рисунок 5 Більшість спеціалістів галузі безпеки усвідомлюють цінність інструментів аналізу поведінки

Надзвичайно добре
69%

2/3 організацій у сфері охорони здоров'я вважають, що поведінкова аналітика/криміналістика допомагає виявляти зловмисників
(Охорона здоров'я: 358)

Надзвичайно добре
38–39%

Менша кількість організацій у сфері транспорту та урядових установ погоджується, що поведінкова аналітика/криміналістика працює надзвичайно добре
(Транспорт: 175; Уряд: 639)

Порівняльне дослідження рішень безпеки за 2018 рік, проведене компанією Cisco

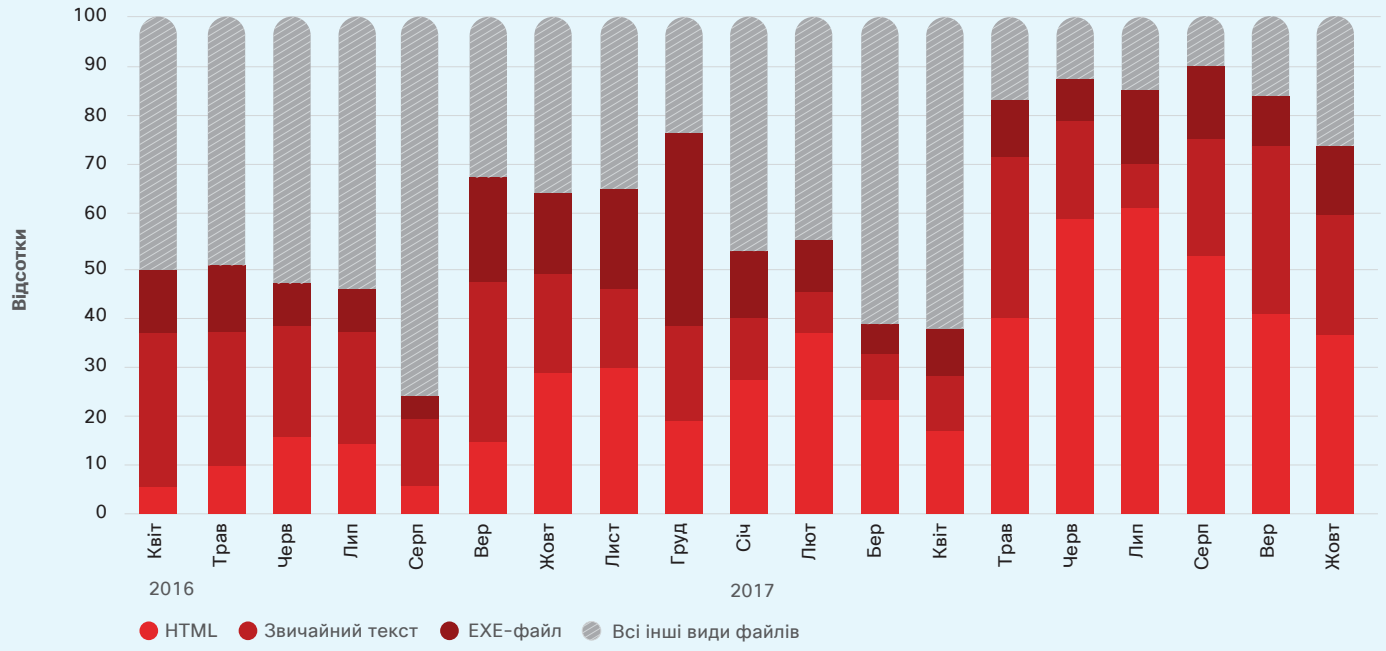
Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Методи веб-атак показують, що зловмисники активно зосереджуються на недоліках браузера

Аналіз методів веб-атак за 18-місячний період з квітня 2016 по жовтень 2017 року демонструє збільшення використання зловмисниками шкідливого веб-контенту (Рисунок 6). Ця тенденція збігається з агресивним націлюванням на веб-браузер Microsoft Internet Explorer з боку активних наборів експлойтів.

Дослідники загроз з компанії Cisco помічали, що кількість випадків виявлення шкідливого веб-контенту на JavaScript упродовж цього періоду була істотною та стабільною. Це підкреслює ефективність цієї стратегії для зараження вразливих веб-браузерів з метою сприяння іншій зловмисній діяльності, такій як переадресування браузера чи завантаження програм-троянів.

Рисунок 6 Активність блоку на основі шкідливого програмного забезпечення за типом контенту, квітень 2016 – жовтень 2017 року

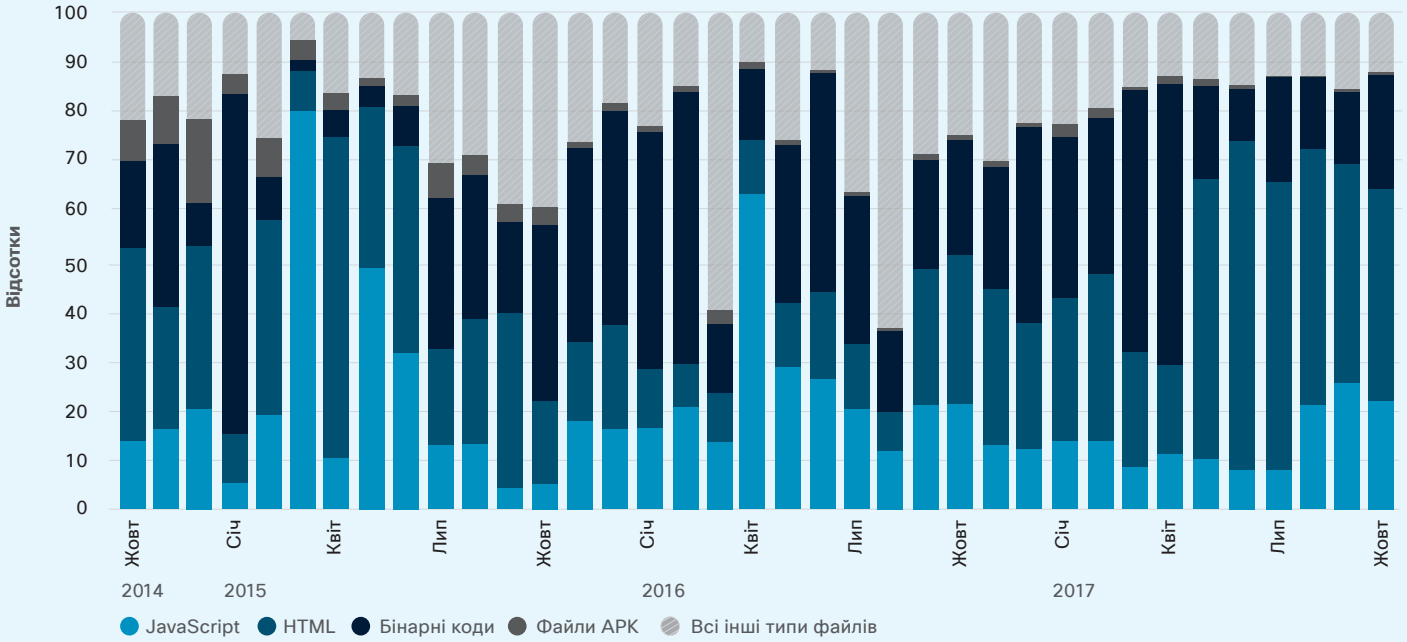


Джерело: дослідження Cisco щодо безпеки

Рисунок 7 містить огляд методів веб-атаки за три роки, починаючи з жовтня 2014 по жовтень 2017 року. Протягом цього періоду зловмисники послідовно використовували підозрілі бінарні коди, у першу чергу для доставки рекламного та шпигунського програмного забезпечення. Як зазначено у звіті Cisco 2017 Midyear Cybersecurity Report (Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року), ці типи потенційно небажаних програм (PUA) можуть створювати ризики для безпеки, такі як збільшення кількості інфікування шкідливим програмним забезпеченням та викрадення інформації про користувача чи компанію[8].

Трирічний огляд, представлений на Рисунку 7, також підтверджує, що обсяг шкідливого веб-контенту коливається залежно від часу, оскільки зловмисники запускають і завершують кампанії та змінюють свої тактики задля уникнення їх виявлення.

Рисунок 7 Активність блоку на основі шкідливого програмного забезпечення за типом контенту, жовтень 2014 – жовтень 2017 року



Джерело: дослідження Cisco щодо безпеки

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

8 *Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

ЗАГРОЗИ З БОКУ ЕЛЕКТРОННОЇ ПОШТИ

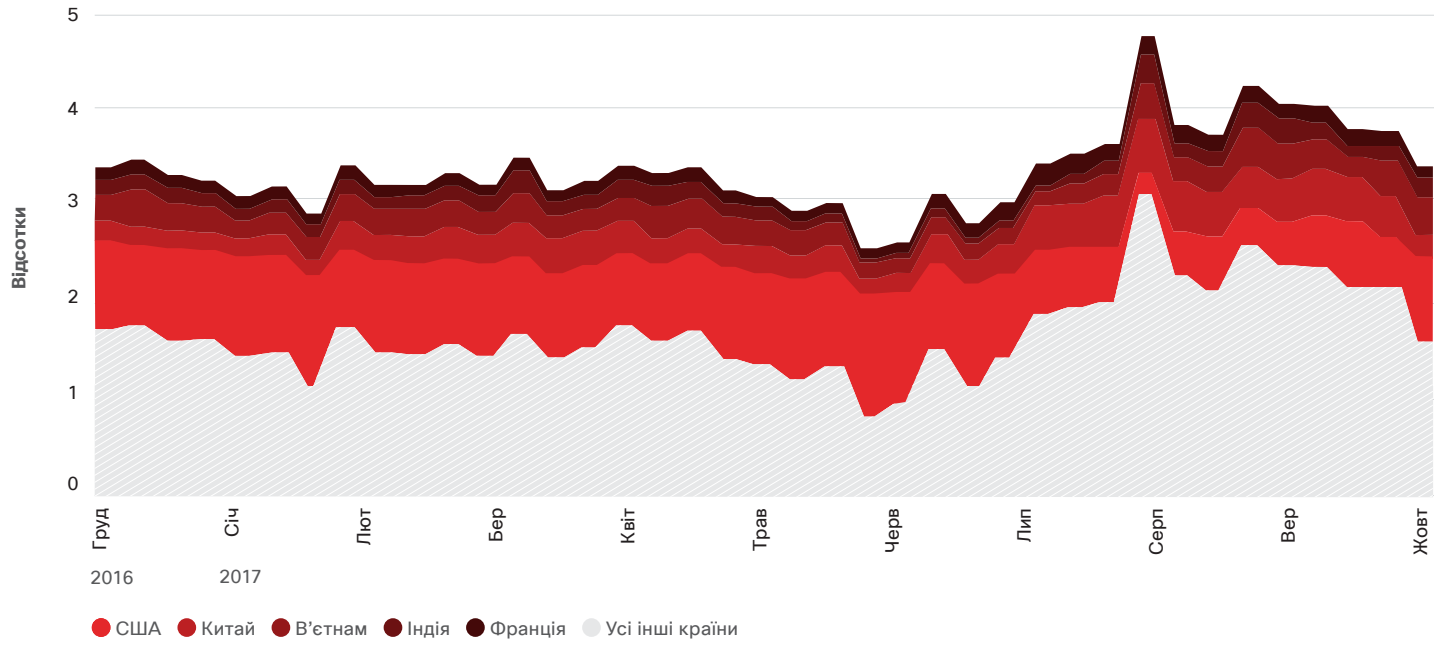
Незалежно від того, наскільки змінюється ландшафт загроз, шкідливі електронні листи та спам й надалі залишаються важливими інструментами зловмисників для поширення шкідливого програмного забезпечення, оскільки вони спрямовують загрози безпосередньо в точку призначення. Поєднавши технології соціальної інженерії, такі як фішинг, шкідливі посилання та вкладення, зловмисникам залишається тільки сидіти і чекати, поки користувачі, які нічого не підозрюють, активують їхні експлойти.

Коливання активності бот-мережі спаму впливають на загальний обсяг

Наприкінці 2016 року дослідники загроз із компанії Cisco помітили істотне зростання активності спам-кампаній, яке, як виявилось, співпадало зі зниженням активності наборів експлойтів. В той час як провідні набори експлойтів, такі як Angler, швидко зникли з ринку, багато користувачів таких наборів почали або повернулись до використання вектору електронної пошти для збереження прибутковості[9].

Проте, після початкового швидкого повернення до електронної пошти, глобальний обсяг спаму знизився і вирівнявся протягом більшої частини першої половини 2017 року. Потім, наприкінці травня та на початку червня 2017-го, глобальний обсяг спаму знизився перед значним збільшенням, що відбулось протягом середини літа і тривало аж до його кінця (див. Рисунок 8).

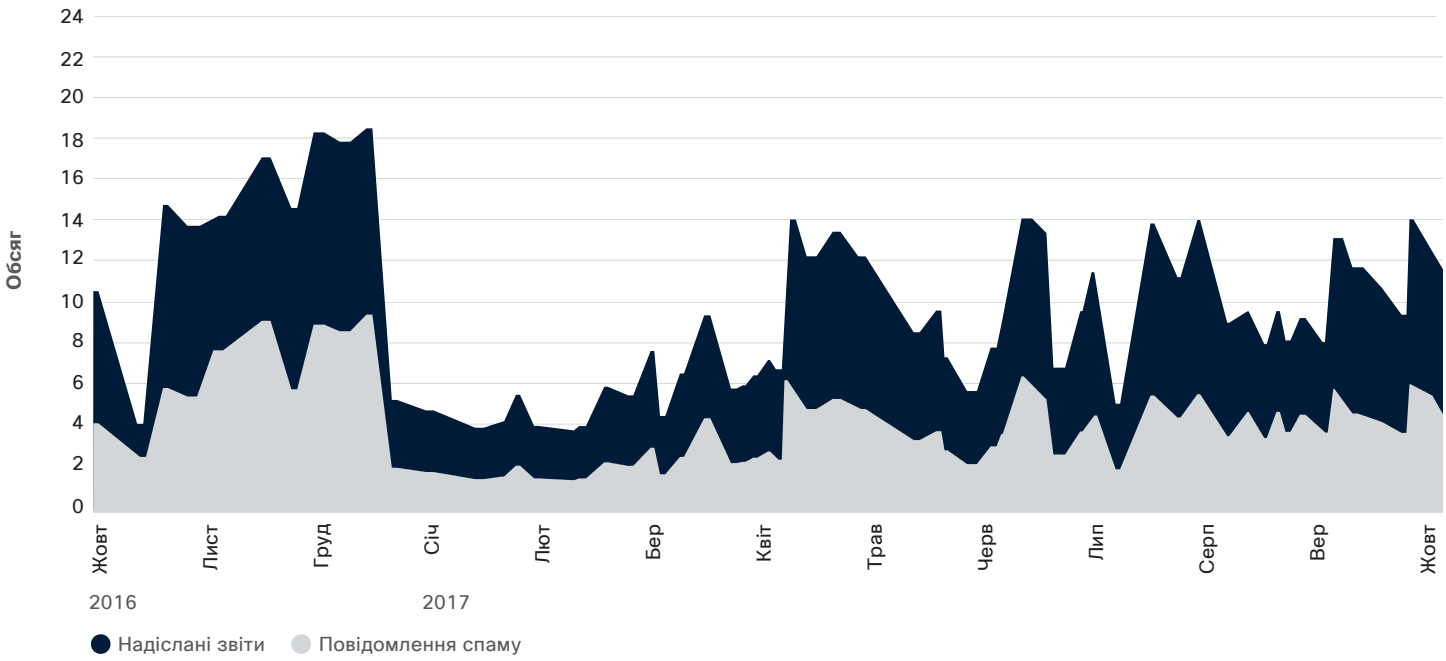
Рисунок 8 Блоки репутації IP-адрес за країнами, грудень 2016 – жовтень 2017 року



Джерело: дослідження Cisco щодо безпеки

9 Див. Decline in exploit kit activity likely influencing global spam trends, стор. 18, *звіт Cisco з інформаційної безпеки за перше півріччя 2017 року:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Рисунок 9 Активність бот-мережі спаму, жовтень 2016 – жовтень 2017 року



Джерело: Cisco SpamCop

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Зниження обсягу спаму в період із січня до квітня 2017 року співпадає із затишшям в активності бот-мережі спаму. Це видно на внутрішньому графіку, згенерованому сервісом Cisco® SpamCop (Рисунок 9).

Дослідники загроз компанії Cisco повідомляють, що бот-мережа Necurs, основний постачальник усього світового обсягу спаму, була активною, але в період із січня по квітень розсилала менше спаму. У травні бот-мережа поширювала програму-здирника Jaff, проводячи масові спам-кампанії.

В рамках такої кампанії розсилався PDF-файл з вбудованим шкідливим документом Microsoft Office та початковим завантажувачем програми-здирника Jaff[10]. Дослідники знайшли слабке місце в Jaff, яке дозволило їм створити дешифратор, що змусило операторів Necurs швидко повернутись до поширення їхньої звичної загрози, програми-здирника Locky[11]. Час, який був необхідний учасникам Necurs для повернення до Locky, співпадає з періодом істотного зменшення світового обсягу спаму, що спостерігалось протягом перших двох тижнів червня (Рисунок 9).

10 *Jaff Ransomware: Player 2 Has Entered the Game,* автори Nick Biasini, Edmund Brumaghin та Warren Mercer, за участю Colin Grady, блог Cisco Talos, травень 2017 року: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

11 *Player 1 Limps Back Into the Ring–Hello Again, Locky!* автори Alex Chiu, Warren Mercer та Jaeson Schultz, за участю Sean Baird та Matthew Molyett, блог Cisco Talos, червень 2017 року: blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

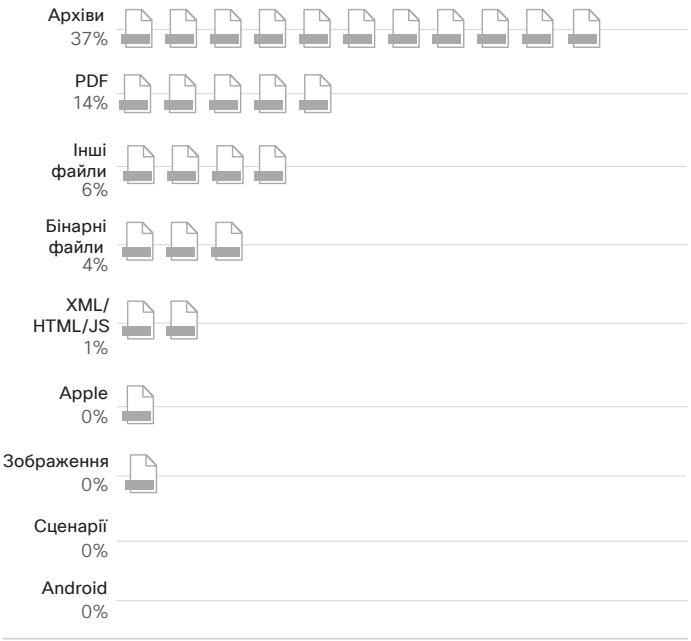
Розширення шкідливих файлів у електронній пошті: Топ-10 інструментів найпоширеніших сімейств шкідливих програм

Дослідники загроз з компанії Cisco проаналізували телеметрію електронної пошти за період із січня по вересень 2017 року. Мета – виявити типи розширень шкідливих файлів у документах електронної пошти, які найчастіше використовувались найпоширенішими сімействами шкідливого програмного забезпечення. У результаті аналізу було отримано перелік 10 типів, який демонструє, що найпоширенішою групою розширень шкідливих файлів 38%) були формати Microsoft Office, такі як Word, PowerPoint та Excel (див. Рисунок 10).

Файли архівів, такі як .zip та .jar, становили близько 37% від загальної кількості всіх типів шкідливих файлів, помічених у нашому дослідженні. Зовсім не дивно, що зловмисники часто використовують архівні файли, оскільки вони вже давно вважаються улюбленими місцями приховування зловмисного програмного забезпечення. Користувачам необхідно відкрити файли архіву, щоб побачити їхній вміст, що є важливим кроком у ланці зараження багатьма загрозами. Шкідливі файли архівів також часто досягають успіху в тому, щоб обійти інструменти автоматизованого аналізу, особливо якщо вони містять загрози, які потребують взаємодії з користувачем для активації. Зловмисники також використовують незрозумілі типи файлів, такі як .7z та .rar, для уникнення їх виявлення.

Розширення шкідливих PDF-файлів закрили першу трійку найпоширеніших розширень у нашому аналізі, склавши приблизно 14% від загального обсягу проаналізованих розширень шкідливих файлів. (Примітка: категорія «інші розширення» застосовується до розширень файлів, включених у наше розширення, які не можуть бути легко віднесені до жодного з відомих типів файлів. Відомо, що деякі типи шкідливого програмного забезпечення використовують випадкові розширення файлів).

Рисунок 10 Топ-10 розширень шкідливих файлів, січень – вересень 2017 року

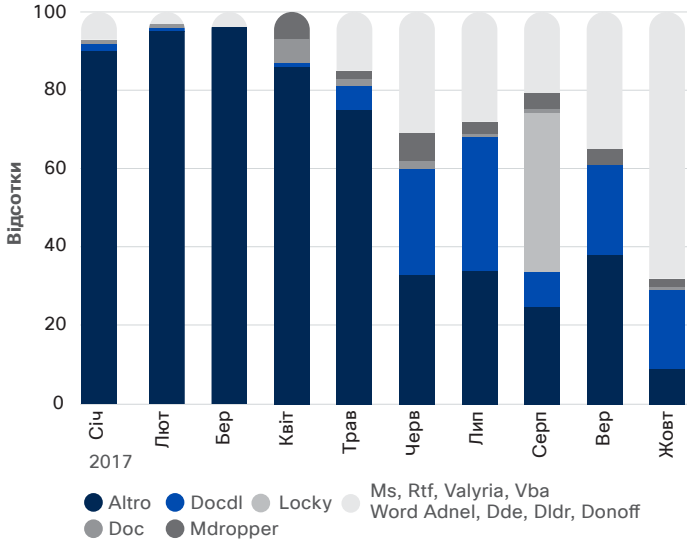


Джерело: дослідження Cisco щодо безпеки

Рисунки 11 a–c представляють загальний огляд сімейств шкідливих програм, включених до нашого дослідження, які були пов'язані з трьома найбільш вживаними типами розширень шкідливих файлів: файлами MS Office, архівами та PDF. На Рисунку 12 показано відсоток виявлення за сімействами, що включає розширення файлу зі шкідливим вмістом. За даними дослідників загроз Cisco, різкі зростання активності співпадають зі спам-кампаніями, які спостерігалися протягом цих місяців.

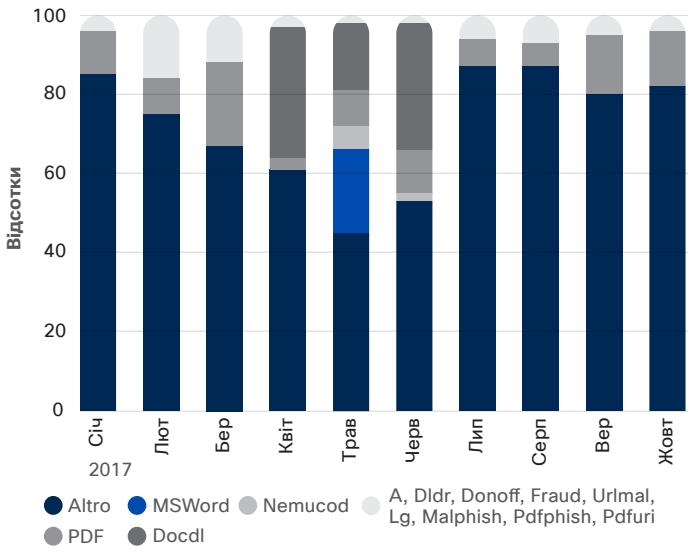
Наприклад, наприкінці літа спостерігались великі кампанії з поширення Nemucod та Locky – двох загроз, які часто працюють разом. Відомо, що Nemucod надсилає шкідливий вміст в архівних файлах, таких як.zip, що містять шкідливий скрипт, але виглядають як звичайні файли .doc. (Dwnldr, який також представлений на Рисунку 12, є ймовірним варіантом Nemucod).

