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

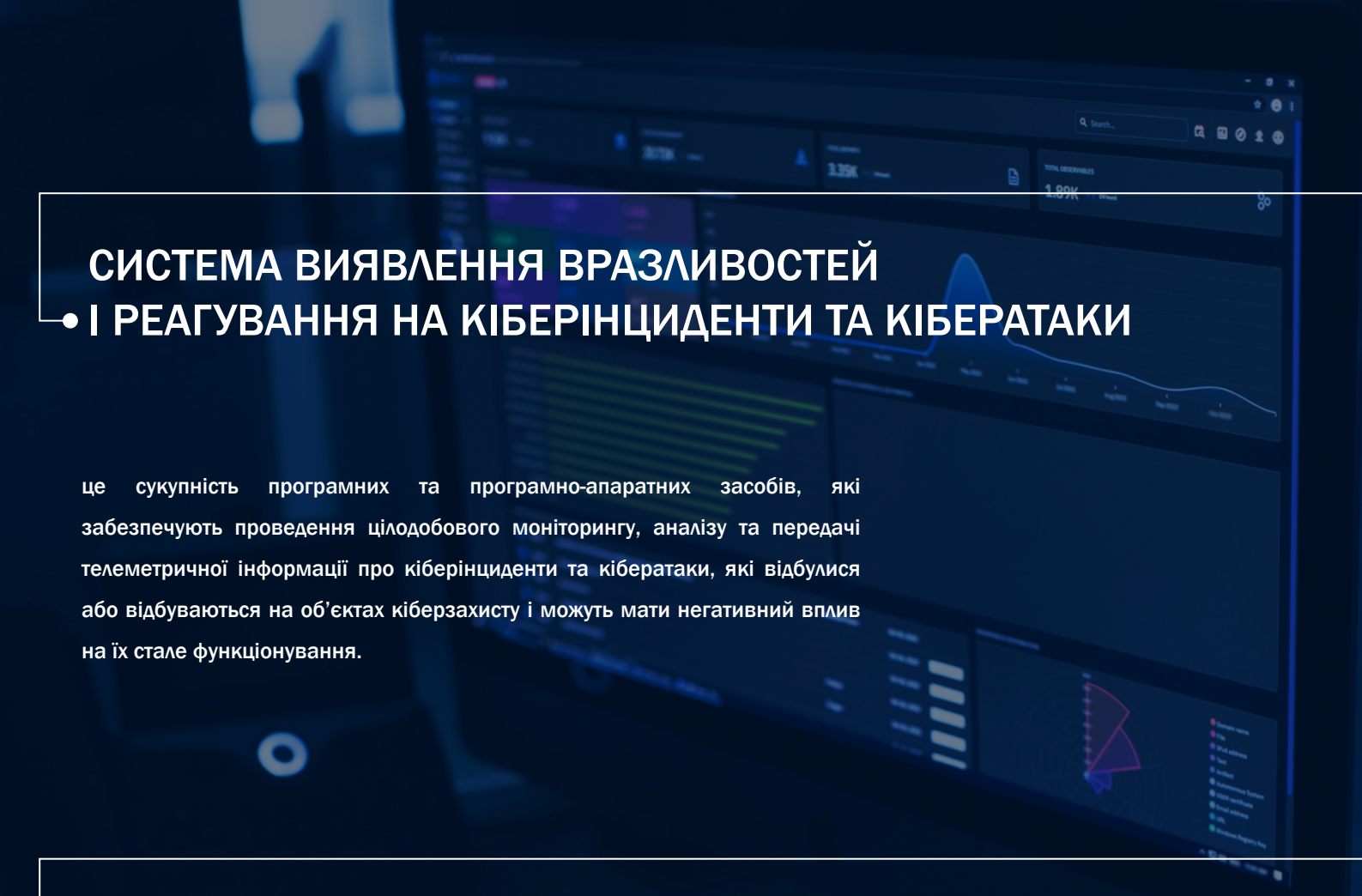
Q1

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

- опрацьовано 9 мільярдів подій, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;
- детектовано 7 мільйонів підозрілих подій інформаційної безпеки (при первинному аналізі);
- опрацьовано 34 тисячі критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);
- зафіксовано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти.

BARAT, Emotet, Cobalt Strike та Meris представляють найчастіше експлуатовану С2 інфраструктуру, детектовану як джерело спроб мережевих вторгнень або порушень політик безпеки організацій, виявлених у вхідному мережевому трафіку Підсистемою збору телеметрії Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Серед сімейств ШПЗ, детектованих у подіях ІБ категорії “02 Шкідливий програмний код” протягом звітного періоду, переважають Snake Keylogger, Agent Tesla, LokiBot, PurpleFox та Formbook.

З початку 2023 року помітно (з різницею у 1.5-2.9 разів для різних секторів) знизилась кількість атак, організованих проросійськими угрупованнями хактивістів, націлених на комерційний, фінансовий сектор, уряд та місцеві органи влади, сектор безпеки та оборони (порівняно з IV кварталом 2022 року). При цьому інтенсивність атак на сектор енергетики та ЗМІ залишається на тому ж рівні.
XakNet, NoName057(16), RussianHackersTeam, RaHDit та Free Civillian є найактивнішими проросійськими угрупованнями хактивістів, кількість атак, організованих якими протягом І кварталу 2023 року, складає 90% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями протягом звітного періоду.

Згідно популярного Кібертрекеру російсько-Української війни, підтримуваного користувачем @Cyberknow20, месенджер Telegram активно використовується проросійськими хактивістами як провідна платформа для організації зловмисної активності. Інтерес до платформи, як до "екосистеми кіберзлочинності", підтверджується нещодавним релізом статті Telegram - How a messenger turned into a cybercrime ecosystem by 2023 від компанії KELA, що займається кіберрозвідкою.

