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

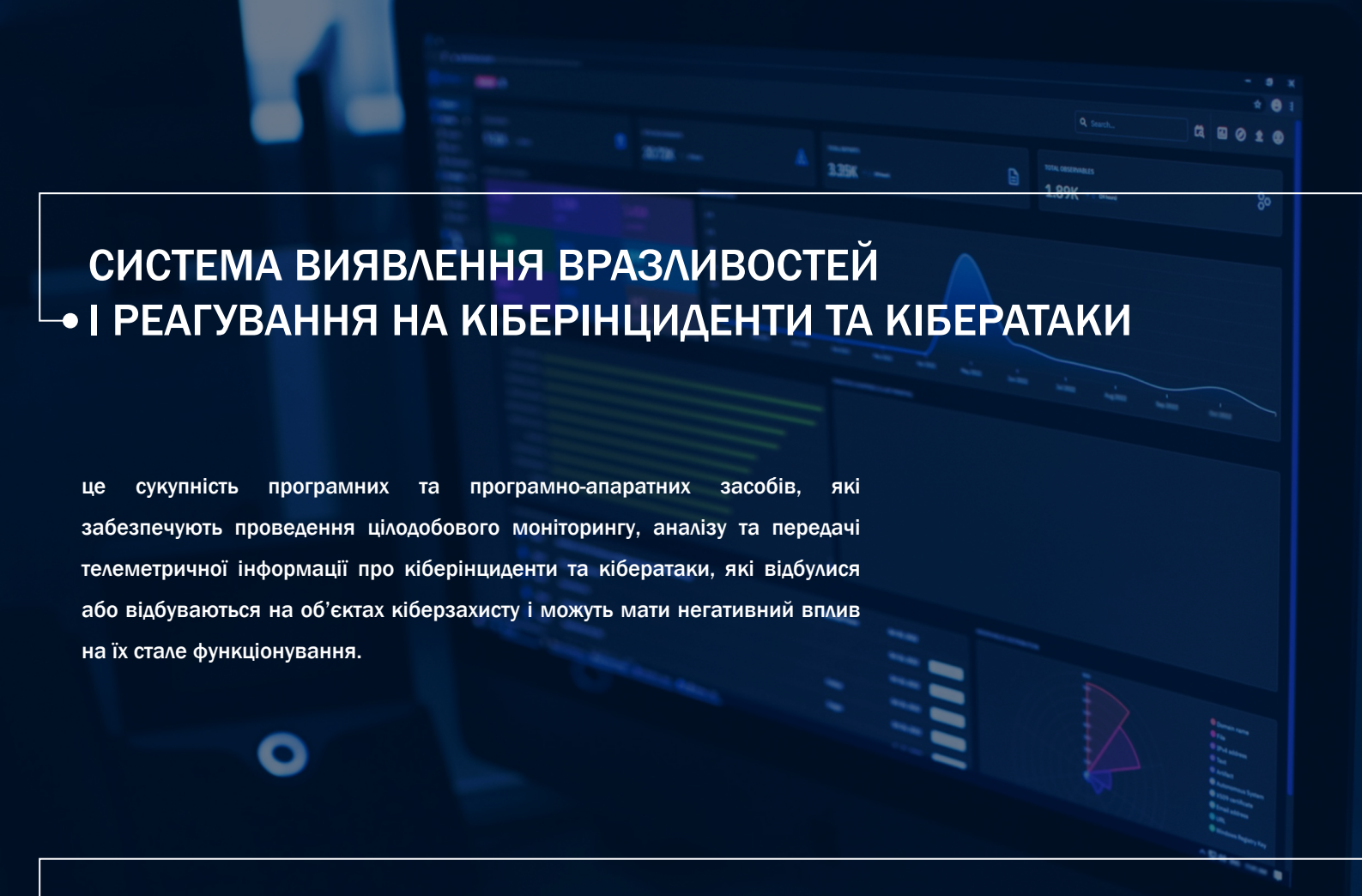
Q2

2023

ЗВІТ ПРО РОБОТУ

СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP:WHITE



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

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

- опрацьовано 3 мільярди подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;
- детектовано 122 мільйони підозрілих подій інформаційної безпеки (при первинному аналізі);
- опрацьовано 55 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);
- зафіксовано та оброблено безпосередньо аналітиками безпеки 191 кіберінцидент.

Порівняно з І кварталом 2023 року, кількість подій ІБ зросла:
• у категорії «Шкідливий програмний код» **на** 95,8%;
• у категорії «Збір інформації зловмисником» **на** 35,8%.
Загальна кількість критичних подій ІБ зросла на 38,1%.

