Державна служба спеціального зв'язку
та захисту інформації України

TLP:CLEAR

Кібер-загрози: Україна

Аналітика за І півріччя 2026

Зміст

Передмова

CERT-UA

Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози

Кібероперації давно перестали бути допоміжним інструментом війни й перетворилися на самостійний напрям, через який противник досягає розвідувальних, інформаційних та операційних цілей. Визначальною рисою останнього часу стало здешевлення й прискорення підготовки атак – застосування штучного інтелекту, загальнодоступного коду та легітимних сервісів знижує поріг входу й дозволяє швидко масштабувати та видозмінювати кампанії.

Тактики акторів та кластерів кіберзагроз не стоять на місці – вони безперервно оновлюються й ускладнюються. Зловмисники випробовують нові підходи, поєднують технічні засоби із соціальною інженерією та за потреби повертаються до раніше дієвих сценаріїв. Саме тому спроможність держави вчасно виявляти, аналізувати й ефективно реагувати на кіберзагрози є критично важливою для національної безпеки.

Цей звіт підсумовує спостереження CERT-UA за кіберінцидентами першого півріччя 2026 року. У ньому окреслено ключові напрями розвитку загроз, розглянуто діяльність окремих кластерів і докладно розібрано тактики, техніки та процедури, до яких вдавалися зловмисники протягом періоду.

Окрема вдячність усім причетним до захисту українського кіберпростору – саме їхня злагоджена робота дозволяє вчасно розпізнавати загрози, протидіяти противнику й нарощувати стійкість наших систем.

Висновки та інсайти

Інсайти

ШІ по всьому ланцюжку атаки

У попередніх звітах уже відзначалося застосування штучного інтелекту для написання фішингових повідомлень і створення окремих компонентів шкідливих програм. У першому півріччі 2026 року ця тенденція набула системного характеру: ознаки використання ШІ виявлялися на різних етапах – від тексту листа й дизайну вебсторінки до скриптів, завантажувачів та окремих функцій ШПЗ.

Зловмисникам більше не потрібно витрачати значний час на ручне створення кожного повідомлення чи сторінки: один сценарій швидко адаптується під іншу установу, професію, регіон або інформаційний привід, так само як і код програми чи спосіб її запуску. Результат не завжди технічно складний, проте навіть недосконалий код буває достатнім для одноразового зараження чи викрадення даних. Водночас грамотний текст, коментарі в коді чи характерна структура файлів самі по собі не є доказом застосування ШІ й не можуть бути підставою для атрибуції – їх слід розглядати лише в сукупності з іншими результатами технічного аналізу.

Легітимне як прикриття

Зловмисники системно вбудовували легітимні публічні сервіси у свої операції. Файлові сховища й GitHub слугували для розповсюдження шкідливих файлів, Telegram – для передавання викрадених даних, сервіси тунелювання (зокрема ngrok, Cloudflare) – для приховування мережевої активності, а легітимні програми віддаленого адміністрування – для отримання доступу до систем.

Окремим напрямом стало використання вразливих і зламаних легітимних ресурсів: сайти з вразливістю до міжсайтового скриптингу (XSS) та скомпрометовані вебресурси перетворювалися на точки прихованої доставки шкідливого коду. Такий трафік складно відрізнити від звичайної активності користувачів, а суцільне блокування відповідних платформ здебільшого неможливе, – тому сам факт звернення до відомого сервісу не є ознакою безпечності.

Висновки

Ключовою рисою першого півріччя 2026 року стало співіснування двох рівнів кіберзагроз: масового й технічно простого – та високотехнологічного, за яким стоять держави.

З одного боку – технічно нескладні, але масові й швидкі кампанії, що спираються на загальнодоступний інструментарій, легітимні сервіси та штучний інтелект. З іншого – операції ресурсних, спонсорованих державами угруповань, здатних швидко озброюватися новими вразливостями та проводити цілеспрямовані й деструктивні атаки. Ці рівні різняться за складністю, проте обидва демонстрували зростання, тому ефективний захист має враховувати їх одночасно.

Оскільки штучний інтелект і загальнодоступні інструменти спрощують підготовку та проведення кібератак, технічний поріг входу для зловмисників знижується. Як наслідок, збільшується кількість кіберзагроз та загальний масштаб активності в кіберпросторі.

Тенденції

У І півріччі 2026 року зафіксовано 3 137 кіберінцидентів. Це приблизно на 8% більше, ніж у другому півріччі 2025 року.

