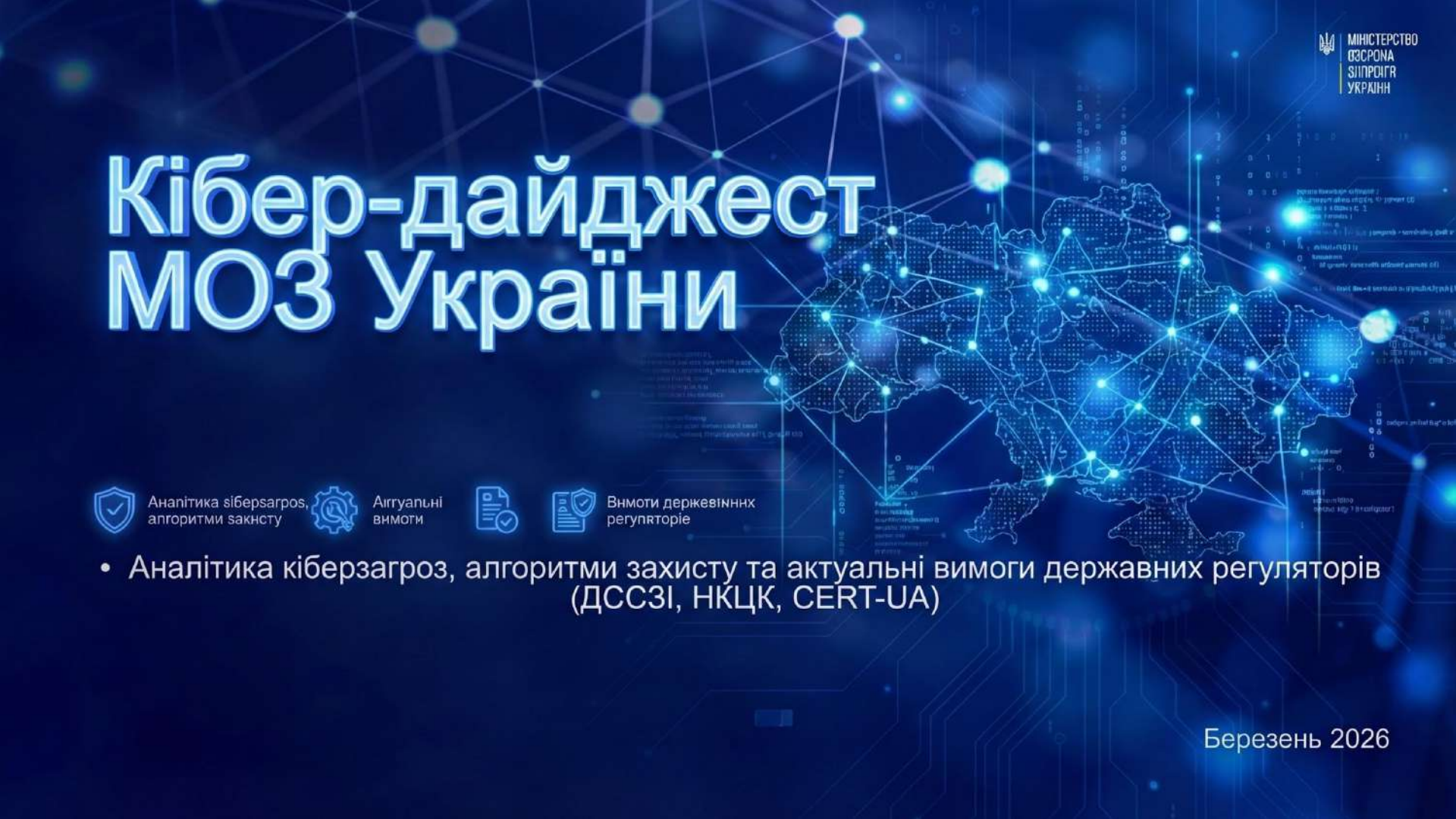

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
Кібер-дайджест МОЗ України
Аналітика кіберзагроз, алгоритми захисту
Актуальні вимоги
Вимоги державних регуляторів
• Аналітика кіберзагроз, алгоритми захисту та актуальні вимоги державних регуляторів (ДССЗІ, НКЦК, CERT-UA)
Березень 2026

Зміна парадигми — Від КСЗІ до Авторизації з безпеки та RMF (постанова КМУ № 712, наказ ДССЗІ № 75)

Суть оновлення Фахівці Держспецзв'язку надали офіційні роз'яснення щодо переходу до ризик-орієнтованого підходу (RMF). Відповідно до Постанови КМУ № 712, замість статичних атестатів КСЗІ впроваджується **Авторизація з безпеки**, яка базується на розробці профілів безпеки (базового, галузевого, цільового). Одночасно Наказом Адміністрації Держспецзв'язку № 75 затверджено новий Каталог заходів з кіберзахисту (на базі стандарту NIST CSF 2.0) та введено обов'язковий для всіх установ документ — **План кіберзахисту**.

Простими словами (Оцінка ризику) Раніше класична система КСЗІ була досить статичною: хоча дрібні поточні оновлення можна було зафіксувати у формулярі, будь-яка суттєва модернізація інфраструктури (докорінна зміна мережевої архітектури, перехід у хмару або масштабування системи) вимагала проходження нової довгої та дорогої експертизи. Тепер держава переходить на світовий стандарт — систему управління ризиками (RMF). Замість паперового «Атестата на 5 років» вводиться процес Авторизації. Це означає, що безпека стає безперервним процесом: ви можете гнучко оновлювати обладнання та впроваджувати нові технології, постійно моніторячи ризики, без необхідності щоразу отримувати новий дозвіл з нуля.