Серед сімейств ШПЗ, детектованих у подіях ІБ категорії "02 Шкідливий програмний код" протягом звітного періоду, переважають Agent Tesla, Snake Keylogger, SmokeLoader, Formbook та Remcos.

Протягом ІІ кварталу 2023 року продовжується фіксуватися тренд до зменшення загальної кількості кібератак, націлених на українські організації різних форм власності та галузей, що спостерігається з початку 2023 року.

"Народная CyberАрмия", "WE ARE BIOODNET", "Солнцепек", "Xaknet" та "NoName057(16)" є найактивнішими проросійськими угрупованнями хактивістів, кількість атак, організованих якими протягом ІІ кварталу 2023 року, складає 89% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями.
При цьому найбільша кількість атак була націлена на фінансовий, урядовий, медійний, енергетичний та телекомунікаційний сектори.

З основними подіями у сфері кібербезпеки протягом звітного періоду можна ознайомитись із дайджестів за квітень, травень та червень, що підготовлені Національним координаційним центром кібербезпеки при Раді національної безпеки і оборони України.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

29.7k
FPS

24.7k
хостів

3.9 Tb
отримано вхідних даних

17.2 Gbit/s
швидкість вхідного трафіку сенсорної мережі

опрацьовано подій

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

детектовано підозрілих подій ІБ

при первинному аналізі

опрацьовано критичних подій ІБ

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

зареєстровано кіберінцидентів

критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

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

- 02 Шкідливий програмний код
- 03 Збір інформації зловмисником
- 10 Інше
- 04 Спроби втручання
- 07 Порушення властивостей інформації
- 06 Порушення доступності
- 01 Шкідливий (образливий) вміст
- 05 Втручання
- 08 Шахрайство
- 09 Відома вразливість

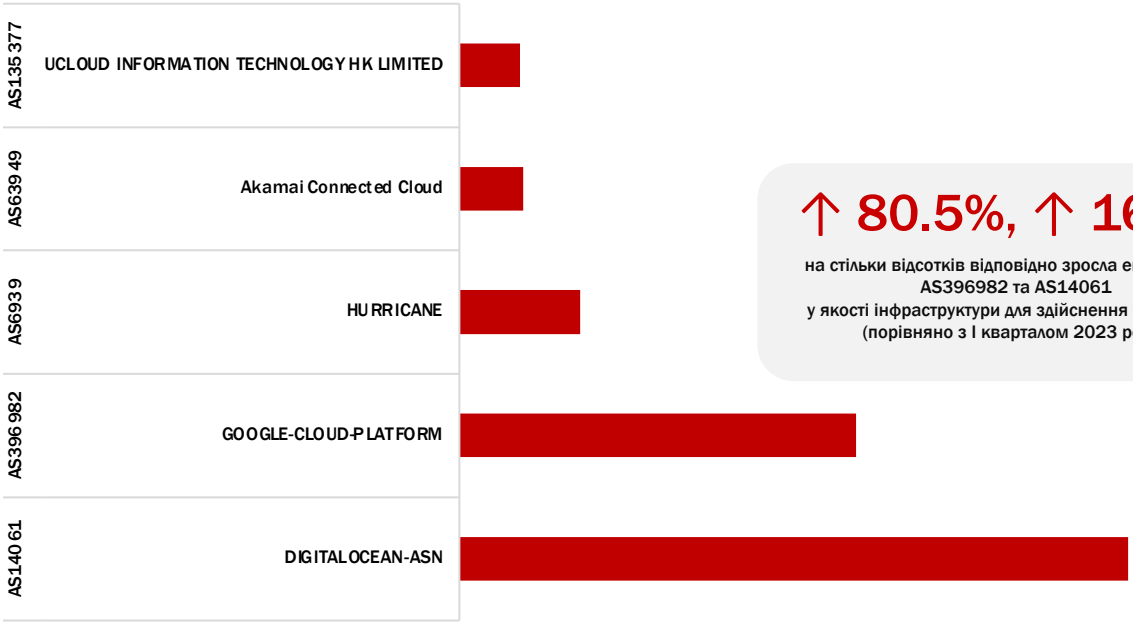
↑ 95.8% та ↑ 35.8%

на стільки відсотків відповідно зросла кількість подій ІБ категорій
"02 Шкідливий програмний код",
"03 Збір інформації зловмисником"
(порівняно з І кварталом 2023 року)

типи подій ІБ

топ 5 ASN джерел сканування

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



↑ 80.5%, ↑ 16.8%

на стільки відсотків відповідно зросла експлуатація AS396982 та AS14061 у якості інфраструктури для здійснення сканування (порівняно з I кварталом 2023 року).