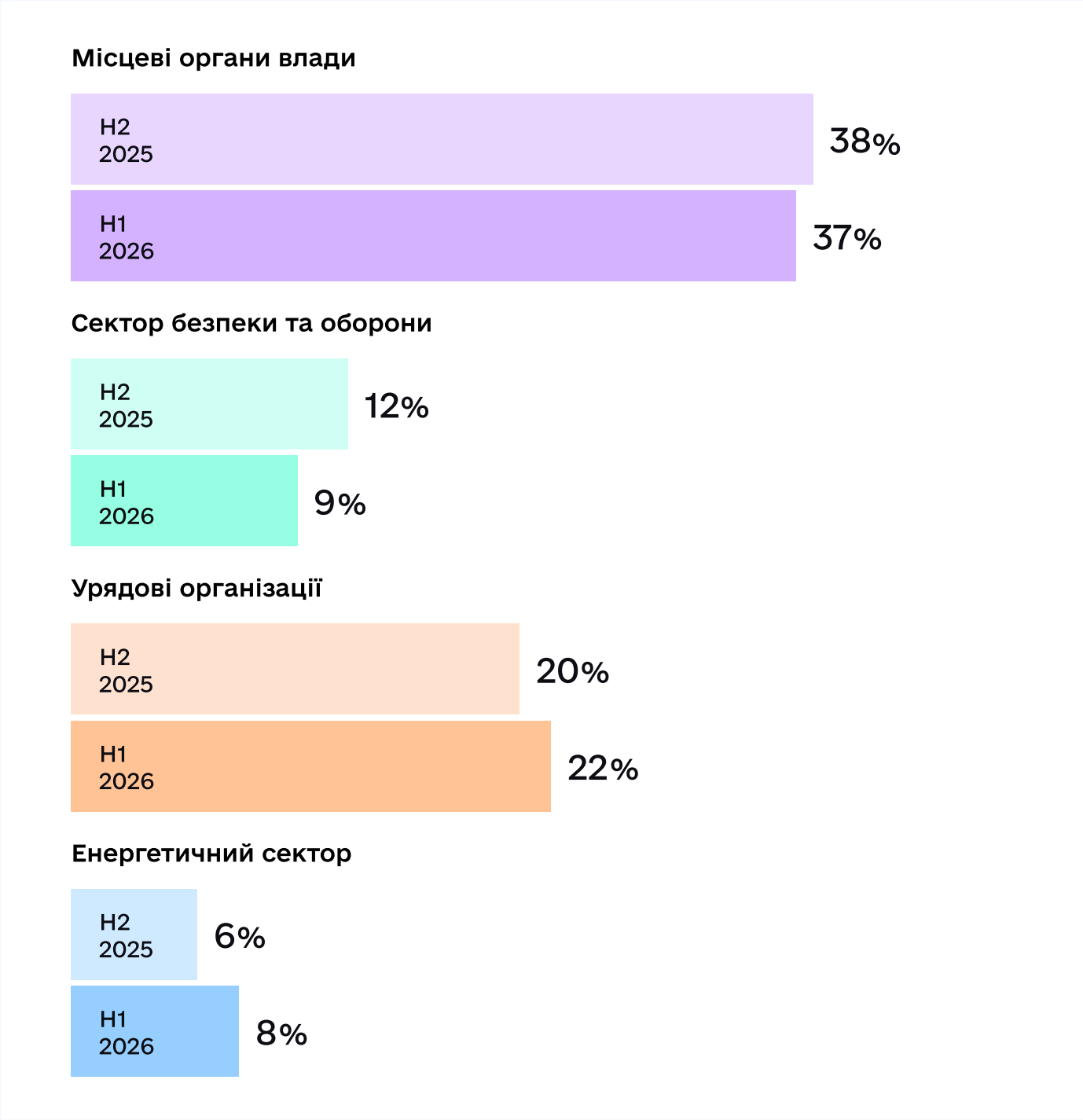
Рівень критичності	H2 2025	H1 2026	Зміна за період
Критичний	0	1	-
Високий	5	4	-20%
Середній	2895	2898	+0,1%
Низький	9	234	+2500%
Загалом	**2 909**	**3 137**	**+8%**

Наведена у звіті статистика відображає кіберінциденти, зафіксовані та опрацьовані CERT-UA. Вона не є вичерпною оцінкою всіх кібератак, здійснених проти українських організацій і користувачів упродовж звітного періоду.

Частина організацій має власні команди реагування та самостійно опрацьовує кіберінциденти без залучення CERT-UA. Насамперед це стосується окремих органів сектору безпеки і оборони, у яких функціонують відомчі підрозділи кіберзахисту.

Тому менша частка певного сектору у статистиці CERT-UA не свідчить про нижчу інтенсивність атак або менший інтерес з боку противника. Вона також може бути наслідком більшої спроможності відповідних організацій самостійно виявляти, локалізовувати та досліджувати кіберінциденти.