З початку 2023 року , порівняно з IV кварталом 2022 року, зафіксовано зменшення загальної кількості кібератак, організовуваних угрупованнями проросійських хактивістів, проте їх систематичність та інтенсивність продовжує залишатись на високому рівні. Але, зважаючи на посилення кремлем інформаційних операцій щодо виправдання неспровокованого вторгнення в Україну і, таким чином, створення умов для затяжної війни в Україні, немає фундаментальних підстав вважати, що тренд до зменшення кількості кібератак, націлених на українські організації різних форм власності та галузей, буде зберігатись і надалі.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

9.6 k
FPS

17.3 k
хостів

2.5 Tb
отримано вхідних даних

13.2 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

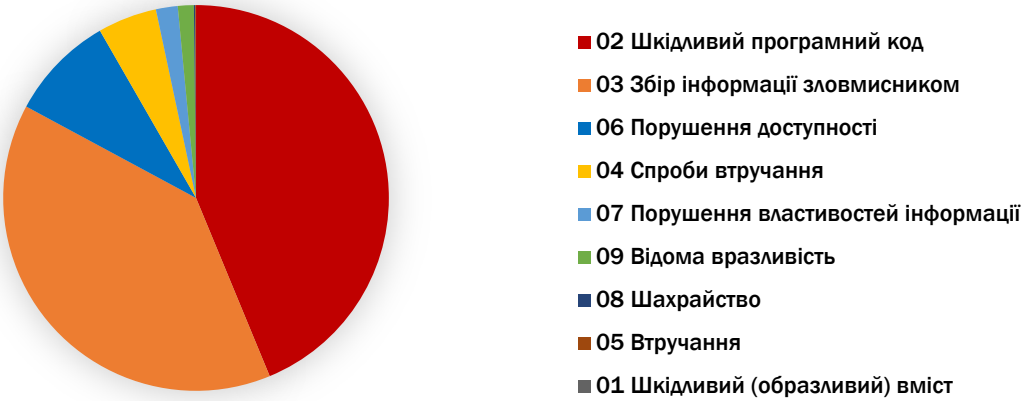
критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

СТАТИСТИКА ПОДІЙ ІБ

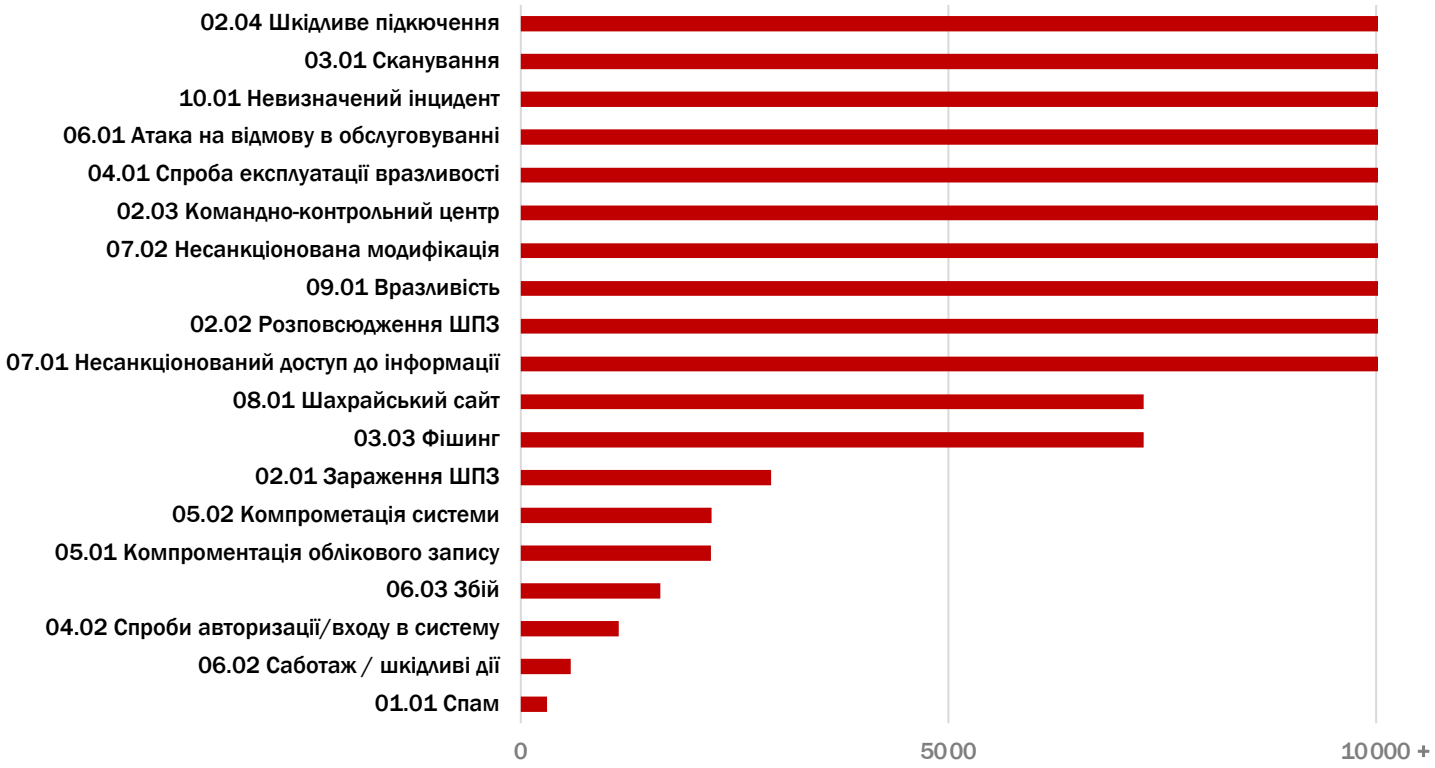
КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

представлена згідно Переліку категорій кіберінцидентів схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України