топ 10 ASN джерел сканування

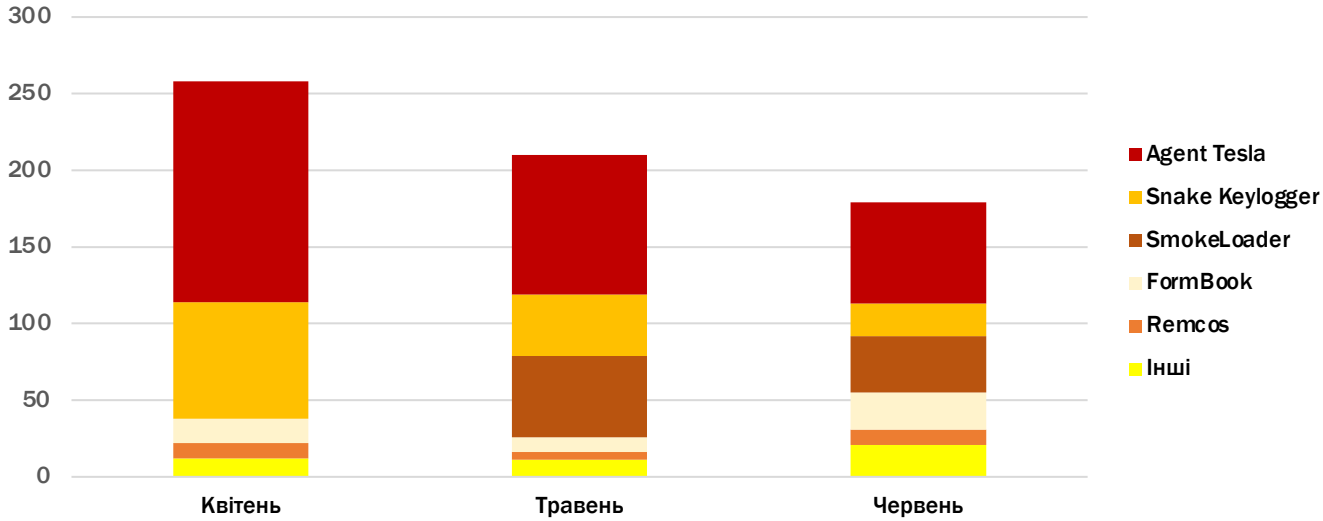
графік відображає топ 10 IP-адрес джерел (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
185.174.137.26	Finland	AS210644	AEZA GROUP Ltd	8.36%
185.246.130.106	Sweden	AS42237	W1N Ltd	1.6%
109.205.213.26	United State	AS19318	Interserver INC	1.3%
45.143.200.102	Bulgaria	AS212283	ROZA HOLIDAYS E00D	0.98%
148.153.34.102	Germany	AS63199	CDS Global Cloud Co., Ltd	0.83%
89.248.163.200	Netherlands	AS202425	IP Volume inc	0.8%
185.224.128.17	Netherlands	AS49870	Alsycon B.V.	0.52%
89.248.165.14	Netherlands	AS202425	IP Volume inc	0.51%
89.248.165.109	Netherlands	AS202425	IP Volume inc	0.47%
78.11.84.52	Netherlands	AS202425	IP Volume inc	0.45%