Водночас зростання кількості зафіксованих кіберінцидентів не слід автоматично трактувати як пропорційне збільшення кількості успішних кібератак. На статистику також впливають видимість загроз, обмін інформацією та спроможність засобів захисту виявляти окремі етапи атаки.



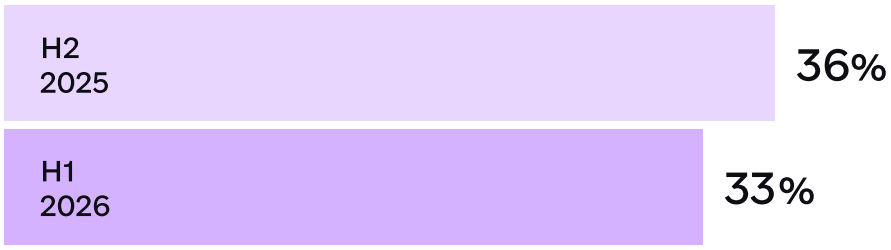
Протягом звітного періоду відбувся перехід на нову Національну таксономію кіберінцидентів. [1]

Для формування цілісної статистики старі типи було приведено до найближчих за змістом типів нової таксономії.

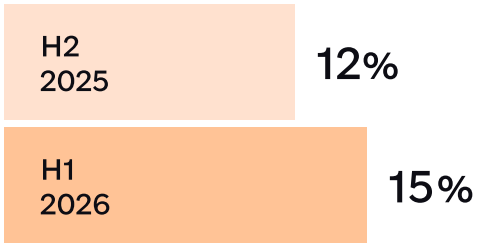
[1] Затверджено Наказом Адміністрації Держспецзв'язку від 18.02.2026 № 143 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози»

https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-18-02-2026-143-deyaki-pitannya-reaguvannya-na-kiberincidenti-kiberataki-ta-kiberzagrozi

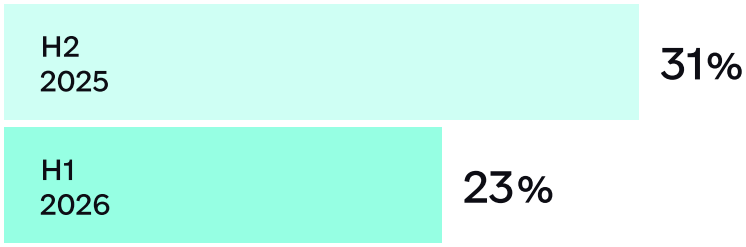
02.02 Розповсюдження ШПЗ (Malware distribution)



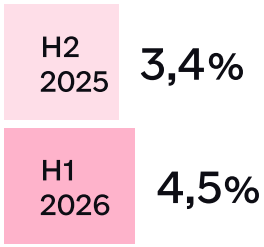
02.01 Зараження ШПЗ (Malware infection)



03.03 Соціальна інженерія (Social engineering)



Компрометація систем і деструктивне втручання



Разом ці чотири типи становлять майже 84% усіх зафіксованих кіберінцидентів.

Такий розподіл підтверджує, що основними початковими векторами залишаються повідомлення зі шкідливим вмістом, соціальна інженерія та викрадення облікових даних.

При цьому значна кількість випадків розповсюдження ШПЗ не означає таку саму кількість успішних заражень. Розсилка може бути заблокована поштовим сервісом, засобами захисту або самим користувачем.

HeatMap інтенсивності

Для наочного відображення розподілу кіберінцидентів за окремими кластерами кіберзагроз нижче наведено теплову карту інтенсивності (HeatMap).

Вона відображає загальну кількість кіберінцидентів, атрибутованих до відповідних кластерів, та дозволяє оцінити відносну активність різних угруповань у звітному періоді.

