Державна служба спеціального зв'язку
та захисту інформації України

TLP:CLEAR

Кібер-загрози: Україна

Аналітика за II півріччя 2025

Зміст

Передмова

CERT-UA

Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози

Кіберпростір залишається невід'ємною складовою сучасної війни. Поряд із традиційними видами впливу противник активно використовує кібероперації для досягнення розвідувальних, інформаційних та операційних цілей. У таких умовах здатність держави своєчасно виявляти кіберзагрози, аналізувати їх та ефективно реагувати на кіберінциденти є критично важливою для забезпечення національної безпеки.

Активність хакерських угруповань у кіберпросторі постійно змінюється та еволюціонує. Противник експериментує з новими підходами, адаптує свої інструменти та тактики, а також використовує комбінації технічних засобів і методів соціальної інженерії для досягнення своїх цілей.

Виявлення таких змін та їх системний аналіз дозволяють своєчасно формувати ефективні підходи до протидії кіберзагрозам і підвищувати стійкість інформаційних систем.

У звіті узагальнено результати спостережень за кіберінцидентами у II півріччі 2026 року, висвітлено основні тенденції розвитку кіберзагроз, проаналізовано активність окремих кластерів кіберзагроз та описано нові тактики, техніки і процедури, які застосовуються хакерськими угрупованнями.

Окремо висловлюємо вдячність усім фахівцям, які щоденно працюють над захистом кіберпростору України – підрозділам кібербезпеки державних органів, сектору безпеки і оборони, спеціалістам на місцях, а також міжнародним партнерам. Саме завдяки спільним зусиллям вдається своєчасно виявляти загрози, протидіяти кібероперціям противника та підвищувати стійкість українського кіберпростору.

Висновки та інсайти

Інсайти

Вперше з початку повномасштабного вторгнення можна констатувати, що кількість кіберінцидентів у цьому півріччі є меншою порівняно з попереднім. Таке зниження є незначним і може свідчити про поступову адаптацію українських організацій до поточного рівня кіберзагроз, а також підвищення ефективності заходів протидії. Водночас інтенсивність кібератак загалом залишилася на попередньому рівні, проте простежуються зміни у підходах противника.

Знову ж таки, ми продовжуємо спостерігати появу нових кластерів кіберзагроз, що свідчить про постійний пошук противником більш ефективних підходів до проведення операцій. Зловмисники експериментують із різними тактиками, оцінюють їх результативність та можуть повертатися до попередніх сценаріїв атак, якщо вони демонструють вищу ефективність, водночас не відмовляючись повністю від раніше випробуваних підходів.

Окремо фіксується тенденція спроб повернення зловмисників до раніше скомпрометованих систем. На жаль, інколи такі спроби виявляються частково успішними через неповне усунення причин попереднього інциденту.

Загалом наведені спостереження свідчать про збереження складної та динамічної ситуації в кіберпросторі.

Фокус на персистентності

У попередньому півріччі значна частина кіберінцидентів була пов’язана з використанням тактики «Steal & Go», яка передбачала розповсюдження стілерів без механізмів закріплення в системі. Такий підхід дозволяв зловмисникам швидко викрадати необхідну інформацію, зменшуючи час перебування в інфраструктурі жертви та ризик виявлення.

Протягом звітного півріччя спостерігається поступове зміщення акценту атак з одноразового викрадення інформації на отримання несанкціонованого доступу до інформаційних систем.

Зловмисники дедалі частіше зосереджуються на збереженні можливості повторного входу в уражену інфраструктуру, зловживанні легітимними сервісами віддаленого доступу та розвитку первинної компрометації.

Такий підхід може свідчити про прагнення підвищити довгострокову цінність атак, зокрема шляхом подальшого використання доступу для підготовки до наступних фаз атаки. У цьому контексті компрометація дедалі частіше розглядається не як одноразова подія, а як початкова точка для подальших дій у межах інфраструктури жертви.

Повернення

Варто зауважити, що в межах окремих інцидентів фіксувалися випадки повторної активності зловмисників щодо раніше скомпрометованих систем через певний проміжок часу після первинної атаки. Такі дії можуть бути спрямовані на перевірку того, чи зберігається можливість доступу, чи залишилися експлуатовані вразливості, або чи залишаються дійсними отримані раніше облікові дані.