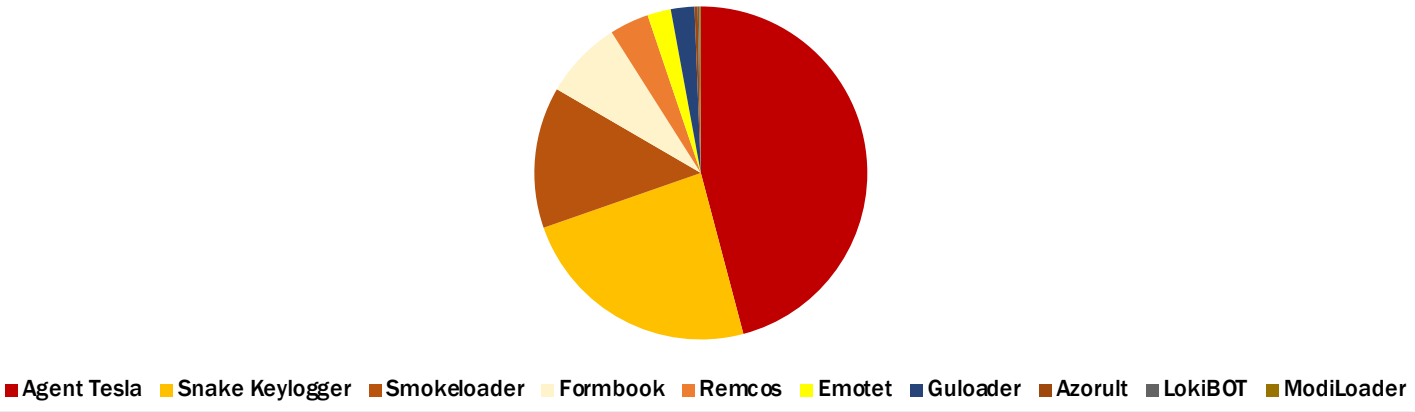
60 075

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

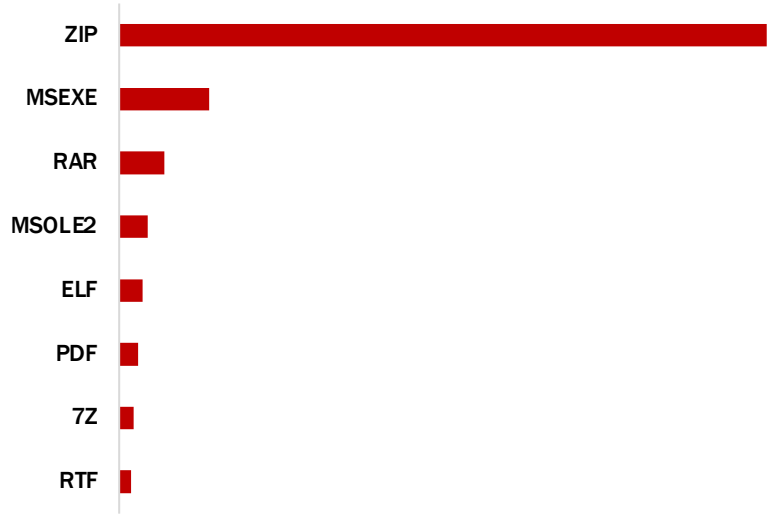
часовий розподіл подій ІБ категорії "02 Шкідливий програмний код" за сімействами ШПЗ



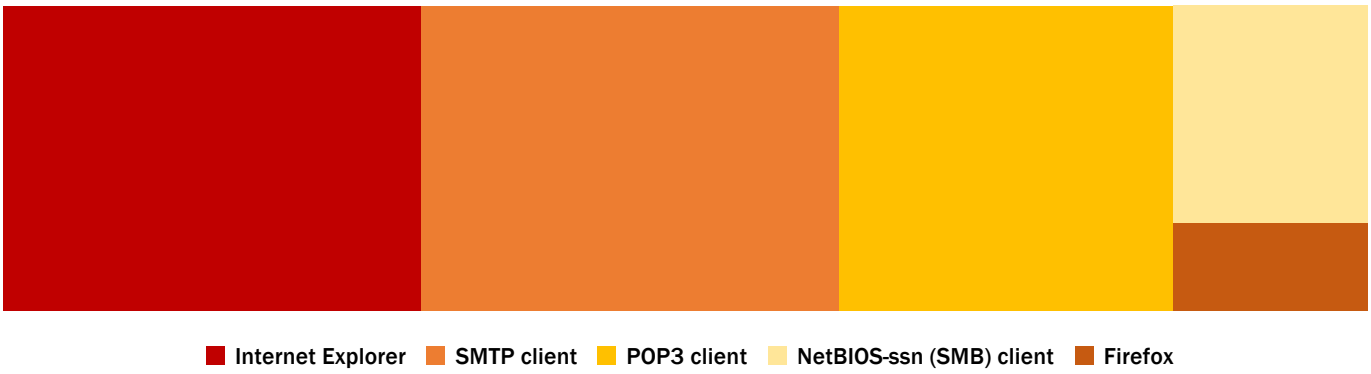
типи сімейств ШПЗ, детектовані в подіях ІБ категорії "02 Шкідливий програмний код"