категорії подій ІБ



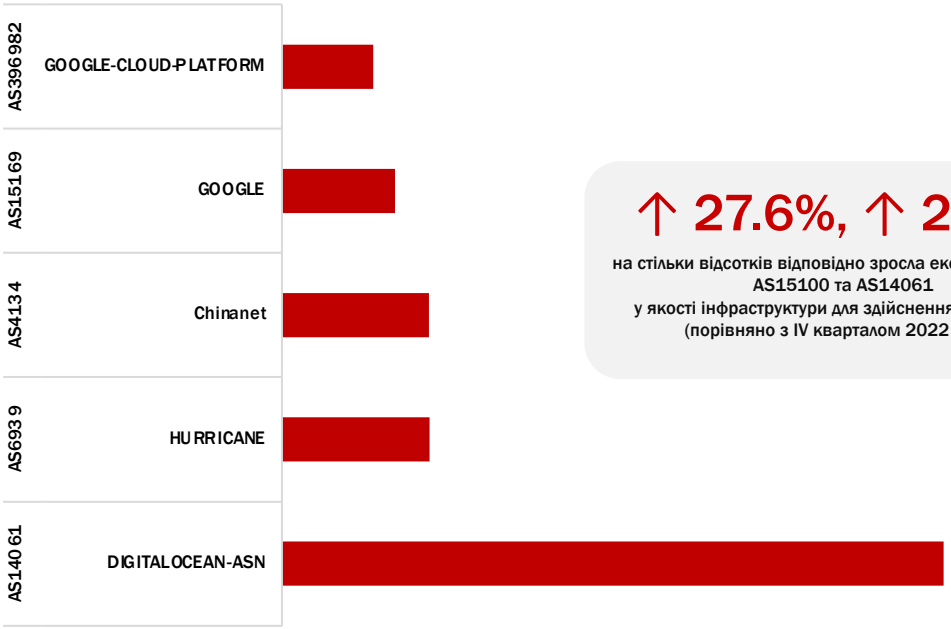
типи подій ІБ



2023 (Q1)

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



↑ 27.6%, ↑ 218%

на стільки відсотків відповідно зросла експлуатація ASN AS15100 та AS14061 у якості інфраструктури для здійснення сканування (порівняно з IV кварталом 2022 року).

топ 10 ASN джерел сканування

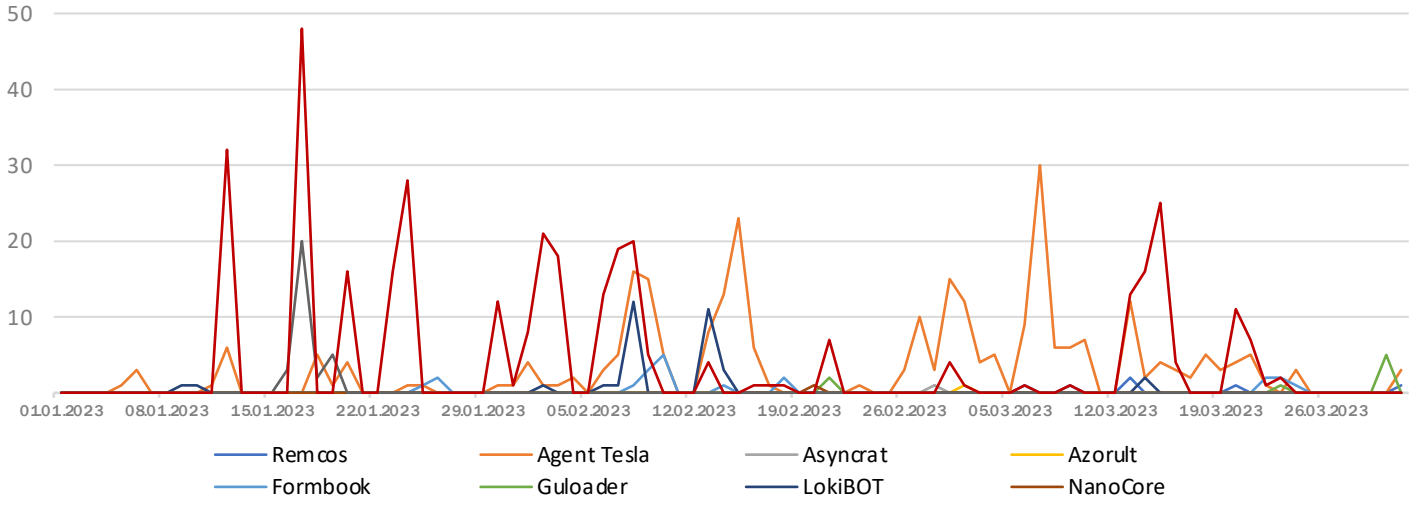
графік відображає топ 10 IP-адрес джерел (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
91.191.209.218	Bulgaria	AS57509	L&L Investment Ltd.	0.95
103.14.224.123	Vietnam	AS135918	Viet Digital Technology Liability Company	0.61
79.124.59.74	Bulgaria	AS50360	Tamatiya EOOD	0.58
185.224.128.17	Netherlands	AS49870	Alsycon B.V.	0.30
51.158.46.120	France	AS12876	ONLINE S.A.S.	0.29
170.39.218.4	France	AS49434	Harmony Hosting SARL	0.25
89.248.163.200	Netherlands	AS202425	IP Volume inc	0.19
89.248.165.14	Netherlands	AS202425	IP Volume inc	0.16
146.88.240.4	The United States of America	AS20052	Arbor Networks, Inc.	0.15
89.248.165.209	Netherlands	AS202425	IP Volume inc	0.14