Рисунок 11a Три найпоширеніші типи розширень шкідливих файлів та взаємозв'язки сімейств шкідливих програм



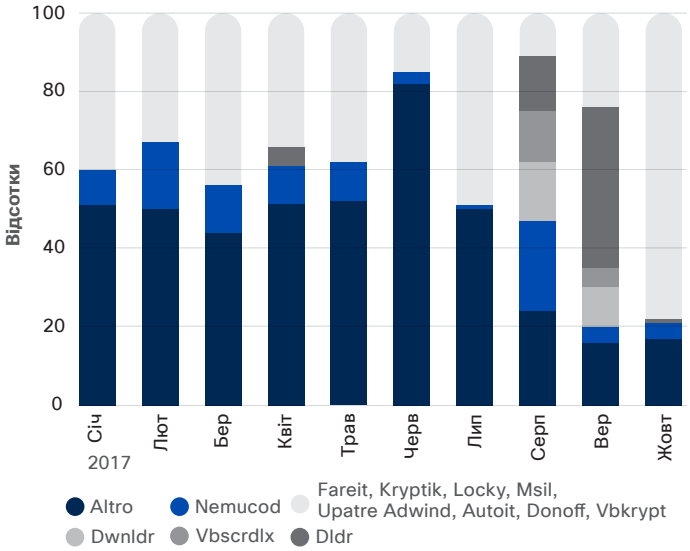
Джерело: дослідження Cisco щодо безпеки

Рисунок 11b Три найпоширеніші типи розширень шкідливих файлів та взаємозв'язки сімейств шкідливих програм



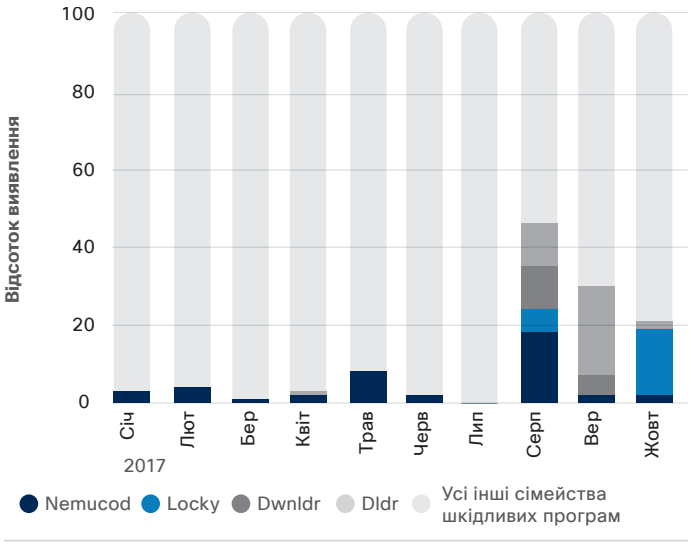
Джерело: дослідження Cisco щодо безпеки

Рисунок 11c Три найпоширеніші типи розширень шкідливих файлів та взаємозв'язки сімейств шкідливих програм



Джерело: дослідження Cisco щодо безпеки

Рисунок 12 Картина найпоширеніших сімейств шкідливих програм, січень – жовтень 2017 року



Джерело: дослідження Cisco щодо безпеки

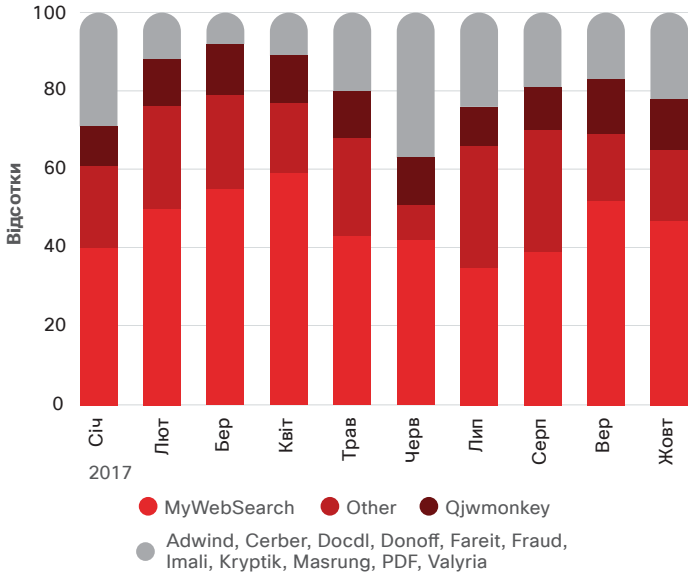
Шпигунська програма MyWebSearch – найактивніший користувач «інших розширень»

У нашому дослідженні категорія «інші розширення» включає декілька добре відомих типів шкідливого програмного забезпечення. Але MyWebSearch, шкідливе рекламне програмне забезпечення та зловмисний браузер, який позиціонується як корисна панель інструментів, є найактивнішим гравцем (див. Рисунок 13). Він використовує виключно файли з розширенням.exe, іноді лише один тип на місяць. Потенційно небажана програма застосовується вже протягом багатьох років і заражає різні типи браузерів. Вона часто поєднується із шахрайськими програмними продуктами та може розсилати користувачам масову рекламу.

Наш аналіз типів розширень шкідливих файлів показує, що сьогодні навіть за наявності середовища надсучасних і складних загроз електронна пошта продовжує бути ефективним каналом розповсюдження шкідливого програмного забезпечення. Основні стратегії захисту для компаній:

- Застосування потужних та комплексних засобів захисту електронної пошти.
- Навчання користувачів щодо загрози, яку несуть шкідливі вкладення та посилання у фішингових електронних листах та спам-повідомленнях.

Рисунок 13 MyWebSearch – найактивніший користувач «інших розширень»



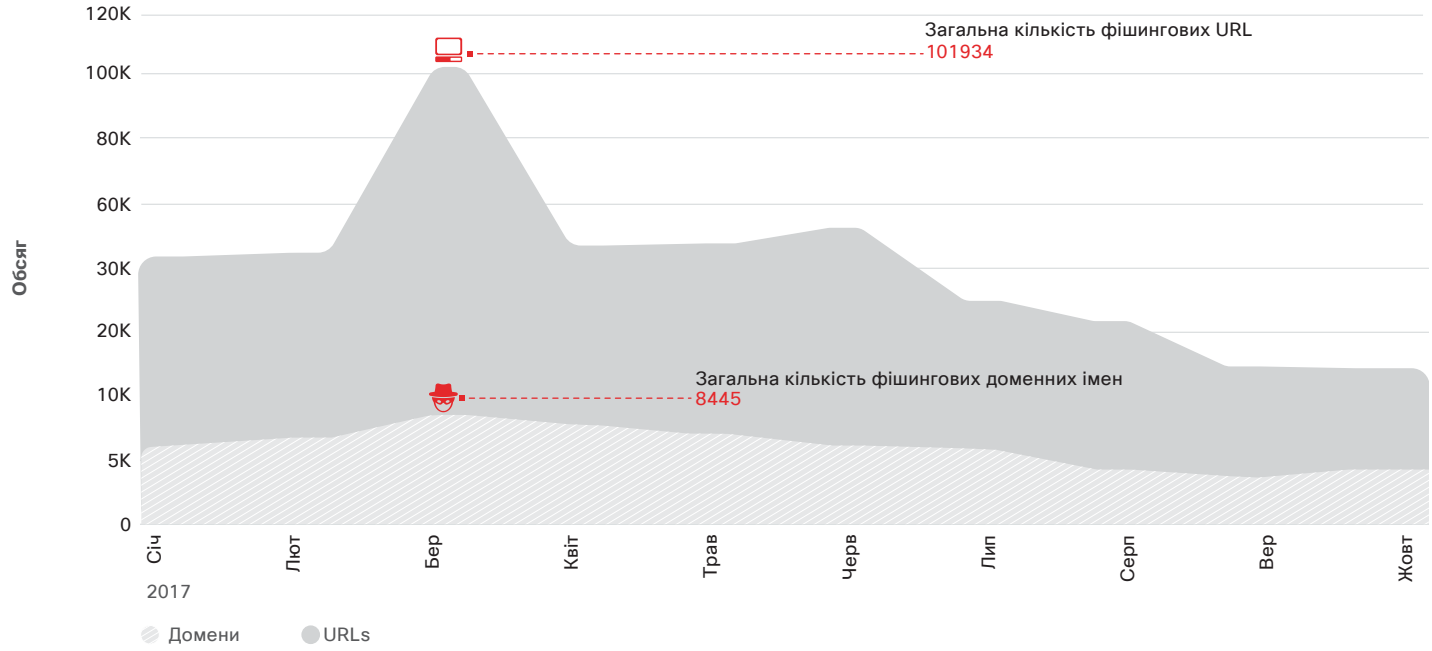
Джерело: дослідження Cisco щодо безпеки

Соціальна інженерія надалі залишається важливою платформою для запуску кібератак з використанням електронної пошти.

Фішинг і цільовий фішинг є найбільш вживаними тактиками для викрадення особистих даних користувачів та іншої конфіденційної інформації, тому що вони дуже ефективні. Фактично саме розсилання електронних повідомлень з такими зловмисними елементами стало причиною одних з найбільших і загальновідомих витоків інформації протягом останніх років. Двома прикладами таких випадків, що сталися у 2017 році, є широкомасштабна атака, спрямована на користувачів Gmail[12], та злам енергетичних систем Ірландії[13].

Для оцінювання того, наскільки активно використовуються фішингові URL та домени, дослідники з компанії Cisco перевірили дані з джерел, які вивчають потенційно «фішингові» електронні адреси, що були надані користувачами через мережу колективного виявлення фішингових загроз. Рисунок 14 відображає кількість фішингових URL та фішингових доменів, помічених за період із січня по жовтень 2017 року.

Рисунок 14 Кількість зафіксованих фішингових URL та доменів по місяцях



Джерело: дослідження Cisco щодо безпеки

Піки, що спостерігаються в березні та червні, можуть бути пов'язані з двома різними хвилями атак. Перша була спрямована на ураження користувачів великого провайдера телекомунікаційних послуг. Ця кампанія включала:

- 59 651 URL, що містили субдоменні імена під доменом aaaainfomation[dot]org;
- субдоменні імена, які містили довільні ланцюги, що складалися з 50–62 символів.

Кожне із субдоменних імен (довжиною 50–62 символи) містило приблизно 3500 адрес, що дозволило програмоване використання субдоменів (приклад: Cewekonuxykysowegulukoz apojygepuqybyteqe johofopefogu[dot]aaaainfomation[dot]org).

Зловмисники застосовували дешевий сервіс забезпечення конфіденційності для реєстрації доменних імен, які були помічені в цій кампанії.

12 *Massive Phishing Attack Targets Gmail Users,* автор Alex Johnson, *NBC News,* травень 2017 року: nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501.

13 *Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure,* автор Lizzie Deardon, *The Independent,* липень 2017: independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

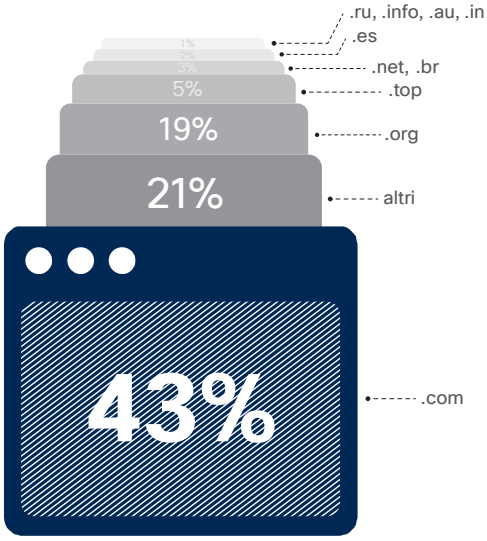
Під час другої атаки, найбільша активність якої припадає на червень, зловмисники використовували назву існуючого податкового органу в Сполучному Королівстві з метою приховування своїх дій. Вони застосували 12 доменних імен верхнього рівня (TLDs). Одинадцять із них були URL-адресами із шести випадкових шестизначних ланцюжків (приклад: jyzwyp[dot]top). А ще у дев'яти з доменних імен кожне було пов'язане з більш ніж 1600 фішинговими сайтами.

Так само, як і під час березневої кампанії, зловмисники реєстрували доменні імена, використовуючи сервіс забезпечення конфіденційності з метою приховування реєстраційної інформації домену. Усі домени були зареєстровані протягом двох днів. На другий день близько 19 000 пов'язаних з кампанією адрес було помічено та виявлено в межах п'ятигодинного вікна. (Для отримання детальнішої інформації стосовно того, як швидко зловмисники використовували новозареєстровані доменні імена, див. розділ «Зловмисне використання легітимних ресурсів для обходження систем захисту каналів керування» на стор. 24).

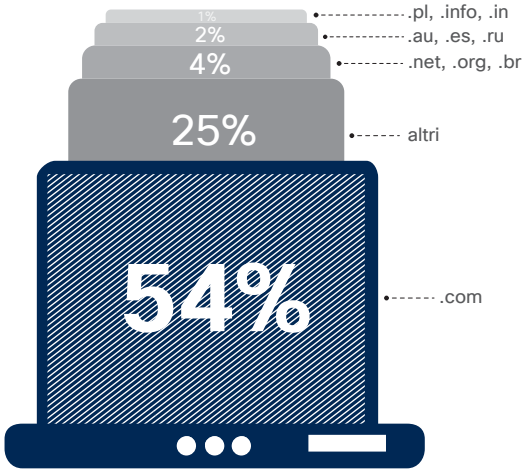
Розповсюдження доменів верхнього рівня серед відомих фішингових сайтів

Наш аналіз фішингових сайтів за період із січня по серпень 2017 року виявив, що зловмисники застосовували для своєї діяльності 326 унікальних доменів верхнього рівня, серед яких такі, як .com, .org, .top (переважно через проведення кампанії, спрямованої на податковий орган у Сполученому Королівстві), та домени верхнього рівня з прив'язкою до певної країни (див. Рисунок 15). Використання менш відомих доменів високого рівня може бути вигідним для зловмисників; зазвичай такі домени є недорогими і, як правило, пропонують недорогі рішення для захисту конфіденційності.

Рисунок 15 Розповсюдження доменів верхнього рівня серед відомих фішингових сайтів



Процентне співвідношення всіх сайтів з доменами високого рівня (усі дані).



Процентне співвідношення сайтів з доменами високо рівня (за виключенням конкретних доменів високого рівня, та двох кампаній, спрямованих на податковий орган та телекомунікаційний сервіс).

Джерело: дослідження Cisco щодо безпеки

Засоби захисту повинні пильно відстежувати цю «стару» загрозу.

У 2017 році десятки тисяч спроб фішингових атак щомісяця фіксувалися мережами колективного виявлення фішингових загроз, включених до нашого аналізу. Деякі із загальних тактик та інструментів, які використовують зловмисники для проведення фішингових кампаній, містять:

- **Доменний сквотинг:** домени, які отримують назви, що схожі на дійсні домени (наприклад: cisc0[dot]com).
- **Створення тіньового домену:** субдомени, додані під дійсним доменом, без відома власника (приклад: badstuff[dot]cisco[dot]com).
- **Домени, що були зареєстровані зі зловмисним наміром:** домен, який був створений для реалізації злочинних намірів (приклади: viqpbe[dot]top).
- **Засоби скорочення URL:** зловмисна URL-адреса, що приховується за допомогою засобу скорочення URL (приклад: bitly[dot]com/random-string).

  Примітка: у даних, які ми перевірили, Bitly.com був інструментом для скорочення URL, що використовувався зловмисниками найчастіше. Скорочені зі зловмисними намірами URL-адреси становлять 2 % від загальної кількості фішингових сайтів у нашому дослідженні. Цей показник досяг пікового значення 3.1 відсотка в серпні.
- **Послуги субдоменів:** сайт, який був створений під сервером субдоменів (приклад: mybadpage[dot]000webhost[dot]com).

Зловмисники, які застосовують технології фішингу та цільового фішингу, постійно вдосконалюють методи соціальної інженерії, що спонукають користувача натиснути на зловмисне посилання або відвідати шахрайські веб-сторінки та надати персональні дані чи будь-яку іншу інформацію, яка має велику цінність. Підготовка та високий рівень відповідальності користувачів, а також застосування технологій забезпечення безпеки електронної пошти залишаються найважливішими стратегіями в боротьбі з цими загрозами.

ТАКТИКА УХИЛЕННЯ ВІД «ПІСОЧНИЦІ»

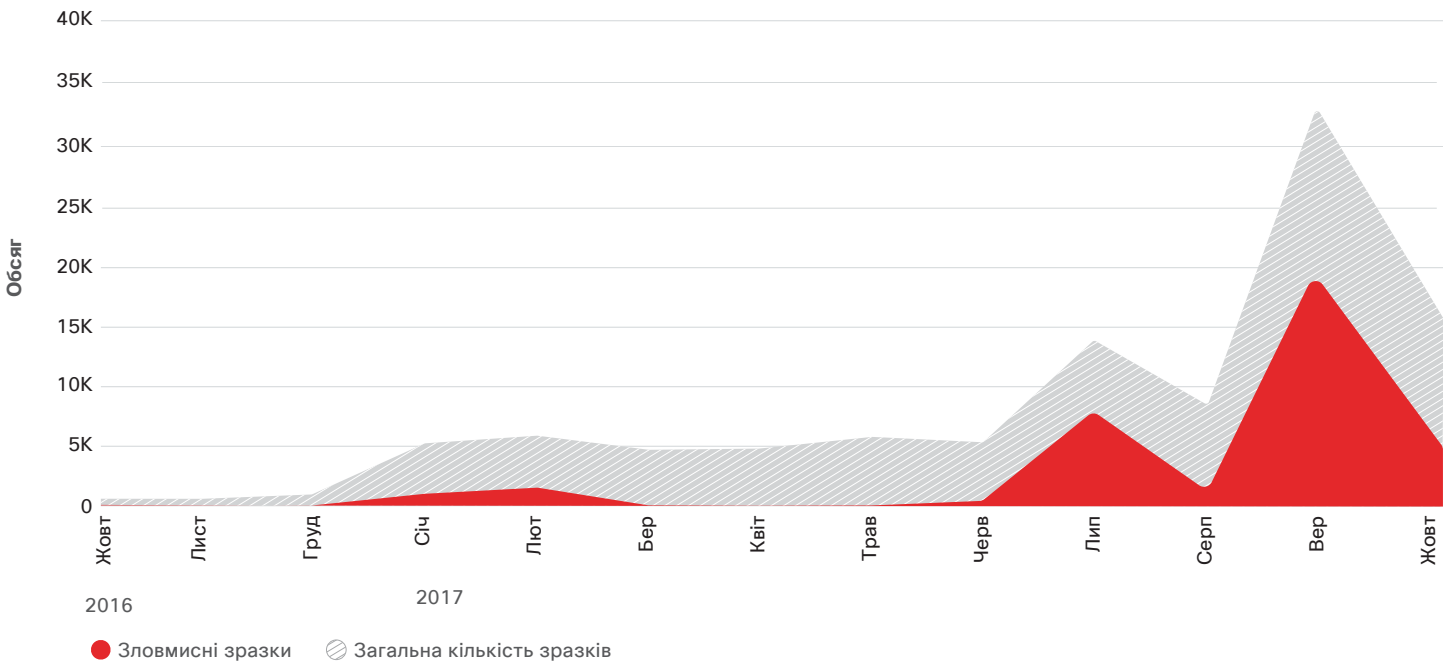
Зловмисники стають більш вправними в розробці загроз, які можуть уникати «пісочниць» – середовища для безпечного виконання комп'ютерних програм, що постійно розвиваються. Коли дослідники з компанії Cisco аналізували шкідливі програми в електронних повідомленнях, які застосовували різноманітні техніки ухилення від «пісочниці», вони виявили, що кількість шкідливих зразків демонструвала різке підвищення до пікових показників, а потім різко знижувалася. Це ще один приклад того, як швидко зловмисники можуть збільшити обсяг спроб зламу програмного захисту, щойно вони знаходять ефективний спосіб реалізації.

Розробники вірусних програм використовують брудні прийоми в «пісочницях» розробників програмного захисту.

У вересні 2017 року дослідники загроз компанії Cisco зафіксували велику кількість прикладів, коли зловмисні дані завантажувалися після закриття документа (Рисунок 16). У цьому випадку зловмисний код активується з використанням функції «закрити документ». Ця технологія працює, тому що в багатьох випадках документи не закриваються після того, як вони були відкриті та проаналізовані в «пісочниці». Оскільки «пісочниця» не закриває документ окремо, вкладення сприймаються нею як безпечні й будуть доставлені передбачуваним одержувачам. Коли одержувач відкриває доданий документ, а потім закриває його, у цей момент і доставляється зловмисний код. Використовуючи цю технологію, існує можливість ухилитися від «пісочниць», які не забезпечують чітке виявлення дій під час закриття документа.

Використання дії «закриття документа» є вигідним варіантом для зловмисників. Вони використовують макрофункціональність, що вбудовано в Microsoft Office, а також схильність користувачів відкривати вкладення, які, на їхню думку, призначені для саме них. Щойно користувачі розуміють, що вкладення їх не стосується, вони закривають документ, активуючи таким чином макрос, в якому заховано зловмисний код.

Рисунок 16 У вересні 2017 року зафіксовано великий обсяг зловмисних документів Microsoft Word, які використовують виклики функції «закрити документ»

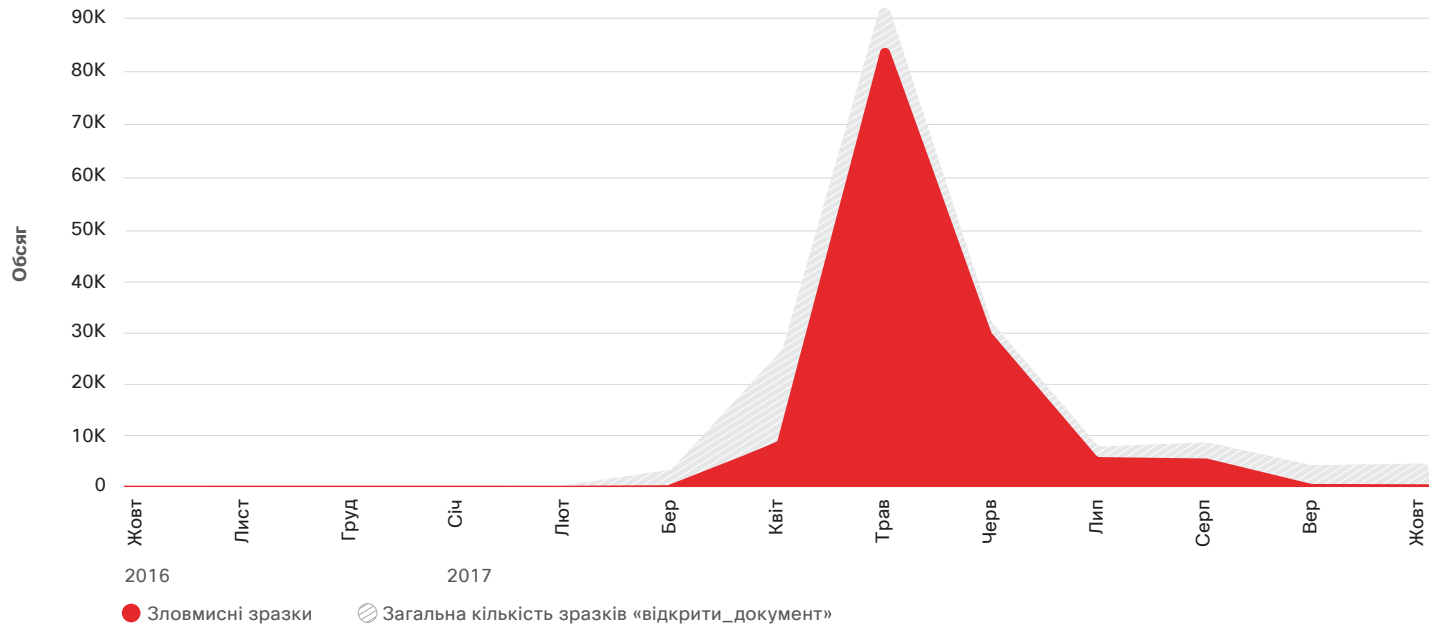


Джерело: дослідження Cisco щодо безпеки

Деякі зі зловмисників уникають перевірки «пісочницею», приховуючи тип документа, в якому існує зловмисний код. Як зображено на Рисунку 17, у травні 2017 року ми зафіксували потужну атаку, що була побудована навколо зловмисних документів Microsoft Word, які, у свою чергу, були включені в PDF-документи. Такі документи можуть обходити «пісочниці», які просто виявляють і відкривають файл PDF, замість того, щоб також відкрити та проаналізувати вкладений документ Word. Документ PDF зазвичай містив приманку для того, щоб користувач натиснув та відкрив документ Word, що зі свого боку активізує зловмисний код. Використовуючи цю технологію, існує можливість обійти «пісочниці», які не відкривають і не аналізують документи, вкладені у файли PDF.

Зафіксувавши різке збільшення випадків зловмисних кодів з використанням таких файлів PDF, наші дослідники загроз удосконалили середовище «пісочниці» з метою визначення того, чи містили документи PDF дії або приманки для відкриття вкладених у них документів Word.

Рисунок 17 Потужна атака в травні 2017 року, під час якої були використані PDF-файли з доданими до них зловмисними документами Word



Джерело: дослідження Cisco щодо безпеки

Пікові збільшення зразків зловмисного коду, що використовують різноманітні прийоми з метою обминути «пісочниці», вказують на те, що зловмисники мають бажання застосовувати метод, який, на їхню думку, є ефективним у застосуванні як для них, так і для інших зловмисників. Крім того, якщо зловмисники докладають зусиль для створення зловмисного коду та пов'язаної із цим інфраструктури, вони очікують прибутків від своїх вкладених інвестицій. Якщо вони визначають, що зловмисний код здатний обійти перевірку «пісочниці», вони, у свою чергу, збільшуватимуть кількість спроб здійснення атак та постраждалих користувачів.

Дослідники компанії Cisco рекомендують використовувати «пісочниці», які забезпечують можливості аналізу вмісту з метою гарантування того, що зловмисним програмам, які використовують зазначену вище тактику, не вдасться уникнути аналізу в «пісочниці». Наприклад, технологія «пісочниці» повинна забезпечувати можливості аналізу метаданих зразків, які вона аналізує, як, наприклад, визначення того, чи містить зразок будь-яку дію після закриття документа.

ЗЛОЧИННЕ ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ ТА ІНШИХ ЛЕГІТИМНИХ РЕСУРСІВ

Оскільки програми, дані та ідентифікатори мігрують до хмар, команди з питань безпеки повинні керувати ризиками, пов'язаними з втратою контролю над традиційним периметром мережі. Зловмисники використовують той факт, що спеціалісти з безпеки мають певні складнощі в забезпеченні захисту із появою та розширенням хмар та IoT. Однією з причин є нестача ясності стосовно того, хто саме несе відповідальність за захист цих середовищ.