за форматом розповсюджуваного ШПЗ

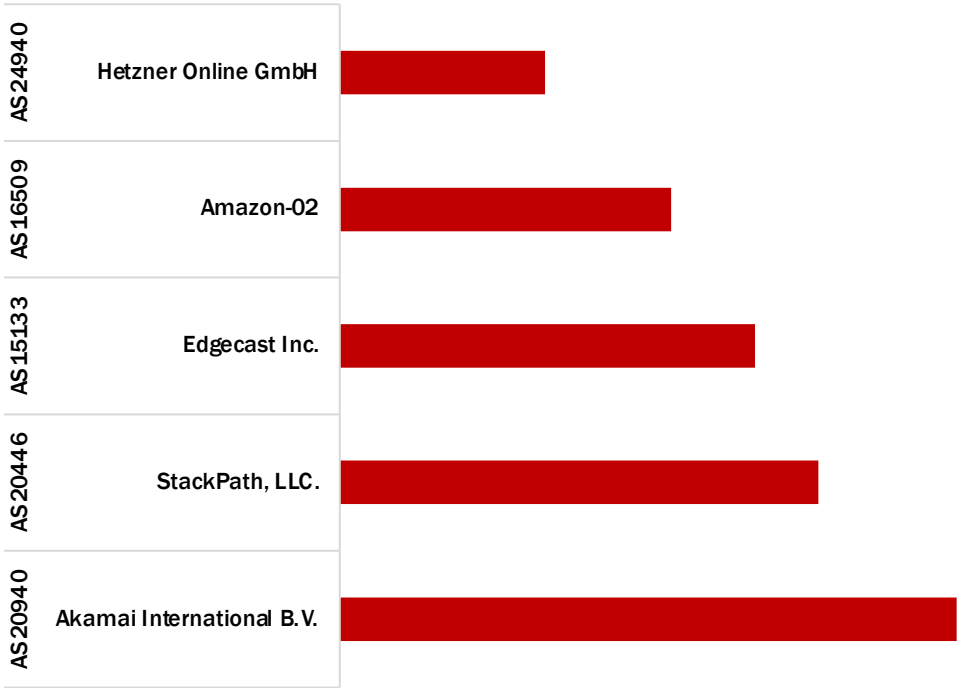


за асоційованим ПЗ клієнтів



топ 5 джерел - ASN

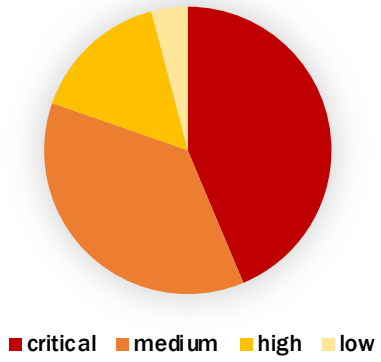
графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного розповсюдження ШПЗ



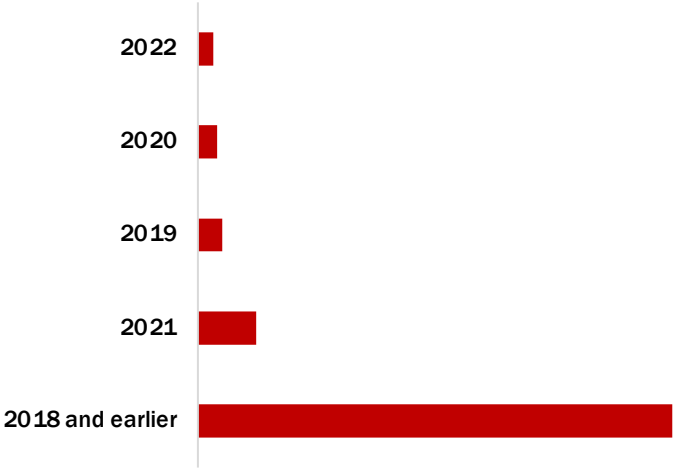
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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