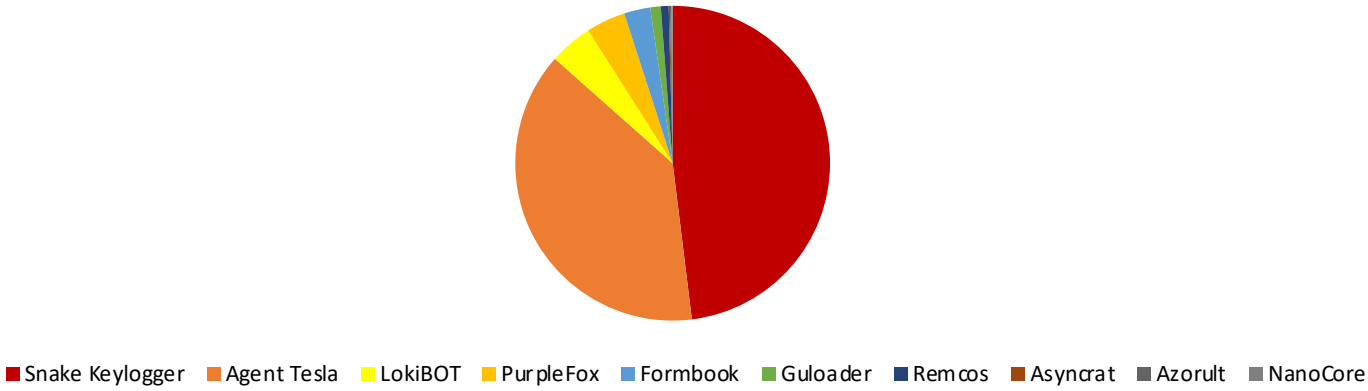
43 946

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

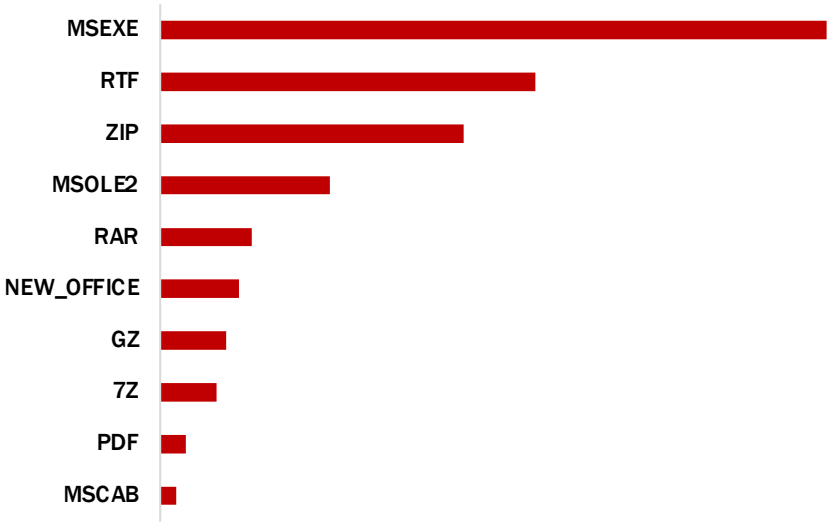
часовий розподіл подій ІБ категорії “02 Шкідливий програмний код” за сімействами ШПЗ



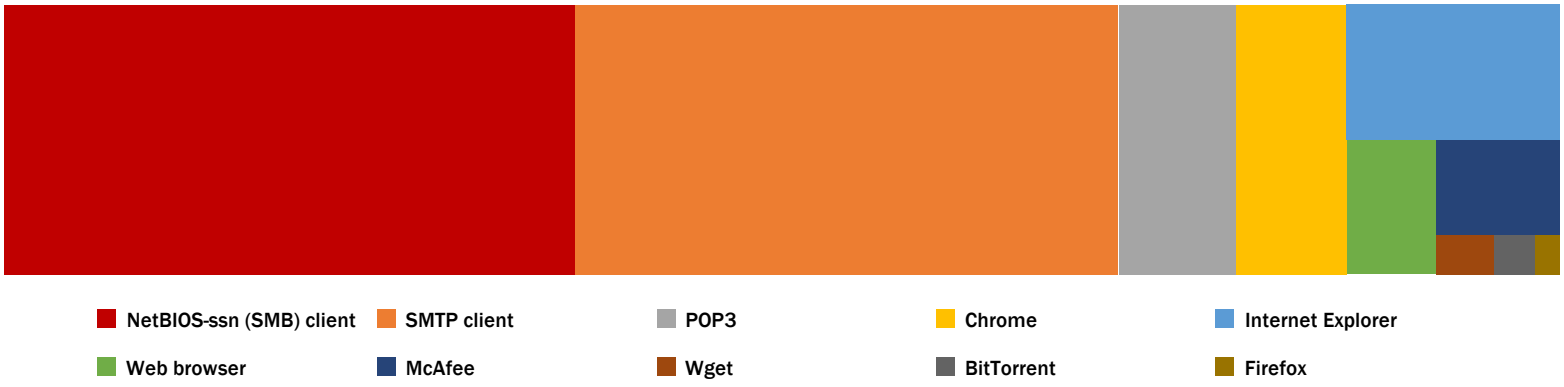
типи сімейств ШПЗ, детектовані в подіях ІБ категорії “02 Шкідливий програмний код”