Подібна практика підкреслює важливість комплексного реагування на інциденти та усунення першопричин компрометації. Обмеження реагування лише відновленням працездатності систем або точковим блокуванням виявленої активності без аналізу причин інциденту та вирішення усіх виявлених проблем суттєво підвищує ризик повторної компрометації. За відсутності належних висновків та коригувальних заходів організація може повторно стати жертвою тієї самої або подібної атаки.

Висновки

У другому півріччі кіберпростір України продовжував залишатися одним із важливих напрямів протистояння з противником. Кібератаки і надалі застосовуються як інструмент отримання розвідувальної інформації, порушення роботи критично важливих систем та впливу на функціонування державних інституцій.

Характерною особливістю звітного періоду є подальша еволюція підходів зловмисників. Фіксується поява нових кластерів кіберзагроз, активне тестування різних тактик і технік, а також повторне використання вже перевірених сценаріїв атак. Окрему увагу привертає уніфікація інструментарію – ефективні вразливості та підходи швидко поширюються між різними угрупованнями.

Водночас спостерігається зміна акцентів у початкових векторах компрометації. Зростає роль складніших методів соціальної інженерії, що базуються на встановленні довіри до зловмисника, використанні легітимних каналів комунікації та персоналізованому підході до жертв. Паралельно з цим продовжується використання технічних механізмів забезпечення стійкої присутності в уражених системах.

Разом із цим результати звітного періоду свідчать про поступове підвищення стійкості інформаційних систем та ефективності заходів протидії. Водночас збереження активності противника, його адаптивність та факти повернення до раніше скомпрометованих систем підкреслюють необхідність системного підходу до кіберзахисту, зокрема повного усунення наслідків інцидентів та впровадження превентивних заходів безпеки.