якісна оцінка за CVSS Base Score

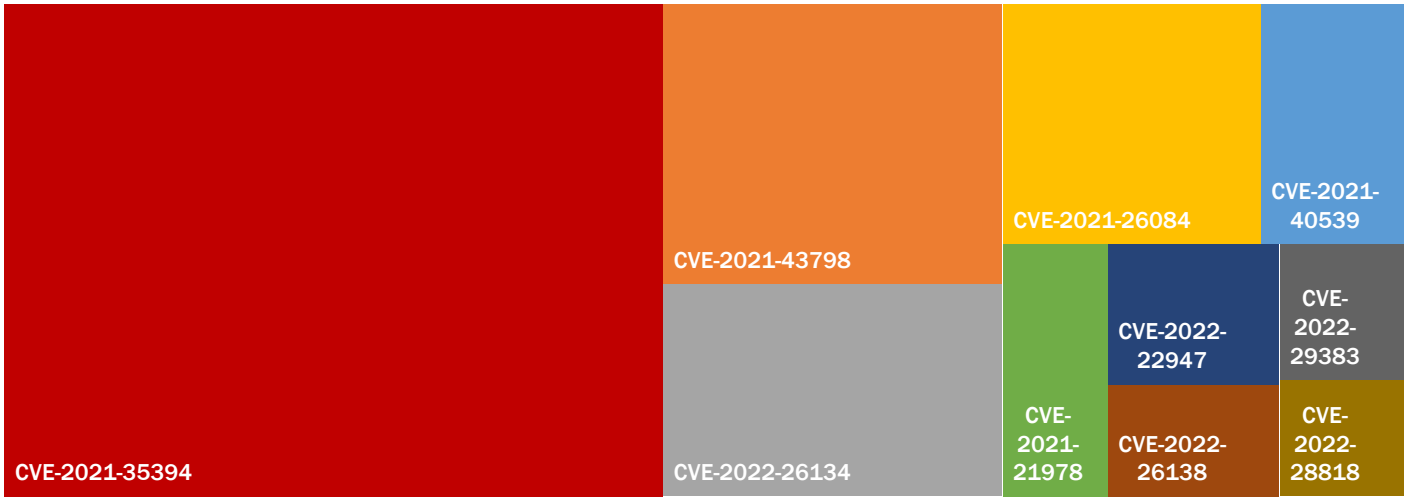
згідно з визначеним специфікацією CVSSv3.1 підходом до співставлення оцінок CVSS Base Score (1-10) до якісної шкали оцінювання



експлуатовані CVE за роком реєстрації



топ 10 експлуатовуваних CVE



російсько-УКРАЇНСЬКА КІБЕРВІЙНА

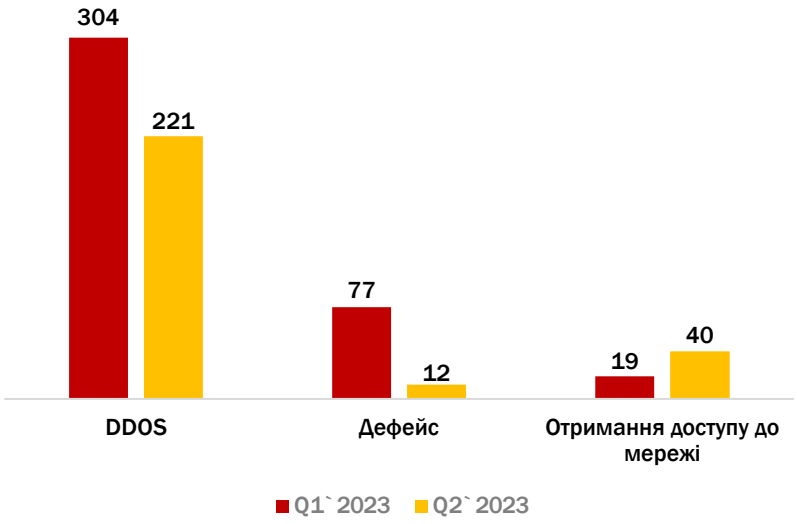
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу даних з відкритих комунікаційних каналів проросійських угруповань хактивістів, що публікують анонси та результати майбутніх або вже реалізованих кібератак, таргетованих на українські організації, а також проводять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

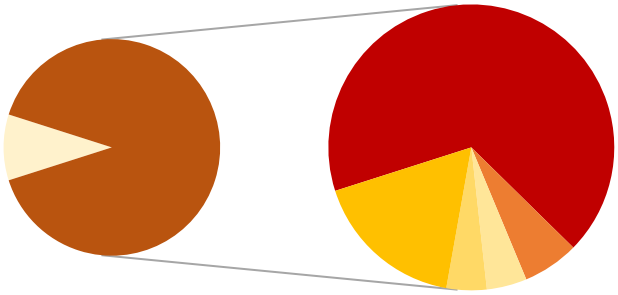
динаміка активності проросійських хакерських угруповань за типами

Показник довіри до даних, отриманих із відкритих комунікаційних каналів проросійських угруповань хактивістів, 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.

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

Протягом II кварталу 2023 року продовжується фіксуватися тренд до зменшення загальної кількості кібератак, націлених на українські організації різних форм власності та галузей, що спостерігається з початку 2023 року.

