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

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:

- впровадження 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 та 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 24.06.2022 № 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 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 та 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 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 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було:

• **опрацьовано 18 мільярди подій**, отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки;

• **детектовано 133 мільйони підозрілих подій ІБ** (при первинному аналізі);

• **опрацьовано 148 тисяч критичних подій ІБ** (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу);

• **зафіксовано та оброблено** безпосередньо аналітиками безпеки **1105 кіберінцидентів**. Кількість зареєстрованих кіберінцидентів зросла на 62.5% порівняно з попереднім роком.

Також протягом 2023 року до Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки протягом звітного періоду було **підключено 24 нових об'єктів кіберзахисту**, що належать до урядового (22), енергетичного (1) та військового (1) секторів.

Серед автономних систем (**AS**), **інфраструктура яких найчастіше ідентифікувалась як джерело активного сканування** під час звітного періоду, можна виокремити **"Google", "Hurricane", "Google-Cloud-Platform", "Cloudflarenet", "DigitalOcean-ASN"**.

Підсистемами, що належать до складу Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, в автоматичному режимі було детектовано 1 516 861 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, Formbook**.

СТРУКТУРА ТА ОРГАНІЗАЦІЯ

ОПИС ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ, КОМАНД, ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

Фахівці

ОЦРК

20+

Фахівців

Засоби кіберзахисту

Підсистема збору телеметрії	Підсистема захисту кінцевих точок	Сканування вразливостей
NDR	**EDR**	**VA**
Підключено організацій:	Підключено організацій:	Підключено організацій:
64 +24	27 +24	33
Передано сенсорів:	Захищено хостів:	Перевірено активів:
65 +24	4200+	820+

Сектори та організації

Об’єкти кіберзахисту

62 +22	1 +1	2 +1
Урядовий	Енергетичний	Військовий

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

зареєстровано кіберінцидентів

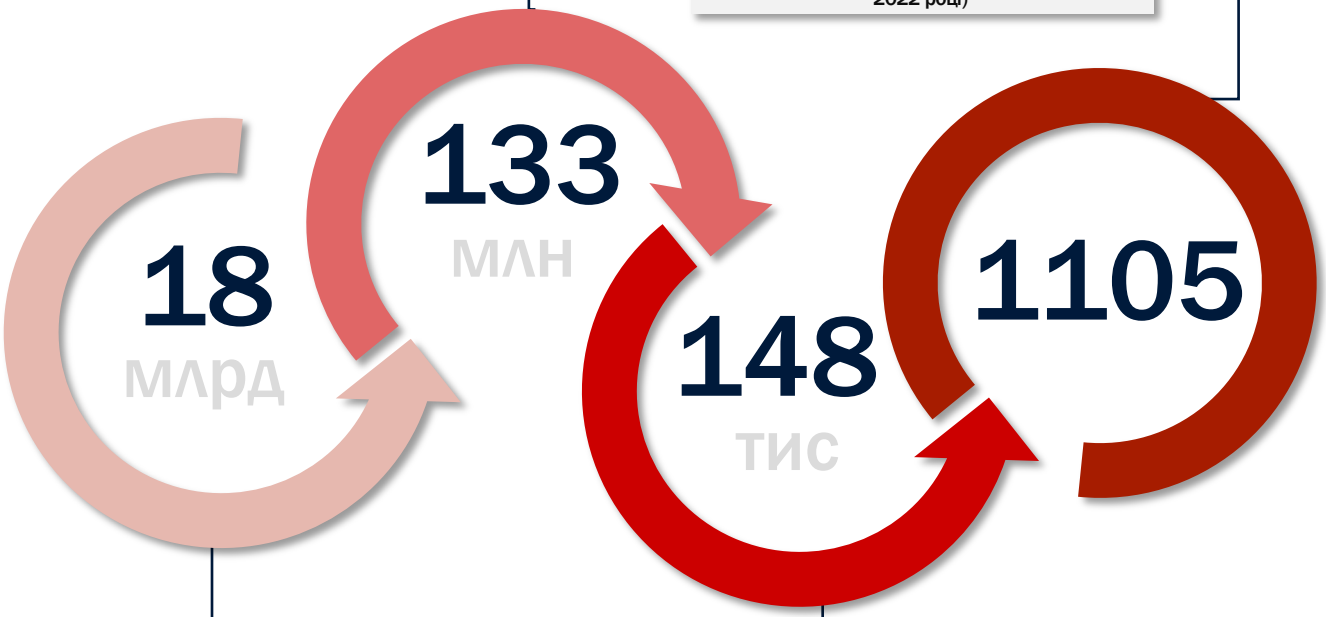
критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