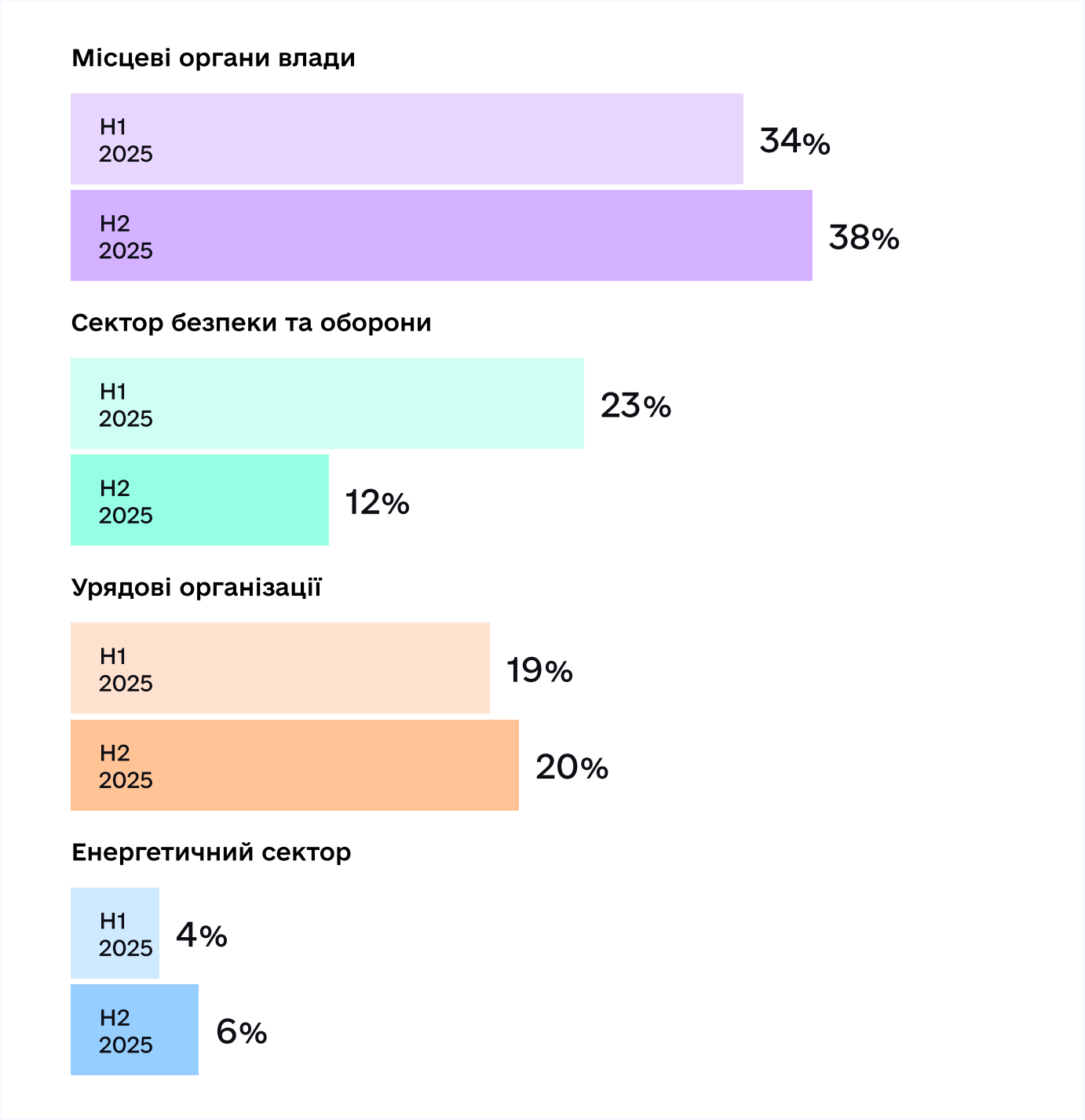
Тенденції

У звітному періоді інтенсивність кіберінцидентів загалом залишалася на рівні І півріччя, хоча їх загальна кількість дещо зменшилася. Водночас не було зафіксовано жодного критичного інциденту, кількість інцидентів високого рівня також знизилася.

Рівень критичності	H1 2025	H2 2025	Зміна за період
Критичний	1	0	-100%
Високий	6	5	-17%
Середній	2 944	2895	-2%
Низький	67	9	-87%
Загалом	**3 018**	**2 909**	**-4%**

Щодо цілей противника – вони залишаються незмінними. Попри те, що в нашій статистиці кількість кібератак на сектор безпеки та оборони зменшилася, це не повною мірою відображає реальну картину.

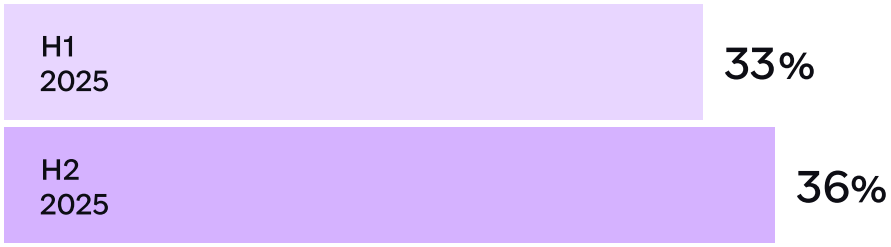
Значна частина таких інцидентів опрацьовується безпосередньо підрозділами кібербезпеки військових формувань. Водночас сектор безпеки та оборони й надалі залишається однією з пріоритетних цілей кібератак з боку противника, оскільки вплив на нього може безпосередньо позначатися на перебігу бойових дій.



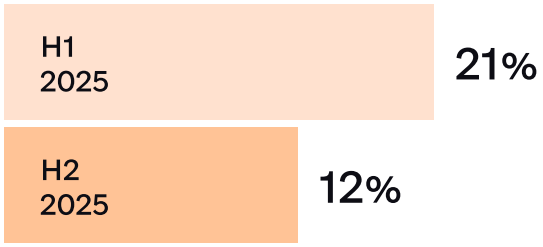
У II півріччі спостерігалася позитивна тенденція: попри незначне зростання кількості розсилок шкідливих програм, кількість інфікувань зменшилася.

Цьому сприяли підвищення обізнаності користувачів щодо кіберзагроз, а також заходи з виявлення та блокування шкідливих активностей, що здійснюються нашою командою.

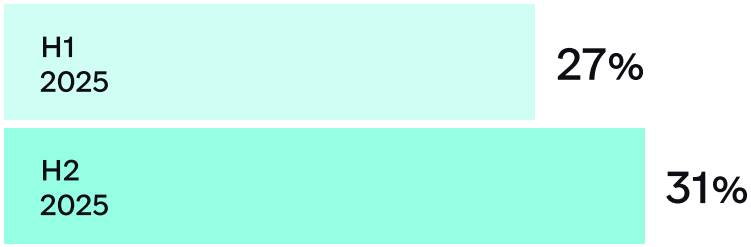
02.02 Розповсюдження ШПЗ (Malware distribution)



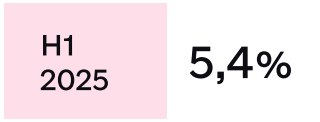
02.01 Зараження ШПЗ (Malware infection)



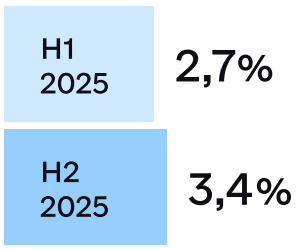
03.03 Фішинг (Phishing)



05.01 Компрометація облікового запису (Account Compromise)



05.02 Компрометація системи (System Compromise)



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.