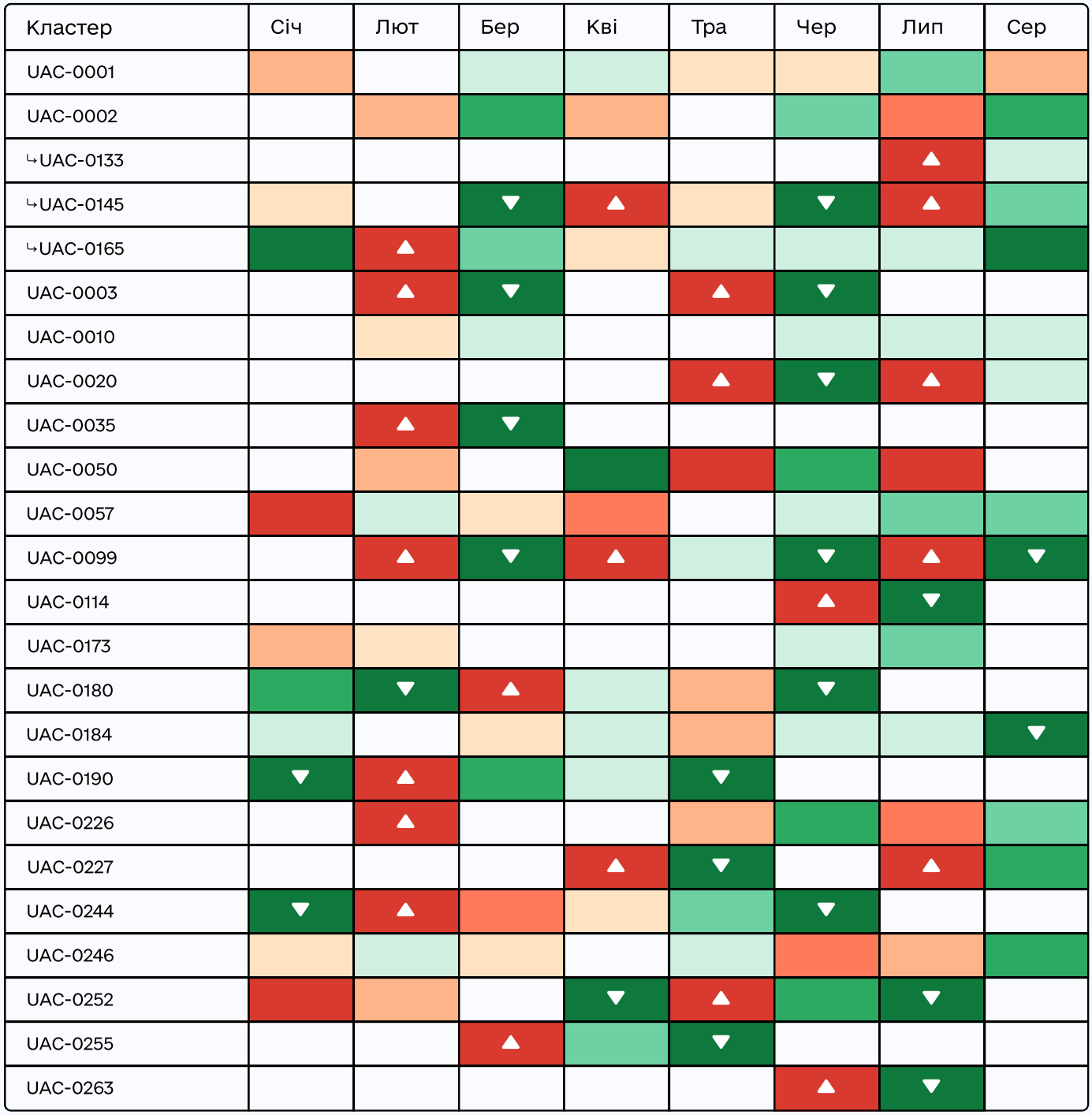
Кластер	Січ	Лют	Бер	Кві	Тра	Чер	Лип	Сер
UAC-0001								
UAC-0002								
↳UAC-0133								
↳UAC-0145								
↳UAC-0165								
UAC-0003								
UAC-0010								
UAC-0020								
UAC-0035								
UAC-0050								
UAC-0057								
UAC-0099								
UAC-0114								
UAC-0173								
UAC-0180								
UAC-0184								
UAC-0190								
UAC-0226								
UAC-0227								
UAC-0244								
UAC-0246								
UAC-0252								
UAC-0255								
UAC-0263								

low high

HeatMap динаміки

Для відображення тенденцій активності окремих кластерів кіберзагроз нижче також наведено теплову карту, що демонструє динаміку кіберінцидентів, атрибутованих до цих кластерів, у розрізі місяців.

Значення в клітинках відображають появу нової активності або зміну інтенсивності атак порівняно з попереднім місяцем.



Поява/відновлення активності

Активність припинилась

значний спад

no changes

значний приріст

Актуальні загрози

Нові загрози

Упродовж звітного періоду CERT-UA фіксувала подальше формування нових кластерів кіберзагроз. Їх поява не завжди свідчить про виникнення нового актора кіберзагроз: окремий ідентифікатор може присвоюватися активності, щодо якої наявних даних недостатньо для впевненої атрибуції. Використання штучного інтелекту, загальнодоступного коду та легітимних сервісів додатково ускладнює атрибуцію й потребує системного спостереження за розвитком таких загроз.

Мобільні пристрої – окрема поверхня атаки

У першому півріччі мобільні пристрої дедалі чіткіше виокремлюються як самостійна поверхня атаки. Противник орієнтується як на Android, так і на iOS, як розповсюджує шкідливі застосунки, так і експлуатує вразливості мобільних платформ. Зростання ролі смартфонів у комунікації військовослужбовців, працівників державних органів та громадян підвищує їхню привабливість для розвідувальної діяльності, подальшого розвитку компрометації та фінансово мотивованих атак.