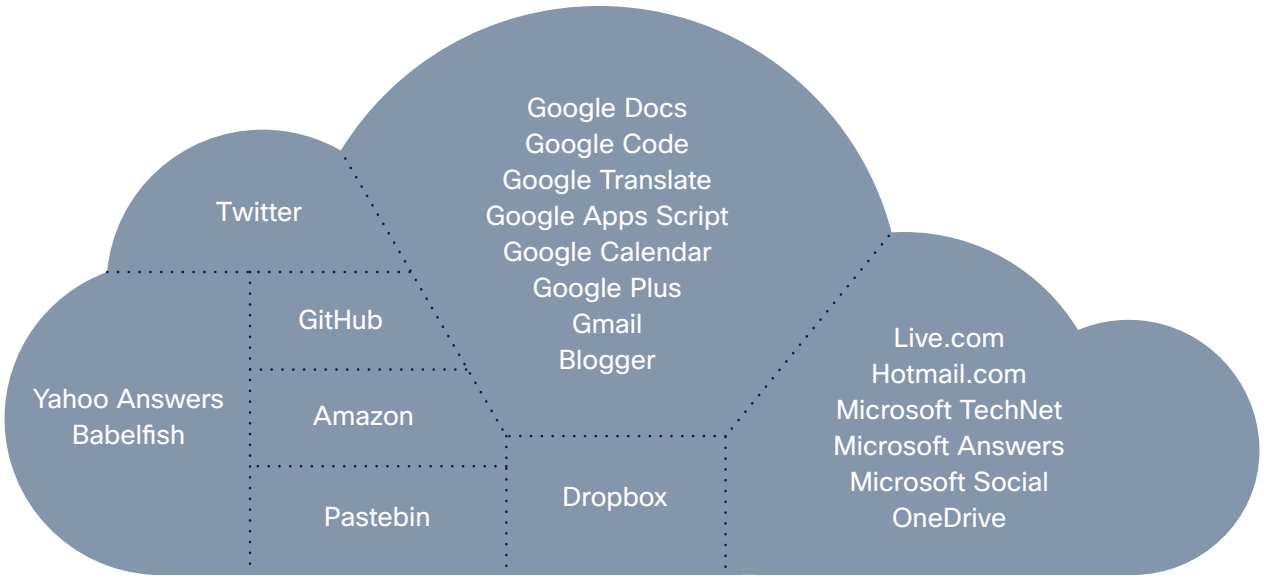
Задля адекватної відповіді на цей виклик підприємствам, можливо, доведеться застосовувати поєднання найкращих практик, передових технологій у сфері безпеки, таких як машинне навчання. А також навіть деяких експериментальних методів, залежно від того, які сервіси вони використовують для ведення свого бізнесу й які загрози виникають у даному контексті.

Зловмисне використання легітимних ресурсів для маніпулювання каналами керування зловмисним кодом.

Якщо зловмисники застосовують легітимні сервіси в якості каналів керування зловмисним кодом, спеціалістам з безпеки практично неможливо ідентифікувати зловмисний трафік, тому що він копіює поведінку легітимного мережного трафіку. Зловмисники використовують велику кількість інтернет-шуму в якості прикриття, тому що велика кількість людей сьогодні користуються сервісами на зразок Google Docs та Dropbox, незалежно від того, чи такі сервіси пропонуються або узгоджуються їхніми роботодавцями.

Рисунок 18 демонструє декілька добре відомих легітимних сервісів, які, згідно з даними дослідників з Anomali, компанії-партнера Cisco та постачальника послуг дослідження загроз, використовувалися в схемах уникнення систем захисту для каналів керування зловмисним кодом[14] протягом останніх декількох років. (Примітка: вказані типи сервісів стикалися з проблемою протистояння порушенням, оскільки ускладнення для користувачів можливості створювати аккаунти та використовувати ці сервіси може негативно вплинути на їхню здатність генерувати прибуток.)

Рисунок 18 Приклади легітимних сервісів, що були використані зі злочинною метою як канали керування зловмисним кодом



Джерело: Anomali

14 Anomali визначає схему каналів керування C2 як «сукупність IP-адрес, доменів, легітимних сервісів та всіх систем віддаленого керування, що є частиною ... комунікаційної архітектури» зловмисних програм.

Відповідно до дослідження Anomali, зловмисники, що становлять постійну загрозу підвищеної складності (advanced persistent threat, APT), та групи, які отримували підтримку від держав, одними з перших використали легітимні сервіси для каналів керування зловмисним кодом. Проте цю технологію наразі використовує більш широкий загал зловмисників, особливо в тіньовій економіці. Використання легітимних сервісів в якості каналів керування дуже цікавить зловмисників, зважаючи на те, як легко:

- Зареєструвати нові аккаунти в цих сервісах.
- Створити веб-сторінку в Інтернеті, до якої є доступ широкого загалу.
- Використовувати шифрування для протоколів каналів керування. (Замість створення серверів в якості каналів керування з шифруванням або вбудовування шифру у зловмисний код нападники можуть просто адаптувати SSL-сертифікат легітимного сервісу.)
- Адаптувати та трансформувати ресурси на ходу. (Наприклад, зловмисники можуть повторно застосовувати імпланти в нових нападах без повторного використання DNS або IP-адрес)
- Зменшити ймовірність «згорання» інфраструктури. (Зловмисники, які використовують легітимні сервіси в якості каналів керування, не мають потреби застосовувати конкретні значення змінних у зловмисному коді з IP-адресами або доменами. Після завершення їхньої роботи вони просто можуть видалити свої сторінки в легітимних сервісах – й ніхто не дізнається їхні IP-адреси).
- Зловмисники використовують цю технологію через те, що вона дозволяє зменшувати накладні витрати та збільшувати їхній дохід на вкладені інвестиції.

Для спеціалістів у сфері захисту використання зловмисниками легітимних сервісів в якості каналів керування створює певні істотні проблеми:

Легітимні сервіси важко заблокувати

Чи можуть організації, чисто з точки зору бізнесу, навіть розглядати можливість блокування частин легітимних інтернет-сервісів, таких як Twitter або Google?

Легітимні сервіси часто є зашифрованими та складними в перевірці

Дешифрування кодів SSL коштує дорого й не завжди можливе в рамках одного підприємства. Тому зловмисні програми ховають свою комунікацію всередині зашифрованого трафіку, створюючи таким чином суттєві труднощі або навіть унеможливлюючи командам з питань безпеки ідентифікувати зловмисний трафік.

Використання легітимних сервісів руйнує логічні функції доменів та сертифікатів і ускладнює ідентифікацію

Зловмисникам не потрібно реєструвати домени, оскільки аккаунт у легітимному сервісі розглядається як початкова адреса каналу керування. Також існує низька ймовірність продовження реєстрації SSL-сертифікатів або використання самозавірених SSL-сертифікатів для схем каналів керування зловмисним кодом. Обидва тренди вочевидь матимуть негативний вплив на показник фільтрування репутації та занесення до чорного списку, що базуються на новостворених і новозареєстрованих доменах, а також пов'язаних із ними сертифікатах та IP-адресах.

Виявити використання легітимних сервісів в якості каналів керування зловмисним кодом дуже складно. Проте дослідники загроз з компанії Anomali рекомендують спеціалістам із захисту розглянути можливість застосування деяких експериментальних методів. Наприклад, зловмисні програми можна виявити, зафіксувавши наступне:

- приєднання до легітимних сервісів без застосування браузерів і програм;
- унікальні або невеликі розміри відповіді сторінки з легітимних сервісів;
- високу частоту обміну сертифікатами з легітимними сервісами;
- поповнення бази зразків «пісочниці» підозрілими DNS-запитами до легітимних сервісів.

Усі ці специфічні особливості вимагають подальшого вивчення вихідних програм та процесів.[15]

15 Для отримання більш детальної інформації стосовно цих експериментальних методів, а також додаткової інформації про те, як зловмисники використовують легітимні сервіси для каналів керування зловмисним кодом, завантажте повний документ з результатами досліджень компанії Anomali, Rise of Legitimate Services for Backdoor Command and Control, доступний за посиланням: anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf.

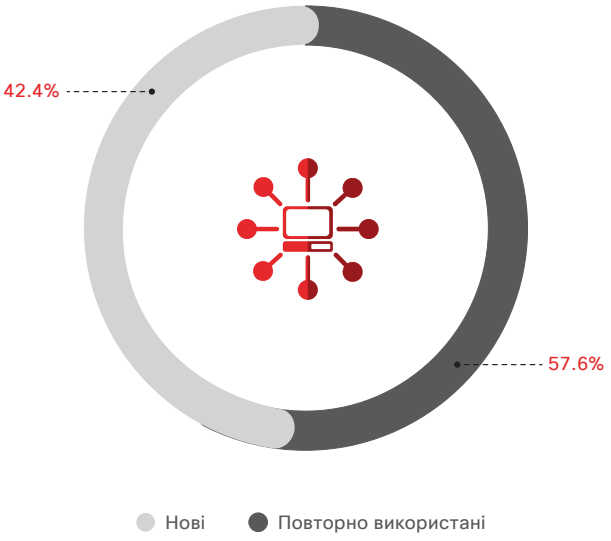
Отримання максимальної користі від ресурсів

Дослідники загроз з компанії Cisco проаналізували новозафіксовані унікальні імена запитів (домени), пов'язані із запитами DNS, здійсненими протягом семи днів у серпні 2017 року. Варто зауважити, що в цьому контексті поняття «новозафіксовані» не стосується того, коли саме було створено домен. Це стосується того, коли домен вперше був зафіксований технологією хмарної безпеки Cisco протягом періоду спостереження.

Метою цього дослідження є краще розуміння того, як часто зловмисники застосовують та повторно використовують домени рівня «зареєстрований» (RLD) у своїх атаках. Розуміння поведінки зловмисника на рівні доменів може допомогти фахівцям із захисту ідентифікувати зловмисні домени та пов'язані субдомени, що повинні бути заблоковані інструментами першої лінії захисту, такими як платформи хмарної безпеки.

Таким чином наші дослідники змогли акцентувати увагу виключно на цільовій групі унікальних RLD – близько 4 мільйонів. Субдомени були виключені зі зразків новозафіксованих доменів. Лише невеликий відсоток доменів RLD у цьому прикладі були класифіковано як зловмисні. З-поміж тих доменів RLD, що були зловмисними, більше половини (приблизно 58%) використовувалися повторно, як зображено на Рисунку 19.

Рисунок 19 Відсоток нових проти повторно використаних доменів



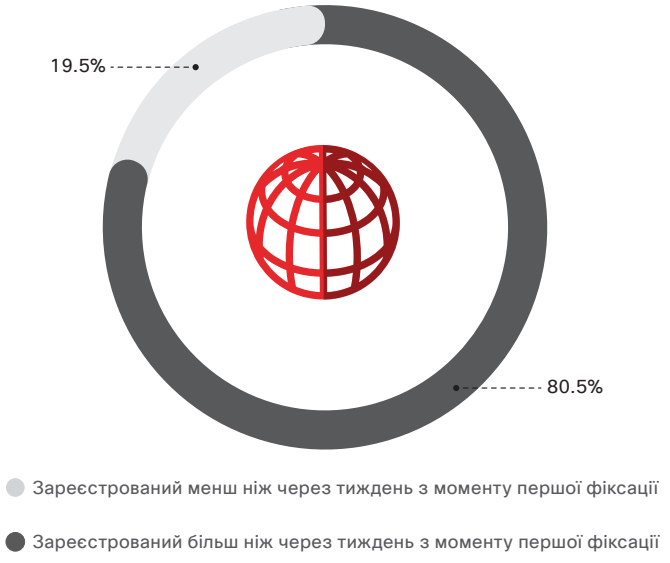
Джерело: дослідження Cisco щодо безпеки

Результати показують, що в той час як більшість зловмисників створюють нові домени для своїх кампаній, багато з них фокусуються на тому, щоб отримати якомога більше зиску від своїх інвестицій шляхом запуску декількох кампаній з одного домену. Реєстрація домену може бути дорогою, особливо беручи до уваги масштаби, які потрібні більшості зловмисників для реалізації своїх кампаній та уникнення їх виявлення.

Одна п'ята зловмисних доменів швидко починає застосовуватися на практиці

Зловмисники можуть перебувати на доменах днями, місяцями або навіть роками після їх реєстрації, очікуючи вдалої митті для їх використання. Проте, дослідники загроз з компанії Cisco зафіксували, що значний відсоток зловмисних доменів (приблизно 20%) було використано в компаніях менш ніж через тиждень після того, як вони були зареєстровані (див. Рисунок 20).

Рисунок 20 Час реєстрації RLD

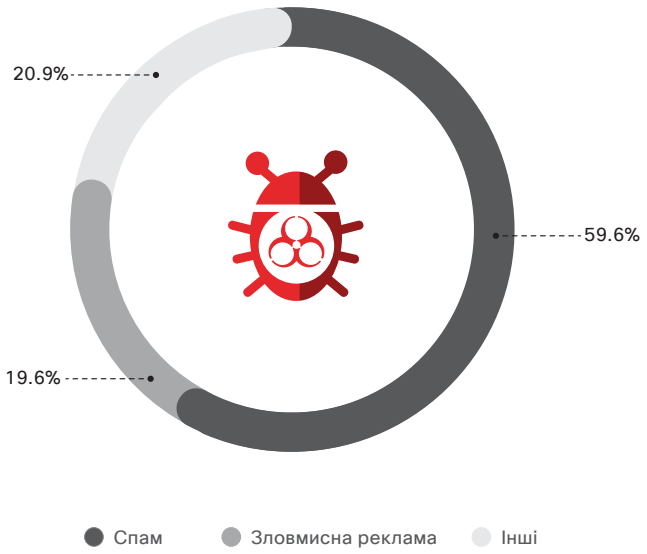


Джерело: дослідження Cisco щодо безпеки

Багато з нових доменів пов'язані зі зловмисними рекламними кампаніями

Більшість зловмисних доменів, які були проаналізовані, виявились пов'язаними зі спам-кампаніями – приблизно 60 %. Близько однієї п'ятої частини доменів були пов'язані зі зловмисними рекламними кампаніями (див Рисунок 21). Зловмисні рекламні кампанії стали ключовим інструментом для спрямування користувачів на набори експлойтів, у тому числі ті, що розповсюджують програми-здирники.

Рисунок 21 Класифікація зловмисного трафіку



Джерело: дослідження Cisco щодо безпеки

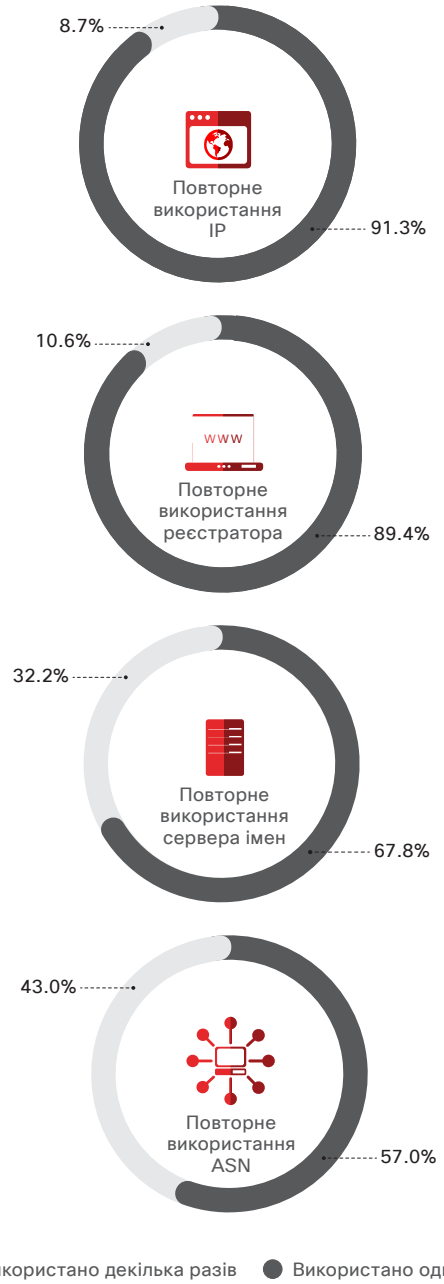
Добре продумані пов'язані з доменами технології для створення зловмисних рекламних кампаній містять коригування домену. Використовуючи цей прийом, зловмисники крадуть дані облікового запису легітимного домену для створення субдоменів, спрямованих на зловмисні сервери. Інша тактика полягає у зловживанні безкоштовними динамічними DNS-сервісами з метою створення зловмисних доменів та субдоменів. Це у свою чергу дозволяє зловмисникам здійснювати доставку шкідливих програм з хостингових IP-адрес, що постійно змінюються, або інфікованих комп'ютерів користувачів, або недостатньо захищених публічних веб-сайтів.

Домени повторно використовують ресурси інфраструктури

У нашому прикладі також виявилось, що зловмисні RLD повторно використовували ресурси інфраструктури, такі як електронні адреси реєстратора, IP-адреси, номери в автономній системі (ASNs) та сервери імен (див. Рисунок 22).

Як зазначають наші дослідники, це ще один доказ того, що зловмисники намагаються отримати якомога більшу зиску зі своїх інвестицій у нові домени та зберегти власні ресурси. Наприклад, IP-адреса може використовуватися більш ніж одним доменом. Таким чином, зловмисник, який створює основу для кампанії, може вирішити інвестувати в декілька IP-адрес та ряд доменних імен замість серверів, які коштують більше.

Рисунок 22 Повторне використання інфраструктури зловмисними RLD



Джерело: дослідження Cisco щодо безпеки

Ресурси, які домени RLD використовують повторно, дають підказки стосовно того, чи може бути конкретний домен зловмисним. Наприклад, повторне використання електронної пошти реєстратора або IP-адрес відбувається несистематично, таким чином, модель повторного використання, з будь-якого погляду, вказує про підозрілу поведінку. Спеціалісти із захисту можуть зі значним рівнем упевненості блокувати такі домени, знаючи, що подібні дії, ймовірно, не матимуть негативного впливу на бізнес-діяльність.

Статичне блокування номерів у автономних системах та серверів назв швидше за все виявиться недоцільним у більшості випадків. Проте, моделі повторного використання доменами RLDs варті додаткового дослідження з метою визначення того, чи потрібно блокувати певні домени.

Використання інтелектуальних інструментів першої лінії захисту хмарної безпеки для виявлення та аналізу потенційно зловмисних доменів та субдоменів може допомогти спеціалістам із захисту відстежити дії зловмисника та отримати відповідь на наступні питання:

- До якої IP-адреси прив'язаний домен?
- Які номери автономних систем прив'язані до конкретної IP-адреси?
- Хто зареєстрував відповідний домен?
- Які інші домени пов'язані з цим доменом?

Відповіді можуть допомогти спеціалістам із захисту не тільки покращити політики безпеки та блокувати атаки, а й убезпечити користувачів від під'єднання до зловмисних ресурсів в Інтернеті, поки вони знаходяться в корпоративній мережі.

DevOps під загрозою атак з боку програм-здирників

У 2017 році відбулося зростання рівня атак програм-здирників у сфері DevOps, починаючи з кампанії в січні, націленої на платформу бази даних з відкритим кодом, MongoDB.[16] Зловмисники зашифрували публічні зразки MongoDB та вимагали оплату за надання ключів і програмного забезпечення для дешифрування. Невдовзі після цього вони почали намагатися порушити роботу баз даних, таких як CouchDB та Elasticsearch, із застосуванням націленої на сервери програми-здирника.

Компанія Rapid7 є партнером Cisco та постачальником даних і аналітичних рішень у сфері безпеки. Як пояснили дослідники Rapid7 у Звіті Cisco з інформаційної безпеки за перше півріччя 2017 року, сервіси DevOps часто використовуються неналежним чином або навмисно залишаються відкритими для зручного доступу легітимними користувачами, що у свою чергу залишає ці сервіси відкритими для атак.

Компанія Rapid7 проводить регулярні інтернет-аналізи технологій та каталогів DevOps – як щодо відкритих зразків, так і для зразків програм-здирників. Деякі із сервісів DevOps, що вони зустрічають під час своїх досліджень, можуть містити персональні дані, що базуються на назвах таблиць, викладених в Інтернеті.

Для зменшення ризику бути ураженими атаками програм-здирників DevOps організації, які користуються загальнодоступними в Інтернеті зразками технологій DevOps, повинні:

- Розробити потужні стандарти щодо безпечного розгортання технологій DevOps.
- Підтримувати актуальний рівень знань про публічну інфраструктуру, що використовується компанією.
- Систематично оновлювати технології DevOps.
- Проводити сканування для виявлення вразливих місць.

Для отримання більш детальної інформації щодо дослідження Rapid7 див. розділ «Не дозволяйте технологіям DevOps створювати ризик для вашого бізнесу», у Звіті Cisco з інформаційної безпеки за перше півріччя 2017 року.

16 *After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters,* автор Lucian Constantin, *IDG News Service,* 13 січня 2017 року: **pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.**

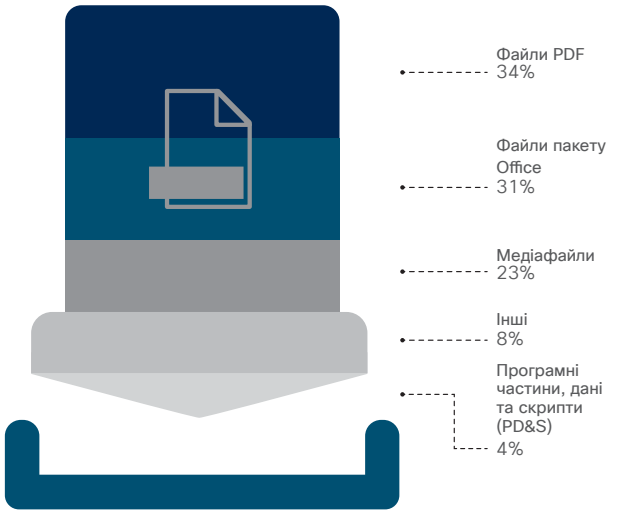
Внутрішні загрози: використання переваг хмари

У попередніх звітах стосовно захисту було обговорено цінність дозволів OAuth та привілеїв суперкористувачів для визначення того, хто має можливість заходити в мережу та яким чином вони можуть отримати доступ до даних.[17] З метою додаткового дослідження впливу діяльності користувачів на безпеку дослідники загроз з компанії Cisco нещодавно перевірили тренди ексфільтрації даних. Вони застосували алгоритм машинного навчання для аналізу профілів 150 000 користувачів у 34 країнах, усі з яких використовують провайдерів хмарних послуг, за період із січня по червень 2017 року. Алгоритм ураховував не лише обсяг документів, які завантажувались, а й такі змінні, як час доби завантаження, IP-адреси та локації.

Після аналізу профілів користувачів протягом шести місяців наші дослідники провели півтора місяці, досліджуючи аномалії, й зафіксували 0,5% користувачів, які здійснили підозрілі завантаження. Це незначна кількість, проте ці користувачі завантажили в цілому більше 3,9 млн документів з корпоративних хмарних систем, що в середньому становить 5200 документів на користувача протягом півтора місяця. З числа підозрілих завантажень 62% відбувались поза межами звичайного робочого часу; а 40% – у вихідні дні.

Дослідники компанії Cisco також провели інтелектуальний текстовий аналіз назв 3,9 млн підозрілих документів, які були завантажені.

Рисунок 23 Документи, які було завантажено найчастіше



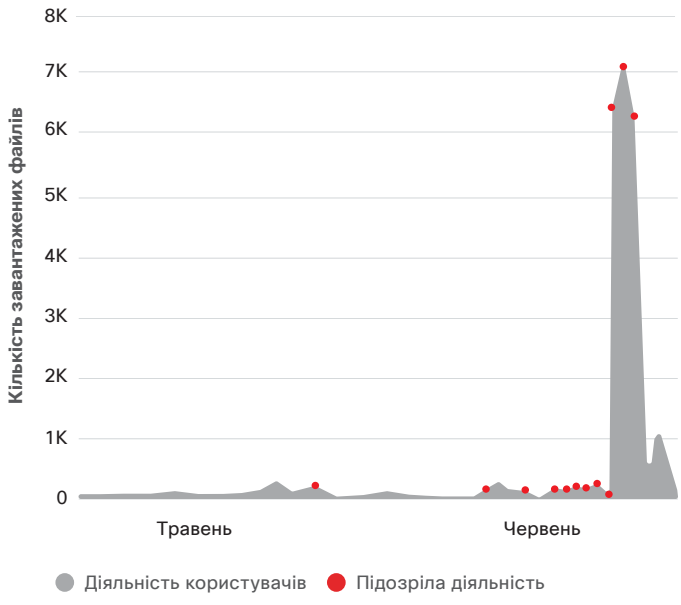
Джерело: дослідження Cisco щодо безпеки

Одним з найпопулярніших ключових слів у назвах документів було слово «дані». Ключові слова, які найчастіше використовувались разом зі словом «дані» – слова «працівник» та «клієнт». Щодо типів документів, які завантажувались: 34% – це файли PDF і 31% – документи Microsoft Office (див. Рисунок 23).

Застосування алгоритмів машинного навчання дозволяє більш ретельно відстежувати діяльність користувачів у хмарі, а не просто кількість завантажень. У нашому аналізі 23% користувачів, яких ми перевіряли, було більше трьох разів відмічено через підозрілі завантаження, що зазвичай починалося з невеликої кількості документів. Кожного разу обсяг поступово збільшувався і врешті-решт ці користувачі демонстрували значне зростання кількості завантажень (Рисунок 24).