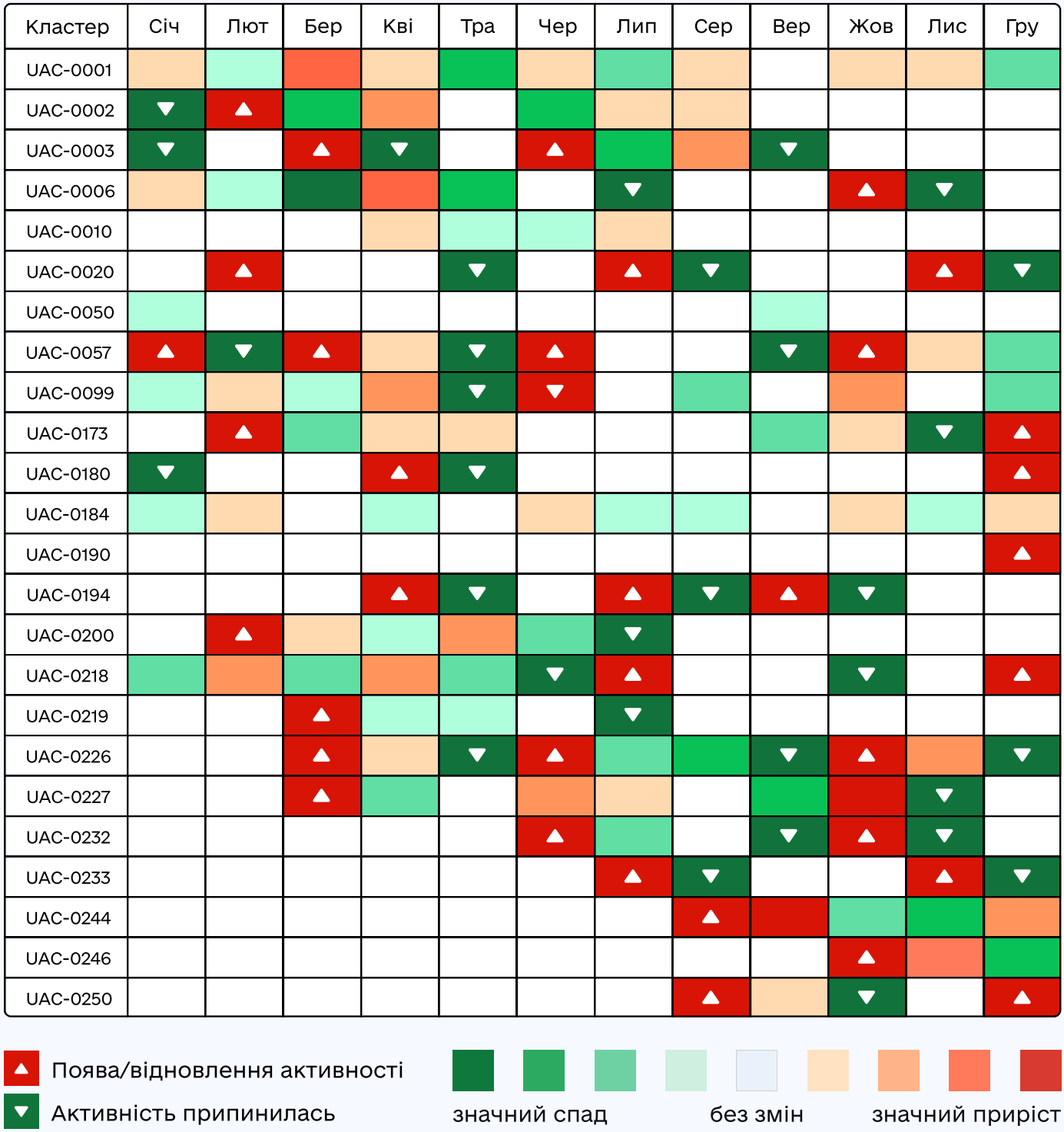
Кластер	Січ	Лют	Бер	Кві	Тра	Чер	Лип	Сер	Вер	Жов	Лис	Гру
UAC-0001												
UAC-0002												
UAC-0003												
UAC-0006												
UAC-0010												
UAC-0020												
UAC-0050												
UAC-0057												
UAC-0099												
UAC-0173												
UAC-0180												
UAC-0184												
UAC-0190												
UAC-0194												
UAC-0200												
UAC-0218												
UAC-0219												
UAC-0226												
UAC-0227												
UAC-0232												
UAC-0233												
UAC-0244												
UAC-0246												
UAC-0250												