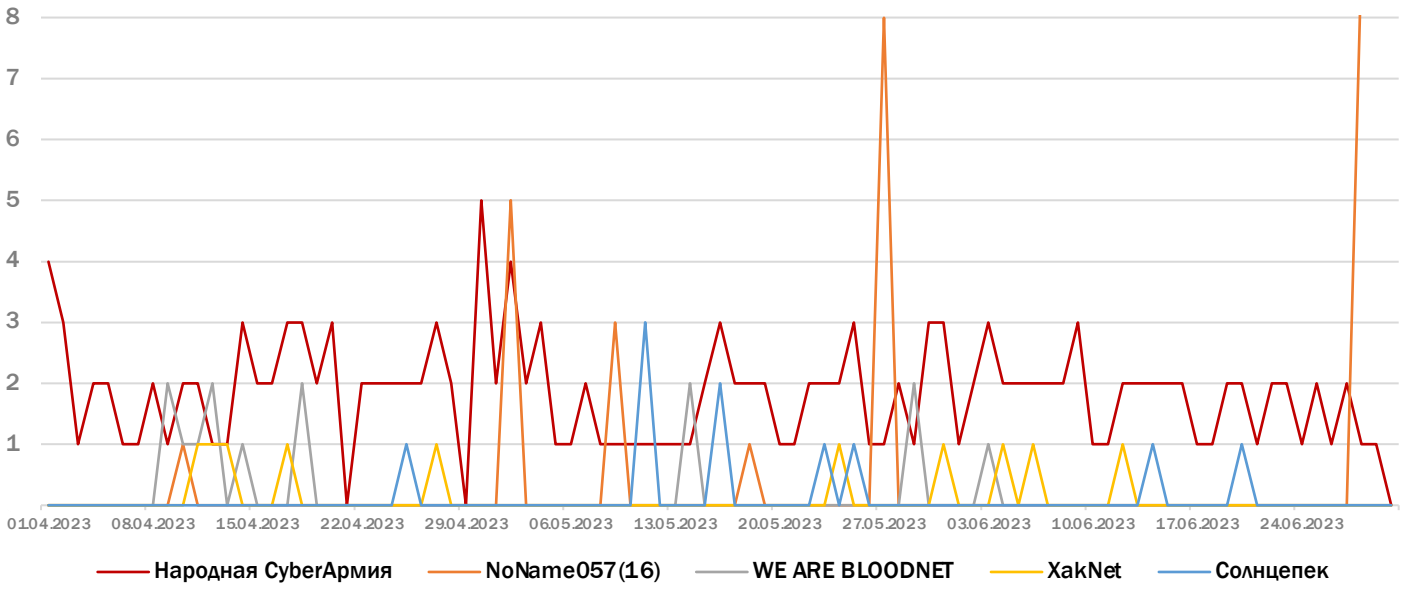




- Народная CyberАрмия
- NoName057(16)
- WE ARE BLOODNET
- XakNet
- Солнцепек
- Інші

5 найактивніших проросійських угруповань хактивістів, кількість атак, організованих якими протягом II кварталу 2023 року, складає 89% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями протягом звітного періоду

динаміка активності проросійських хакерських угруповань



російсько-УКРАЇНСЬКА КІБЕРВІЙНА

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

Зокрема, 4 квітня в Telegram-каналі було оголошено про запуск офіційного навчання від команди KillNet «ДАРК ШКОЛИ». Перелік 9 курсів для «ведення професійної кібервійни та примноження балансу власного гаманця» включає:

1) DDOS(L7/4);
2) Арбітраж Google AdWords;
3) Фейки (створення, просування, прибуток);
4) Кардинг (Європа, Америка);
5) OSINT/DEANON (кіберрозвідка);
6) Pegasus (шпигунське ПЗ для Android/IOS);
7) Соціальна інженерія;
8) Методи кібервійни (психологія і вплив на підсвідомість будь-якого учасника всесвітньої павутини);
9) Диверсія в мережі (методика).

Навчання доступне чотирма мовами – російською, англійською, іспанською та гінді. Раніше, до квітня 2023 року, KillNet не створювали та не посилались на гінді-мовний контент.

24 травня було опубліковано новину про розпуск основного складу Killnet з причини, що 50 угруповань (1250 людей) "займаються не хактивізмом", а також велика кількість учасників керується особистими мотивами, просуваючи власні сервіси, користуючись популярністю угруповання. Того ж дня було анонсовано набір нових учасників.

З 28 квітня офіційно відкритим є проект DDoS-ботнету Tesla, який використовує методи MACAN-TLS, HTTP-FLOOD та SMYKL-FLOOD для здійснення атак. 23 травня афішовано розробку оновлення TESLA-BOTv3, що буде включати обхід статичних і динамічних рейт-лімітів, класичного UAM, CAPTCHA та DDG, а також режим DOOMINATE. Незважаючи на попередню заяву Radis (лідера угруповання Anonymous Russia і головного розробника Tesla Botnet) від 4 червня, реліз запланований на серпень 2023 року.