Окремо варто відзначити появу експлойт-кіту DarkSword, орієнтованого на пристрої iOS. Компрометація здійснюється за схемою watering hole – через скомпрометовані легітимні, зокрема українські новинні та урядові, вебсайти, з яких у браузер жертви завантажується ланцюг експлойтів для низки вразливостей Safari та ядра. Такий підхід може забезпечувати компрометацію пристрою без помітної взаємодії користувача. У разі успішної атаки зловмисники отримують доступ до чутливих даних, зокрема облікових даних, повідомлень, контактів та історії дзвінків.

Інструмент асоціюється з російськими акторами, а його застосування проти українських цілей свідчить про інтерес противника до платформи iOS, яка раніше сприймалася як відносно захищена.

Кластери кіберзагроз UAC-0244 та UAC-0263 для компрометації мобільних пристроїв використовують шкідливі Android-застосунки. Для їх розповсюдження створюються вебсторінки-приманки: у випадку UAC-0244 – ресурси, що імітують сайт 3-го армійського корпусу (з пропозицією «пройти тест»), «чоловічого клубу» тощо; у випадку UAC-0263 – сторінки, з яких нібито можна завантажити застосунки для попередження про повітряні загрози, отримання знижок на пальне з іншою суспільною тематикою. При цьому кластери застосовують різні ШПЗ. UAC-0244 розповсюджує CAMELSPY, що збирає системну інформацію пристрою, геолокацію, відомості про SIM-карти, контакти, журнали дзвінків і зображення з галереї. UAC-0263 використовує BTMOB RAT – інструмент віддаленого доступу (RAT), який надає зловмисникам контроль над інфікованим пристроєм та можливість викрадення даних.

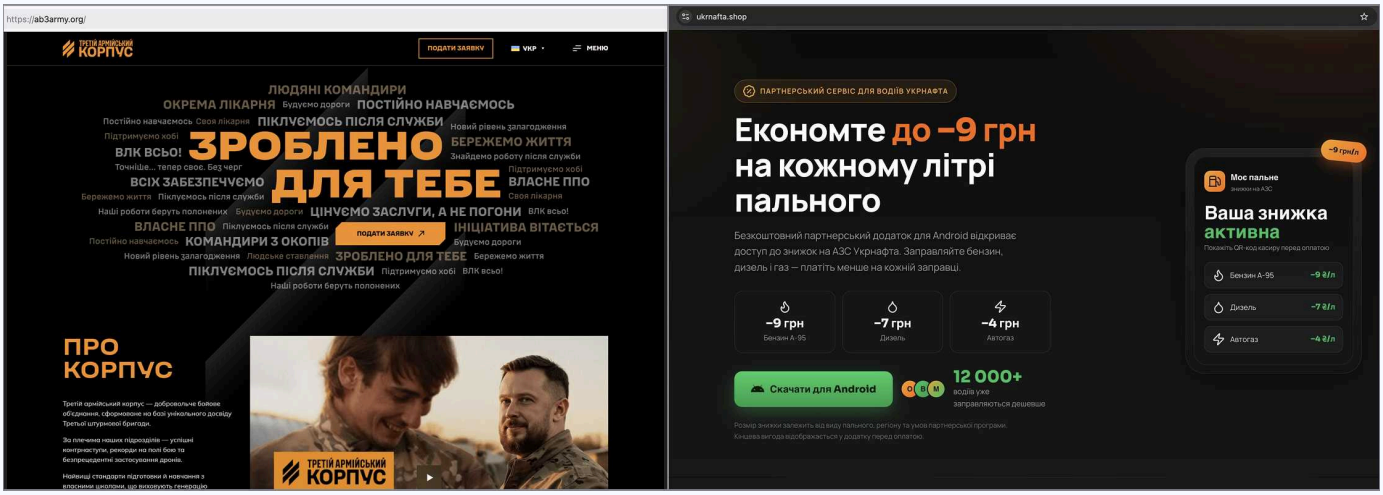


Рис. 1. Вебсторінки-приманки UAC-0244 та UAC-0263

Змінний інструментарій, стала мета: UAC-0252

Починаючи із січня 2026 року CERT-UA фіксувала кібератаки UAC-0252 проти органів місцевого самоврядування, об'єктів критичної інфраструктури та військових формувань. У листах жертвам пропонувалося встановити нібито оновлення або службовий модуль, зокрема від імені державних установ чи CERT-UA. Доставка здійснювалася через вкладені архіви з виконуваним файлом або посилання на легітимні, проте вразливі до

міжсайтового скриптингу (XSS) вебсайти, відвідування яких ініціювало завантаження шкідливого файлу; при цьому саме шкідливе навантаження розміщувалося на ресурсах легітимних сервісів, зокрема GitHub, що ускладнювало його виявлення.