Рекомендовані напрями для опрацювання (Для керівників / Підрозділів захисту інформації та кіберзахисту)

1. **Практичний крок: Інвентаризація та формування Плану кіберзахисту**
   - **Пропозиція:** Розпочати системну підготовку до процедури Авторизації з безпеки.
   - **Дія:** Зіставити наявні атестати КСЗІ з планами модернізації IT-інфраструктури на рік. Паралельно розпочати заповнення уніфікованої форми Плану кіберзахисту (згідно з Наказом ДССЗІ № 75), здійснивши чесну самооцінку заходів захисту за 6 функціями (Управління, Ідентифікація, Забезпечення захисту, Виявлення, Реагування, Відновлення).
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Управління та Планування)**
   - **Пункт: GV.OC-02** (План з кіберзахисту) та **GV.RM-03** (Інтеграція управління ризиками).
   - **Обґрунтування:** Наявність затвердженого Плану кіберзахисту, що переглядається щорічно, є обов'язковим базовим заходом та головним фундаментом для проходження Авторизації з безпеки.
3. **Перехід до безперервного моніторингу (Стратегічний крок)**
   - **Пропозиція:** Налаштувати процеси IT-відділу так, щоб архітектурні зміни інфраструктури одразу синхронізувалися з безпековою документацією.
   - **Дія:** Усвідомити, що будь-яка модернізація системи відтепер вимагає оперативного оновлення цільового профілю безпеки та ініціації позапланової авторизації (протягом 6 місяців згідно з Постановою КМУ № 712).

Додаткові матеріали

- Офіційні роз'яснення ДССЗІ (Відео): Перехід від КСЗІ до RMF. Авторизація з безпеки
- Нормативна база: Постанова КМУ № 712 від 18.06.2025; Наказ Адміністрації Держспецзв'язку № 75.

Наслідки використання 1С, BAS та іншого з переліку забороненого ПЗ і обладнання — скасування Авторизації та штрафи

Суть оновлення Держспецзв'язку офіційно попереджає про відповідальність за використання забороненого програмного забезпечення та комунікаційного обладнання. Наразі на сайті Адміністрації Держспецзв'язку опубліковано перелік із 40 програмних продуктів, які напряму потрапили під санкції (згідно із Законом України «Про санкції» та рішеннями РНБО). Використання таких продуктів є порушенням закону. Виявлення їх під час перевірок призводить до негайного **скасування Авторизації з безпеки (або КСЗІ)** та складання адмінпротоколів. Крім того, у Верховній Раді вже розглядається законопроєкт щодо суттєвого посилення відповідальності за невиконання законних вимог у сфері кіберзахисту в цілому (штрафи до 100 мінімальних зарплат та можливе позбавлення волі).

Простими словами (Оцінка ризику) Використання бухгалтерських програм типу «1С», BAS або закупівля дешевих підсанкційних камер відеоспостереження — це більше не просто «небажана практика», а порушення закону. Ворожі спецслужби використовують це ПЗ для шпигунства та викрадення даних. Якщо інспектори ДССЗІ знайдуть російський софт у вашій мережі, систему буде офіційно визнано незахищеною. Якщо ПЗ не замінять у встановлений термін — керівник отримає штраф. Загалом, держава переводить усі порушення у сфері кіберзахисту (включно з відсутністю Авторизації) із суто технічної площини у жорстку юридичну та фінансову.

Рекомендовані напрями для опрацювання (Для керівників / IT-підрозділів та закупівельників)

1. **Практичний крок: Жорстка інвентаризація та міграція даних**
   - **Пропозиція:** Провести позаплановий аудит автоматизованих робочих місць бухгалтерських, кадрових та фінансових підрозділів.
   - **Дія:** За наявності забороненого ПЗ (1С, BAS, Парус тощо) — негайно ініціювати процес переходу на українські або міжнародні аналоги. Задокументувати план міграції у Плані кіберзахисту установи, щоб під час перевірки продемонструвати реальні кроки щодо усунення порушення..
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Технічний контроль ПЗ)**
   - **Пункт: PR.PS-05** (Заборона встановлення та виконання несанкціонованого програмного забезпечення) та **PR.PS-02** (Заміна та видалення ПЗ відповідно до ризиків).
   - **Обґрунтування:** Згідно з базовими заходами кіберзахисту, після організаційної відмови від підсанкційного ПЗ та його видалення, IT-підрозділам доцільно налаштувати технічні обмеження (наприклад, через групові політики безпеки). Це унеможливить випадкове встановлення заборонених програм звичайними користувачами в майбутньому і вбереже установу від штрафів.
3. **Контроль на етапі державних закупівель (Організаційний крок)**
   - **Пропозиція:** Інтегрувати обов'язкову перевірку на санкції в процес підготовки тендерної документації.
   - **Дія:** Зобов'язати фахівців із публічних закупівель ще на етапі маркетингових досліджень ретельно перевіряти походження апаратного забезпечення (камер, маршрутизаторів тощо). Якщо є сумніви щодо виробника обладнання — звертатися за офіційною консультацією до регіональних управлінь Держспецзв'язку.

Додаткові матеріали

- Офіційне роз'яснення: Скасування КСЗІ та адмінпротоколи: що чекає на держустанови за використання 1С та іншого підсанкційного ПЗ (Сайт Держспецзв'язку)

Безпека штучного інтелекту — нові рекомендації Адміністрації Держспецзв’язку (наказ № 154)

Суть оновлення Адміністрація Держспецзв’язку затвердила (Наказ від 23.02.2026 № 154) спеціалізовані рекомендації з кіберзахисту інформаційно-комунікаційних систем, що використовують технології штучного інтелекту (ШІ). Документ базується на передових міжнародних стандартах (ISO/IEC 42001, NIST AI 100-1) та деталізує новітні вектори атак: «отруєння» даних (внесення спотвореної інформації до вибірки), «промпт-ін’єкції» (маніпулятивні запити для витоку даних) та крадіжку ШІ-моделей.