↑62.5%

на скільки відсотків **зросла кількість** зареєстрованих кіберінцидентів (порівняно з аналогічним часовим проміжком у 2022 році)

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

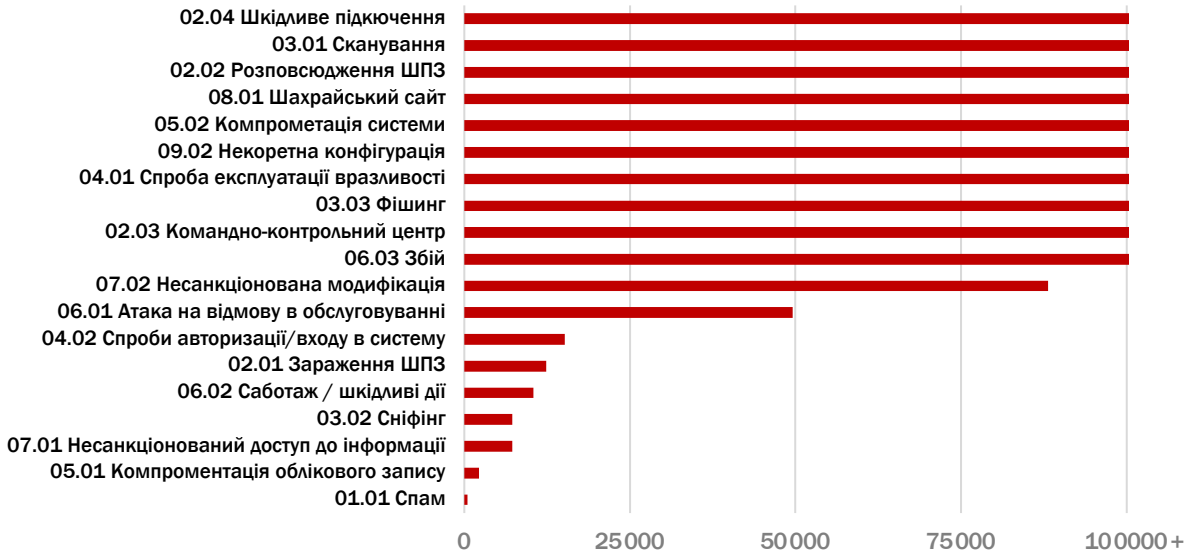
представлена згідно Переліку категорій кіберінцидентів схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України

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

↑ 36.2% та ↑ 43.8%

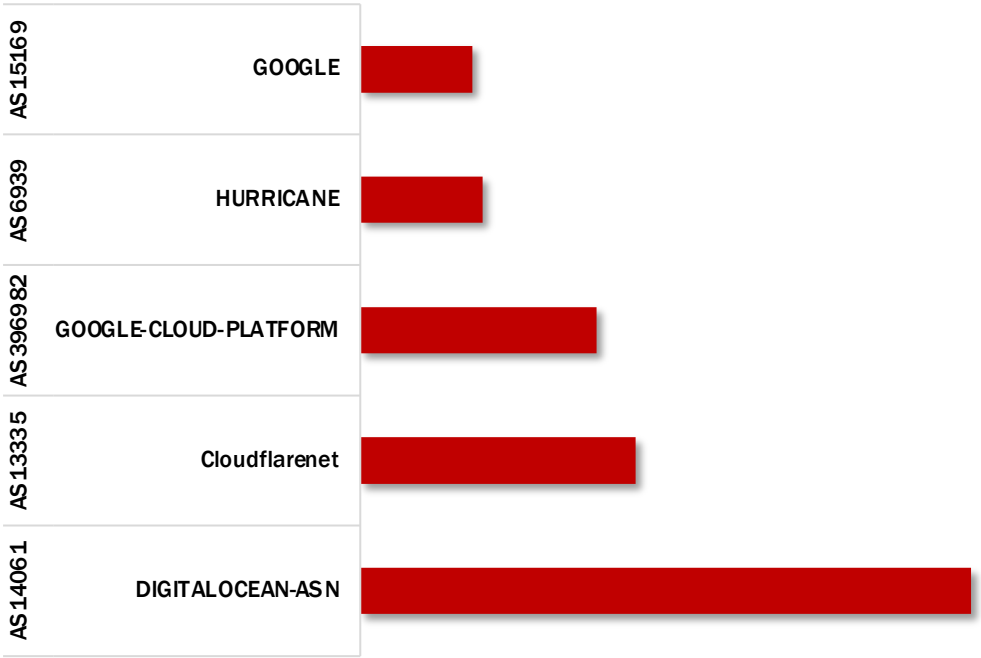
на стільки відсотків відповідно зросла кількість подій ІБ категорій "02 Шкідливий програмний код", "03 Збір інформації зловмисником" (порівняно з аналогічним часовим проміжком у 2022 році)