У різних кампаніях використовувалися SHADOWSNIFF, SALATSTEALER, DEAFTICK, DEAFTICKV2 та EGGSFILL.

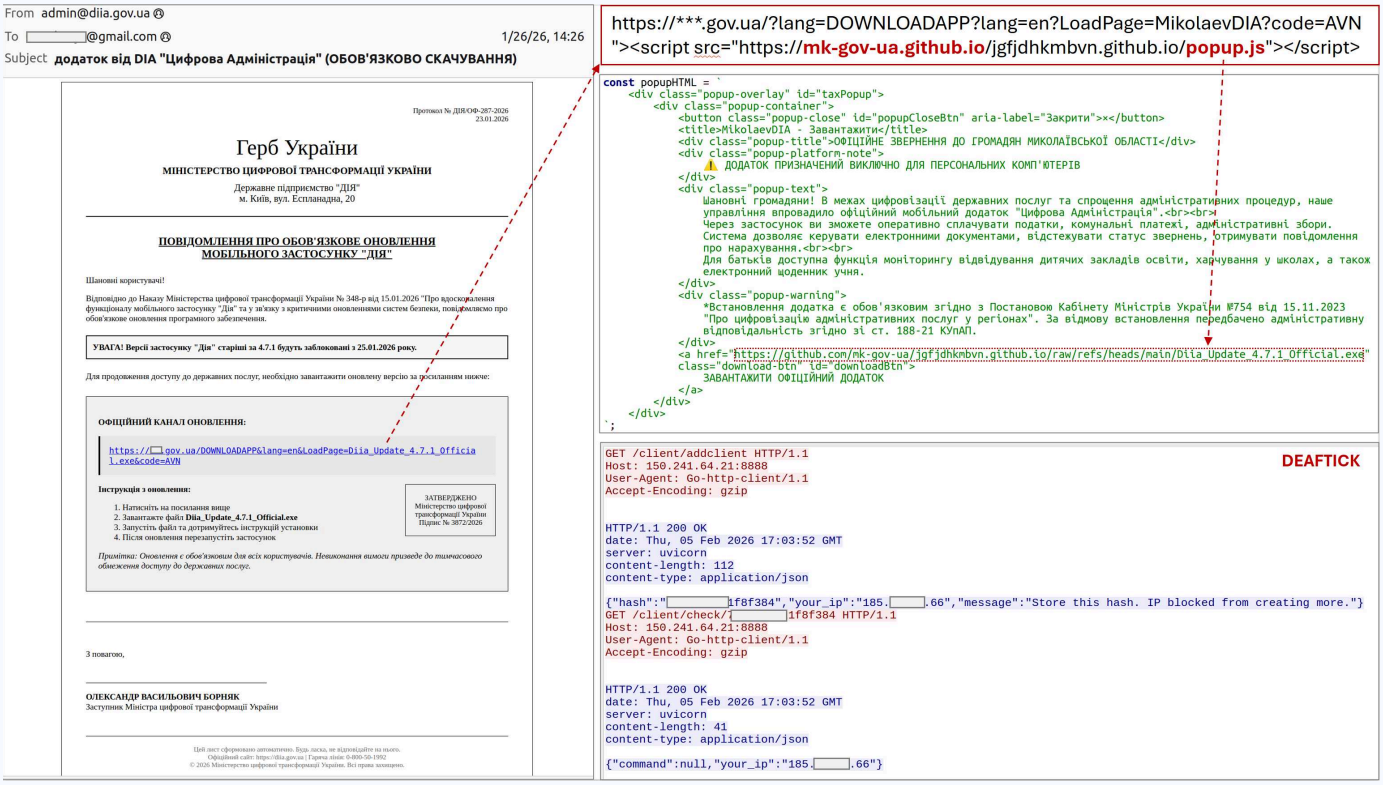


Рис. 2. Фейкова вебсторінка hXXps://cert-ua[.]tech/

Правдоподібне прикриття: UAC-0255

Упродовж березня–травня 2026 року зафіксовано три кампанії UAC-0255, у межах яких зловмисники імітували повідомлення CERT-UA, оновлення системи захищеного документообігу Верховної Ради України та застосунок Brave1 Security Hub. В усіх випадках використовувалося ШПЗ AGEWHEEZE, а одна з підроблених вебсторінок, що імітувала ресурс CERT-UA, мала технічні ознаки створення з використанням штучного інтелекту.

Показовим у цьому випадку є не рівень складності ШПЗ, а швидкість підготовки переконливого прикриття. Зловмисники експлуатували тематику кіберзахисту, щоб спонукати користувачів самостійно завантажити та запустити шкідливу програму, роблячи ставку радше на довіру, ніж на технічну витонченість.