за форматом розповсюджуваного ШПЗ

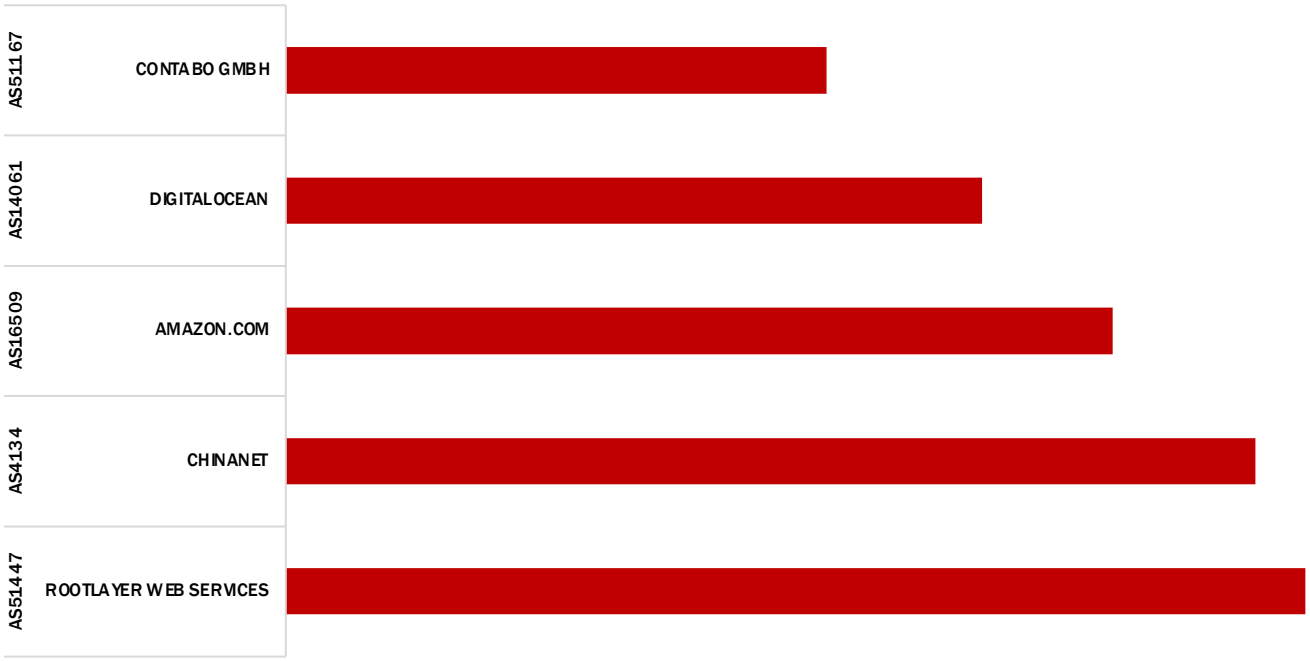


за асоційованим ПЗ клієнтів



топ 5 джерел - ASN

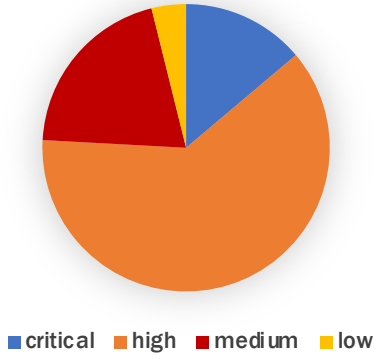
графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного розповсюдження ШПЗ під час звітного періоду



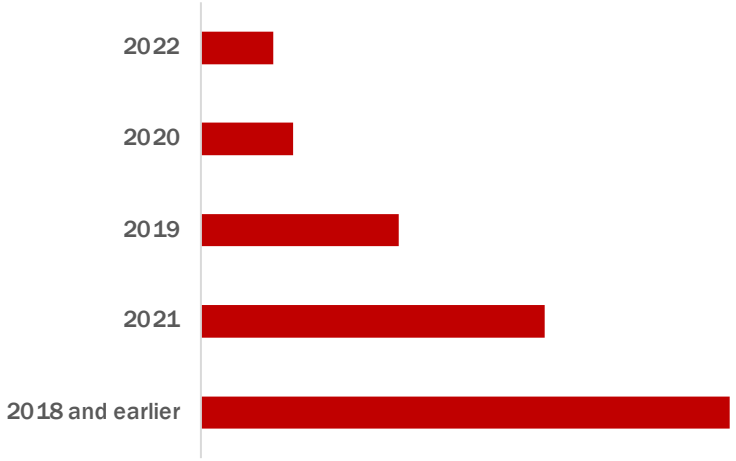
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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

якісна оцінка за CVSS Base Score

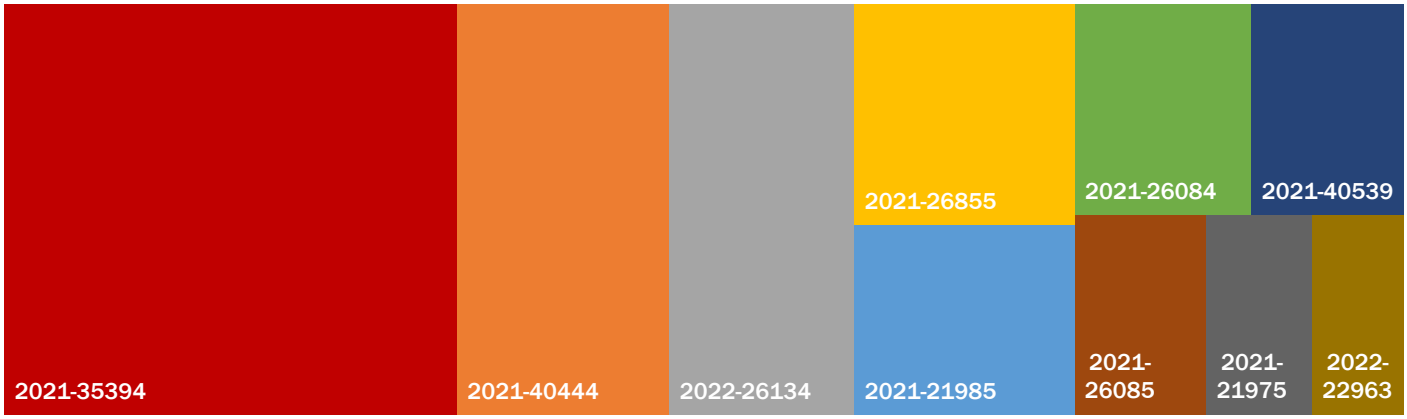
згідно з визначеним специфікацією CVSSv3.1 підходом до співставлення оцінок CVSS Base Score (1-10) до якісної шкали оцінювання