Алгоритми машинного навчання дозволяють сподіватися на забезпечення більшої прозорості в хмарі та в поведінці користувача. Якщо спеціалісти з безпеки почнуть передбачати поведінку користувача в контексті завантажень, вони зможуть зберегти час, який, можливо, знадобиться для вивчення легітимної поведінки. Вони також можуть долучитися до зупинення потенційної атаки або ексфільтрації даних ще до того, як це станеться.

Рисунок 24 Алгоритми машинного навчання фіксують підозрілу поведінку завантажень користувачем



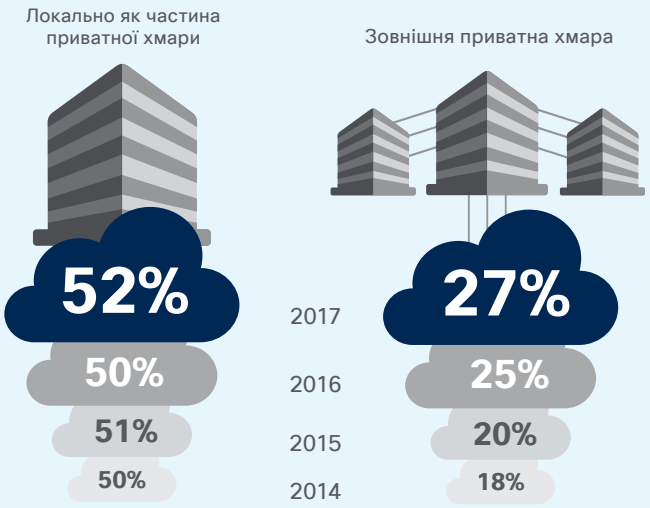
Джерело: дослідження Cisco щодо безпеки

17 *Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco: безпека як ключова перевага хостингу мереж у хмарі

Відповідно до результатів проведеного Cisco порівняльного дослідження рішень безпеки за 2018 рік, рівень використання локальної та публічної хмарної інфраструктури зростає, хоча багато організацій й надалі здійснюють локальний хостинг мереж. У дослідженні за 2017 рік 27% спеціалістів із безпеки зазначали, що використовують зовнішні приватні хмари, порівняно з 25% у 2016 році та 20% у 2015 році (Рисунок 25). 52% спеціалістів зазначили, що хостинг їхніх мереж є локальним у рамках приватної хмари.

Рисунок 25 Більше організації використовують приватні хмари



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

З-поміж організацій, які використовують хмару, 36% тримають від 25% до 49% своєї інфраструктури в хмарі. В той час як 35% тримають в хмарі від 50% до 74% своєї інфраструктури (Рисунок 26).

Безпека є найбільшою перевагою хостингу мереж у хмарі, відповідно до даних спеціалістів з безпеки, серед яких проводилось опитування. 57% з них зазначили, що вони тримають мережі в хмарі через кращий рівень безпеки даних; 48% – через можливість масштабування; та 46% – через легкість у використанні (див. Рисунок 27).

Опитані також зазначили, що по мірі збільшення рівня перенесення інфраструктури в хмару вони можуть розглянути можливість інвестування в програми безпеки доступу до хмари (CASB) для додаткового рівня безпеки в хмарних середовищах.

Рисунок 26 53% організацій тримають щонайменше половину своєї інфраструктури в хмарі

Джерело: порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Рисунок 27 57% спеціалістів з безпеки вірять, що хмара забезпечує кращу безпеку даних

Джерело: порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

ІНТЕРНЕТ РЕЧЕЙ ТА DDOS-АТАКИ

Технології Інтернету речей (IoT) досі розвиваються, проте зловмисники вже використовують слабкість захисту в пристроях IoT для отримання доступу до систем. У тому числі до систем промислового контролю, що підтримують критично важливу інфраструктуру. Мережі IoT-ботів також збільшуються як за розмірами, так і за потужністю й отримують усе більше можливостей для здійснення потужних атак. Зміщення зловмисниками акцентів у напрямі більшого застосування програмного рівня вказує на те, що є їхньою справжньою метою. Проте велика кількість спеціалістів з безпеки не розуміють або не приділяють належної уваги загрозам, які можуть становити мережі ботів IoT. Організації збільшують кількість пристроїв IoT у своїх IT-середовищах, мало або абсолютно не приділяючи уваги безпеці. Або навіть ще гірше: не знаходять час оцінити те, скільки пристроїв IoT приєднано до їхньої мережі. Таким чином, вони спрощують завдання зловмисникам щодо отримання контролю над IoT.

Небагато організацій розглядають мережі ботів IoT в якості неминучої загрози – але їм варто про це подумати

Як розвивається та розширюється IoT, те саме відбувається і з мережами ботів IoT. Та оскільки ці мережі ботів зростають та вдосконалюються, зловмисники використовують їх для запуску DDoS-атак з усе більшою інтенсивністю та масштабністю. Компанія Radware, партнер Cisco, виконала аналіз трьох найбільших мереж ботів IoT – Mirai, Brickerbot та Hajime, та повторно розкрила тему мереж ботів IoT в останньому звіті для того, щоб підкреслити важливість загрози.[18] Їх дослідження демонструє, що лише 13% організацій вважають, що мережі ботів стануть великою загрозою для їхнього бізнесу у 2018 році.

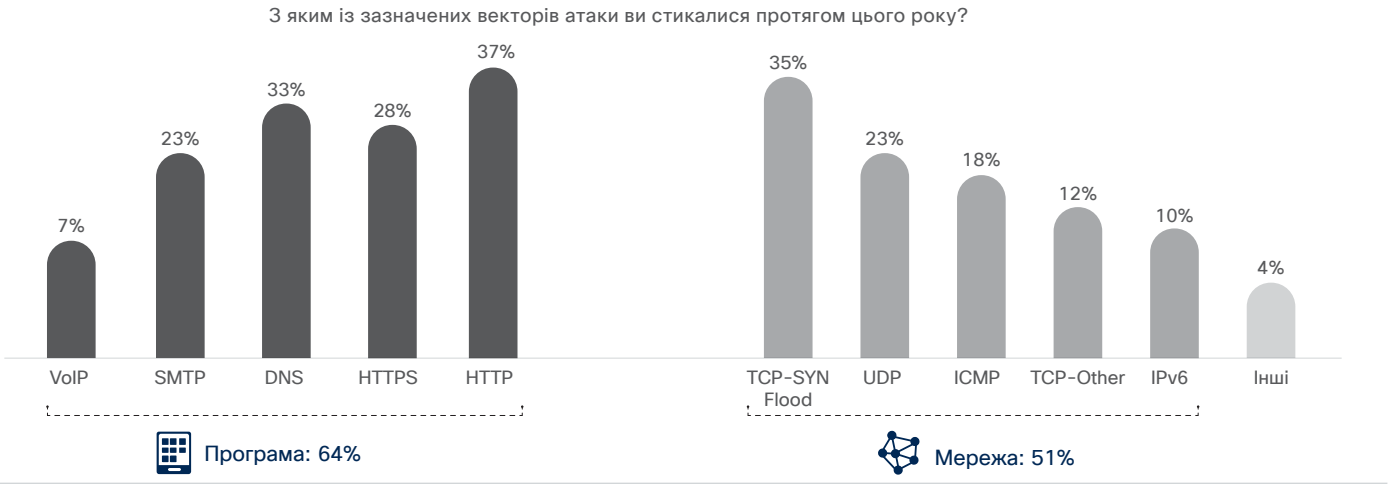
Мережи ботів IoT процвітають, тому що організації та користувачі швидко запускають дешеві IoT-пристрої, мало, або зовсім не звертаючи уваги на безпеку. IoT-пристрої базуються на системах Linux та Unix, тому вони часто стають ціллю для бінарних кодів у форматі exe-файлів та посилань (ELF). Вони також не є проблемними в плані отримання контролю порівняно з ПК. Це означає, що зловмисники можуть з легкістю створити велику «армію».

Пристрої IoT працюють 24 години на добу та можуть бути миттєво приведені в дію. І тому зі збільшенням зловмисниками розмірів своїх мереж ботів IoT вони інвестують у створення більш складного коду та зловмисних програм і рухаються в напрямі DDoS-атак вищої складності.

Програмна DDoS-атака переважає над мережною DDoS

Кількість атак на програмному рівні дедалі збільшується, в той час як обсяг мережних атак зменшується (див. Рисунок 28). Дослідники з компанії Radware підозрюють, що це зміщення може бути пов'язане зі зростанням мереж ботів IoT. Цей тренд непокоїть, тому що програмний рівень є настільки різноманітним і містить таку велику кількість пристроїв, що означає: атаки, націлені на цей рівень, можуть потенційно паралізувати роботу великих сегментів Інтернету.

Рисунок 28 Кількість програмних DDoS-атак збільшилась у 2017 році



Джерело: Radware

18 Для отримання детальної інформації про дослідження Radware щодо ботів мережі IoT, див. The IoT is only just emerging but the IoT botnets are already here, стор. 39. *Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Згідно з даними дослідників компанії Radware, усе більше зловмисників віддають перевагу програмному рівню, тому що на мережному рівні залишилось мало можливостей для використання. Створення мереж ботів IoT також потребує менше ресурсів, ніж бот-мережі ПК. Це означає, що зловмисники можуть інвестувати більше ресурсів у розробку складного коду та зловмисних програм. Оператори багатовекторної мережі ботів Mirai, яка стала відомою завдяки здійсненню програмних атак підвищеного рівня, є серед тих, що здійснюють інвестиції такого типу.

Зростає складність, частота та тривалість вибухових атак

Одним з найпотужніших трендів DDoS-атак, який зафіксовано спеціалістами компанії Radware у 2017 році, було збільшення коротких вибухових атак, які стають складнішими, частішими та тривалішими. 42% усіх організацій з дослідження Radware стали жертвами цього типу DDoS-атак у 2017 році (Рисунок 29). У більшості атак такі «вибухи» тривали лише декілька хвилин.

Рисунок 29 Зафіксовані DDoS-атаки з повторними «вибухами»

Джерело: Radware

Вибухова тактика зазвичай спрямована на ігрові веб-сайти та сервіс-провайдерів через необхідність цих сервісів бути постійно доступними та їхню нездатність захиститись від маніпуляцій у рамках таких атак. «Вибухи» (спалахи) високого трафіку з певною чи довільною періодичністю протягом декількох днів або навіть тижнів можуть не залишити цим організаціям часу на адекватну відповідь, призводячи до серйозних збоїв у роботі сервісів.

Дослідники компанії Radware кажуть, що вибухові атаки:

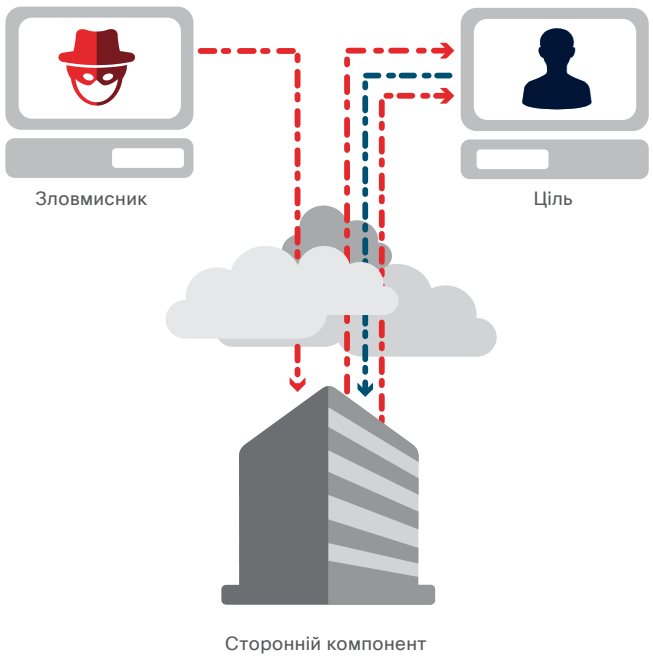
- Складаються з декількох змінних векторів. Атаки є географічно розподіленими та проявляються як тривала серія точних великомасштабних потоків SYN, потоків ACK та потоків UDP на декількох портах.
- Поєднують великомасштабні атаки зі змінною тривалістю – від 2 до 50 секунд великої кількості трафіку з інтервалами приблизно від 5 до 15 хвилин.
- Часто поєднуються з іншими довготривалими DDoS-атаками.

Збільшення атак з відбиттям та посиленням даних (amplification attacks)

Іншим DDoS-трендом, який був зафіксований Radware протягом 2017 року, є кількість DDoS-атак з відбиттям та посиленням даних у якості основного вектору дії проти широкого спектра сервісів. Відповідно до даних Radware, двоє з п'яти бізнесів стали жертвами атаки з відбиттям та посиленням даних у 2017 році. Третина таких організацій повідомляла, що вони не мають змоги протистояти таким атакам.

Атака з відбиттям та посиленням даних використовує потенційно легітимний сторонній компонент для спрямування зловмисного трафіку на ціль, приховуючи особу зловмисника. Зловмисники надсилають пакети на дзеркальні сервери з вихідною IP-адресою, встановленою на IP-адресу цільового користувача. Це створює можливість опосередковано переповнити цільовий канал пакетами даних відповідей та вичерпати можливості використання ресурсів жертви (див. Рисунок 30).

Рисунок 30 Атака з відбиттям та множенням даних



Джерело: Radware

Для успішного виконання атак з відбиттям та посиленням даних зловмисники повинні володіти більшою пропускною спроможністю, ніж їхні цілі. Дзеркальні сервери створюють таку можливість: зловмисник просто відтворює трафік з однієї чи більшої кількості сторонніх машин. Зважаючи на те, що це звичайні сервери, цьому типу атак особливо важко протистояти. Загальні приклади включають:

Повторні атаки з посиленням даних DNS

Ця сучасна атака типу «відмова в обслуговуванні» використовує поведінку сервера DNS для посилення атаки. Стандартний запит DNS є меншим, ніж відповідь DNS. У ході повторюваної атаки з множенням даних DNS зловмисник ретельно обирає запит DNS, результат якого представлений тривалою відповіддю, що є у 80 разів довшою, ніж запит (наприклад, ANY). Зл,овмисник надсилає цей запит за допомогою мережі ботів стороннім серверам DNS, підміняючи при цьому вихідну IP-адресу на IP-адресу цільового користувача. Сторонні сервери DNS надсилають свої відповіді на IP-адресу цілі. За допомогою цієї технології здійснення атак відносно невелика мережа ботів може створити канал об'ємного потоку великих відповідей у напрямі цілі.

Відбиття NTP

Цей тип атаки з лавиноподібним множенням даних використовує загальнодоступні сервери Протоколу мережного часу (NTP) для пригнічення та виснаження засобів захисту трафіком UDP. Протокол мережного часу NTP є старим мережним протоколом для синхронізації годинників між комп'ютерними системами в мережах з пакетною комутацією. Він і надалі широко застосовується на просторах Інтернету десктопами, серверами та навіть телефонами для забезпечення синхронізації годинників. Декілька старих версій серверів NTP містять команду, яка має назву monlist, що направляє запитувачу перелік із 600 останніх хостів, які приєднувались до запитуваного сервера.

За базовим сценарієм зловмисник багаторазово надсилає запит get monlist на довільний сервер NTP та імітує вихідну IP-адресу для сервера, що здійснює запит як цільовий сервер. Після цього відповіді сервера NTP перенаправляються на цільовий сервер для істотного збільшення трафіку UDP з вихідного порту 123.

Відбиття SSDP

Ця атака використовує Простий протокол виявлення сервісів (SSDP), який використовується для забезпечення універсальним самоналаштовувальним пристроям (UPnP) можливості повідомляти про своє існування. Це також сприяє визначенню й управлінню пристроями та послугами, що приєднані до мережі, такими як камери, мережні принтери та багато інших видів електронного обладнання.

Щойно пристрій UPnP приєднується до мережі та після отримання ним IP-адреси пристрій має можливість пропонувати власні сервіси іншим комп'ютерам у мережі шляхом відправлення повідомлень на багатоадресний IP. Коли комп'ютер отримує повідомлення про пристрій, він генерує запит на отримання повного опису сервісів пристрою. Після цього пристрій UPnP надає у відповідь безпосередньо тому комп'ютеру повний перелік будь-яких сервісів, що він може запропонувати.

Так само як і з DDoS-атаками з множенням даних NTP та DNS, зловмисник може використати невелику мережу ботів для здійснення того останнього запиту на отримання сервісів. Після чого зловмисник підмінює вихідну IP-адресу на IP-адресу цільового користувача та перенаправляє відповіді безпосередньо на ціль.

Спеціалісти із захисту повинні закрити шляхи витоку

Шлях витоку, як визначає партнер Cisco – Lumeta, це порушення політики чи сегментації або несанкціоноване чи неправильно сконфігуроване з'єднання з Інтернетом з корпоративної мережі, в тому числі з хмари, що дозволяє перенаправляти трафік до конкретного місця в Інтернеті, наприклад, до зловмисного веб-сайту. Ці неочікувані приєднання також можуть виникати всередині між двома різними сегментами мережі, між якими не повинно бути комунікації. Зокрема, в середовищах критичної інфраструктури неочікуваний шлях витоку між IT-системами виробничого майданчика та компанії може свідчити про зловмисну діяльність. Шляхи витоку також можуть виникнути через неправильно налаштовані роутери та перемикачі.

Пристрої, які не мають правильно налаштованих дозволів або залишаються відкритими та некерованими, становлять легку здобич для зловмисників. Пристрої та мережі, пов'язані з несертифікованим або тіньовим IT, також створюють гарну базу для зловмисників щодо формування шляхів витоку, тому що вони зазвичай знаходяться без управління та не отримують належні оновлення. За оцінками компанії Lumeta, приблизно 40 % динамічних мереж, кінцевих точок та хмарної інфраструктури на підприємствах сприяють виникненню істотних сліпих точок в інфраструктурі та нестачі поінформованості про актуальний стан справ для спеціалістів із захисту.

Визначення існуючих шляхів витоку є дуже важливим, оскільки вони можуть бути використані в будь-який час. Проте важливо виявляти новостворені шляхи витоку в режимі реального часу, тому що вони є безпосередніми показниками слабких місць та пов'язані з найбільш складними атаками, включаючи програми-здирники.

Проведений нещодавно компанією Lumeta аналіз IT-інфраструктури в більш ніж 200 організацій у декількох галузях демонструє слабкі місця видимості в кінцевих точках. Він також показує, що велика кількість компаній суттєво недооцінюють кількість кінцевих точок у своїх IT-середовищах (див. Рисунок 31). Нестача обізнаності щодо кількості IoT-пристроїв з IP-доступом, приєднаних до мережі, є часто основною причиною недооцінювання кінцевих точок.

Рисунок 31 Огляд сліпих точок в інфраструктурі в різних галузях

Дійсні клієнти Lumeta	Уряд	Охорона здоров'я	Технології	Фінанси
Очікувані кінцеві точки	150 000	60 000	8000	600 000
Визначені кінцеві точки	170 000	89 860	14 000	1 200 000
Слабкі місця видимості в кінцевій точці	12%	33%	43%	50%
Некеровані мережі	3278	24	5	771
Неавторизовані або незахищені передавальні пристрої	520	75	2026	420
Відомі, але недосяжні мережі	33 256	4	16 828	45
Шляхи витоків в Інтернет, виявлені під час розгортання	3 000	120	9400	220

Джерело: Lumeta

Дослідники компанії Lumeta прогнозують, що число шляхів витоку буде зростати. Особливо в хмарних середовищах, де існує менше мережної прозорості, а також застосовується менше заходів безпеки.

Зловмисники не завжди негайно використовують шляхи витоку, які вони знаходять або створюють. Коли вони повертаються до цих каналів, то використовують їх для встановлення зловмисних програм або програм-здирників, крадуть інформацію тощо. Дослідники з компанії Lumeta в якості однієї з причин того, чому шляхи витоку часто залишаються невизначеними, називають те, що зловмисники шифрують та приховують свою діяльність, використовуючи, наприклад, TOR. А також вони є обережними і використовують шляхи витоків продумано, щоб не привернути увагу до своєї діяльності з боку спеціалістів із захисту.

Дослідники з компанії Lumeta стверджують, що прогалини у навичках спеціалістів із захисту, особливо нестача фундаментальних знань про мережі, може негативно вплинути на здатність організацій вчасно виявляти та вирішувати проблеми зі шляхами витоку. Кращий рівень співпраці між мережними та безпековими командами може допомогти прискорити виявлення та усунення шляхів витоку.

Інструменти для автоматизації, які надаються мережним контекстом, також можуть надати аналітикам з безпеки можливість прогнозувати потенційні проблеми зі шляхами витоку. Крім цього, впровадження належних політик сегментації може допомогти командам захисту швидко визначити, чи є неочікувана комунікація між мережами або пристроями зловмисною.

Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco: Нестача спеціалістів із захисту заважає багатьом організаціям запроваджувати нові кіберможливості

Серйозна нестача кадрів залишається основною проблемою для спеціалістів із захисту. Як вказано вище, нестача навичок також може негативно вплинути на спроможність організації досліджувати та усувати певні типи загроз.

Також без наявності певних навичок спеціалісти із захисту не зможуть застосовувати новітні технології та процеси, які могли б допомогти в покращенні існуючої ситуації з безпекою (Рисунок 32).

Багато спеціалістів із захисту, які взяли участь у проведеному Cisco порівняльному дослідженні рішень безпеки за 2018 рік, зазначили, що в ідеалі вони б краще автоматизували чи віддали б на аутсорсинг більшість своєї рутинної діяльності для того, щоб можна було перерозподілити свій персонал на виконання роботи з більшою цінністю.

Рисунок 32 Ключові можливості, які б додали спеціалісти із захисту в разі підвищення рівня підбору персоналу

Джерело: порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Уразливості промислових систем управління наражають на ризик критично важливу інфраструктуру

Промислові системи управління (ICS) – це серце всіх виробничих та технологічних систем управління. ICS підключаються до інших електронних систем, які входять до складу процесу контролю, створюючи взаємопов'язану систему з високим рівнем підключень уразливих пристроїв. Бажання порушити їхню роботу може з'являтися в широкого кола зловмисників.

Кіберзловмисники, які мають намір завдати шкоди системі ICS, аби зруйнувати критично важливу інфраструктуру, активно займаються дослідженням та створенням лазівок за принципом backdoor, які сприятимуть майбутнім атакам. Про це повідомляє партнер Cisco компанія TrapX Security, яка займається розробкою засобів інформаційного захисту, спрямованих на виявлення шахрайства. Серед потенційних кіберзлочинців є експерти, що володіють передовими знаннями у сфері інформаційних систем, архітектури ICS та процесів, якими забезпечується їхня робота. Деякі також розуміються на тому, як програмувати контролери та підсистеми управління життєвим циклом продукту (PLM).

Дослідники загроз з центру TrapX нещодавно провели розслідування стосовно декількох кібератак, які були спрямовані на систему ICS клієнтів, з метою сприяння виявленню непередбачених проблем з кіберзахистом ICS. Два наведені нижче випадки мали місце в 2017 році, та розслідування щодо них усе ще тривають.

Ціль: велика міжнародна компанія, що займається очищенням води та переробкою відходів

Зловмисники використали сервер демілітаризованої зони (DMZ) компанії як лазівку для порушення роботи внутрішньої мережі. Група з операційної безпеки отримала попередження завдяки використанню технології захисту від шахрайства, яка була вбудована в мережу DMZ. Ця фізична або логічна підмережа слугує мостом між внутрішніми мережами та такими ненадійними мережами, як Інтернет, захищаючи іншу внутрішню інфраструктуру. Під час розслідування виявлено наступне:

- Сервер DMZ було зламано внаслідок неправильного налаштування, що дозволяло встановлювати з'єднання RDP.
- Сервер було зламано і взято під контроль з декількох IP-адрес, які були пов'язані з політичною групою професійних хакерів, налаштованих до підприємства вороже.
- Зловмисникам вдалося здійснити численні потужні атаки на декілька інших підприємств компанії з внутрішньої мережі, яку було зламано.

Ціль: електростанція

До складу критично важливих активів цієї електростанції входить дуже велика інфраструктура ICS та необхідні елементи диспетчерського управління і збору даних (SCADA), через які здійснюється управління їхніми процесами. Електростанція є критично важливим об'єктом національної інфраструктури, ретельні перевірки та нагляд за якою здійснюється відповідальною національною агенцією з безпеки. Тому вона вважається об'єктом з високим рівнем безпеки.

Відповідною службою CISO було прийнято рішення про застосування «обманної» технології для захисту стандартних інформаційних ресурсів електростанції від атак програм-здирників. Технологію також було поширено на всю інфраструктуру ICS. Одразу після цього група з операційної безпеки отримала декілька попереджень, які вказували на злам систем експлуатаційних установок критично важливої інфраструктури. Негайно проведеним розслідуванням зазначених інцидентів було встановлено, що:

- Пристрій в мережі управління процесами намагався взаємодіяти з програмними пастками, які були замасковані під контролери PLM. Це була активна спроба відтворити схему розміщення та зрозуміти точну природу кожного контролера PLM усередині мережі.
- Зламаний пристрій зазвичай було б закрито, проте вендор, що проводив обслуговування, не закрив з'єднання після завершення роботи. В результаті зазначеного упущення мережа контролю технологічних процесів залишилися вразливою для зловмисників.
- Інформація, яку збирали зловмисники, точно відповідає тій, яка є необхідною для порушення роботи підприємства та потенційного завдання великої шкоди поточній роботі експлуатаційних установок.