Простими словами (Оцінка ризику) Елементи штучного інтелекту (наприклад, системи аналітики медичних чи статистичних даних, модулі розпізнавання зображень або навіть використання працівниками публічних нейромереж для складання документів) все частіше з'являються в роботі установ. Проте хакерам більше не обов'язково ламати сервери класичним шляхом. Вони можуть «обдурити» ШІ специфічними маніпулятивними запитами (промпт-ін'єкціями), змусивши його видати закриті бази даних, або ж непомітно «отруїти» масив даних, щоб система почала видавати хибні результати. ДССЗІ дає чіткий орієнтир, як захистити ці інновації та не перетворити їх на відкриті двері для витоку конфіденційної інформації.

Рекомендовані напрями для опрацювання (Для керівників / IT-підрозділів)

1. **Практичний крок: Контроль доступу та фільтрація даних для ШІ-модулів**
   - **Пропозиція:** Провести аудит використання інструментів ШІ в установі (включаючи аналітичні модулі в інформаційних системах).
   - **Дія:** Для будь-яких впроваджених ШІ-рішень необхідно обмежити обсяг даних, до яких алгоритм має доступ. Модель ШІ повинна працювати в ізольованому середовищі та не мати прямого неконтрольованого доступу до реєстрів із персональними даними чи медичною таємницею. Також необхідно налаштувати жорстку фільтрацію вхідних запитів.
2. **Відповідність нормативній базі (Інтеграція в План кіберзахисту)**
   - **Пункт:** Наказ ДССЗІ № 154 у зв'язці з **GV.RM-03** (Інтеграція управління ризиками кібербезпеки в загальні процеси).
   - **Обґрунтування:** Використання ШІ не повинно залишатися в зоні «тіньового IT». Згідно з новими рекомендаціями, якщо установа використовує такі технології, специфічні ризики (атаки на ланцюги постачання ШІ чи інверсія моделі) мають бути обов'язково проаналізовані та враховані під час щорічного оновлення Плану кіберзахисту.
3. **Безпека персоналу та захист від витоків (Організаційний крок)**
   - **Пропозиція:** Усунути ризики неконтрольованого використання ШІ-сервісів співробітниками.
   - **Дія:** Критично важливо провести інструктаж персоналу щодо суворої заборони завантаження робочих документів, персональних даних пацієнтів чи фінансової звітності у відкриті публічні ШІ-сервіси (ChatGPT, Claude тощо), адже це є прямим порушенням конфіденційності. Якщо установа планує навчати власні закриті моделі, слід використовувати методи «диференціальної конфіденційності» (математичний захист особистих даних).

Додаткові матеріали

- Офіційне роз'яснення: Держспецзв’язку затвердила рекомендації з кіберзахисту систем ШІ
- Нормативна база: Наказ Адміністрації Держспецзв’язку від 23.02.2026 № 154

Масштабний фішинг під виглядом оновлень «Delta» та держсистем (Угруповання UAC-0252)

Суть загрози Команда CERT-UA (що діє при Держспецзв'язку) зафіксувала нову хвилю цілеспрямованих кібератак. Ворожі хакери (ідентифікатор UAC-0252) масово розсилають електронні листи від імені центральних органів виконавчої влади та ОВА. У листах міститься вимога терміново «оновити» військові та цивільні системи (наприклад, систему «Delta»). Зловмисники використовують XSS-вразливості на легітимних сайтах та розміщують шкідливі файли (стілери SHADOWSNIFF, SALATSTEALER, бекдор DEAFTICK) на офіційному сервісі GitHub, щоб обійти засоби захисту.

Простими словами (Оцінка ризику) Ворог використовує потужний психологічний тиск та маскується під офіційні документи. Лист виглядає як справжній наказ із підписом та печаткою. Якщо ваш співробітник повірить і натисне на посилання «завантажити оновлення», на комп'ютер непомітно встановиться вірус-стілер. Його мета — миттєво викрасти збережені паролі, сесії браузерів та конфіденційні файли. Небезпека в тому, що віруси завантажуються з довіреного сервісу (GitHub), тому багато базових антивірусів просто не бачать загрози, вважаючи цей трафік безпечним.

Рекомендовані напрями для опрацювання (Для IT-підрозділів / Підрозділів захисту інформації)

1. **Практичний крок: Блокування IoC та налаштування політик AppLocker**
   - **Пропозиція:** Негайно оновити правила фільтрації на міжмережевих екранах та обмежити запуск скриптів.
   - **Дія:** На рівні корпоративного фаєрволу заблокувати домени та IP з алерта CERT-UA (наприклад, `nfkavn[.]bond`, `ua-gov[.]info`, `sa1at[.]ru`). Крім того, за допомогою групових політик (AppLocker/SRP) жорстко заборонити запуск виконуваних файлів із тек `%TMP%` та `%APPDATA%\Microsoft\Edge\Cache\`, оскільки саме туди вірус дропає свої модулі (маскуючи їх під `svchost.exe` чи `EdgeUpdate.exe`).
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Обізнаність та Моніторинг)**
   - **Пункт: PR.AT-01** (Систематичне проведення інструктажів з кібергігієни) та **DE.CM-09** (Постійний моніторинг використання комп'ютерного обладнання та ПЗ).
   - **Обґрунтування:** Жоден технічний захист не спрацює на 100%, якщо користувач сам запустить вірус «від імені адміністратора», як того вимагає фішинговий лист. Навчання персоналу критично оцінювати такі "накази" є обов'язковим базовим заходом кіберзахисту.
3. **Контроль системного реєстру (Додаткова порада фахівця)**
   - **Пропозиція:** Налаштувати автоматичний моніторинг змін у ключах автозавантаження операційної системи.
   - **Дія:** Стілери UAC-0252 закріплюються в системі через ключі реєстру гілки `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`. Рекомендується використовувати EDR-системи або утиліту Sysmon для відстеження та блокування створення підозрілих ключів (таких як `WindowsUpdateService` або `MicrosoftEdgeUpdateTask`), що ведуть на файли у тимчасових директоріях.