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

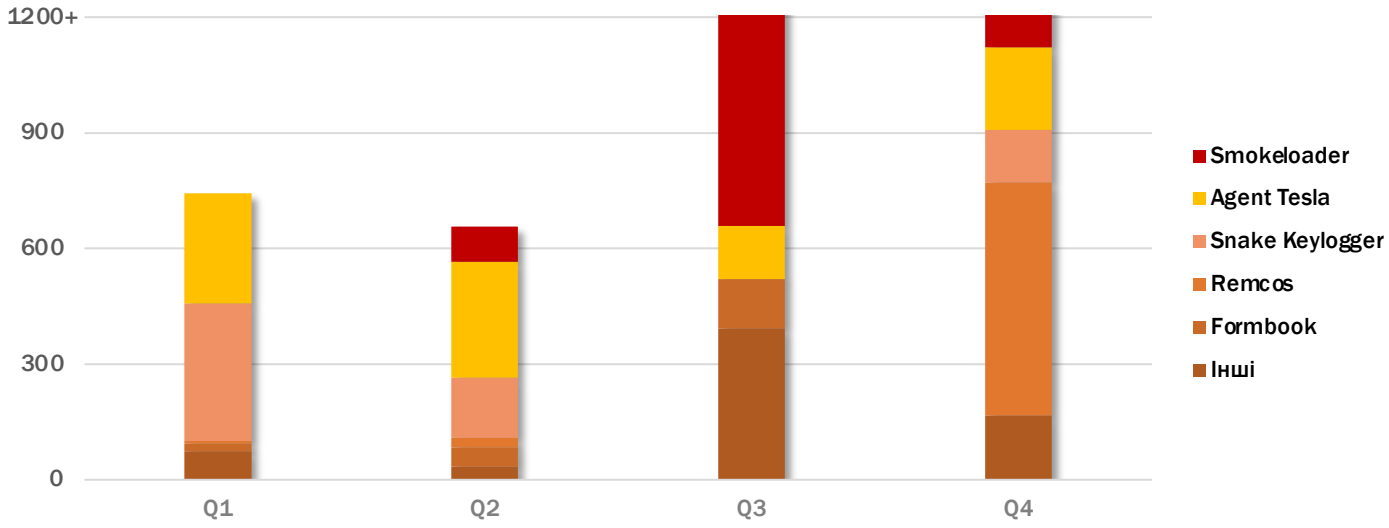
графік відображає топ 10 IP-адрес (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
80.85.141.227	Netherlands	AS204601	Zomro B.V.	3,29%
51.159.196.227	France	AS12876	SCALEWAY S.A.S	3,16%
46.101.146.130	Germany	AS14061	DigitalOcean LLC	2,51%
216.244.66.240	United State	AS23033	Wowrack.com	2,1%
185.174.137.26	Swedish	AS210644	AEZA INTERNATIONAL LTD	1,6%
5.255.231.33	russian federation	AS13238	Yandex LLC	1,38%
62.210.101.204	France	AS12876	SCALEWAY S.A.S	1,14%
212.29.233.209	Israel	AS1680	Cellcom Fixed Line Communication L.P	0,94%
89.208.107.26	Netherlands	AS210644	AEZA INTERNATIONAL LTD	0,59%
61.219.11.155	Republic of China	AS3462	Data Communication Business Group	0,35%