експлуатовані CVE за роком реєстрації



топ 10 експлуатовуваних CVE



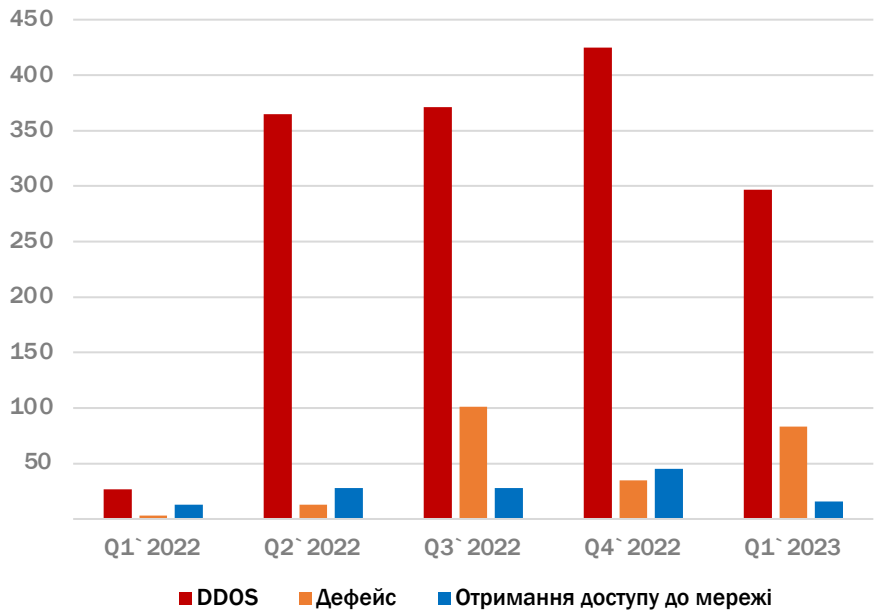
російсько-УКРАЇНСЬКА КІБЕРВІЙНА

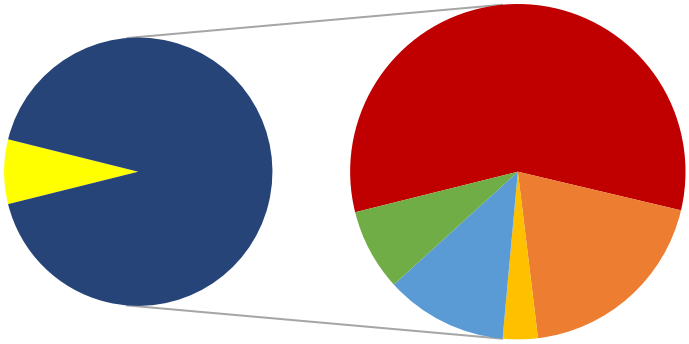
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу даних з відкритих комунікаційних каналів проросійських угруповань хактивістів, що публікують анонси та результати майбутніх або вже реалізованих кібератак, таргетованих на українські організації, а також проводять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

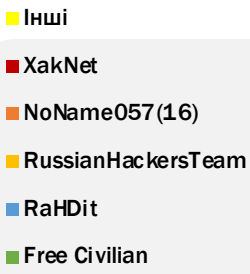
З початку 2023 року (порівняно з IV кварталом 2022 року) зафіксовано зменшення загальної кількості кібератак, організовуваних угрупованнями проросійських хактивістів, проте їх систематичність та інтенсивність продовжує залишатись на високому рівні.

Зважаючи на посилення кремлем інформаційних операцій щодо виправдання неспровокованого вторгнення в Україну і, таким чином, створення умов для затяжної війни в Україні, немає фундаментальних підстав вважати, що тренд до зменшення кількості кібератак, націлених на українські організації різних форм власності та галузей, буде зберігатись і надалі.

динаміка активності проросійських хакерських угруповань за типами атак

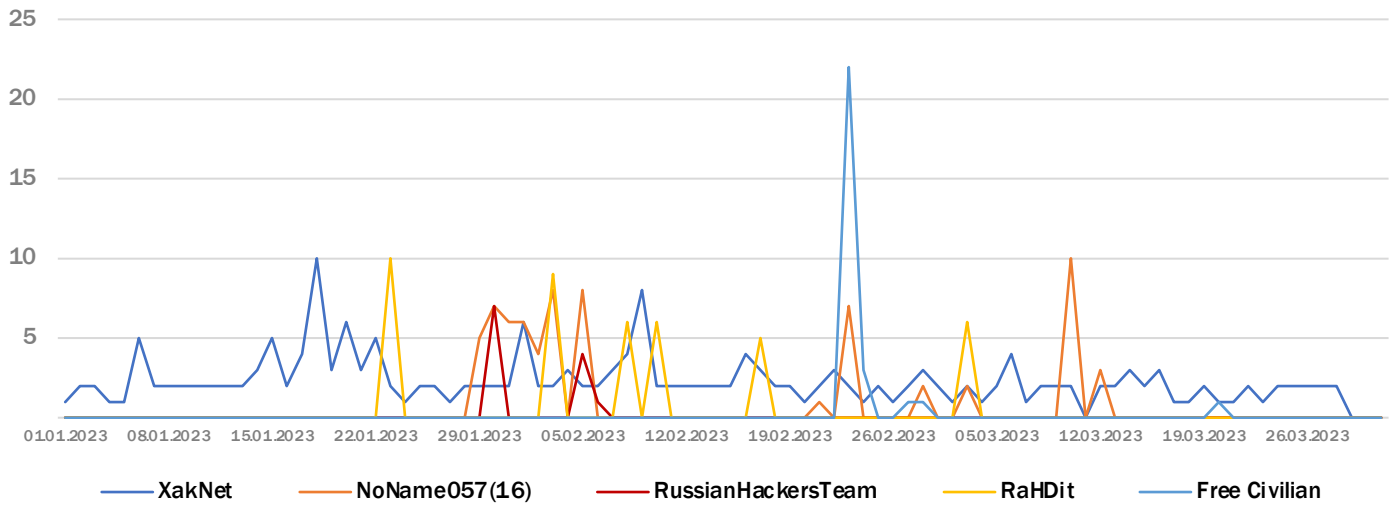






5 найактивніших проросійських угруповань хактивістів, кількість атак, організованих якими протягом I кварталу 2023 року, складає 90% від загальної кількості зафіксованих атак, організованих аналогічними угрупованнями протягом звітного періоду