Додаткові матеріали

- Детальний аналіз та повний перелік індикаторів компрометації: Кібератаки UAC-0252 з використанням стілерів SHADOWSNIFF та SALATSTEALER (Сайт CERT-UA)

Подолання кадрового дефіциту — НКЦК ініціює підтримку жіночого лідерства у кібербезпеці

Суть оновлення Національний координаційний центр кібербезпеки (НКЦК) при РНБО України спільно з партнерами напрацьовує Національну дорожню карту розвитку жіночого лідерства в кібербезпеці на 2026–2030 роки. Головна мета ініціативи — подолання гострого дефіциту кадрів. Держава наголошує: активніше залучення жінок у кібербезпеку, впровадження політик рівності, розвиток менторства та популяризація професії — це не лише про міжнародні тренди, а насамперед про стратегічний ресурс для зміцнення національної стійкості в умовах війни.

Простими словами (Оцінка ризику) Брак кваліфікованих IT-фахівців та спеціалістів із захисту інформації — це реальність, з якою сьогодні стикається практично кожна установа. Держава підказує ефективний і сучасний вихід: розвиток внутрішнього кадрового потенціалу та руйнування стереотипів про "суто чоловічу" професію. Створення умов для навчання, менторської підтримки та кар'єрного зростання співробітниць у сфері кіберзахисту допоможе установам закрити критичні вакансії, сформувати стійкі команди та подивитися на розв'язання безпекових завдань під новим кутом.

Рекомендовані напрями для опрацювання (Для керівників / HR та IT-підрозділів)

1. **Практичний крок: Освітні ініціативи та підтримка (Організаційний захід)**
   - **Пропозиція:** Запровадити практики підтримки для співробітниць, які мають бажання розвиватися в IT та кібербезпеці.
   - **Дія:** Сприяти їхній участі у профільних тренінгах, тематичних воркшопах та спеціалізованих змаганнях (наприклад, CTF for Women, які вже успішно проводяться в Україні). Створення середовища взаємопідтримки та рольових моделей допоможе жінкам швидше адаптуватися до нових технічних чи аналітичних завдань.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Управління персоналом)**
   - **Пункт: GV.RR-04** (Включення питань кібербезпеки в практики управління персоналом) та **PR.AT-02** (Забезпечення навченості співробітників).
   - **Обґрунтування:** Наказ № 75 рекомендує системно підходити до навчання персоналу. Формування інклюзивних команд та заохочення жіночого лідерства — це чудовий та дуже дієвий інструмент для виконання цих організаційних вимог і посилення загальної спроможності установи.
3. **Подолання бар'єрів та залучення до управління ризиками (Порада фахівця)**
   - **Пропозиція:** Активніше залучати жінок-фахівчинь до прийняття рішень та роботи з безпековою документацією.
   - **Дія:** Робота над обов'язковим Планом кіберзахисту, проведення оцінки ризиків, аудит активів чи розробка політик доступу — це надзвичайно важливі напрями, які потребують високого рівня аналітики, уважності та системного підходу. Розширення участі жінок у цих процесах підвищить загальну якість управління безпекою в установі.

Додаткові матеріали

- Офіційні релізи: Посилення ролі жінок у кібербезпеці (Сайт РНБО України)

Мобільна кіберзброя «Coruna» — як російські хакери зламують iPhone українців через легітимні сайти

Суть оновлення Google Threat Intelligence та CISA розкрили деталі безпрецедентної атаки на користувачів Apple. Виявлено потужний експлойт-кіт **«Coruna»** (23 вразливості), який був викрадений у західних спецслужб та потрапив до рук російського угруповання UNC6353. У липні 2025 року росіяни вбудували невидимий фреймворк `Coruna` у легітимні українські вебсайти (промислові, роздрібні та місцеві сервіси). Атака націлена на пристрої з iOS від 13.0 до 17.2.1 і відбувається абсолютно непомітно для користувача (Zero-Click) через прихований `iframe`.

Простими словами (Оцінка ризику) Уявіть ситуацію: головний лікар або фінансовий директор відкриває звичайний український сайт новин чи каталог обладнання зі свого iPhone. Якщо телефон не оновлено до версії 17.3 або вище — пристрій повністю зламується за кілька секунд. Не треба нічого завантажувати чи вводити паролі. Вірус сам перевіряє модель телефону, обходить базовий захист Apple (пісочницю) і встановлює шпигунський модуль `PlasmaLoader`, який викрадає паролі, читає переписку та має доступ до файлів. Це вже не теоретична загроза — ця зброя активно використовувалась саме проти українського сегменту інтернету.

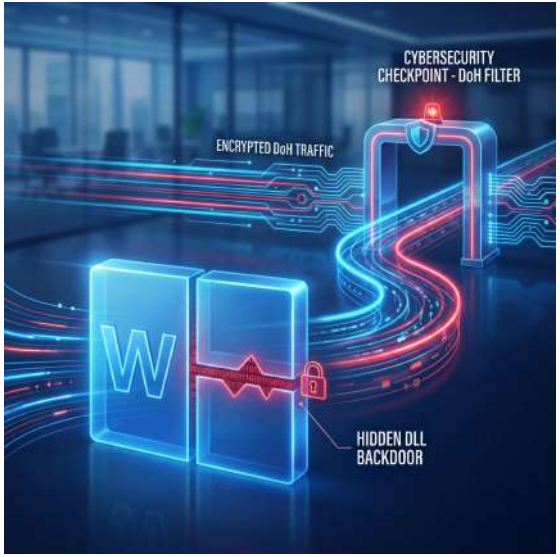
Рекомендовані напрями для опрацювання (Для керівників та IT-підрозділів)