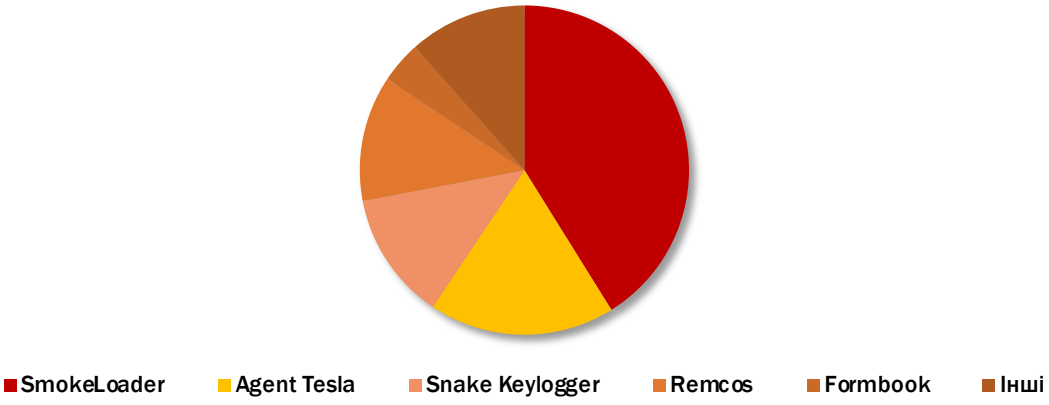
1 516 861

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

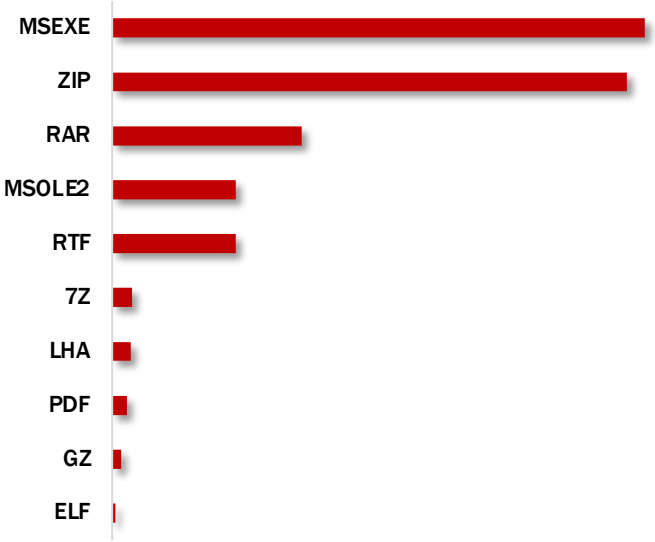
Часовий розподіл подій ІБ категорії “02 Шкідливий програмний код” за сімействами ШПЗ