Рекомендації

Більшість проникнень до системи ICS розпочинається зі зламу вразливих серверів та комп'ютерних ресурсів усередині корпоративної IT-мережі. Дослідники загроз зі служби TrapX рекомендують організаціям вжити наступних заходів з метою зменшення ризиків та забезпечення єдності виробничої діяльності в різних підрозділах.

- Перевіряти постачальників ПЗ і систем та контролювати негайне застосовування всіх патчів і оновлень. (У разі відсутності патчів варто розглянути можливість переходу на нову технологію.)
- Зменшити використання карт пам'яті USB та DVD-приводів.
- Відокремити системи ICS від IT-мереж. Не варто допускати будь-яких прямих з'єднань між вказаними двома компонентами. Це включає в себе мережні підключення, ноутбуки та карти пам'яті.
- Запровадити політики, які суворо обмежують використання мереж ICS для будь-чого іншого, крім необхідних технологічних операцій. Зменшити доступність робочих станцій і моніторів ICS з можливістю доступу із зовнішнього інтернет-браузера. Припускати, що ці політики можуть не спрацювати, й підготувати відповідні плани.
- Відстежувати та видаляти всі вбудовані паролі чи паролі за замовчуванням у вашій виробничій мережі. Також у будь-якому випадку, коли це можливо, запроваджувати дворівневу авторизацію.
- Переглядати плани аварійного відновлення після будь-якої істотної кібератаки.

Для додаткового вивчення окремих прикладів, див. дослідження служби TrapX щодо безпеки:, *Anatomy of an Attack: Industrial Control Systems Under Siege.*

Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco: очікуються нові атаки на виробничу інфраструктуру та IoT-пристрої

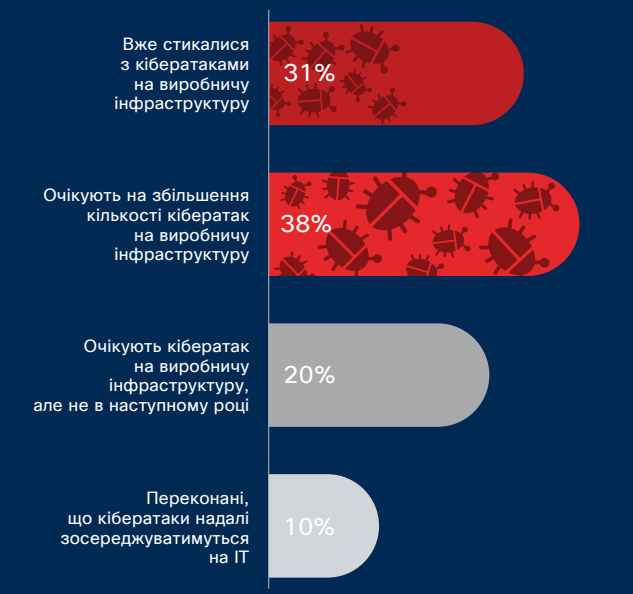
Атаки на операційні системи, наприклад на промислові системи управління, та на IoT-пристрої, усе ще не є досить поширеними. Тож більшість спеціалістів з безпеки не мають безпосереднього досвіду щодо того, як справлятися з ними. Проте, згідно з проведеним компанією Cisco **Порівняльним дослідженням рішень безпеки за 2018 рік,** спеціалісти з безпеки не мають сумнівів, що такі атаки здійснюватимуться, й наразі намагаються визначити, як саме вони реагуватимуть на них.

Спеціалісти з безпеки визнають, що ці системи зазвичай мають обмежену кількість засобів захисту, а також застаріле програмне забезпечення, яке не містить усіх необхідних оновлень, що робить їх уразливими до атак.

«Ми до сих пір використовуємо пристрої старше 25 років, а також компресори та механізми, яким уже по 40 років, – стверджує один з опитуваних. – IT-фахівці звикли все планувати. Вони кажуть: «Скажіть мені, коли Windows X більше не підтримуватиметься» або «Ця версія Oracle доживає свого кінця». У виробничих інфраструктурах такого немає».

Мало хто з фахівців з безпеки може впевнено говорити про проблеми із захистом виробничої інфраструктури своїх організацій. Це пов'язано або з тим, що вони не обслуговують великої кількості виробничих систем, або з тим, що вони тільки нещодавно впровадили технології IoT. 31 % зазначених спеціалістів розповіли, що їхні організації вже стикалися з кібератаками на виробничу інфраструктуру. В той час як 38 % зазначили, що протягом наступного року вони очікують розширення атак з IT на виробничу інфраструктуру (Рисунок 33).

Рисунок 33 31% організацій стикалися з кібератаками на OT-інфраструктуру



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

УРАЗЛИВОСТІ ТА ВИКОРИСТАННЯ ПАТЧІВ

Серед моря ризиків безпеки спеціалісти із захисту можуть втрачати з поля зору уразливості технологій, що використовуються. Будьте певні, зловмисники звертають на них увагу та розмірковують, як саме скористатися цими потенційно слабкими місцями для здійснення атак.

Були часи, коли передовою практикою вважалося використання патчів для усунення відомих уразливих місць протягом 30 днів. Наразі, чекаючи стільки часу на вирішення проблеми, ви можете наразити організацію на підвищений ризик стати мішенню атаки. Оскільки зловмисники швидше можуть розробити і застосувати активні засоби для проникнення, використовуючи вразливі місця. Організаціям також не варто нехтувати малими, проте істотними прогалинами в безпеці, якими можуть скористатися зловмисники – зокрема, на етапі розвідки, коли вони шукають шляхи проникнення до системи.

До складу недоліків у системі інформаційної безпеки, що переважали протягом 2017 року, увійшли помилки переповнення буферу та вразливості Apache Struts

Помилки переповнення буферу посіли перші місця в переліку загальних вразливостей (CWE), які відстежувалися компанією Cisco у 2017 році, у той час як інші категорії демонстрували рух у бік збільшення та зменшення.

Вразливості при перевірці вхідних значень зросли, у той час як зменшилася кількість помилок, пов'язаних з буфером (Рисунок 34).

Рисунок 34 Динаміка категорій загроз CWE

Категорія загрози	Січень–вересень 2016 р.	Січень–вересень 2017 р.	Зміна
CWE-119: Помилки буферу	493	403	(-22%)
CWE-20: Перевірка вхідних даних	227	268	+15%
CWE-264: Дозволи, привілеї та доступ	137	163	+18%
CWE-200: Витік/розголошення інформації	125	250	+100%
CWE-310: Криптографічні питання	27	17	(-37%)
CWE-78: Введені команди ОС	7	15	+114%
CWE-59: Перехід за посиланням	5	0	

Джерело: дослідження Cisco щодо безпеки

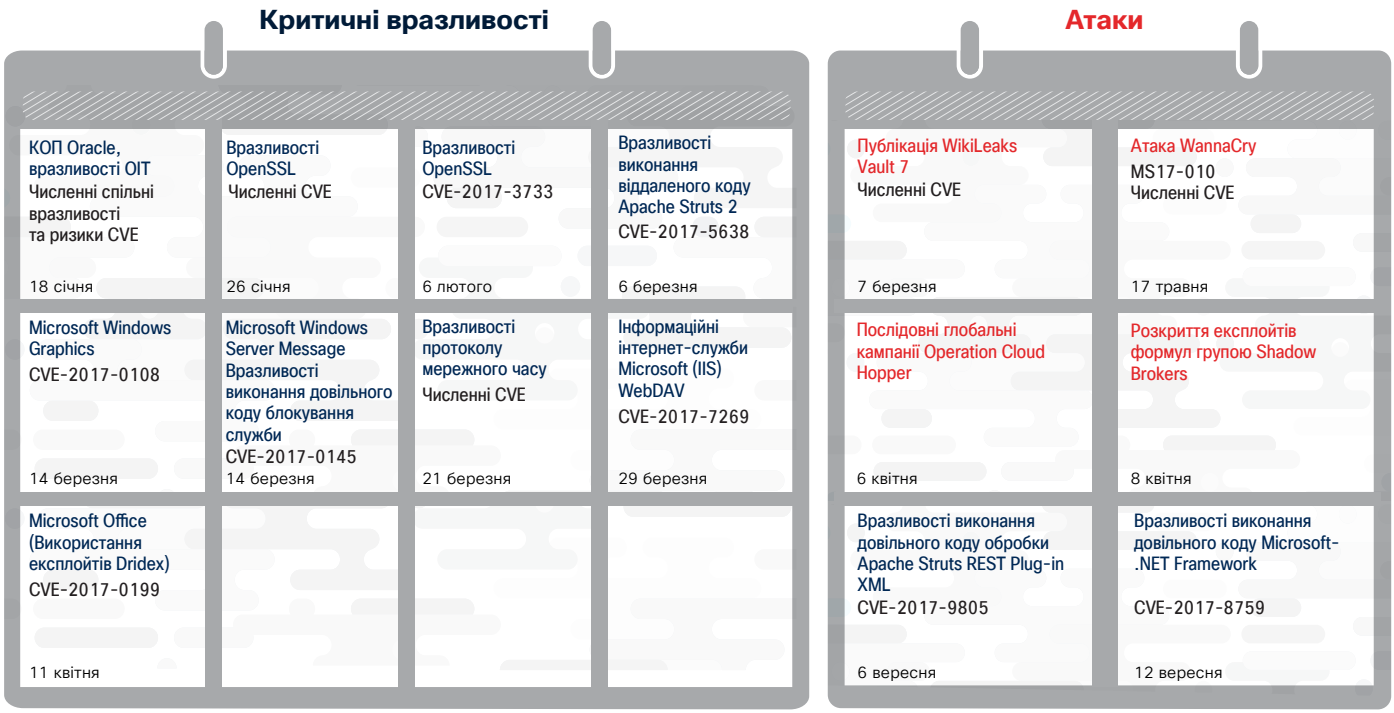
Як демонструє дослідження критичних інформаційних повідомлень (Рисунок 35), уразливості Apache Struts усе ще були досить помітними у 2017 році. Apache Struts – це інфраструктура з відкритим вихідним кодом, що широко використовується для створення Java-додатків. Вразливості Apache Struts були відповідальними за порушення систем безпеки у 2017 році, які виникли в найбільших брокерів даних.

Незважаючи на те, що Apache швидко виявляє вразливості та випускає патчі, ці патчі складно встановлювати на такі інфраструктурні рішення, як Apache Struts, без зниження продуктивності мережі.

Як обговорювалося в попередньому звіті компанії Cisco щодо безпеки,[19] вразливості стороннього програмного забезпечення або програмного забезпечення з відкритим кодом можуть потребувати ручного виправлення з використанням патчів. Це неможливо здійснювати з такою самою частотою, як у випадку автоматичного встановлення патчів, що надаються постачальниками програмного забезпечення. Це дає зловмисникам більший проміжок часу на запуск атак.

Глибинне сканування операційних систем на рівні бібліотек або індивідуальних файлів може забезпечити для організацій інвентаризацію компонентів рішень з відкритим кодом.

Рисунок 35 Критично важливі рекомендації та дії у відповідь на атаки



Джерело: дослідження Cisco щодо безпеки

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

19 *Звіт Cisco з інформаційної безпеки за перше півріччя 2017 року:* cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Вразливості IoT та бібліотек набули більшого розмаху в 2017 році

У період з 1 жовтня 2016 року по 30 вересня 2017 року дослідники загроз із компанії Cisco виявили 224 нових вразливості в продуктах, які не належать Cisco. З них 40 вразливостей були пов'язані з бібліотеками стороннього програмного забезпечення, яке було включено в такі продукти, а 74 – з IoT-пристроями (Рисунок 36).

Відносно велика кількість вразливостей у бібліотеках вказує на необхідність глибшого вивчення сторонніх рішень, які забезпечують основу для багатьох корпоративних мереж. Спеціалісти із захисту мають робити припущення, що бібліотеки стороннього ПЗ можуть стати мішенню для зловмисників; недостатньо лише переконатися в тому, що використовується остання версія програмного забезпечення та покладатися на відсутність розповсюджених вразливостей у звітах. Групи фахівців з безпеки повинні часто перевіряти наявність оновлень, ознайомлюватися з практиками у сфері безпеки сторонніх постачальників. Наприклад, такі групи могли б вимагати від постачальників надавати звіти про життєвий цикл безпечної розробки.

Інша передова практика перевірки стороннього програмного забезпечення допомагає забезпечити безпечне виконання функцій автоматичного оновлення або перевірки на наявність оновлень. Наприклад, при запуску оновлення спеціалісти з інформаційної безпеки повинні переконатися в тому, що зв'язок з таким ПЗ здійснюється через безпечний канал (такий, як SSL) і що програмне забезпечення має цифровий підпис. Обидва елементи є необхідними. Якщо використовується лише цифровий підпис, а канал не є безпечним, зловмисник може перехопити трафік і потенційно замінити оновлення старішою версією ПЗ, що має цифровий підпис, але може містити вразливості. У разі використання лише безпечного каналу зловмисник потенційно здатний зламати сервер оновлень постачальника й замінити оновлення шкідливою програмою.

Рисунок 36 Уразливості сторонніх бібліотек та IoT

Загальна кількість уразливостей: 224

Джерело: дослідження Cisco з інформаційної безпеки

Вразливості Spectre та Meltdown: підготовка на випередження може прискорити відновлення

Зроблена в січні 2018 року заява про вразливості Spectre та Meltdown, які могли дозволити зловмисникам пошкодити дані на платформах, що працюють на процесорах сучасного покоління, викликала занепокоєння щодо здатності фахівців з інформаційної безпеки захиститися від атак. Вразливості могли дозволити зловмисникам переглядати програмні дані в пам'яті на чипсеті з можливістю завдання значної шкоди, оскільки мікропроцесори з вразливостями можна знайти будь-де – від мобільних телефонів до серверного обладнання.

Загрози, які несуть у собі вразливості Spectre та Meltdown, вказують на важливість спілкування з організаціями з інформаційної безпеки щодо таких рішень, як патчі. А також важливість забезпечення, щоб сторонні постачальники, а саме постачальники хмарних технологій і постачальники в ланцюзі поставок, дотримувалися передових практик щодо виправлення недоліків у системі безпеки, які виникають у результаті таких вразливостей. Групи реагування на питання безпеки продуктів або групи PSIRT (наприклад, група PSIRT Cisco) призначені для швидкого реагування на повідомлення про вразливості, надання патчів та повідомлення замовників про те, як уникати ризиків.

Організаціям необхідно планувати свої дії в разі виникнення таких вразливостей, як Spectre та Meltdown, а не сподіватися на те, що вони їх оминуть. Основне завдання полягає в підготовці до таких повідомлень та наявності систем для мінімізації потенційної шкоди. Наприклад, групи спеціалістів з безпеки повинні завчасно скласти перелік пристроїв, наявних у їхньому розпорядженні, та задокументувати конфігурації функцій, що використовуються, оскільки деякі вразливості залежать від конфігурації та впливають на безпеку лише в разі активації певних характеристик.

Групи спеціалістів з безпеки також повинні запитувати сторонніх постачальників, а саме постачальників хмарних технологій, про їхні процеси оновлення та надання патчів. Організаціям необхідно вимагати прозорості від постачальників хмарних технологій стосовно того, як вони справляються з такими вразливостями, а також наскільки швидко вони можуть реагувати на попередження. Проте, врешті-решт відповідальність за готовність покладається на самі організації – вони повинні підтримувати зв'язок з організаціями PSIRT і запроваджувати процеси для швидкого реагування на вразливості.

Для отримання більш детальної інформації, див. пост про Spectre та Meltdown у блозі Talos.

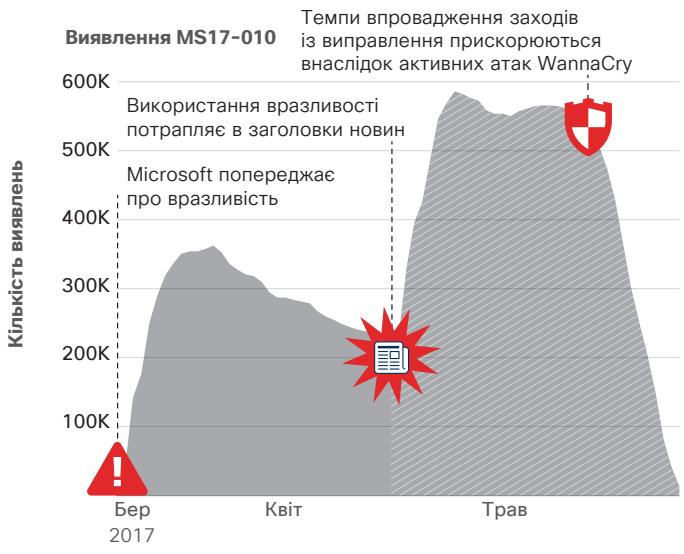
Активні експлойти сприяють пошуку рішення, але не для пристроїв IoT

Компанією Qualys, Inc., партнером Cisco і постачальником хмарних рішень для забезпечення безпеки та відповідності нормативним вимогами, було досліджено в ретроспективі поведінку компаній у сфері управління патчами до та після кампанії WannaCry, яка зачепила велику кількість організацій по всьому світу в травні 2017 року.

Програма-здирник крипточерв'як WannaCry, яка була розроблена, як вважає більшість експертів з інформаційної безпеки, для видалення даних, скористалася вразливістю безпеки Microsoft Windows, що називається EternalBlu. Про неї стало відомо в результаті витоку інформації, здійсненого хакерською групою Shadow Brokers у середині квітня 2017 року. (Для більш детальної інформації з цього питання див. «Вони вже там: у 2018 році захисники мають підготуватися до нових мережних загроз, які розповсюджуються самостійно» на стор. 6)

14 березня 2017 року Microsoft випустила оновлення системи безпеки (MS17-010), яким було попереджено користувачів про критичну вразливість свого SMB-сервера Microsoft Windows. На Рисунку 37 показано різке збільшення кількості пристроїв з виявленими вразливостями і потім поступовий спад протягом періоду із середини березня до середини квітня в міру сканування організаціями своїх систем та застосування патчу.

Рисунок 37 Динаміка використання патчів до та після кампанії WannaCry



Джерело: Qualys

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Тим не менш значна кількість пристроїв усе ще не мала патчів станом на середину квітня. Після цього 14 квітня група Shadow Brokers випустила робочий експлойт, націлений на відому вразливість різних версій Microsoft Windows. На Рисунку 37 показано, що кількість пристроїв з виявленою вразливістю збільшилася майже вдвічі одразу після цього. Це відбулося тому, що організації дізналися про експлойт і його потенційний вплив на підтримувані та непідтримувані версії Windows через дистанційну перевірку Qualys, у якій було використано частину коду експлойту.

Проте навіть після випуску експлойту жодного широкомасштабного використання патчів до середини травня не відбувалося, поки атака WannaCry не потрапила до головних новин по всьому світу. На Рисунку 37 зображено круту криву вирішення проблем після зазначеної кампанії. До кінця травня без патчів залишалася невелика кількість пристроїв.

Проведене компанією Qualys дослідження поведінки клієнтів щодо використання патчів указує на те, що повинна відбутися головна подія, яка змушує більшість організацій застосовувати патчі для вирішення критичних вразливостей – навіть наявність інформації про активний експлойт не є достатньою для прискорення вирішення проблеми. Крім цього, у випадку кампанії WannaCry підприємства мали доступ до патчу для вирішення вразливості Microsoft за два місяці до того, як відбулися атаки програм-здирників.

Інший фактор, який описується дослідниками Lumeta, партнера Cisco та Qualys, полягав у відсутності патчів для невідомих, некерованих, невизначених та тіньових кінцевих IT-пристроїв. Зловмисникам вдалося скористатися цими сліпими точками як важелем. Без знання таких систем сканери вразливостей були нездатні оцінити та рекомендувати патчі для цих систем, залишивши їх вразливими до WannaCry.

По відношенню до IoT-пристроїв процес застосування патчів відбувається навіть повільніше або взагалі не відбувається

Компанією Qualys також було досліджено тенденції використання патчів на IoT-пристроях. До числа пристроїв у зразку ввійшли системи HVAC з підтримкою протоколу IP, дверні замки, панелі пожежної сигналізації та зчитувачі карток.

Дослідники спеціально розглядали IoT-пристрої, вразливі до декількох відомих загроз, у тому числі шкідливе програмне забезпечення Devil's Ivy, яке використовує вразливість у коді під назвою gSOAP. Він має широке застосування в системах фізичної безпеки, а також Mirai, IoT-ботнет, що підключається до цільових машин шляхом здійснення атак на сервери Telnet методом підбирання пароля.

Рисунок 38 Тенденції використання патчів на IoT-пристрої

Джерело: Qualys

Компанія Qualys загалом виявила 7328 пристроїв, проте лише 1206 з них було полагоджено (див. Рисунок 38). Це означає, що 83 % IoT-пристроїв на показаному зразку все ще мають критичні вразливості. У той час коли компанія Qualys не виявила доказів щодо зловмисників, націлених на ці вразливості, організації все ще були наражені на ризик атаки. Тим не менш немає ознак того, що вони мають на меті прискорити процес виправлення.

За інформацією Qualys, існує декілька можливих пояснень інертності щодо використання патчів. Наприклад, деякі пристрої не можуть бути оновлені. Інші можуть потребувати безпосередньої підтримки постачальників. Крім того, не завжди зрозуміло, хто саме всередині організації відповідає за обслуговування IoT-пристроїв. Наприклад, команді інженерів, які дбають про систему HVAC компанії, може бути невідомо про IT-ризики, що можуть вплинути на систему, або навіть про те, що система має підтримку протоколу IP.

Проте ще більше занепокоєння викликає невелика кількість IoT-пристроїв, які були виявлені компанією Qualys. Фактична кількість ймовірно є набагато більшою, оскільки організації просто не знають, скільки IoT-пристроїв підключено до їхньої мережі. Відсутність актуальної інформації наражає їх на серйозний ризик зламу (див. стор. 34 для отримання більш детальної інформації з цього питання).

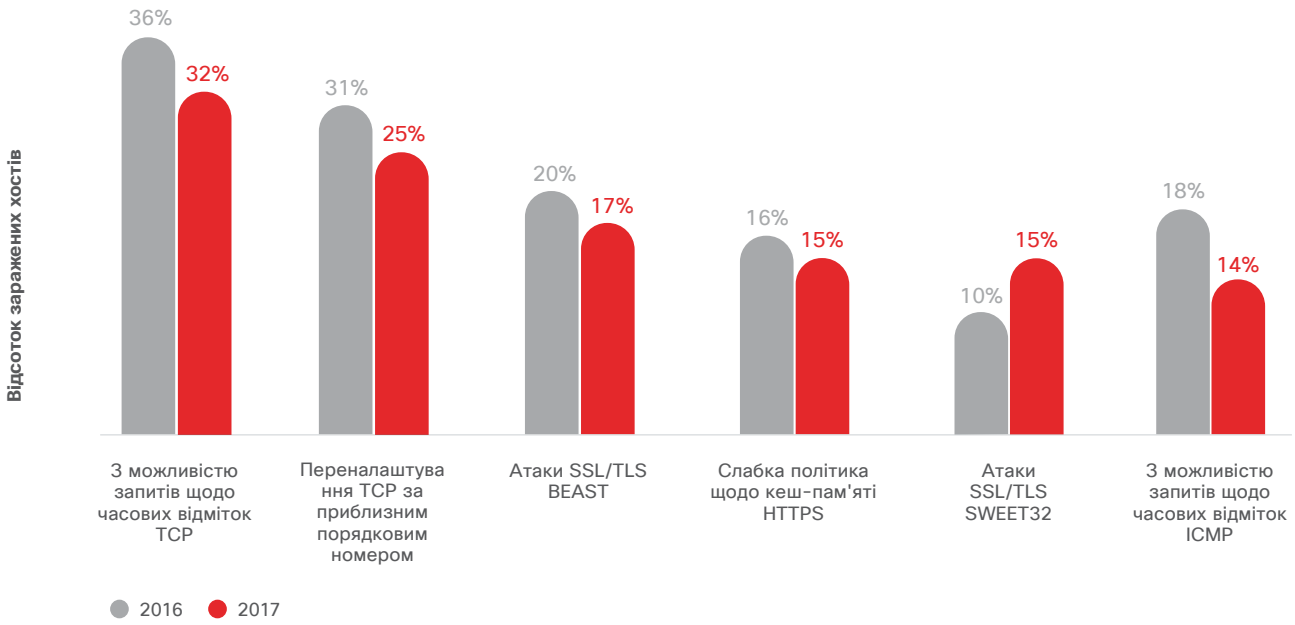
Перший крок на шляху до вирішення зазначеного питання полягає в підготовці переліку всіх IoT-пристроїв у мережі. Після цього організації можуть визначити можливість проведення сканування пристроїв й те, чи все ще підтримуються вони постачальниками, а також які працівники компанії використовують їх та відповідають за них. Організації також можуть покращити IoT-безпеку, якщо вони обслуговуватимуть усі IoT-пристрої так само, як інші комп'ютерні пристрої, дозволяючи забезпечити отримання ними оновлень вмонтованого програмного забезпечення та патчів на регулярній основі.

Більшість поширених вразливостей мають невисоку важливість, але несуть високий ризик

Вразливості з низьким рівнем небезпеки часто залишаються невирішеними протягом років, оскільки компанії або не знають про те, що вони існують, або не вважають їх значними ризиками, як стверджують експерти з питань безпеки SAINT Corporation, компанії-постачальника рішень з безпеки та партнера Cisco. Тим не менш ці малі, проте істотні прогалини у сфері безпеки можуть стати для зловмисників лазівками до системи.