1. **Практичний крок: Своєчасне оновлення та використання "Режиму блокування" (Lockdown Mode)**
   - **Пропозиція:** Захистити смартфони ключового персоналу.
   - **Дія: Рекомендується перевірити** версії iOS у керівного складу (має бути 17.3 або новіше). Аналітики підкреслюють найважливішу деталь: вірус «Coruna» фізично не здатен запуститися, якщо на iPhone увімкнено функцію Lockdown Mode (Режим блокування) або якщо використовується режим приватного перегляду (Incognito). **Доцільно ввімкнути** Lockdown Mode для всіх співробітників, які працюють із критичними даними установи.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Захист кінцевих точок)**
   - **Пункт: PR.PT-03** (Управління мобільними пристроями — MDM).
   - **Обґрунтування:** Використання особистих смартфонів для робочої переписки (BYOD) без централізованого контролю оновлень є критичною вразливістю. Установам **варто впроваджувати** політику, що обмежує доступ до корпоративної пошти та медичних систем з неоновлених мобільних пристроїв.
3. **Моніторинг власних вебресурсів (Додаткова порада фахівця)**
   - **Пропозиція:** Переконатися, що сайти вашої установи не стали розносниками цього вірусу.
   - **Дія:** Веб-адміністраторам **варто проаналізувати** код офіційних сайтів установи на наявність несанкціонованих прихованих `iframe` (зокрема розміром 0x0 пікселів) та звернень до підозрілих доменів (наприклад, `cdn.uacounter[.]com`).

Додаткові матеріали

- Огляд загрози: Coruna iOS Exploit Kit Uses 23 Exploits Across Five Chains Targeting iOS 13–17.2.1 (The Hacker News)

Ціль — медичні заклади. Як новий бекдор «Dohdoor» обходить антивіруси



Суть оновлення Аналітики Cisco Talos виявили нову кіберкампанію (угруповання UAT-10027), яка з грудня 2025 року цілеспрямовано атакує заклади охорони здоров'я (зокрема геріатричні центри) та освіти. Зловмисники використовують раніше невідомий бекдор **«Dohdoor»**. Його головна небезпека — унікальна скритність: для зв'язку з хакерами вірус використовує технологію DNS-over-HTTPS (DoH), ховаючи свій трафік за серверами Cloudflare, а для запуску в системі маскується під легітимні процеси Windows (метод DLL side-loading).

Простими словами (Оцінка ризику) Зловмисники чудово розуміють, що в лікарнях стоять антивіруси. Тому вони діють дуже хитро. По-перше, вірус не запускається сам — він змушує офіційну програму Windows (наприклад, `Fondue.exe`) підвантажити свій шкідливий файл. Антивірус бачить, що працює системна програма, і не блокує її. По-друге, щоб отримувати команди, вірус ховає свої запити в зашифрований трафік (DoH), який для корпоративного фаєрвола виглядає як звичайнісіньке, безпечне підключення до популярних сайтів. Це означає, що без спеціальних налаштувань адміністратори можуть місяцями не помічати присутності ворога в медичній мережі.

Практичний крок: Контроль DNS-трафіку та увага до системних процесів

1. **Практичний крок: Контроль DNS-трафіку та увага до системних процесів**
   - **Пропозиція:** Допомогти системам захисту "побачити" приховану загрозу.
   - **Дія:** IT-фахівцям **доцільно розглянути** можливість блокування протоколу DoH (DNS-over-HTTPS) на рівні корпоративних браузерів та мережевого екрана. Це змусить систему використовувати класичний DNS вашої установи, що дозволить адміністраторам бачити підозрілі запити. Також **рекомендуємо** налаштувати EDR-системи на моніторинг аномальної поведінки стандартних утиліт Windows (таких як `mblctr.exe` або `ScreenClippingHost.exe`).
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Моніторинг та Захист кінцевих точок)**
   - **Пункт: DE.CM-01** (Мережевий моніторинг для виявлення потенційних подій кібербезпеки).
   - **Обґрунтування:** Використання хакерами легітимних сервісів (таких як Cloudflare) для приховування своїх дій вимагає від IT-підрозділів глибшого аналізу трафіку. Установам **рекомендується** регулярно переглядати логі мережевої активності, щоб вчасно виявляти аномальні підключення.
3. **Кібергігієна як перша лінія оборони (Освітній захід)**
   - **Пропозиція:** Нагадати співробітникам про правила роботи з електронною поштою.
   - **Дія:** Оскільки такі складні атаки майже завжди починаються з фішингового листа (з вкладеним скриптом або архівом), **варто провести** коротке дружнє нагадування для медичного та адміністративного персоналу. Проста уважність при відкритті листів від невідомих відправників здатна зупинити атаку ще до того, як вона дійде до етапу обходу антивірусів.

Додаткові матеріали

- Огляд загрози: UAT-10027 Targets U.S. Education and Healthcare with Dohdoor Backdoor (The Hacker News)

Наш кібернаступ — як українське угруповання «Bearlyfy» паралізує російський бізнес

Суть оновлення На цифровому фронті є значні успіхи. За даними міжнародних звітів, проукраїнське кіберугруповання **Bearlyfy** (також відоме як Labubu) успішно атакувало понад 70 великих російських компаній. Наші кіберфахівці еволюціонували: якщо раніше вони використовували відомі віруси, то з березня 2026 року вони застосовують власну унікальну розробку — програму-вимагач **GenieLocker**. Мета цих операцій подвійна: фінансове виснаження ворога (викупи сягають сотень тисяч доларів) та масштабний саботаж їхньої IT-інфраструктури. Також зафіксовано співпрацю з іншими проукраїнськими групами, такими як PhantomCore та Head Mare.

Простими словами (Оцінка ризику) Це чудові новини, які доводять, що українські фахівці здатні завдавати ворогу нищівних ударів у кіберпросторі. Російський бізнес зараз зазнає мільйонних збитків. Але для наших IT-відділів це ще й безкоштовний майстер-клас. Аналітики зазначають, що українські хакери проникають у російські мережі через вразливості в зовнішніх сервісах (вебдодатках) та використовують легітимні програми для віддаленого доступу (наприклад, MeshAgent). Дивлячись на те, як "падає" ворожа інфраструктура, ми маємо переконатися, що наші власні системи захищені від подібних методів.