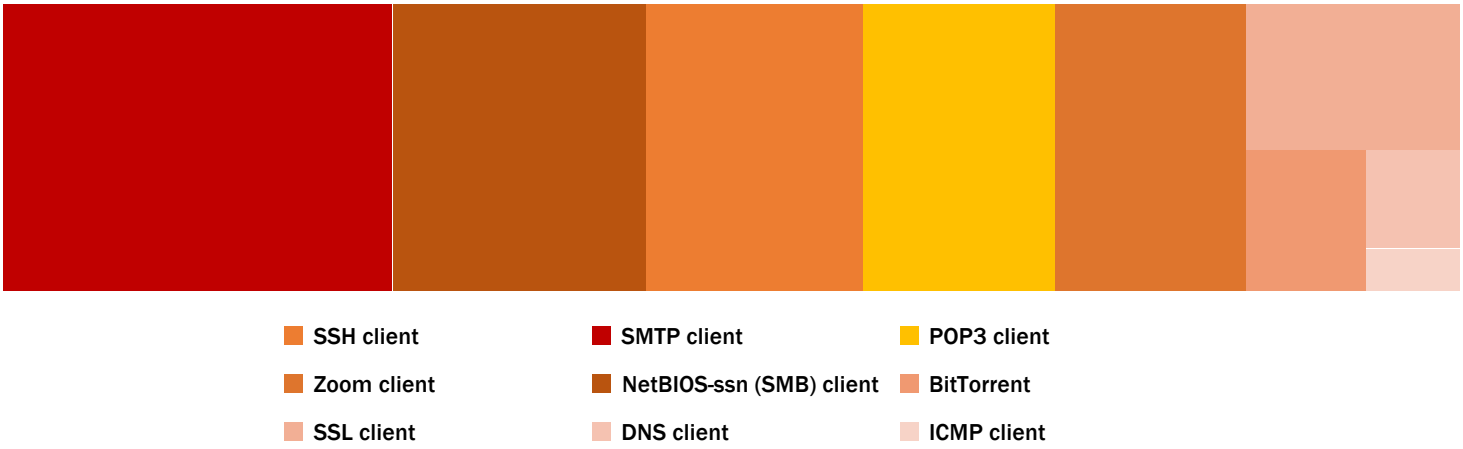
Типи сімейств ШПЗ, детектовані в подіях ІБ категорії “02 Шкідливий програмний код”



За форматом розповсюджуваного ШПЗ

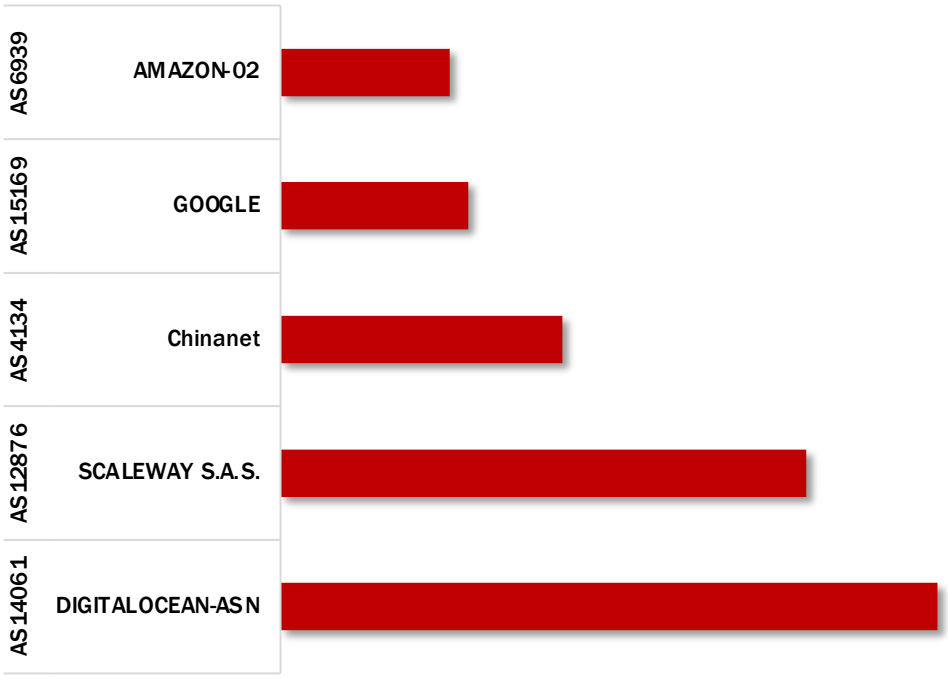


За асоційованим ПЗ клієнтів



Топ 5 ASN - джерел розповсюдження ШПЗ

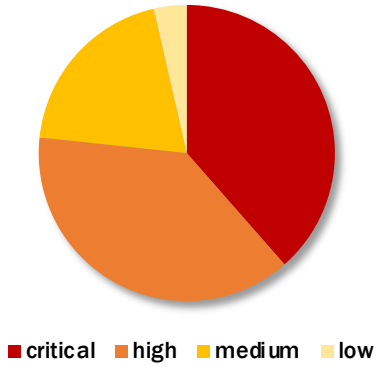
графік відображає топ 5 ASN (у відсотковому відношенні), домінуюча кількість IP-адрес яких була ідентифікована як джерело активного розповсюдження ШПЗ