Дослідники SAINT вивчили дані про ризики вразливості, які були зібрані з-понад 10 000 хост-вузлів у 2016 та 2017 роках. Компанія розробила перелік найпоширеніших вразливостей, які найчастіше виявлялися в усіх організаціях, що досліджувалися, і які вказували на те, що найчастіше мали місце вразливості з низьким рівнем небезпеки (див. Рисунок 39). (Примітка: деякі організації, які брали участь у дослідженні, мали більше одного хост-комп'ютера.)

Рисунок 39 Уразливості з низьким рівнем небезпеки, які виявлялися найчастіше, 2016–2017 рр.



Джерело: SAINT Corporation

Давайте ближче розглянемо перші три вразливості низького рівня серйозності на Рисунку 39 й те, чому вони можуть бути цінними для зловмисників.

Можливість здійснення запитів часової відмітки TCP

Часові відмітки TCP надають інформацію про те, скільки часу працювала машина або коли її було перезавантажено востаннє. Це може допомогти зловмисникам дізнатися, які види вразливостей є наявними. Також у програмному забезпеченні можуть використовуватися системні часові відмітки в якості вихідних даних генератора випадкових чисел для створення шифрувальних ключів.

Переналаштування TCP приблизним порядковим номером

Зловмисники можуть підбирати номери послідовностей і організовувати DoS-атаки проти постійних з'єднань TCP шляхом безперервної відправки пакетів RST TCP, зокрема в протоколах, де використовуються довготривалі з'єднання, наприклад BGP.

Атака BEAST

Зловмисник може використати вразливість Browser Exploit Against SSL/TLS (BEAST) для запуску атаки типу «людина посередині» (MiTM) переважно для того, щоб «прочитати» захищений контент, яким обмінюються сторони. (Примітка: таку програму складно виконати, оскільки зловмисник також повинен контролювати браузер з боку клієнта для того, щоб прочитати і дуже швидко ввести пакети даних.)

Під час свого аналізу дослідники SAINT з питань безпеки не виявили зловмисників, які активно використовували ці вразливості з низьким рівним небезпеки.

Вразливості, показані на Рисунку 39, відомі спільноті фахівців з безпеки, проте про деякі з них зазвичай не виводиться попередження або вони не призводять до автоматичної відмови під час рутинної перевірки на відповідність. Наприклад, це стосується перевірки відповідності Стандарту безпечності даних індустрії платіжних карт (PCI DSS). Вони не є критичними вразливостями, які визначаються відповідно до стандарту, що застосовується в такій індустрії. Кожна індустрія по-різному визначає критичність вразливостей.

Крім цього, найбільш поширені вразливості з низьким рівнем небезпеки, як показано на Рисунку 39, неможливо легко вирішити або вирішити взагалі шляхом використання управління патчами, оскільки вони випливають із проблем з конфігурацією або сертифікатами безпечності (наприклад, слабкі шифри SSL або сертифікат SSL з функцією самопідписання).

Організації повинні діяти негайно щодо подолання вразливостей з низьким рівнем небезпеки – це може призводити до виникнення ризику. Вони мають оцінити і визначити пріоритетність вирішення залежно від того, як вони сприймають ризик, а не покладатися на сторонні рейтинги або часткове використання бальних систем, таких як система вихідної оцінки CVSS, або певного рейтингу дотримання вимог. Лише організаціям відомо про свої власні унікальні середовища та свої стратегії управління ризиками.

Частина II:
Ландшафт захисникі

Частина II: ландшафт захисників

Ми знаємо, що нападники розвивають і пристосовують свої технології швидше, ніж захисники (спеціалісти із захисту). Вони також проводять практичні випробовування експлойтів, стратегій вторгнення та навичок, оскільки можуть запускати атаки все більшого масштабу. Коли зловмисники неминуче вдарять по їхніх організаціях, чи будуть захисники готові до цього й як швидко вони зможуть все відновити? Значною мірою це залежить від заходів, які вони вживають для зміцнення своєї безпеки.

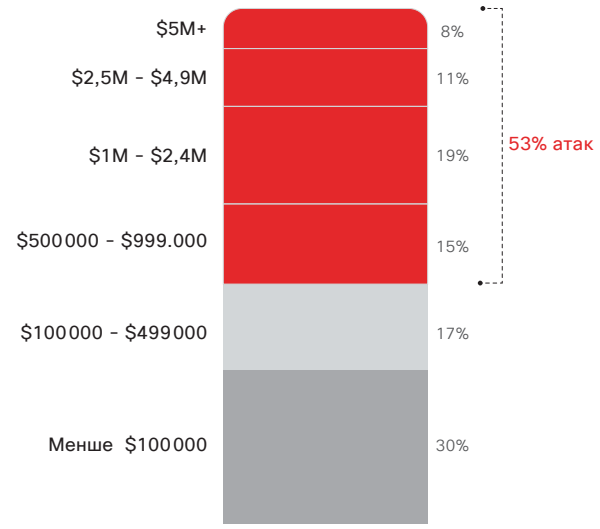
*У результаті проведення нашого **Порівняльного дослідження рішень безпеки за 2018 рік** ми дізналися, що захисники мають багато роботи та викликів, які слід подолати. Щоб оцінити сприйняття захисниками стану безпеки в своїх організаціях, ми запитали у директорів з інформаційної безпеки (CISO) та менеджерів з експлуатаційної безпеки (SecOps) у декількох країнах та в організаціях різного масштабу про їхні ресурси та процедури забезпечення безпеки.*

Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco, пропонує унікальну інформацію про практики безпеки, що наразі використовуються, а також порівняння цих результатів з тими, які були отримані під час досліджень 2017, 2016 та 2015 років. У рамках цього дослідження було опитано понад 3600 осіб у 26 країнах.

Вартість атак

Страх перед атаками ґрунтується на їхній фінансовій вартості, яка більше не є гіпотетичним значенням. Злам системи спричиняє реальну економічну шкоду для організацій – шкоду, на виправлення якої можуть піти місяці або роки.
Як повідомляють респонденти, опитані під час дослідження, більше половини 53%) всіх атак призвели до фінансових збитків у розмірі понад $500 000, включаючи, але не обмежуючись лише цим, неотримані доходи, втрачених клієнтів, втрачені можливості та накладні витрати (Рисунок 40).

Рисунок 40 53% атак призводять до збитків у розмірі $500 тис. або більше



Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Виклики та перешкоди

Докладаючи зусиль для захисту своїх організацій, команди фахівців з безпеки можуть наражатися на численні перешкоди. Організації повинні забезпечити захист у декількох сферах, а також захист декількох функцій, що створює додаткові виклики у сфері безпеки.

Найпроблемнішими з точки зору захисту сферами та функціями є мобільні пристрої, дані в публічних хмарах та поведінка користувачів (Рисунок 41).

Рисунок 41 Найпроблемніші з точки зору захисту сфери: мобільні пристрої та хмарні дані

Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Спеціалісти з інформаційної безпеки вказують бюджет, відсутність взаємодії та персонал в якості основних стримуючих факторів в управлінні безпекою (Рисунок 42). Відсутність підготовленого персоналу також вважається проблемою, коли необхідно запроваджувати передові процеси та технології у сфері безпеки. У 2017 році 27% опитаних вказали на відсутність висококваліфікованих фахівців як на перепону порівняно з 25% у 2016 році та 22% у 2015-му.

Рисунок 42 Найбільша перешкода для безпеки: бюджетні обмеження

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Відсутність кваліфікованих фахівців займає найвищу позицію в переліку перешкод в усіх галузях та в усіх регіонах. «Якби я міг змахнути чарівною паличкою і отримати ще 10% людей, щоб зняти навантаження з тих, хто дійсно працює в авральному режимі з огляду на великий попит послуг саме в їхніх сферах, я був би дуже щасливим», – зазначає CISO великої компанії, яка надає професійні послуги.

У той час коли прогалина з кваліфікованим персоналом залишається невирішеною проблемою, організації повідомляють, що вони намагаються знайти і залучити більше ресурсів до складу своїх команд спеціалістів з безпеки. У 2017 році середня кількість спеціалістів з інформаційної безпеки в штаті організацій становила 40 осіб – значне збільшення порівняно із середньою кількістю у 2016 році, яка нараховувала 33 особи (Рисунок 43).

Рисунок 43 Організації винаймають більше спеціалістів з інформаційної безпеки

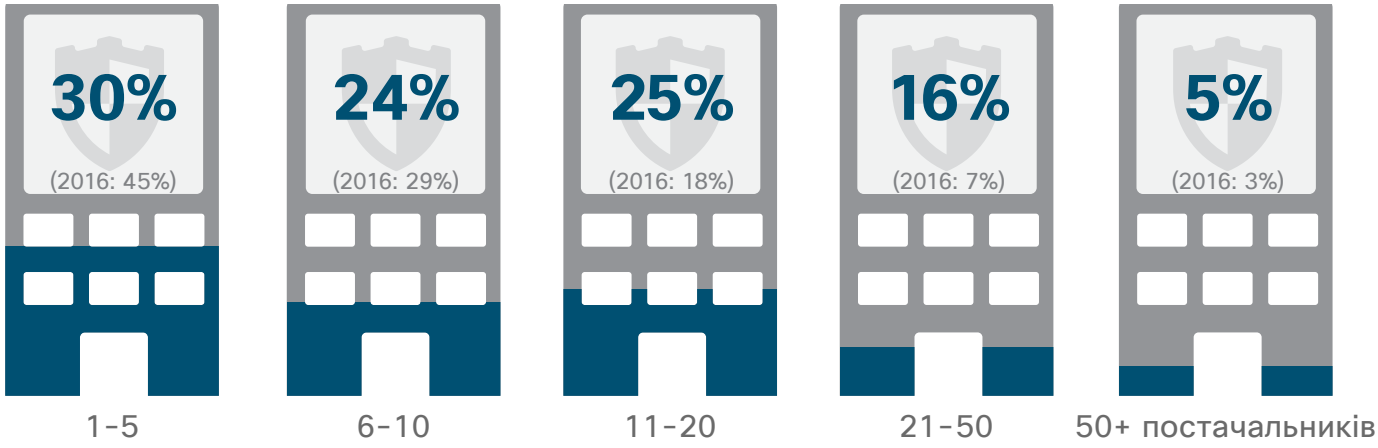
Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Складність, що створюється постачальниками у сфері організації управління

Захисники запроваджують складне поєднання продуктів від різних постачальників: арсенал засобів, який радше зіб'є з пантелику, аніж прояснить ландшафт безпеки. Ці складнощі значно зменшують здатність організації захищатися від атак та збільшують ризик виникнення втрат.

У 2017 році 25% спеціалістів з інформаційної безпеки зазначали, що вони використовують продукти від 11–20 постачальників порівняно з 18% спеціалістів з інформаційної безпеки у 2016 році. Також у 2017 році 16% вказали, що вони використовують у цілому від 21 до 50 постачальників порівняно з 7% респондентів у 2016-му (Рисунок 44).

Рисунок 44 Організації використовували більшу кількість постачальників рішень з безпеки у 2017 році

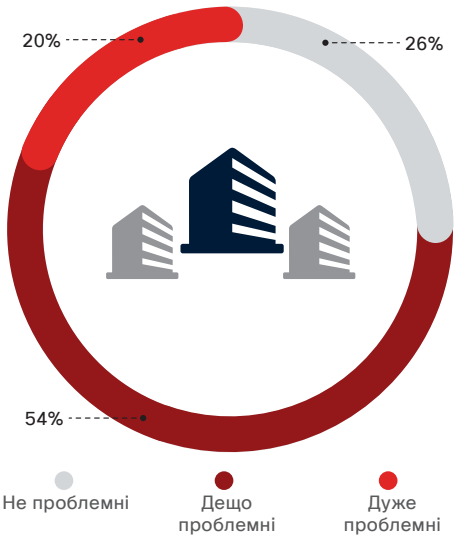


Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Разом з тим зі збільшенням кількості постачальників зростають і виклики організації в управлінні попередженнями, що надходять від рішень такої великої кількості постачальників. Як показано на Рисунку 45, 54% спеціалістів з інформаційної безпеки зазначають, що управління численними попередженнями, які надходять від рішень постачальників, є дещо проблематичним завданням, при цьому 20% вказують, що таке завдання є дуже проблематичним.

Рисунок 45 Проблема з організацією опрацювання попереджень



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

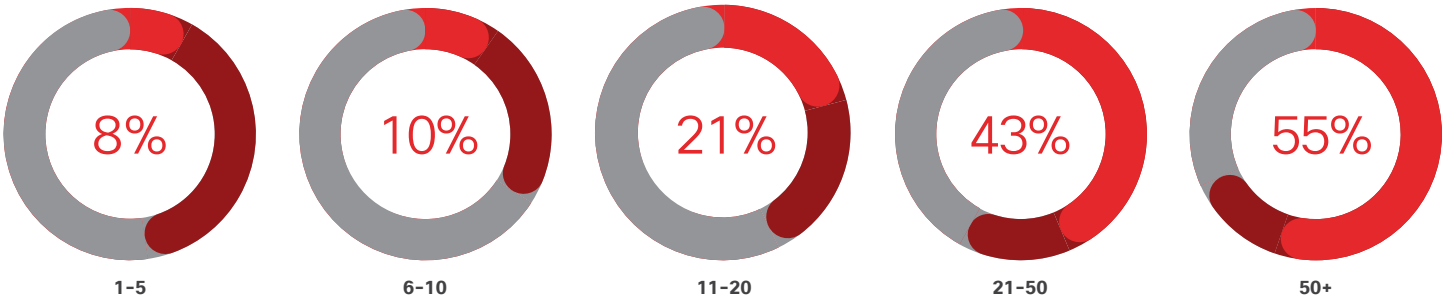
Перед спеціалістами з безпеки постають виклики опрацювання попереджень, що надходять від численних рішень постачальників.

Як показано на Рисунку 46, з числа організацій, які мають усього 1–5 постачальників, 8% зазначають, що управління попередженнями є дуже складним завданням.

Серед організацій, які використовують понад 50 постачальників, 55% зазначили, що таке управління є дуже складним завданням.

Коли організації не можуть організувати управління та не розуміють попереджень, які вони отримують, справжні загрози можуть прослизнути через щілини.

Рисунок 46 Зі збільшенням кількості постачальників зростає проблема організації опрацювання попереджень



	Освіта	Фінансові послуги	Державний сектор	Охорона здоров'я	Виробництво	Фармацевтика	Роздрібна торгівля	Телекомунікації	Транспорт	Комунальні послуги/ Енергетика
Занадто проблемні	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

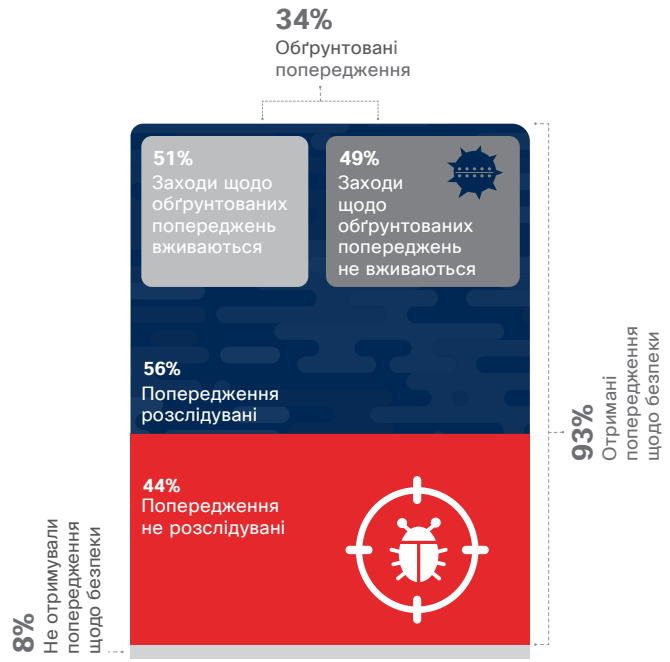
Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Отримана від респондентів інформація вказує на те, що існують прогалини між тими попередженнями, що надійшли, тими, які були розслідувані, та тими, на основі яких встановлюються виправлення. Як показано на Рисунку 47:

- Серед організацій, які отримують щоденні попередження систем безпеки, в середньому 44% таких попереджень не розслідуються.
- З тих попереджень, які були розслідувані, 34% вважаються обґрунтованими.
- Стосовно 51% обґрунтованих попереджень вживаються заходи.
- Стосовно майже половини 49%) обґрунтованих попереджень заходи не вживаються.

У результаті цього процесу більшість обґрунтованих попереджень залишаються без уваги. Однією з причин ймовірно є недостатня кількість працівників та відсутність підготовленого персоналу, який може сприяти вирішенню питання розслідування всіх попереджень.

Рисунок 47 Більшість попереджень про загрозу не було розслідувано чи усунено

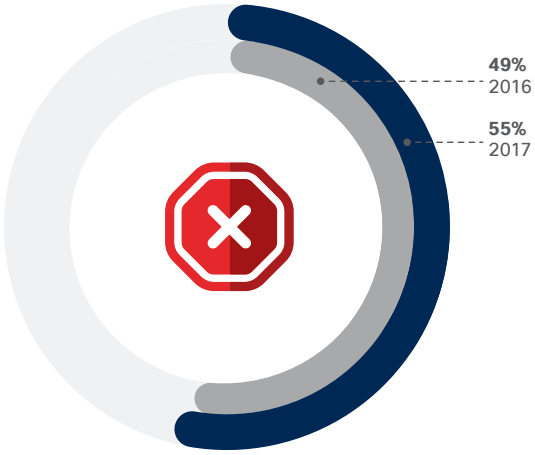


Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Наслідки: пильна увага з боку громадськості в результаті проникнень до системи, збільшення ризику втрат

«Існує два види компаній: ті, які були зламані, й ті, які не знають, що вони були зламані», – стверджував один з респондентів під час порівняльного дослідження. (Відповідь повторює відому цитату колишнього CEO Cisco Джона Чеймберса: «Існує два види компаній: ті, які зазнали хакерської атаки, й ті, які ще не знають, що вони зазнали хакерської атаки».) Незважаючи на те, що організації намагаються впоратись з майбутніми викликами безпеки завдяки відповідній підготовці, спеціалісти з інформаційної безпеки очікують, що вони стануть жертвою атаки, яка приверне пильну увагу громадськості. 55% відсотків опитаних повідомили, що їхні організації були вимушені врегульовувати ситуації з пильною увагою громадськості в результаті здійснення атаки в минулому році (Рисунок 48).

Рисунок 48 55% організацій були вимушені врегульовувати ситуації з пильною увагою громадськості в результаті атаки



2016 (2824), 2017 (3548)

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

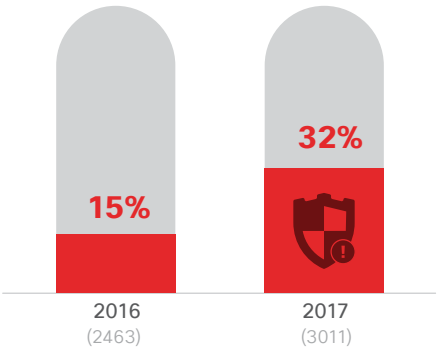
Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Звичним явищем стає те, що майже кожна з 500 компаній з переліку Fortune постраждала від атак протягом останніх 24 місяців. Ви повинні бути готові до цього, зокрема, з точки зору маркетингу та PR», – зазначив один з респондентів під час порівняльного дослідження.

Організації заявили про значно більшу кількість порушень систем безпеки, які відбулися щодо більше 50% систем (Рисунок 49), ніж повідомлялося організаціями, опитаними минулого року. У 2017 році 32% спеціалістів з інформаційної безпеки вказали, що порушення вплинули більше, ніж на половину їхніх систем порівняно з 15% у 2016 році. Від атак переважно страждають такі бізнес-функції, як операційна діяльність, фінанси, інтелектуальна власність та репутація бренду (Рисунок 50).

У складному середовищі систем безпеки організації ймовірніше матимуть справу зі зламом їхніх систем. З числа організацій, які використовують від одного до п'яти постачальників, 28% опитаних стверджують, що вони були вимушені врегульовувати ситуації з пильною увагою громадськості після зламу системи. Ця кількість збільшилась до 80% стосовно організацій, які використовують понад 50 постачальників (Рисунок 51). Зазначене може бути наслідком більшої уваги до загроз, яку може забезпечити більша кількість продуктів.

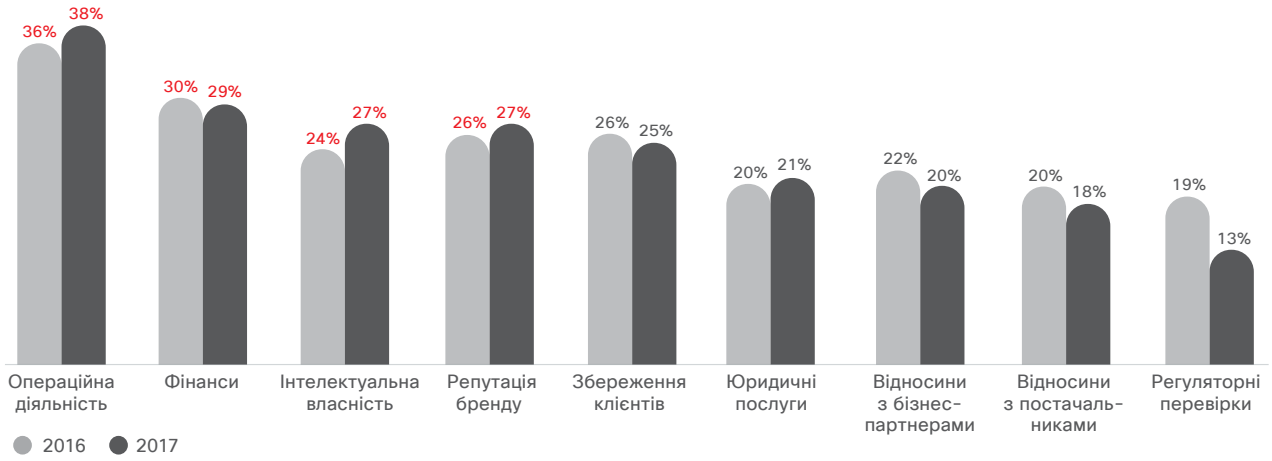
Рисунок 49 Різке збільшення порушень систем безпеки, що впливають на понад 50% систем



Порушення, що призводять до більш ніж половини випадків здійснення впливу на системи організації

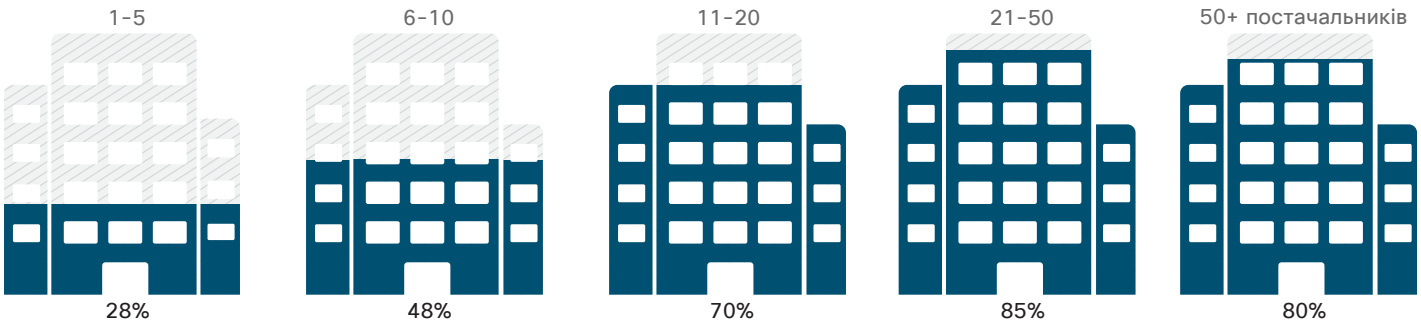
Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Рисунок 50 Операційна діяльність та фінанси ймовірніше можуть постраждати в результаті порушення систем безпеки



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Рисунок 51 80% організацій, які використовують понад 50 постачальників, були вимушені врегульовувати ситуації з пильною увагою громадськості в результаті відкритих атак



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Цінність інтегрованої платформи

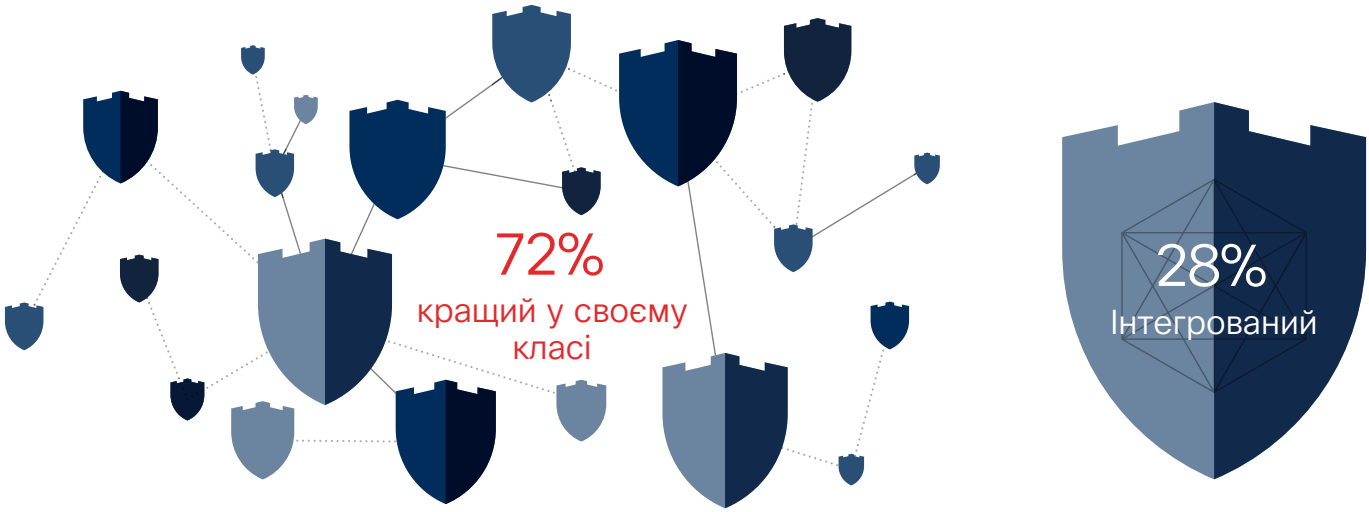
Навіщо використовувати велику кількість продуктів від багатьох постачальників, якщо отримане в результаті середовище є складним для управління? Однією з ключових причин є найкращий у своєму класі підхід, в якому команди спеціалістів з безпеки обирають рішення для кожної потреби, пов'язаної з безпекою. Спеціалісти з інформаційної безпеки, які застосовують на практиці найкращий у своєму класі підхід, також переконані в тому, що він є економічно доцільнішим згідно з результатами порівняльного дослідження.