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.



Актуальні загрози

Нові загрози другого півріччя

Упродовж звітного періоду зафіксовано подальше формування нових кластерів кіберзагроз, що продовжує тенденцію, відзначену у попередньому звіті. Зафіксовано як нові підходи до кібершпигунства, так і кібератаки з використанням вірусів-вимагачів (Ransomware). Водночас актуальною залишається активність, пов'язана з експлуатацією zero-click вразливостей.

Zero-clickers: UAC-0233, UAC-0250

Хоча активність UAC-0233 була вперше зафіксована ще у першому півріччі 2025 року, а використання вразливостей Roundcube (CVE-2024-37383 та CVE-2025-49113) було описано у попередньому аналітичному звіті, на той момент йшлося про поодинокий інцидент. Основна ж активність кластера припала на друге півріччя 2025 року, що зумовило виділення окремого ідентифікатора для відстеження цієї загрози.

Щонайменше з кінця вересня 2025 року зафіксовано серію кампаній, пов'язаних з експлуатацією zero-click вразливостей у поштовому сервері Zimbra. У межах різних атак зловмисники використовували вразливості CVE-2025-48700 та CVE-2025-66376, експлуатація яких забезпечує виконання шкідливого коду без потреби будь-якої взаємодії з боку користувача.

У разі успішної компрометації зловмисники отримували доступ до вмісту поштових скриньок, включно з листуванням, яке збиралося у TGZ-архів, резервними кодами багатофакторної автентифікації, паролями застосунків, а також глобальною адресною книгою. Зазначена активність відстежується під ідентифікатором UAC-0250.

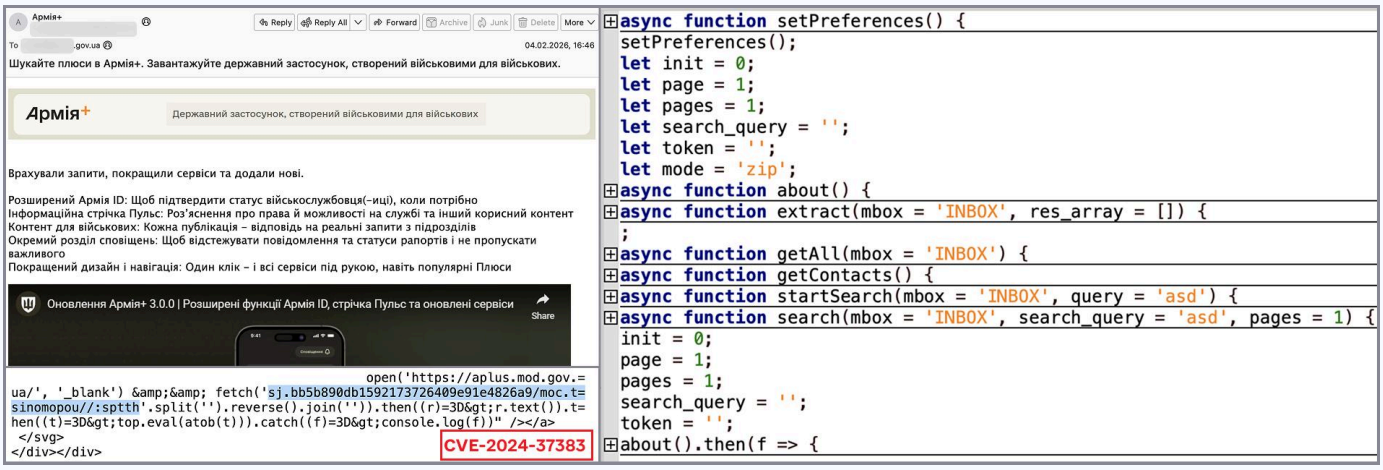


Рис. 1. Приклад активності UAC-0233

Кібервимагачі: UAC-0238, UAC-0243

У другому півріччі 2025 року зафіксовано кібератаки з використанням шкідливих програм-вимагачів (Ransomware) різних угруповань.