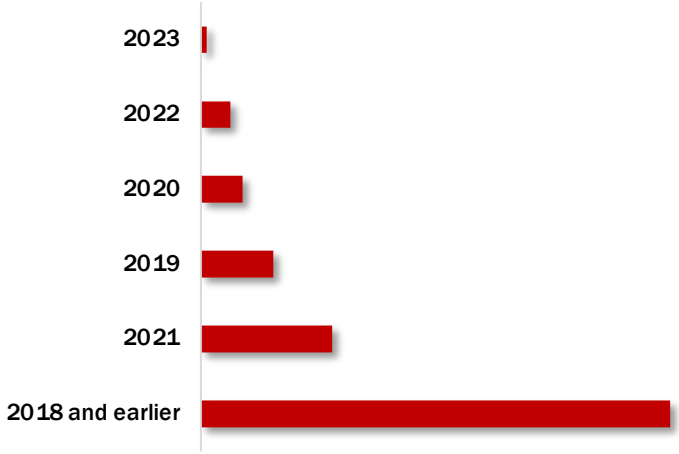
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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

Якісна оцінка за CVSS Base Score

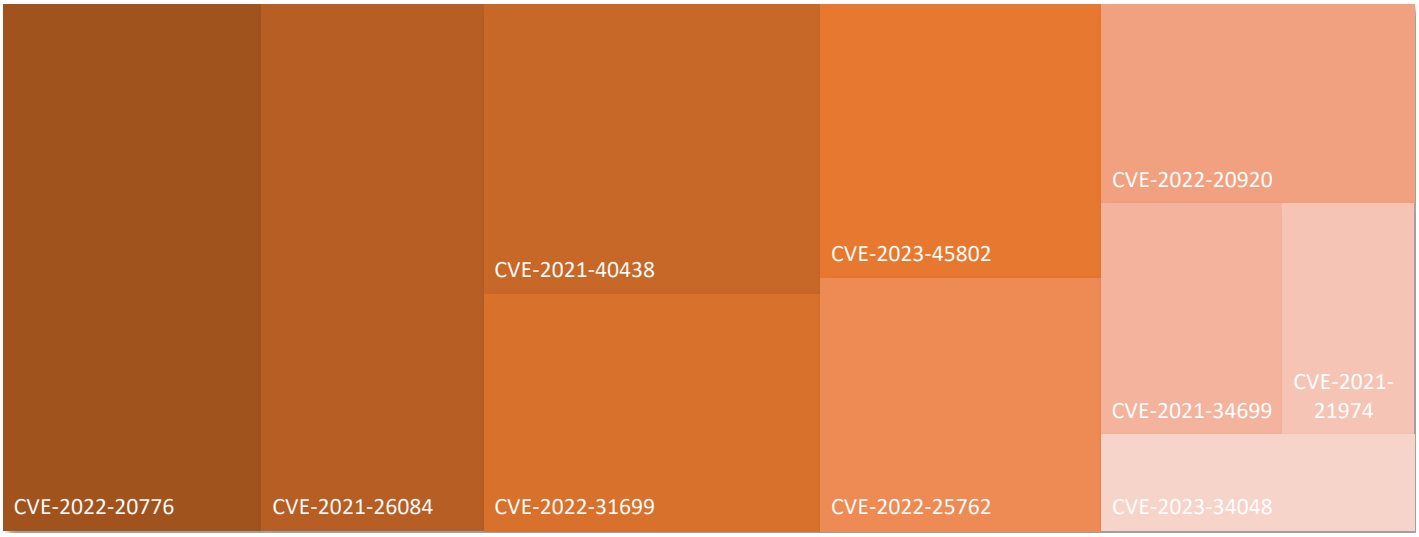
згідно з визначеним специфікацією CVSSv3.1 підходом до зіставлення оцінок CVSS Base Score (1-10) з якісною шкалою оцінювання



Експлуатовані CVE за роком реєстрації



Топ 10 CVE, що експлуатуються



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