Практичний крок: Контроль DNS-трафіку та увага до системних процесів

1. **Практичний крок: Вчимося на помилках ворога (Аудит зовнішнього периметра)**
   - **Пропозиція:** Перевірити надійність сервісів, які "дивляться" в інтернет.
   - **Дія:** Оскільки українські хакери успішно ламають російські компанії через зовнішні вразливості, **рекомендуємо** нашим IT-фахівцям провести профілактичний огляд власних зовнішніх порталів та VPN-шлюзів. Також **корисно** переглянути, які програми для віддаленого адміністрування (TeamViewer, MeshAgent, AnyDesk) дозволені в мережі установи, та залишити лише мінімально необхідні.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Резервне копіювання)**
   - **Пункт: PR.IP-04** (Резервне копіювання інформації та перевірка відновлення).
   - **Обґрунтування:** Росіяни масово втрачають дані через атаки вірусом GenieLocker. Щоб убезпечити українські медичні та державні реєстри від дзеркальних атак ворога, установам **варто регулярно** перевіряти надійність своїх бекапів (вони мають зберігатися ізольовано від основної мережі).
3. **Психологічна стійкість (Освітній захід)**
   - **Пропозиція:** Підготувати персонал до можливих стресових ситуацій.
   - **Дія:** Звіт зазначає, що хакери чинять сильний психологічний тиск через записки з вимогами. **Буде доречно** проговорити з працівниками базовий алгоритм дій під час кіберінциденту: не панікувати, нічого не платити, відключити комп'ютер від мережі та одразу повідомити IT-відділ.

Додаткові матеріали

- Огляд успішних операцій: Bearlyfy Hits Russian Firms with Custom GenieLocker Ransomware (The Hacker News)

Увага, фішинг! Як російські спецслужби зламують Signal та WhatsApp посадовців

Суть оновлення ФБР та CISA випустили спільне термінове попередження: російські розвідслужби проводять масовану кампанію зі зламу акаунтів у популярних месенджерах (Signal, WhatsApp). Головна ціль — посадовці, військові, керівники установ та журналісти. Важливо розуміти: хакери не зламують шифрування самого месенджера. Вони використовують соціальну інженерію — надсилають повідомлення нібито від "Служби підтримки Signal" (Signal Support Bot) з вимогою терміново "підтвердити акаунт", перейшовши за посиланням або надіславши код підтвердження (PIN-код).

Простими словами (Оцінка ризику) Уявіть, що ви отримуєте повідомлення в Signal: "Ваш акаунт намагалися зламати з іншого пристрою. Терміново перейдіть за посиланням, щоб захистити дані, інакше акаунт буде видалено". Якщо в стані стресу ви перейдете за цим посиланням або введете свій PIN-код, зловмисники миттєво прив'яжуть ваш акаунт до свого пристрою. Після цього вони зможуть читати всі ваші робочі та особисті чати, а також розсилати віруси вашим колегам від вашого імені. На жаль, від такого зламу не врятує жоден антивірус, адже користувач сам "відчиняє двері".

Рекомендовані напрями для опрацювання (Для керівників та IT-підрозділів)

1. **Практичний крок: Налаштування приватності в месенджерах**
   - **Пропозиція:** Убезпечити акаунти ключових співробітників від несанкціонованого доступу.
   - **Дія: Рекомендуємо** всім співробітникам зайти в налаштування Signal/WhatsApp і перевірити розділ "Пов'язані пристрої" (Linked Devices). Якщо там є незнайомі комп'ютери — негайно видаліть їх. Також **дуже важливо** увімкнути PIN-код для реєстрації (Registration Lock) у Signal та налаштувати автоматичне зникнення повідомлень для робочих чатів.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Обізнаність персоналу)**
   - **Пункт: PR.AT-01** (Систематичне проведення інструктажів).
   - **Обґрунтування:** Людський фактор залишається найслабшою ланкою. Установам **доцільно** регулярно інформувати персонал про актуальні схеми фішингу. Важливо запам'ятати базове правило: офіційна підтримка Signal або WhatsApp **ніколи** не пише користувачам у самому месенджері з проханням надати коди чи перейти за посиланнями для "верифікації".
3. **Психологічна стійкість (Освітній захід)**
   - **Пропозиція:** Запобігти поширенню атаки всередині колективу.
   - **Дія:** Якщо ви отримали незвичне прохання (переказати гроші, терміново відкрити файл, проголосувати в конкурсі) від свого керівника чи колеги в месенджері, **найкраще правило** — зателефонувати цій людині звичайним зв'язком або перепитати особисто. Найчастіше хакери використовують уже зламані акаунти знайомих людей, щоб приспати вашу пильність.

Додаткові матеріали

- Офіційне попередження: Russian Intelligence Services Target Commercial Messaging Application Accounts (Сайт IC3/FBI)
- Аналітика кампанії: FBI Warns Russian Hackers Target Signal, WhatsApp in Mass Phishing Attacks (The Hacker News)

Шпигунство через браузер — як новий вірус «DRILLAPP» використовує Microsoft Edge

Суть оновлення Аналітики компанії S2 Grupo (LAB52) виявили нову цілеспрямовану кіберкампанію проти українських установ, за якою, ймовірно, стоїть російське угруповання Laundry Bear (UAC-0190). Зловмисники поширюють фішингові листи, замасковані під звіти державних органів, інструкції до Starlink або листи від благодійних фондів (наприклад, «Повернись живим»). Якщо користувач відкриває вкладення, у систему непомітно завантажується бекдор **«DRILLAPP»**. Його унікальність полягає в тому, що він використовує легітимний браузер Microsoft Edge у прихованому режимі розробника, щоб шпигувати за користувачем.

Простими словами (Оцінка ризику) Хакери знайшли дуже хитрий спосіб обійти антивіруси. Замість того, щоб встановлювати підозрілі шпигунські програми, вони змушують працювати на себе звичайний Microsoft Edge, який вже є на вашому комп'ютері. Вірус запускає браузер у "невидимому" фоновому режимі зі спеціальними налаштуваннями, які дозволяють йому без жодних запитів чи вікон увімкнути мікрофон, вебкамеру, робити знімки екрана та завантажувати файли. Оскільки Edge — це офіційна довірена програма Windows, система захисту не бачить у цьому загрози, і зловмисники можуть буквально слухати, що відбувається в кабінеті лікаря чи керівника.