Щонайменше з липня 2025 року UAC-0238 здійснювало атаки проти органів місцевого самоврядування, шифруючи дані на ЕОМ з операційною системою Windows за допомогою програм із сімейства Proton. Первинний доступ до інформаційно-комунікаційних систем (ІКС) зловмисники отримували через доступні з мережі Інтернет інтерфейси для адміністрування, переважно RDP. Перед шифруванням файлів хакери видаляли тіньові копії (shadow copies) операційної системи, що унеможливлювало відновлення даних із їх використанням.

Щодо кіберзагрози UAC-0243, точкою входу зазвичай слугує вразливий сервер Microsoft SharePoint, з якого зловмисники отримують доступ до локальної мережі. Для шифрування застосовували програму-вимагач X2anylock (Warlock), що є варіацією LockBit 3.0.

Слід зазначити, що під час атаки для закріплення в системі, горизонтального переміщення мережею та викрадення файлів зловмисники використовували низку легітимних утиліт, зокрема сервіс тунелювання трафіку Cloudflare Tunnel, а також інструменти Velociraptor та RClone.

Ця активність не є новою на глобальному рівні. Схожі кібератаки зафіксовано проти державних органів Португалії, Хорватії та Туреччини, а також на критичній інфраструктурі та інших організаціях Північної Америки. Перша атака проти України відбулася в жовтні 2025 року.

Кібершпигуни: UAC-0232, UAC-0246

Упродовж звітного періоду зафіксовано появу нових кіберзагроз, спрямованих на здійснення кібершпигунства. Це свідчить про збереження стратегічної мети противника щодо отримання розвідувальної інформації будь-якими способами.

Основними об’єктами інтересу залишаються інформаційні ресурси сил безпеки та оборони, урядових органів, а також органів місцевого самоврядування.

Цікавим підходом вирізняється угруповання UAC-0232. Кожна з його кампаній була націлена на окремий регіон України. Серед державних установ відповідної області здійснювалася розсилка електронних листів із посиланням на вебсторінку, що імітує офіційний сайт обласної військової адміністрації, де нібито розміщено перелік захисних споруд. Замість очікуваного документа завантажується архів із виконуваним файлом, що містить шкідливе програмне забезпечення STELLDOCK, яке поєднує функціонал стілера та бекдору (зокрема забезпечує збір даних і виконання обмеженого набору команд на інфікованому комп’ютері).