Найактивніші кластери півріччя

На відміну від нових кластерів, розглянутих вище, в цьому блоці описано кластери ти актори кіберзагроз, які зберігали стабільно високу активність упродовж усього звітного періоду. Їх поєднує не спільний інструментарій чи мотивація, а сталість цілей за гнучкості засобів: тактики, приманки та шкідливе програмне забезпечення змінюються, тоді як завдання лишаються незмінними. Спільною рисою є зловживання легітимними сервісами та засобами, що ускладнює виявлення й блокування такої активності.

UAC-0050

Кластер UAC-0050 залишається одним із найсталіших за своїми тактиками, техніками та процедурами. Упродовж звітного періоду цей актор проводив численні кампанії масового розсилання електронних листів зі шкідливим програмним забезпеченням – інколи по кілька кампаній на тиждень, – традиційно експлуатуючи тематику бухгалтерського та фінансового характеру. Фінальним навантаженням слугували програми віддаленого керування російської розробки RemoteUtilities та Litemanager.

Також фіксувались атаки з використанням Remcos RAT та NetSupport.

Характерною особливістю є конфігурація цього програмного засобу: вона містить сотні IP-адрес і доменних імен, серед яких лише кілька відповідають реальним серверам управління, а решта – адреси легітимних ресурсів. Таке «розчинення» справжніх C2 серед довірених адрес ускладнює виявлення та блокування активності й свідчить про свідоме прагнення актора підвищити прихованість за загалом незмінного підходу.

UAC-0173

UAC-0173 залишається одним із найактивніших кластерів звітного періоду. Атаки спрямовувалися на приватних нотаріусів, центри надання адміністративних послуг (ЦНАП), територіальні центри комплектування та медичні заклади. Кінцевою метою активності є отримання доступу до інформаційних систем для внесення неправдивих відомостей до державних реєстрів, що робить цей кластер загрозою не лише для конфіденційності, а й для цілісності офіційних даних.

У типовій кампанії потенційним жертвам – наприклад, приватним нотаріусам від імені регіонального нотаріату – надсилалися листи на тематику проведення семінару з посиланням, сформованим через сервіс скорочення TinyURL, на завантаження ZIP-архіву з файлообмінного ресурсу (SendItToYou, YDRAY, SwissTransfer, HiDrive тощо). Архів містив легітимний виконуваний файл і шкідливу DLL-бібліотеку; запуск першого призводив до виконання коду з бібліотеки (техніка DLL Side-Loading), який розшифровував і запускав засіб віддаленого доступу DarkCrystal RAT (DCRat). Для розгортання серверів управління зловмисники зловживали легітимними сервісами, зокрема ngrok.

UAC-0246

У першому півріччі 2026 року UAC-0246 імітував офіційні повідомлення різної тематики, спонукаючи отримувача відкрити вкладення або перейти за посиланням. Спочатку розсилки були орієнтовані переважно на персональні поштові скриньки користувачів одного з українських поштових сервісів, згодом – і на корпоративні адреси працівників державних органів, органів місцевого самоврядування та сектору безпеки і оборони. Незмінною метою залишалося отримання віддаленого доступу до пристрою жертви: розсилка слугувала первинним вектором, а очікуваним результатом – контроль над ураженою системою.

Тематика та відправники листів варіювалися – вони надсилались нібито від імені різних компаній і державних установ, зокрема податкових і банківських. Відрізнялися й ланцюги доставки: від RAR-архівів із виконуваним файлом-завантажувачем (наприклад, DarkTortilla) до посилань, що ініціювали завантаження ZIP-архівів зі скриптами.

При цьому фінальним навантаженням послідовно виступало ШПЗ XenoRAT, для доставки активно використовувалися легітимні файлові сервіси, а закріплення в системі забезпечувалося, зокрема, копіюванням до каталогу автозавантаження. Така варіативність прикриття за сталого кінцевого інструменту робить UAC-0246 стабільно небезпечним попри відносно просту схему атак.

UAC-0226

UAC-0226 – кластер кібершпигунського спрямування, активний щонайменше з початку 2025 року. Його цілями є осередки розвитку військових інновацій, військові формування, правоохоронні органи та органи місцевого самоврядування. Первинним вектором залишаються тематичні електронні листи, зміст яких відображає актуальний порядок денний – від розмінування та виробництва БПЛА до судових повісток і відомостей з реєстру військовозобов'язаних.