Рекомендовані напрями для опрацювання (Для керівників та IT-підрозділів)

1. **Практичний крок: Налаштування безпеки браузерів та фільтрація файлів**
   - **Пропозиція:** Обмежити нетипове використання програм на робочих комп'ютерах.
   - **Дія:** IT-фахівцям **доцільно розглянути** можливість блокування (через групові політики GPO) запуску браузерів із параметрами розробника, такими як `--remote-debugging-port` або `--headless`, для звичайних користувачів. Також **рекомендуємо** налаштувати заборону на автоматичний запуск скриптів та виконуваних файлів (зокрема розширень `.lnk` та `.cpl`) із тимчасових папок завантажень.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Захист даних та кінцевих точок)**
   - **Пункт: PR.PT-01** (Управління конфігураціями кінцевих пристроїв).
   - **Обґрунтування:** Налаштування безпечних конфігурацій для стандартних програм (таких як веббраузери) є важливою частиною захисту інфраструктури. Правильно налаштований браузер просто не дозволить шкідливому коду отримати доступ до камери чи мікрофона без явної згоди користувача.
3. **Кібергігієна: обережність із чутливими темами (Освітній захід)**
   - **Пропозиція:** Попередити колег про нові хитрощі зловмисників.
   - **Дія:** Хакери цинічно використовують болючі та важливі для нас теми (допомога ЗСУ, офіційні звіти, налаштування Starlink), щоб змусити працівників втратити пильність. **Буде дуже корисно** нагадати команді, що всі подібні документи варто отримувати лише через перевірені офіційні канали зв'язку і ніколи не відкривати незрозумілі посилання чи ярлики з електронної пошти.

Додаткові матеріали

- Огляд загрози: DRILLAPP Backdoor Targets Ukraine (The Hacker News)
- Технічний аналіз: DRILLAPP: new backdoor targeting Ukrainian entities (LAB52)

Багаторівневе маскування — як російський вірус «MeowMeow» ховається в картинках з котиками

Суть оновлення Дослідники з ClearSky виявили нову кіберкампанію проти України, за якою стоїть російське угруповання APT28 (Fancy Bear). Атака починається з електронного листа (часто з домену `ukr.net`), який містить посилання на архів із фальшивим урядовим документом щодо "правил перетину кордону". Разом із документом на комп'ютер непомітно завантажується завантажувач **«BadPaw»**, який згодом встановлює повноцінний бекдор **«MeowMeow»**.

Простими словами (Оцінка ризику) Ця атака вражає своєю продуманістю. Щоб обійти антивіруси, хакери заховали основний шкідливий код... у звичайнісінькому файлі картинки (технологія стеганографії). Більше того, якщо фахівець із безпеки знайде цей вірус і спробує запустити його для перевірки (в ізольованому середовищі), вірус "зрозуміє", що за ним стежать. Замість того щоб розгорнути шпигунську діяльність, програма просто покаже картинку котика та виведе жартівливе повідомлення «Meow Meow Meow». Вірус активується лише на комп'ютерах реальних жертв, надаючи хакерам повний віддалений доступ до файлів і можливість запускати будь-які команди.

Рекомендовані напрями для опрацювання (Для керівників та IT-підрозділів)

1. **Практичний крок: Протидія складним вкладенням (Налаштування пошти)**
   - **Пропозиція:** Ускладнити хакерам доставку вірусів через електронну пошту.
   - **Дія:** IT-фахівцям **доцільно розглянути** посилення фільтрації вхідної пошти. Варто налаштувати блокування або суворий карантин для листів, які містять архіви з нетиповими виконуваними скриптами (наприклад, `.hta` або `.vbs` файли). Саме такі формати найчастіше використовуються для старту подібних багаторівневих атак.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Захист від шкідливого ПЗ)**
   - **Пункт: PR.PT-02** (Запровадження механізмів захисту від шкідливого коду).
   - **Обґрунтування:** Оскільки новітні віруси (як BadPaw) вміють розпізнавати "пісочниці" та ховатися від базових антивірусів, установам **рекомендується** переходити на використання сучасних систем класу EDR (Endpoint Detection and Response), які аналізують поведінку програм у реальному часі, а не лише шукають відомі сигнатури.
3. **Критичне мислення під час читання листів (Освітній захід)**
   - **Пропозиція:** Попередити колег про нові хитрощі зловмисників.
   - **Дія:** Хакери цинічно використовують болючі та важливі для нас теми (допомога ЗСУ, офіційні звіти, налаштування Starlink), щоб змусити працівників втратити пильність. **Буде дуже корисно** нагадати команді, що всі подібні документи варто отримувати лише через перевірені офіційні канали зв'язку і ніколи не відкривати незрозумілі посилання чи ярлики з електронної пошти.

Додаткові матеріали

- Огляд кампанії: APT28-Linked Campaign Deploys BadPaw Loader and MeowMeow Backdoor in Ukraine (The Hacker News)
- Звіт аналітиків: Exposing a Russian Campaign Targeting Ukraine (ClearSky Security)

Глобальна аналітика — чому хакери посилюють атаки на лікарні та змінюють тактику шантажу

Суть оновлення Аналітична компанія Chainalysis випустила звіт щодо активності вірусів-вимагачів (Ransomware) за 2025–2026 роки. Дані показують парадоксальну тенденцію: загальна сума викупів, які отримали хакери, впала на 8%, але кількість самих атак зросла на рекордні 50%. Зловмисники змінюють стратегію. Замість складних атак на корпорації-гіганти, вони масово атакують середній бізнес та заклади охорони здоров'я. Наприклад, один зі зламів медичної компанії DaVita призвів до витоку 2,7 млн карток пацієнтів. При цьому середній розмір викупу від тих, хто все ж таки платить, зріс майже в 4 рази (до ~$60 000).