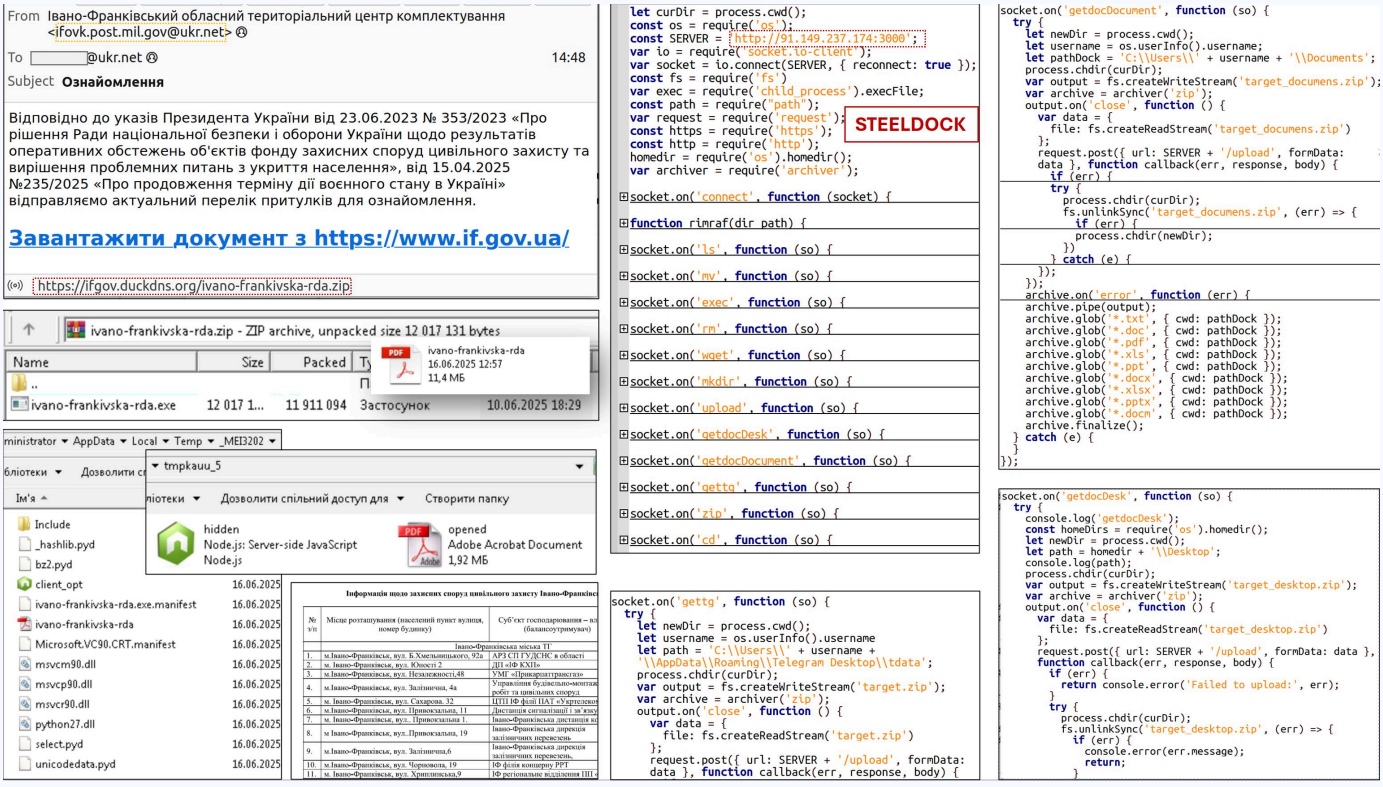


Рис. 2. Приклад активності UAC-0232

Корпоративні поштові сервери зазвичай оснащені впровадженими засобами кіберзахисту, унаслідок чого значна частина шкідливих повідомлень блокується ще до їх доставки користувачам. Угруповання UAC-0246 застосовує інший підхід, здійснюючи розповсюдження шкідливих листів на особисті поштові скриньки громадян України.

Основною ціллю зловмисників є користувачі поштового сервісу I.UA. При цьому шкідливий файл не додається як вкладення – жертва отримує посилання на файлове сховище того ж сервісу I.UA, де розміщено виконуваний файл, запуск якого призведе до інфікування системи програмою для віддаленого керування XenoRAT.

Актуальні тактики, техніки та процедури

У звітному періоді зафіксовано окремі зміни в тактиках, техніках та процедурах, що застосовуються хакерськими угрупованнями. Окремі техніки виявилися достатньо результативними, що зумовило їх поширення та одночасне використання різними угрупованнями.

CVE-2025-8088

Досить поширеною у звітному періоді стала вразливість WinRAR CVE-2025-8088. Інформацію про неї було оприлюднено в серпні, і вже з вересня почали фіксуватися розсилки листів із вкладеними архівами, що містили експлойт цієї вразливості. Вона дозволяє здійснювати запис файлів за межами обраної користувачем директорії під час розпакування архіву.

В результаті у вразливих версіях WinRAR непомітно для користувача створюється додатковий файл у каталозі, визначеному зловмисниками. Найчастіше експлуатація використовується для розміщення шкідливих файлів у директорії автозавантаження, що забезпечує їх автоматичне виконання під час наступного входу користувача в систему.

Перша зафіксована нами кібератака з використанням цієї вразливості була атрибутована до UAC-0010. Водночас у подальшому експлуатацію CVE-2025-8088 фіксували також в активностях, пов’язаних з UAC-0002, UAC-0226 та інших угруповань.

Alternate Data Streams (ADS)

У звітному періоді також фіксувалося використання механізму альтернативних потоків даних (Alternate Data Streams (ADS)). Це штатна функціональна можливість файлової системи NTFS у середовищі Windows, яка дозволяє зберігати додаткові потоки даних, пов’язані з файлом чи каталогом. Такий механізм зловмисники використовують для приховування шкідливого коду.