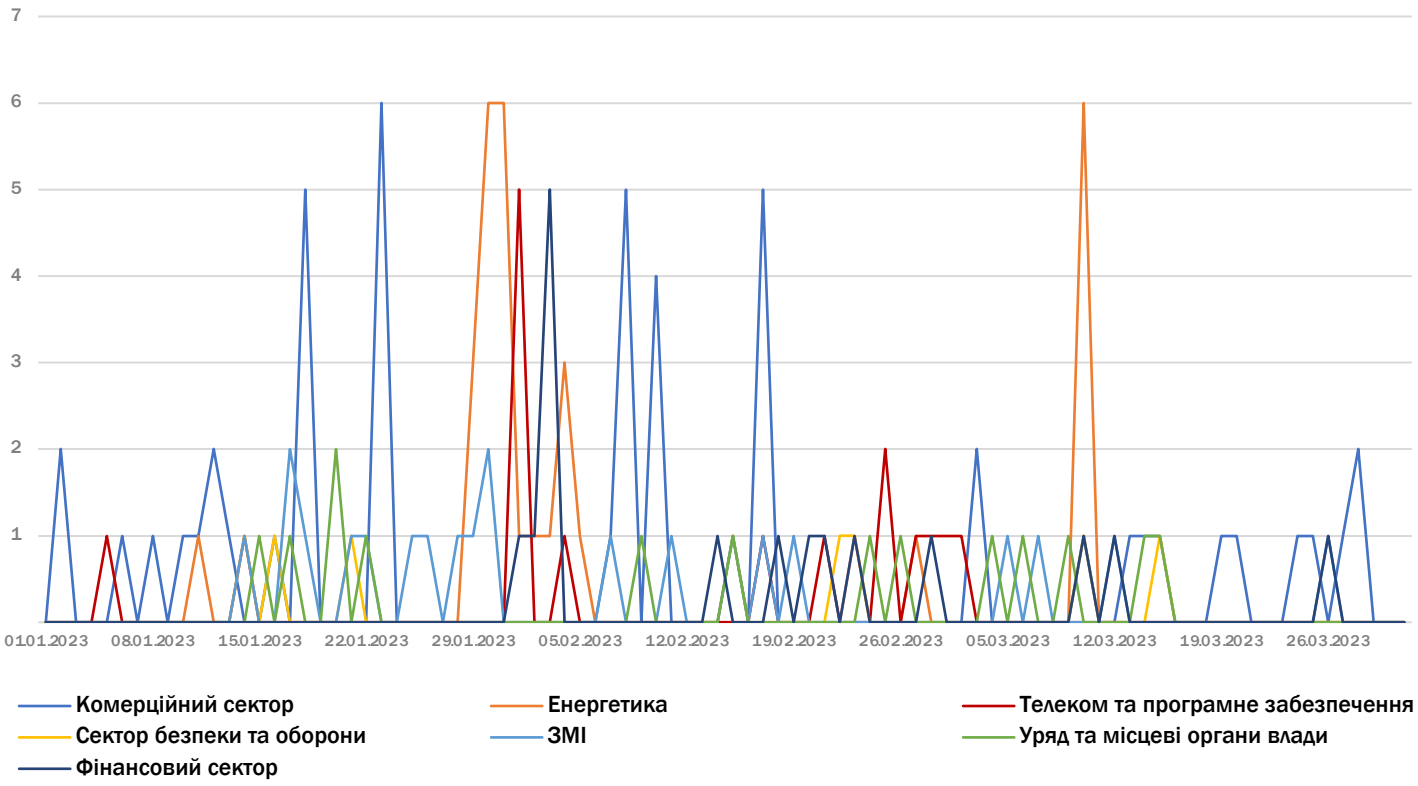
динаміка активності проросійських хакерських угруповань



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

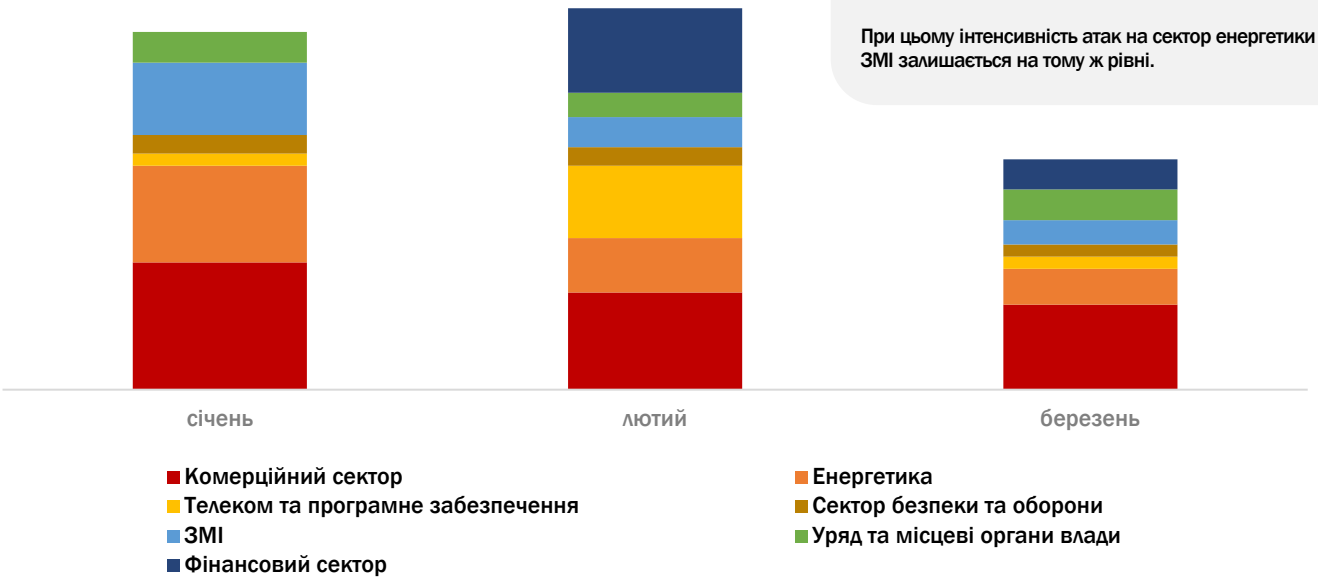
динаміка активності проросійських хакерських угруповань за секторами