Упродовж звітного періоду простежується еволюція інструментарію. Якщо раніше основою кампаній були документи Excel із макросами, то у першому півріччі 2026 року цей кластер перейшов до розсилання захищених паролем архівів, які експлуатують вразливість WinRAR (CVE-2025-8088), із закріпленням через ярлик (LNK) у каталозі автозавантаження. Сталим інструментом залишається стілер GIFTEDCROOK, можливості якого розширилися від викрадення даних браузерів до файлів із каталогів профілю користувача, а ексфільтрація змістилася з Telegram безпосередньо на сервер управління.

російські (і не тільки) спецслужби

Кібератаки акторів кіберзагроз, спонсорованих державами, – насамперед афілійованих до спецслужб рф і білорусі, – залишаються найнебезпечнішим сегментом кіберзагроз. Значні ресурси та стабільне фінансування дозволяють їм швидко озброюватися новими вразливостями, розробляти власний інструментарій і роками підтримувати доступ до уражених систем задля розвідки та деструктивних операцій проти критичної інфраструктури й державних інституцій.

UAC-0001

UAC-0001 (APT28), пов'язаний з головним управлінням генерального штабу збройних сил рф, залишається одним із найнебезпечніших акторів кіберзагроз, а його визначальною рисою є швидке озброєння щойно оприлюдненими вразливостями. Вже через кілька днів після публікації інформації про вразливість Microsoft Office CVE-2026-21509 вони використали її для розповсюдження програмного засобу COVENANT. Слід зазначити, що закріплення в системі забезпечувалося технікою підміни COM-об'єктів (COM hijacking), а роль інфраструктури управління відігравало легітимне хмарне сховище Filen (filen.io).

Іншою свіжою вразливістю в їх арсеналі стала zero-click вразливість поштового вебклієнта SOGo (CVE-2026-8496). Відкриття листів з її експлойтом призводило до викрадення автентифікаційних даних та сесії користувача, а також ексфільтрації вмісту самої поштової скриньки.

Водночас актор не відмовляється й від старих, перевірених, але, на жаль, досі дієвих підходів. Зокрема, фіксувались атаки з використанням експлойтів XSS-вразливостей поштового вебклієнта Roundcube. А для подальшого розповсюдження COVENANT застосовувалися документи Excel із макросами.

UAC-0165 (субкластер UAC-0002)

UAC-0165 – субкластер, асоційований з діяльністю UAC-0002 (Sandworm). У першому кварталі 2026 року виявлено та досліджено низку кіберінцидентів в організаціях різного профілю: постачальників електронних комунікаційних послуг, підприємств тепло-, водо-, газо- та енергопостачання, державних органів (у тому числі органів місцевого самоврядування), розробників програмного забезпечення та інших. Задум зловмисників полягав у проведенні деструктивних кібератак, що узгоджувалося із загальною спрямованістю Sandworm на ураження об'єктів критичної інфраструктури.

Характерною особливістю був спосіб мережевої взаємодії з об'єктами атак: безпосереднє з'єднання з елементами їхніх інформаційно-комунікаційних систем здійснювалося через проміжні вузли – скомпрометоване активне мережеве обладнання та інші технічні засоби, фізично розташовані на території України.

UAC-0057

UAC-0057 (UNC1151) – актор кіберзагроз, пов'язаний з білоруссю. У звітному періоді воно оновило власний інструментарій, застосовуючи в кампаніях проти державних організацій нове сімейство ШПЗ OYSTER. Первинним вектором залишалися електронні листи: засобами електронної пошти розповсюджувався PDF-документ із посиланням, перехід за яким ініціював завантаження ZIP-архіву з JS-файлом.

Запуск цього файлу (OYSTERFRESH) відкривав документ-приманку та розгортав компоненти OYSTERBLUES і OYSTERSHUCK із закріпленням у системі через заплановане завдання. OYSTERSHUCK виконував роль декодера, що розшифровував і запускав бекдор OYSTERBLUES; останній збирав базову інформацію про систему, надсилав її на сервер керування та виконував отриманий у відповідь код. На наступному етапі можливе було довантаження фреймворку Cobalt Strike, а для приховування інфраструктури управління цей актор традиційно використовувало сервіс Cloudflare зі значною часткою доменних імен у зоні .icu.

Попередні звіти

Для розуміння цілісної картини трансформацій у сфері кібероперацій під час повномасштабної війни, ознайомтесь з попередніми аналітичними звітами на сторінці:

Аналітичні матеріали Держспецзв'язку

Контакт-центр для ЗМІ:

press@cip.gov.ua

Залишайтеся на зв'язку:

https://x.com/SSSCIP

https://x.com/_CERT_UA

https://www.linkedin.com/company/dsszzi

https://www.linkedin.com/company/cert-ua

https://www.facebook.com/dsszzi

https://www.facebook.com/UACERT

Державна служба спеціального зв'язку
та захисту інформації України

Кіберзагрози: Україна

Аналітика за І півріччя 2026