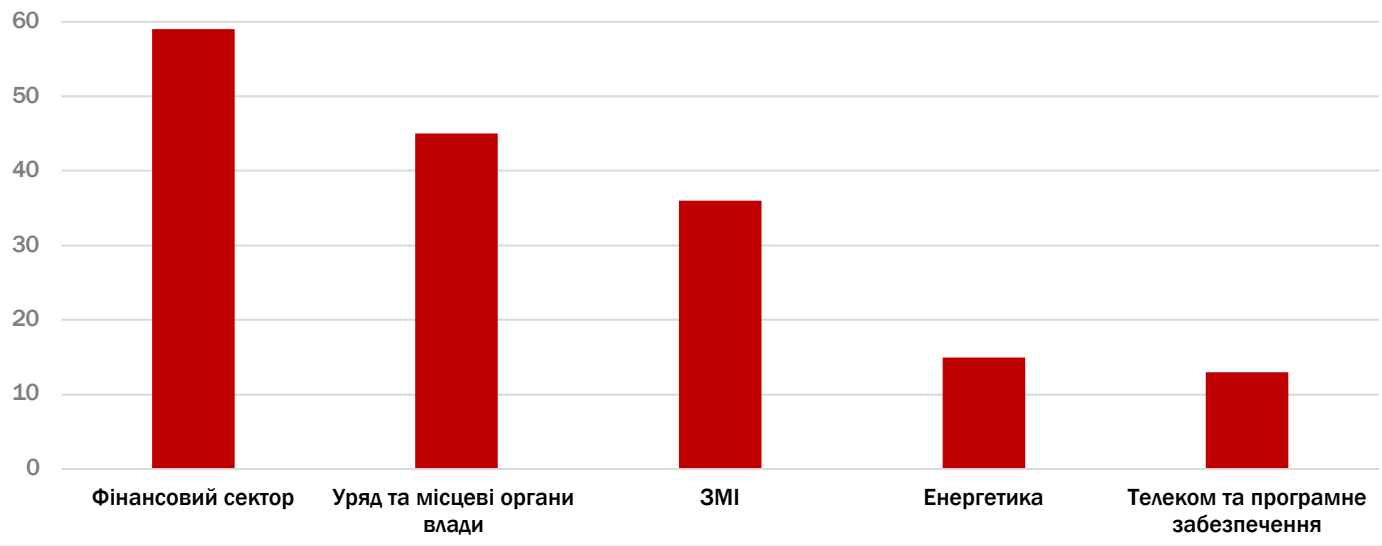
З 1 травня угруповання PHOENIX розширило перелік власних TTP, доповнивши його поширенням персональних даних громадян "недружніх країн" – членів НАТО та ЄС. Також, з 27 березня цього року в їх Telegram-каналі поширюються скомпрометовані дані облікових записів до платформ, функціонування яких асоціюється з діяльністю іноземних країн.

11 травня в Telegram-каналі "Солнцепек" (адміністратори якого згадуються як послідовники "Джокера ДНР"), що є активним щонайменше з 25 квітня 2022 року і до цього функціонував виключно як база персональних даних українців, нібито задіяних у воєнних діях, було афішовано "початок кібервійни Україні". Відповідно, починаючи з 11 травня на каналі періодично публікуються новини, що стосуються злому сайтів та отримання доступу до мереж українських організацій (зокрема, провайдерів та державних відомств).

24 травня угруповання "Anonymous Sudan" розширило перелік власних TTP, доповнивши його прийомом викупів за запобігання та припинення DDoS атак. Першим випадком такої активності стала атака на Скандинавську систему авіаліній, первинна величина викупу за припинення DDoS атаки на яку становила $3,500.

5 червня в Telegram-каналі "Devils Sec – 1967", який функціонує з 26 травня, було анонсовано координування операцій з угрупованням KillNet: "Ми заявляємо про солідарність із росією в її кібератаках на Україну і будемо таргетувати дуже критичні об'єкти для української сторони." Проте, зважаючи на допис від 14 червня, "Devils Sec – 1967" прагне деасоціювати себе з виключно проросійською позицією.

розподіл активності проросійських хакерських угруповань за секторами



НОРМАТИВНО-ПРАВОВА БАЗА

- **Закон України «Про основні засади забезпечення кібербезпеки України»**, що визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

- **Постанова Кабінету Міністрів України від 23.12.2020 №1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки»**, що визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об'єктів кіберзахисту, визначених частиною другою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України».

КОНТАКТИ

Оперативний центр
реагування на кіберінциденти

Державний центр кіберзахисту

Державна служба спеціального зв’язку
та захисту інформації України

e-mail: soc@scpc.gov.ua
тел.: +38 (044) 281 87 37