У процесі порівняння найкращих у своєму класі інтегрованих рішень 72% фахівців з інформаційної безпеки зазначили, що вони купують найкращі у своєму класі точкові рішення для задоволення спеціальних потреб, порівняно з 28%, які купують продукти, призначені для спільної роботи в якості інтегрованого рішення (див. Рисунок 52). З числа організацій, які визнали підхід як «найкращий у своєму класі», 57% вказують на більшу економію. У той час як 39% зазначають, що підхід «найкращий у своєму класі» легше запровадити.

Цікаво, що ті організації, які прийняли інтегрований підхід до безпеки, посилаються на такі ж самі причини свого вибору. 56% з них зазначають, що інтегрований підхід є більш економним, а 48% стверджують про те, що його легше впровадити.

На легкість впровадження все більше посилаються як на фактор використання підходу інтегрованої архітектури. Лише 33% організацій зазначають, що легкість впровадження була причиною вибору інтегрованого підходу у 2016 році порівняно із 47% – у 2017-му. Оскільки рішення від єдиного постачальника можуть бути недостатньо практичними для всіх організацій, покупці рішень з безпеки повинні переконатися в сумісності рішень між собою для зменшення ризику та підвищення ефективності роботи.

Рисунок 52 72% купують найкращі у своєму класі рішення, оскільки вони задовольняють специфічні потреби



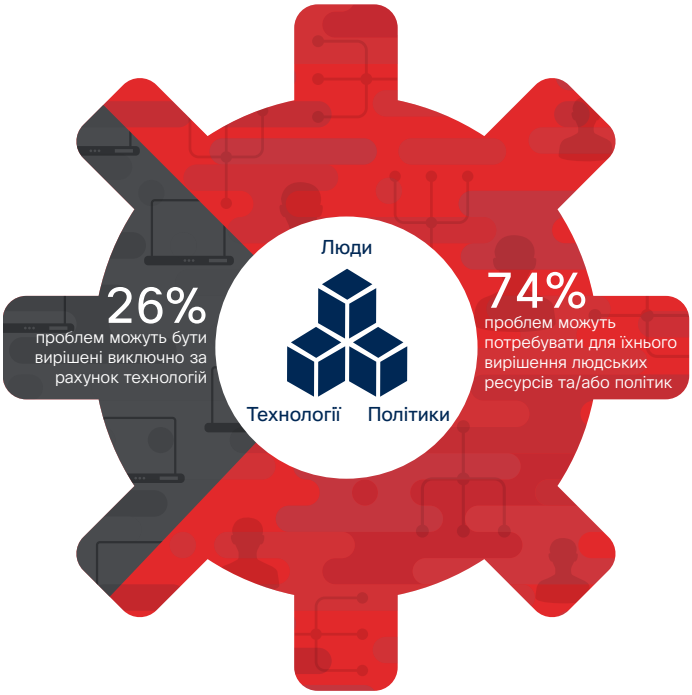
Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Послуги: охопити людей та політики, а не лише технології

Стикнувшись з можливими втратами та несприятливим впливом на системи, організаціям потрібно відмовитися від практики покладатися для захисту виключно на технології. Це означає вивчення інших можливостей для покращання безпеки, наприклад, застосовування політик або навчання користувачів. Необхідний комплексний підхід до безпеки можна віднайти серед тих проблем, які були виявлені під час дослідження Intelligence Lead Security Assurance (відомого як Red Team), яке було проведене Консультаційною групою Cisco з питань удосконалення безпеки сервісів.

У процесі вивчення наведених у рекомендаціях даних, отриманих у результаті проведення певних оцінок командою Red Team у 2017 році, представники сервісних груп зазначили три основні фактори захисту: люди, політики та технології. Якби організація використовувала виключно технології для усунення вразливостей, їй вдалося б вирішити лише 26% проблем, які були виявлені в ході моделювання атак командою Red Team. У результаті 74% проблем залишаються невирішеними (див. Рисунок 53). Аналогічним чином, якщо організації використовують лише політики для вирішення питань безпеки, вони зможуть вирішити лише 10% проблем, а з підготовкою користувачів – 4% проблем. Необхідно одночасно охопити всі три сфери захисту.

Рисунок 53 Лише 26% проблем у сфері безпеки можуть бути вирішені завдяки самим продуктам



Джерело: дослідження Cisco щодо безпеки

На Рисунку 54 наведено приклади проблем, які були виявлені за категорією під час моделювання. Деякі проблеми, такі як слабкі паролі, трапляються в усіх трьох категоріях. Зміцнення паролів може потребувати покращання в таких категоріях, як люди (підготовка користувачів), продукти (конфігурація серверів для більш складних паролів) та політики (встановлення вимог щодо використання сильніших паролів).

Рисунок 54 Типи проблем, які були виявлені під час моделювання атак, розподілені за категоріями вимог щодо відновлення

Джерело: дослідження Cisco щодо безпеки

Організації можуть збільшити свої шанси на успішне управління всіма трьома факторами, якщо вони зможуть забезпечити інтеграцію безпеки на всіх рівнях, а не фрагментарну. Вони також повинні уникати практики покладатися виключно на продукти чи технічні вдосконалення для вирішення проблем безпеки. Для того щоб продукт був успішний, організації повинні розуміти та запроваджувати обґрунтовані політики та процеси у сфері технологій.

Очікування: інвестиції в технології та навчання

Спеціалісти з інформаційної безпеки в цілому очікують, що загрози, які постають перед їхніми організаціями, залишатимуться складними та створюватимуть проблеми. Вони очікують, що зловмисники розроблятимуть більш витончені та шкідливі шляхи зламу мереж. Їм також відомо про те, що сучасне робоче місце створює умови, які є сприятливими для зловмисників: мобільність працівників та застосування IoT-пристроїв надають нападникам нові можливості. Разом із все більшою кількістю загроз багато спеціалістів з інформаційної безпеки очікують, що вони стануть предметом додаткового ретельного вивчення з боку регуляторів, вищого керівництва, зацікавлених осіб, партнерів та клієнтів.

Для зменшення ймовірності виникнення ризиків і збитків захисники повинні визначити, куди саме інвестувати обмежені ресурси. Здебільшого спеціалісти з інформаційної безпеки стверджували, що бюджети на безпеку залишалися відносно стабільними, якщо до їх переосмислення не призводила істотна публічна атака та нові витрати на технології й процеси. 51 % опитаних стверджують, що витрати на безпеку ґрунтуються на бюджетах попередніх років, у той час як такий самий відсоток респондентів стверджують, що бюджет визначається залежно від очікуваних результатів (Рисунок 55). Більшість керівників служб інформаційної безпеки стверджують, що, на їхню думку, компанії витрачають належні ресурси на безпеку.

Рисунок 55 51% опитаних стверджують, що витрати на безпеку визначаються на основі бюджетів попередніх років

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Плануючи бюджет, більшість компаній систематично відпрацьовують списки побажань, які були розроблені в рамках комплексних планів безпеки, визначаючи пріоритетність інвестицій, як тільки з'являються ресурси. Інвестиції можуть бути переглянуті в разі виникнення нових вразливостей, як у результаті внутрішнього інциденту, публічної атаки, що набула широкого розголосу, так і в разі рутинної перевірки ризиків, пов'язаних з третіми особами.

Вбачається, що саме порушення систем безпеки і є найбільш важливими чинниками, які визначають майбутні інвестиції, а отже і вдосконалення технологій та процесів. Порівняно з 37 % у 2016 році, у 2017-му 41 % спеціалістів з інформаційної безпеки зазначають, що чинником порушень систем безпеки є зростання обсягу інвестицій у технології та рішення у сфері безпеки (Рисунок 56). 40 % опитаних наголосили, що порушення систем безпеки сприяють збільшенню інвестицій у навчання персоналу у сфері інформаційної безпеки порівняно з 37 % у 2016 році.

Рисунок 56 Порушення систем безпеки є чинником інвестицій у технології та навчання

2016 (1375), 2017 (1933)

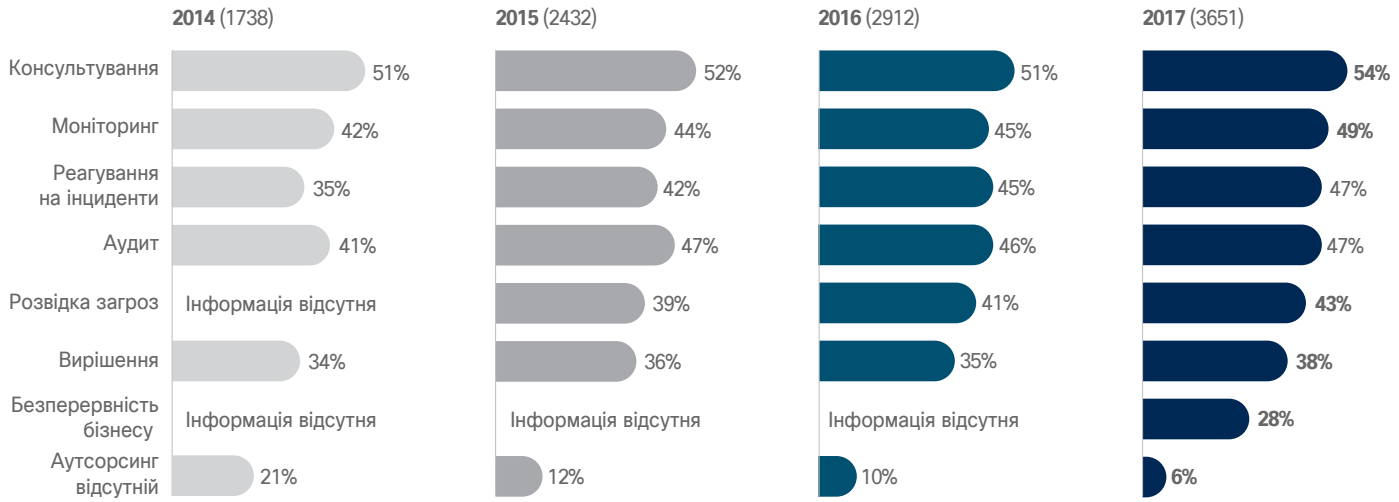
Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Спеціалісти з інформаційної безпеки очікують на збільшення витрат на засоби, в яких використовується штучний інтелект та машинне навчання, для покращання захисту та допомоги щодо перерозподілу робочого навантаження. Крім того, вони планують інвестиції в інструменти, які забезпечать захист критично важливих систем, а саме критичних інфраструктурних сервісів.

Для збільшення кількості ресурсів та зміцнення засобів безпеки організації починають покладатися на аутсорсинг. Серед спеціалістів з інформаційної безпеки 49% зазначили, що вони отримували послуги з моніторингу на умовах аутсорсингу у 2017 році порівняно із 44% у 2015-му; 47% віддавали на аутсорсинг питання реагування на інциденти у 2017 році порівняно із 42% у 2015-му (Рисунок 57).

Рисунок 57 Використання аутсорсингу для моніторингу та реагування на інциденти з роками зростає



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Більше інформації про результати Порівняльного дослідження рішень безпеки за 2018 рік, проведеного Cisco, див. додаток на **стор. 64.**

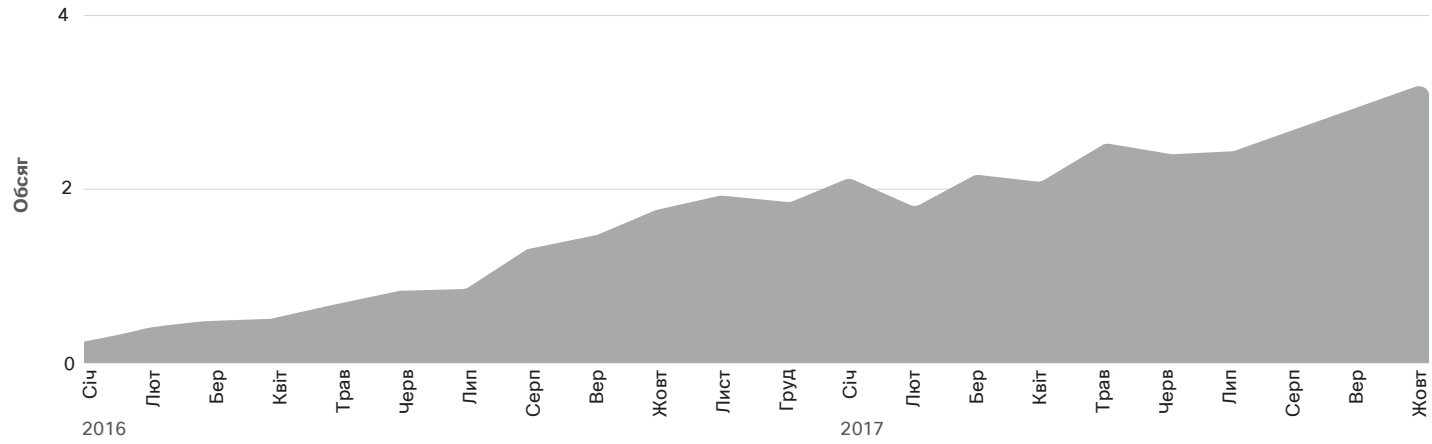
Висновок

Висновок

Зловмисники розуміються на тому, як уникати виявлення. Вони мають ефективні засоби, наприклад шифрування, та майстерні тактики на кшталт зловживання легітимним трафіком, щоб приховати свою діяльність та обійти традиційні технології захисту. І вони постійно розвивають свої тактичні прийоми, щоб їхнє шкідливе програмне забезпечення залишалося актуальним і дієвим. Кожна загроза, про яку відомо спільноті спеціалістів з безпеки, може потребувати багато часу для її виявлення.

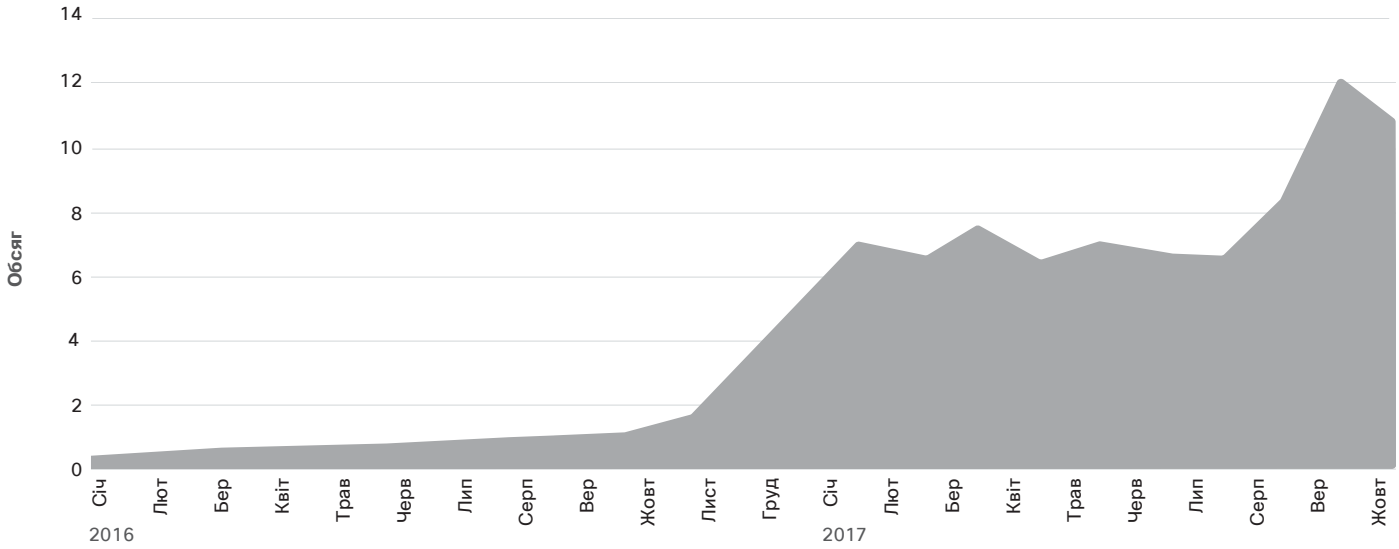
Одна причина, з якою захисники борються, щоб піднятися над хаосом війни з нападниками, – це лише обсяг потенційно небезпечного трафіку, з яким вони стикаються. Наше дослідження демонструє, що обсяг загальних подій, які були виявлені продуктами Cisco, що забезпечують безпеку кінцевих точок з використанням хмарних технологій, збільшився в чотири рази із січня 2016 року по жовтень 2017-го (див. Рисунок 58). «Загальні випадки» – це підрахунок усіх випадків, зловмисних або незловмисних, які були виявлені нашими продуктами, що забезпечують безпеку кінцевих точок на основі хмарних технології, за період спостереження.

Рисунок 58 Загальний обсяг подій



Джерело: дослідження Cisco щодо безпеки

Рисунок 59 Загальний обсяг шкідливого програмного забезпечення



Джерело: дослідження Cisco щодо безпеки

Наші продукти у сфері безпеки також відмітили 11-кратне збільшення загальних обсягів шкідливого програмного забезпечення протягом того ж самого періоду, як показано на Рисунку 59.

Тенденції щодо обсягів шкідливого програмного забезпечення мають вплив на час виявлення (TTD) захисниками. Це важливий показник для будь-якої організації, що хоче зрозуміти, наскільки добре працюють її засоби захисту під тиском постійного потоку атак з боку зловмисників.

Медіанне значення TTD Cisco близько 4,6 години протягом періоду з листопада 2016 року по жовтень 2017 року допомагає охарактеризувати невирішену проблему швидкого виявлення загроз у їхньому хаотичному ландшафті. Разом з тим це значно менше за 39-годинний середній показник TTD, про який ми повідомили в листопаді 2015 року після того, як уперше почали відстежувати значення TTD. Й також менше 14-годинного середнього значення, яке було вказане в Річному звіті Cisco з інформаційної безпеки за 2017 рік за період з листопада 2015-го по жовтень 2016 року.[20]

Використання хмарних технологій безпеки стало ключовим фактором, який допоміг Cisco просуватися вперед і утримувати середнє значення TTD на низькому рівні. Хмарні технології, що дозволять масштабувати та підтримувати продуктивність як щодо обсягу загальних випадків, так і шкідливого ПЗ, націленого на кінцеві точки, продовжують розвиватися. Локальні рішення з безпеки не зможуть запропонувати таку ж саму гнучкість. Розробка рішення такого масштабу, щоб справлятися з удесятеро більшим обсягом зловмисних атак протягом дворічного періоду та зберегти чи збільшити час реагування, є дуже складним і витратним завданням для будь-якої організації.

Cisco визначає «час на виявлення», або TTD, як часовий проміжок з моменту проникнення в систему до виявлення загрози. Ми визначаємо цей час з використанням узгодженої телеметрії безпеки, яка надходить від продуктів Cisco у сфері безпеки, що використовуються по всьому світу. Користуючись нашою глобальною присутністю та моделлю безперервної аналітики, ми здатні вимірювати показники з моменту завантаження шкідливого файлу на кінцевий пристрій до моменту його виявлення як загрози, яка не була класифікована на час виявлення.

«Середнє значення TTD» – це середнє значення щомісячних середніх величин за період спостереження.

20 *Річний звіт Cisco з інформаційної безпеки за 2017 рік:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

Про Cisco

Про Cisco

Компанія Cisco створює інтелектуальні системи кібербезпеки для реального світу. Наш портфель рішень є одним з найбільш комплексних в галузі, він захищає від широкого спектра загроз. Наш підхід до інформаційної безпеки, орієнтований на нейтралізацію загроз і відновлення працездатності, робить систему безпеки більш цілісною. Він забезпечує можливість детального моніторингу, постійного контролю і вдосконаленого захисту від загроз до, під час та після атаки.

Дослідники з екосистеми колективної аналітики інформаційної безпеки (Cisco Collective Security Intelligence, CSI) об'єднують «під одним дахом» найбільш повну в галузі аналітику загроз. Вони використовують для цього телеметричні дані від величезної кількості пристроїв та сенсорів, інформацію із загальнодоступних та приватних веб-каналів, а також від спільноти розробників відкритого ПЗ. Щоденний обсяг цієї інформації складають мільярди веб-запитів, мільйони повідомлень електронної пошти, зразків шкідливого ПЗ та даних про мережні вторгнення.

Ці дані обробляються в складній інфраструктурі, яка дозволяє аналітикам і самонавчальним системам відслідковувати загрози в різних мережах, центрах обробки даних, кінцевих і мобільних пристроях, віртуальних системах, на веб-сайтах, в електронній пошті та хмарних системах з метою визначення основних причин і масштабів поширення загроз. Підсумкові аналітичні дані перетворюються на засоби захисту в режимі реального часу для наших продуктів та сервісів, які одразу ж поширюються по всьому світу серед клієнтів Cisco.

Для отримання додаткової інформації про підхід Cisco до забезпечення безпеки відвідайте веб-сайт cisco.com/go/security.

УЧАСНИКИ ДОСЛІДЖЕННЯ ДЛЯ РІЧНОГО ЗВІТУ CISCO З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА 2018 РІК

Ми хотіли б подякувати нашій команді дослідників загроз та іншим експертам Cisco, а також нашім технологічним партнерам, які сприяли створенню **Річного звіту Cisco з інформаційної безпеки за 2018 рік.** *Їхні дослідження та здобутки допомогли Cisco надати спільноті спеціалістів, бізнесу та користувачам аналітичну інформацію про складність та масштабність сучасного глобального ландшафту кіберзагроз, а також представити передові практики для покращення їхнього захисту.*

Наші технологічні партнери також відіграють важливу роль. Вони допомагають нашій компанії розвивати прості автоматизовані засоби безпеки, які дозволяють організаціям захищати своє середовище.

Система захисту від зловмисного коду Cisco AMP для кінцевих пристроїв

Система Cisco Advanced Malware Protection (AMP) для кінцевих пристроїв надає можливості для автоматичного запобігання, виявлення та реагування в єдиному рішенні. Вона забезпечує постійний моніторинг та аналіз ознак зловмисної діяльності для розкриття загроз, які обходять первинні засоби безпеки і створюють найбільший ризик. В ньому використовуються різні методи виявлення, включаючи технологію «пісочниці», профілактику експлойтів, а також машинне навчання для швидкого виявлення та знешкодження загроз. Cisco AMP для кінцевих пристроїв – це єдине рішення, що забезпечує ретроспективну безпеку для швидкого реагування на загрози та виявлення обсягу, походження та способів локалізації загрози з тим, щоб організації залишалися захищеними.

Cisco Cloudlock

Cisco Cloudlock пропонує рішення брокера безпеки доступу до хмарного середовища (CASB). Це допомагає організаціям використовувати хмарні системи безпечним чином, забезпечує наочність і контроль користувачів, даних і програм для середовищ «програмне забезпечення, як послуга» (SaaS), «платформа, як послуга» (PaaS) та «інфраструктура, як послуга» (IaaS). Також компанія забезпечує аналіз кібербезпеки завдяки власному центру CyberLab, а також за принципом краудсорсингу.

Когнітивний аналіз загроз Cisco

Когнітивний аналіз загроз представляє собою хмарну службу, яка виявляє порушення безпеки, шкідливе ПЗ, що працює всередині захищених мереж, та інші загрози безпеки шляхом статистичного аналізу даних мережного трафіку. Служба бореться з прогалинами в захисті периметру, визначаючи симптоми зараження шкідливим ПЗ або витоку даних шляхом поведінкового аналізу і виявлення аномалій. Когнітивний аналіз загроз Cisco ґрунтується на розширених можливостях статистичного моделювання і машинного навчання, які допомагають незалежно знаходити нові загрози, визначати їх джерело і з часом пристосовуватися до них.

Підрозділ Cisco з реагування на інциденти в продуктах (PSIRT)

Product Security Incident Response Team (PSIRT) – це глобальна організація, яка відповідає за збір, розслідування та публічне оголошення інформації щодо вразливості в сфері безпеки та проблеми, пов'язані з продуктами і послугами Cisco. PSIRT отримує звіти стосовно безпеки продуктів або мереж від незалежних дослідників, галузевих організацій, постачальників, замовників та з інших джерел.

Підрозділ реагування на інциденти комп'ютерної безпеки (CSIRS)

Підрозділ Cisco з послуг реагування на інциденти комп'ютерної безпеки Security Incident Response Services (CSIRS) складається з кращих фахівців у цій сфері. Їх завданням є допомагати клієнтам Cisco до, під час і після інциденту. CSIRS використовує кращий персонал, корпоративні рішення безпеки, новітні методи реагування та досвід, накопичений за роки боротьби з зловмисниками, щоб гарантувати здатність наших клієнтів попереджати, а також швидко реагувати і усувати наслідки будь-яких атак.