розподіл активності проросійських хакерських угруповань за секторами

З початку 2023 року (порівняно з IV кварталом 2022 року) помітно (з різницею у 1.5-2.9 разів для різних секторів) знизилась кількість атак, організованих проросійськими угрупованнями хактивістів, націлених на комерційний, фінансовий сектор, уряд та місцеві органи влади, сектор безпеки та оборони.

При цьому інтенсивність атак на сектор енергетики та ЗМІ залишається на тому ж рівні.



ШКІДЛИВА C2 ІНФРАСТРУКТУРА

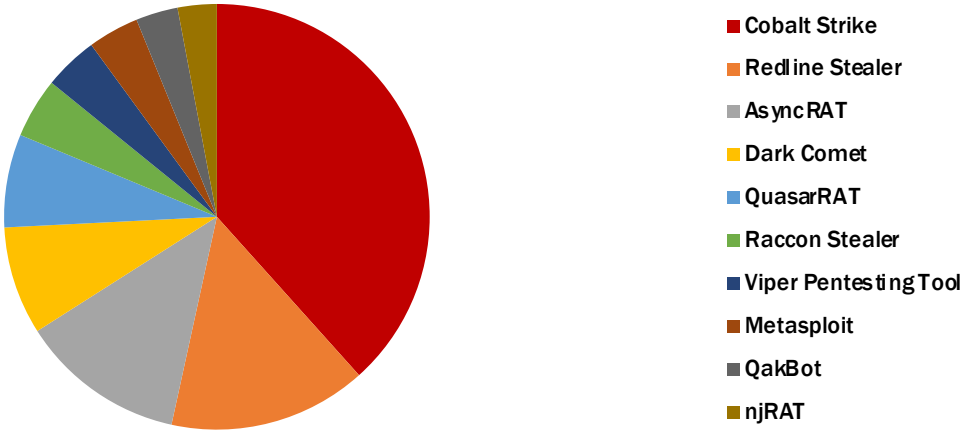
З початку 2023 року було зафіксовано понад 80 000 спроб мережевого вторгнення та 600 вихідних з'єднань з унікальними командно-контрольними серверами (C2) (ідентифікованими як такі згідно з даними, отриманими з платформи Recorded Future).

За допомогою методів проактивного сканування та збору даних Recorded Future постійно відстежує створення та модифікацію інфраструктури, експлуатовуваної інструментами пост-експлуатації, кастомними шкідливими програмами та троянами віддаленого доступу з відкритим кодом у зловмисних цілях.

Серед таких серверів, причетних до потенційно шкідливої мережевої активності та порушень політик безпеки організацій, у першому кварталі 2023 року переважають OST (Cobalt Strike, Metasploit), RAT (BARAT, AsyncRAT, QuasarRAT, njRAT) та сімейства ботнетів (Emotet, Mirai, Meris).

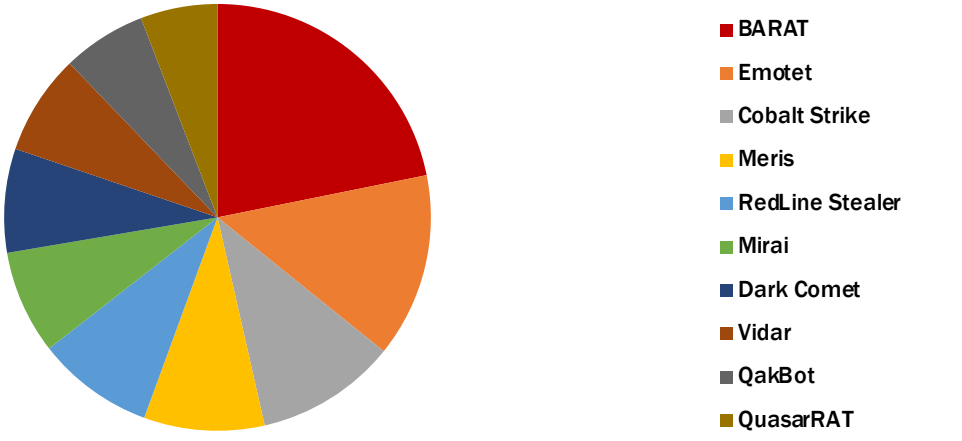
C2 детектування в подіях ІБ, пов'язаних із вихідним трафіком

на діаграмі представлено інфраструктуру управління та контролю (C2), залучену до потенційно шкідливої мережевої активності або порушень політик безпеки організацій, виявлених у вихідному мережевому трафіку Підсистемою збору телеметрії Системи виявлення вразливостей та реагування на кіберінциденти/кібератаки.



C2 детектування в подіях ІБ, пов'язаних із вхідним трафіком

на діаграмі представлено інфраструктуру управління та контролю (C2), залучену до потенційно шкідливої мережевої активності або порушень політик безпеки організацій, виявлених у вхідному мережевому трафіку Підсистемою збору телеметрії Системи виявлення вразливостей та реагування на кіберінциденти/кібератаки.



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