Угруповання UAC-0010 відоме тим, що на інфікованому комп’ютері може створювати більше сотні шкідливих файлів в різних директоріях та зберігати шкідливий код в реєстрі Windows. Водночас у 2025 році зафіксовано розширення їхнього інструментарію – додаткове розміщення компонентів ШПЗ в альтернативних потоках даних порожніх (0 байт) файлів і каталогів, що ускладнює виявлення та аналіз активності.

Аналогічний підхід може застосовуватися і щодо віртуальних дисків (VHD-файлів), які після підключення відображаються в системі як окремий носій із файловою структурою NTFS та підтримкою ADS. Саме цей механізм використало угруповання UAC-0099. Зловмисники розповсюджували посилання на завантаження VHD-файлів, що містили LNK-файл, VBS-скрипт і текстові файли з формально безпечним вмістом (наприклад, «Hello First»). Водночас шкідливе навантаження зберігалося в альтернативних потоках даних (ADS) цих файлів і зчитувалося та виконувалося за допомогою згаданого скрипту.

російські спецслужби

Кібератаки угруповань, афілійованих до головного управління гш зс рф та й інших спецслужб країни-агресора, одні з найнебезпечніших. Вони постійно знаходять нові шляхи для компрометації систем з метою шпигунства та проведення деструктивних кібератак.

Еволюція методів соціальної інженерії

У звітному періоді простежується трансформація підходів до соціальної інженерії. Традиційні фішингові листи чи повідомлення в месенджерах з вкладеннями поступово втрачають ефективність через зростання обізнаності користувачів та підвищену обережність. Натомість первинна взаємодія з об'єктами атак дедалі частіше здійснюється з використанням телефонних номерів українських мобільних операторів і легітимних облікових записів. Зловмисники спілкуються українською мовою, застосовують аудіо- та відеозв'язок і демонструють релевантне знання про особу чи організацію, що дозволяє їм підвищувати рівень довіри та ефективність атак.

Зазначену тактику застосовували, зокрема, угруповання UAC-0001 (APT28) та UAC-0190 (Void Blizzard, Laundry Bear) під час атак на представників сил оборони та державних органів України. Шкідливі файли надсилалися жертвам у месенджери вже після безпосереднього телефонного спілкування.

Так, UAC-0001 здійснило масштабну кібероперацію проти українських військовослужбовців і працівників підприємств

оборонно-промислового комплексу. Метою кампанії була розвідка, зокрема отримання несанкціонованого віддаленого доступу до уражених систем та збір інформації, що становить інтерес для зловмисників.

У межах взаємодії потенційним жертвам надсилався файл формату XLS із вбудованим шкідливим макросом, замаскований під службову документацію. Деталі цієї активності висвітлено в публікації CERT-UA.

Скомпрометовані пристрої як джерело атак UAC-0002

Дослідження кіберінциденту зазвичай не завершується встановленням та усуненням його першопричини. Так, після активної фази дослідження кіберінциденту на об`єкті критичної інфраструктури та масової зміни облікових даних, моніторинг журналів подій було зосереджено на виявленні спроб повторної автентифікації у скомпрометовані облікові записи. Таким чином було виявлено неуспішні спроби підключень з низки українських IP-адрес, що мали спільну ознаку – належали до українського сегмента мережі та мали публічно доступну панель адміністрування мережевого пристрою.

В ході дослідження окремих пристроїв було виявлено увімкнення штатного функціоналу SOCKS та налаштування SSH-forwarding, що дозволяло використовувати їх як проміжні вузли для маршрутизації та тунелювання трафіку під час подальших атак.

Моніторинг трафіку таких вузлів дозволяє ідентифікувати додаткові елементи інфраструктури зловмисників, включно з іншими скомпрометованими пристроями, а також потенційних жертв їхніх атак.

З метою ускладнення встановлення фактичного джерела атаки часто використовувався ланцюг із кількох таких пристроїв. Проміжними точками також могли виступати скомпрометовані публічні вебресурси, на яких розміщувалися інструменти для тунелювання трафіку.

Отже, під час відновлення після кіберінциденту критично важливо забезпечити комплексне усунення виявлених недоліків: обмежити адміністративний доступ, усунути вразливості, змінити облікові дані та переглянути налаштування віддаленого керування. Лише повноцінне впровадження таких заходів дозволяє мінімізувати ризик повторної компрометації.

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 II півріччя 2025