Простими словами (Оцінка ризику) Чому кількість атак зростає, а прибутки хакерів падають? Тому що у світі все більше організацій принципово відмовляються платити викуп завдяки наявності якісних резервних копій. Через це кіберзлочинці починають діяти агресивніше. Вони зміщують фокус на заклади охорони здоров'я та державні установи, оскільки такі організації просто не можуть дозволити собі тривалий простій інформаційних систем. Блокування доступу до електронних реєстрів чи обладнання критично паралізує їхню роботу, що, на думку хакерів, змусить керівництво швидше піти на поступки. Більше того, хакери не просто шифрують файли — вони вивчають вкрадені бази даних та можуть погрожувати оприлюдненням чутливої інформації (наприклад, персональних чи медичних даних), щоб створити додатковий психологічний тиск.

Рекомендовані напрями для опрацювання (Для керівників та IT-підрозділів)

1. **Практичний крок: Надійні бекапи та шифрування чутливих даних (Анти-шантаж)**
   - **Пропозиція:** Забезпечити безперебійність роботи та мінімізувати наслідки витоку інформації.
   - **Дія:** По-перше, **критично важливо** мати ізольовані (офлайн) або незмінні (immutable) резервні копії, до яких вірус фізично чи логічно не зможе дістатися з основної мережі — саме це дозволить швидко відновити роботу установи без сплати викупу. По-друге, оскільки хакери погрожують публікацією вкраденого, **рекомендуємо** переконатися, що найбільш чутливі бази даних зберігаються у зашифрованому вигляді. Тоді навіть у разі витоку ці файли залишаться нечитабельними для ворога.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Реагування на інциденти)**
   - **Пункт: RS.CO-02** (Інформування про інциденти та взаємодія із зацікавленими сторонами).
   - **Обґрунтування:** Якщо зловмисники почнуть писати вашим пацієнтам чи лікарям у месенджери з погрозами, це може викликати паніку. Установі **доцільно** мати заздалегідь підготовлений план кризових комунікацій: як швидко заспокоїти персонал та куди звертатися за допомогою (наприклад, до урядової команди CERT-UA).
3. **Обережність із зовнішніми підрядниками (Додаткова порада фахівця)**
   - **Пропозиція:** Перевірити так званий «ланцюг постачання» послуг.
   - **Дія:** У звіті зазначається, що хакери масово купують готові доступи до мереж у «брокерів». Дуже часто ці доступи отримуються через зламаних IT-підрядників (тих, хто віддалено обслуговує ваші MIC, сервери чи бухгалтерське ПЗ). **Варто** провести дружній аудит акаунтів, якими користуються ваші партнери для віддаленого підключення, та обов'язково увімкнути для них двофакторну автентифікацію (2FA).

Додаткові матеріали

- Глобальний звіт: Total Ransomware Payments Stagnate for Second Consecutive Year, While Attacks Escalate (Chainalysis)

Інструментарій захисника — вийшов Kali Linux 2026.1 з новими засобами для аудиту безпеки

Суть оновлення Компанія Offensive Security випустила оновлену версію найпопулярнішої операційної системи для аудиту кібербезпеки — **Kali Linux 2026.1**. Окрім нового дизайну та ювілейного режиму "BackTrack", система отримала 8 нових професійних інструментів. Серед них — `Atomic-Operator` для тестування систем захисту (емуляція атак Red Team), `SSTImap` для пошуку вразливостей у вебдодатках та `WPProbe` для швидкого сканування WordPress-сайтів на наявність дірок у плагінах.

Простими словами (Оцінка ризику) Kali Linux — це класичний інструмент хакерів, але водночас це і головний інструмент адміністраторів та фахівців із кібербезпеки, які прагнуть перевірити власну мережу *до того*, як туди прийдуть справжні злочинці. Новий реліз дає в руки профільним підрозділам потужні засоби, щоб просканувати офіційні сайти установи на вразливості, перевірити стійкість Wi-Fi мереж та протестувати, чи дійсно встановлені в організації засоби захисту здатні заблокувати сучасні атаки.

Рекомендовані напрями для опрацювання (Для IT-підрозділів та Підрозділів захисту інформації і кіберзахисту)

1. **Практичний крок: Самоаудит вебсайтів установи**
   - **Пропозиція:** Перевірити стійкість офіційних веб-ресурсів за допомогою нових утиліт.
   - **Дія:** Фахівцям **рекомендується** завантажити новий реліз Kali та використати спеціалізовані інструменти (наприклад, `WPProbe` або `XSStrike`) для безпечного сканування публічних ресурсів установи. Це дозволить виявити та закрити вразливості до того, як їх знайдуть ворожі сканери.
2. **Відповідність вимогам Наказу ДССЗІ № 75 (Оцінка безпеки)**
   - **Пункт: PR.IP-10** (Регулярне тестування та оцінка планів реагування) та **ID.RA-01** (Оцінка вразливостей активів).
   - **Обґрунтування:** Нормативна база ДССЗІ прямо вимагає від установ (особливо від об'єктів критичної інфраструктури — ОКІ) регулярно перевіряти свої системи на наявність вразливостей. Використання професійних дистрибутивів на зразок Kali Linux стандартизує процес внутрішнього аудиту та допомагає виконати ці обов'язкові вимоги.
3. **Перевірка систем виявлення (Емуляція атак)**
   - **Пропозиція:** Переконатися, що системи моніторингу працюють коректно.
   - **Дія:** Новий інструмент `Atomic-Operator` дозволяє безпековим командам безпечно імітувати дії реальних хакерів у власній мережі (наприклад, спробу несанкціонованого вивантаження бази даних). Це ідеальний спосіб перевірити, чи спрацюють сповіщення на дашбордах вашого корпоративного антивірусу або системи EDR.

Додаткові матеріали

- Офіційний реліз:Kali Linux 2026.1 Release (Offensive Security)