Підрозділ з аналітики та досліджень Cisco Talos

Підрозділ Talos – одна з найбільших в світі груп з аналітики комерційних загроз. До його складу входять дослідники, аналітики та розробники світового класу. Talos користується найкращою телеметрією та складними системами для створення точної, миттєвої та дієвої аналітики щодо загроз для клієнтів, продуктів та сервісів Cisco. Група Talos захищає замовників Cisco від відомих та нових загроз, виявляє нові вразливості в спільному програмному забезпеченні та попереджує загрози на ранніх стадіях перед тим, як вони зможуть завдати значної шкоди в Інтернеті. Аналітичні дані Talos – це основа продуктів Cisco, які виявляють, аналізують та захищаються від відомих загроз та загроз, що з'являються. Talos дотримується офіційних правил Snort.org, ClamAV, SenderBase.org і SpamCop в доповнення до випуску багатьох дослідницьких та аналітичних інструментів з відкритим кодом.

Cisco Threat Grid

Cisco Threat Grid – це платформа для аналізу шкідливого програмного забезпечення та збирання аналітичних даних про загрози. Threat Grid виконує статичний та динамічний аналіз підозрілих зразків шкідливого програмного забезпечення, які вона отримує від користувачів та інтегрованих продуктів, що знаходяться в різних частинах світу. Сотні тисяч зразків у файлах різноманітних типів щодня передаються до хмарного сховища Threat Grid через інтерфейс користувача або API. Threat Grid може також розгортатися як локальна система.

Cisco Umbrella

Cisco Umbrella – це безпечний Інтернет-шлюз, який забезпечує першу лінію захисту від загроз в Інтернеті, незалежно від того, куди може зайти користувач. За рахунок інтеграції з фундаментальними структурами Інтернету Umbrella забезпечує повну прозорість дій в Мережі всіх користувачів на всіх пристроях в будь-якій точці, та блокує загрози ще до того, як вони проникнуть в мережу або на кінцеві пристрої. Шляхом аналізу та вивчення такої діяльності, Umbrella автоматично викриває інфраструктуру зловмисників і блокує запити на випередження – до встановлення з'єднання.

Дослідження і забезпечення безпеки (SR&O)

Група SR&O відповідає за управління загрозами і вразливостями усіх продуктів та служб Cisco, в тому числі Cisco PSIRT. SR&O допомагає замовникам вивчити мінливий ландшафт загроз на таких заходах, як Cisco Live та Black Hat, а також в процесі спільної роботи з колегами в Cisco і галузі в цілому. Крім того, SR&O розробляє нові служби, наприклад, спеціальну службу аналізу загроз (CTI) Cisco, що дозволяє визначити індикатори компрометації, які не були виявлені або оброблені поточними інфраструктурами безпеки.

Організація інформаційної безпеки та довіри

Організація інформаційної безпеки і довіри Cisco підкреслює прагнення Cisco вирішити дві найбільш критичні проблеми багатьох рад директорів і світових лідерів. Основні цілі організації – це захист публічних і приватних замовників Cisco, реалізація та підтримка безпечного життєвого циклу розробки для всього портфеля продуктів і послуг Cisco, а також захист від мінливих кіберзагроз. Cisco застосовує всебічний підхід до комплексного забезпечення інформаційної безпеки і довіри, який об'єднує людей, процеси, технології і політики. Формування системи інформаційної безпеки і довіри спрямоване на оптимізацію інформаційної безпеки, інжинірингу з урахуванням безпеки, захисту і конфіденційності даних, безпеки хмарного середовища, прозорості та перевірки, розширених функцій безпеки і управління. Більш детальну інформацію дивіться на веб-сайті trust.cisco.com.

Технологічні партнери *Річного звіту Cisco з інформаційної безпеки за 2018 рік*

ANOMALI®

Набір рішень для аналізу загроз Anomali дозволяє виявляти і досліджувати активні загрози кібербезпеки і реагувати на них. Визнана платформа аналізу загроз ThreatStream збирає і оптимізує мільйони індикаторів загроз, складаючи «чорний список». Anomali інтегрується з внутрішньою інфраструктурою для виявлення нових атак, аналізу даних за минулий рік для виявлення вже здійснених атак, а також дозволяє швидко розібратися в загрозах і локалізувати їх. Anomali пропонує безкоштовний інструмент STAXX для збору та обміну результатами аналізу загроз, а також надає безкоштовну готову до використання стрічку аналітики Anomali Limo. Для отримання додаткової інформації відвідайте веб-сайт anomali.com, а також стежте за нами в Twitter: @anomali.

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta надає критично важливі дані про ситуації з кіберзагрозами і дозволяє групам з безпеки і управління мережею виявляти загрози і запобігати вторгненням. Lumeta пропонує безпрецедентну можливість знаходити відомі, невідомі, тіньові і підставні елементи мережної інфраструктури, а також здійснювати моніторинг мережі та кінцевих пристроїв в режимі реального часу і аналізувати сегментацію елементів для динамічних мереж, кінцевих пристроїв, віртуальних машин і хмарної інфраструктури. Більш детальну інформацію дивіться на веб-сайті lumeta.com.

Qualys, Inc. (NASDAQ: QLYS) є піонером і провідним постачальником хмарних рішень у сфері безпеки та дотримання нормативних вимог, обслуговуючи понад 9 300 клієнтів більш, ніж в 100 країнах, більша частина яких входить в списки Forbes Global 100 та Fortune 100. Хмарна платформа Qualys та інтегрований набір рішень допомагає організаціям спростити процес забезпечення безпеки і знизити витрати на дотримання нормативних вимог, надаючи необхідний аналіз критично важливої інфраструктури безпеки та автоматизуючи усі операції аудиту, забезпечення відповідності та захисту для IT-систем і веб-програм. Створена у 1999 році компанія Qualys встановила стратегічні партнерські відносини з провідними постачальниками адміністративних послуг та консалтинговими організаціями по всьому світу. Більш детальну інформацію див. на веб-сайті qualys.com.

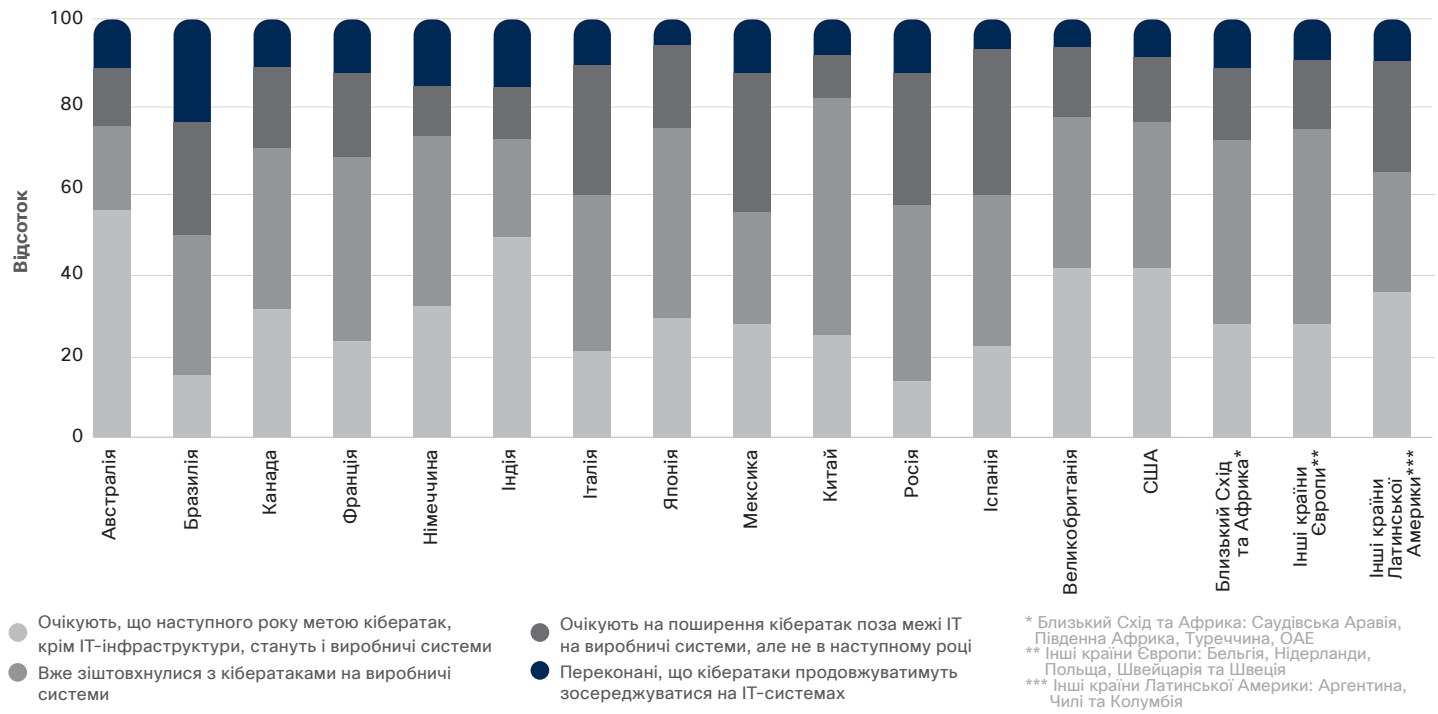
Radware (NASDAQ: RDWR) є глобальним лідером на ринку прикладних програм та рішень у сфері інформаційної безпеки для віртуальних, хмарних і програмно-визначених центрів обробки даних. Її визнаний нагородами портфель рішень захищає більше 10 000 компаній по всьому світу. Додаткові ресурси та інформацію можна переглянути в онлайн-центрі безпеки Radware, що пропонує комплексний аналіз інструментів DDoS-атак, тенденцій та загроз: security.radware.com.

Корпорація SAINT, лідер у сфері інтегрованих рішень управління вразливостями наступного покоління, допомагає компаніям і держустановам визначати та знижувати рівень вразливості до ризиків на всіх рівнях організації. Завдяки SAINT доступ, безпека і конфіденційність мирно співіснують і приносять користь усім зацікавленим сторонам. SAINT дозволяє клієнтам посилити засоби захисту інформаційної безпеки і при цьому знизити сукупні витрати на цю сферу. Більш детальну інформацію дивіться на веб-сайті saintcorporation.com.

TrapX Security пропонує автоматизовану захисну мережу для автоматичного маскування і захисту, що дозволяє припиняти загрози в режимі реального часу, одночасно маючи практичну цінність для аналітика, коли йдеться про блокування зловмисників. TrapX DeceptionGrid™ дозволяє компаніям виявляти, перехоплювати і аналізувати шкідливе ПЗ нульового дня, що використовується провідними глобальними групами, які здійснюють APT-атаки. Компанії використовують TrapX для посилення своїх IT-екосистем і зниження ризиків виникнення дорогих та руйнівних компрометацій, витоків даних і порушення нормативних вимог. Засоби захисту TrapX вбудовуються в саме серце мережі та критично важливої інфраструктури, без необхідності застосування агентів чи налаштування. Новітні методи виявлення шкідливого ПЗ, аналізу загроз і комп'ютерно-технічної експертизи в рамках єдиної платформи допомагають знижувати складність та рівень витрат. Більш детальну інформацію дивіться на веб-сайті trapx.com.

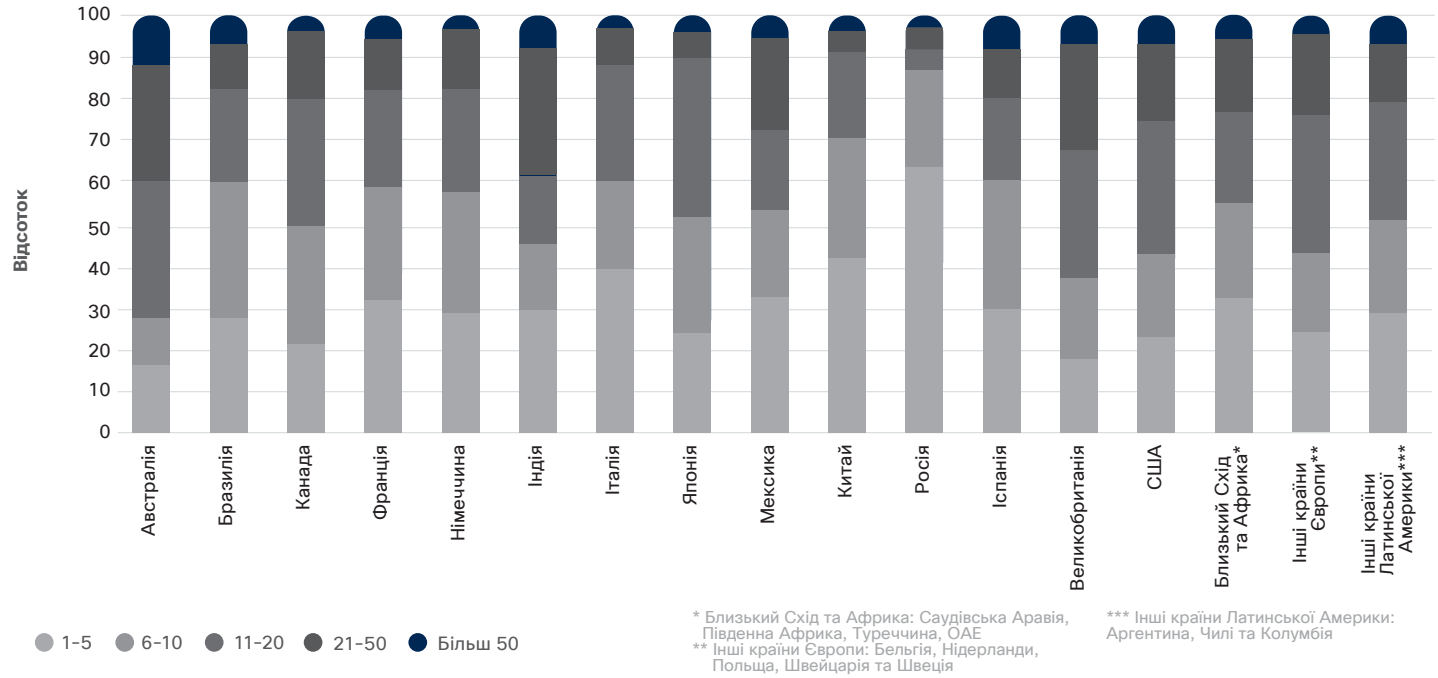
Додаток

Рисунок 60 Очікування щодо кібератак на виробничу та IT-інфраструктуру за країною або регіоном



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

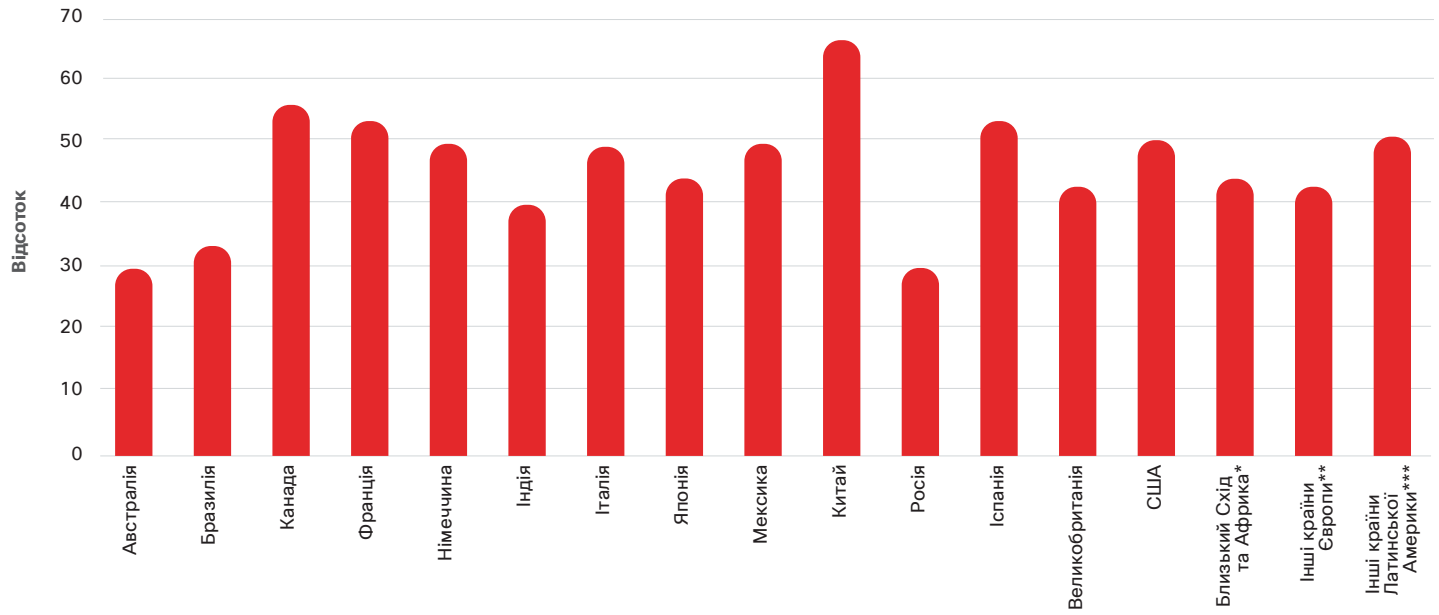
Рисунок 61 Кількість постачальників рішень з безпеки для інфраструктури за країною або регіоном



Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Рисунок 62 Відсоток оповіщень, які не були розслідувані, за країною або регіоном



* Близький Схід та Африка: Саудівська Аравія, Південна Африка, Туреччина, ОАЕ

** Інші країни Європи: Бельгія, Нідерланди, Польща, Швейцарія та Швеція

*** Інші країни Латинської Америки: Аргентина, Чилі та Колумбія

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Рисунок 63 Перешкоди на шляху впровадження передових процесів та технологій у сфері безпеки за країною або регіоном

Що з наступного ви вважаєте найбільшою перешкодою для запровадження передових процесів та технологій у сфері безпеки?

	Австралія	Бразилія	Канада	Франція	Німеччина	Індія	Італія	Японія	Мексика	Китай	Росія	Іспанія	Великобританія	США	Близький Схід та Африка*	Інші країни Європи**	Інші країни Латинської Америки***
Бюджеті обмеження	23%	35%	29%	33%	25%	36%	38%	31%	31%	38%	60%	33%	27%	34%	36%	37%	35%
Інші пріоритети	28%	11%	29%	27%	28%	26%	24%	27%	16%	27%	20%	18%	32%	32%	25%	18%	24%
Нестача підготовленого персоналу	25%	28%	19%	22%	24%	31%	24%	28%	30%	25%	35%	33%	31%	26%	25%	23%	26%
Відсутність знань про передові процеси та технології в сфері безпеки	26%	26%	24%	21%	22%	24%	21%	26%	23%	29%	18%	21%	27%	22%	22%	17%	21%
Питання сумісності із застарілими системами	27%	19%	30%	27%	30%	30%	22%	23%	32%	40%	25%	25%	24%	28%	30%	25%	28%
Вимоги щодо сертифікації	33%	27%	29%	29%	24%	27%	27%	22%	27%	23%	22%	27%	27%	30%	24%	33%	21%
Організаційна культура / ставлення до питань безпеки	30%	23%	25%	20%	16%	26%	17%	21%	26%	17%	19%	24%	28%	25%	20%	20%	27%
Небажання здійснювати покупку до перевірки на ринку	19%	20%	23%	26%	25%	29%	20%	28%	15%	16%	17%	20%	21%	22%	22%	21%	25%
Поточне робоче навантаження занадто високе для виконання нових обов'язків	22%	16%	28%	18%	28%	28%	26%	27%	23%	21%	15%	28%	22%	22%	20%	17%	19%
Організація не є цінною метою для атак	25%	18%	21%	22%	24%	17%	14%	20%	12%	16%	11%	13%	21%	21%	21%	20%	16%
Безпека не є пріоритетом для керівництва	22%	10%	17%	17%	20%	13%	13%	23%	15%	18%	11%	11%	19%	19%	17%	19%	21%

* Близький Схід та Африка: Саудівська Аравія, Південна Африка, Туреччина, ОАЕ

** Інші країни Європи: Бельгія, Нідерланди, Польща, Швейцарія та Швеція

*** Інші країни Латинської Америки: Аргентина, Чилі та Колумбія

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Рисунок 64 Закупівлі рішень для захисту від загроз за країною або регіоном

Що краще визначає, як саме ваша організація закуповує рішення в сфері безпеки для захисту від загроз?

Країна	Кількість	Зазвичай купуються найкращі в своєму класі продукти, які задовольняють специфічні потреби	Зазвичай купуються продукти, які добре працюватимуть разом
Австралія	203	86	14
Бразилія	197	72	28
Канада	185	67	33
Франція	191	59	41
Німеччина	195	69	31
Індія	199	78	22
Італія	201	71	29
Японія	223	72	28
Мексика	198	77	23
Китай	205	63	37
Росія	196	58	42
Іспанія	148	70	30
Великобританія	194	76	24
США	393	81	19
Близький Схід та Африка*	249	69	31
нші країни Європи**	199	73	27
Інші країни Латинської Америки***	196	71	29

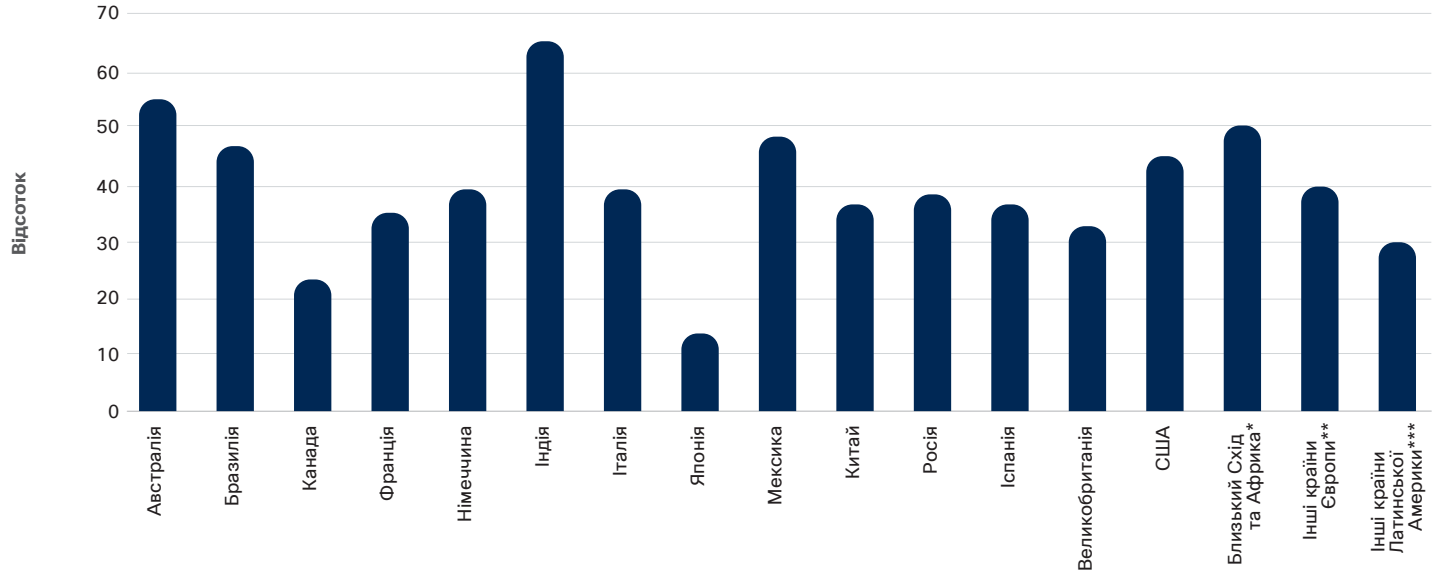
* Близький Схід та Африка: Саудівська Аравія, Південна Африка, Туреччина, ОАЕ

** Інші країни Європи: Бельгія, Нідерланди, Польща, Швейцарія та Швеція

*** Інші країни Латинської Америки: Аргентина, Чилі та Колумбія

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Рисунок 65 Відсоток організацій, які вважають, що дотримуються стандартних практик інформаційної безпеки (за країною або регіоном)



* Близький Схід та Африка: Саудівська Аравія, Південна Африка, Туреччина, ОАЕ

** Інші країни Європи: Бельгія, Нідерланди, Польща, Швейцарія та Швеція

*** Інші країни Латинської Америки: Аргентина, Чилі та Колумбія

Джерело: Порівняльне дослідження рішень безпеки за 2018 рік, проведене Cisco

Ви можете завантажити графіки за 2018 рік за посиланням: cisco.com/go/acr2018graphics

Завантаження графіків

Усі графіки у цьому звіті можна завантажити за адресою: cisco.com/go/mcr2018graphics.

Оновлення та виправлення

Оновлення та виправлення інформації, наведеної в цьому проекті, див. за адресою: cisco.com/go/errata.

Американський головний офіс
Cisco Systems, Inc.
Сан-Хосе, Каліфорнія

Центральне представництво
в Азіатсько-Тихоокеанському регіоні
Cisco Systems (USA) Pte. Ltd.
Сінгапур

Штаб-квартира в Європі
Cisco Systems International BV Амстердам,
Нідерланди

Компанія Cisco має більше 200 офісів по всьому світі. Адреси, номери телефонів та факсів вказано на веб-сайті Cisco за адресою: www.cisco.com/go/offices.

Опублікований в лютому 2018 року