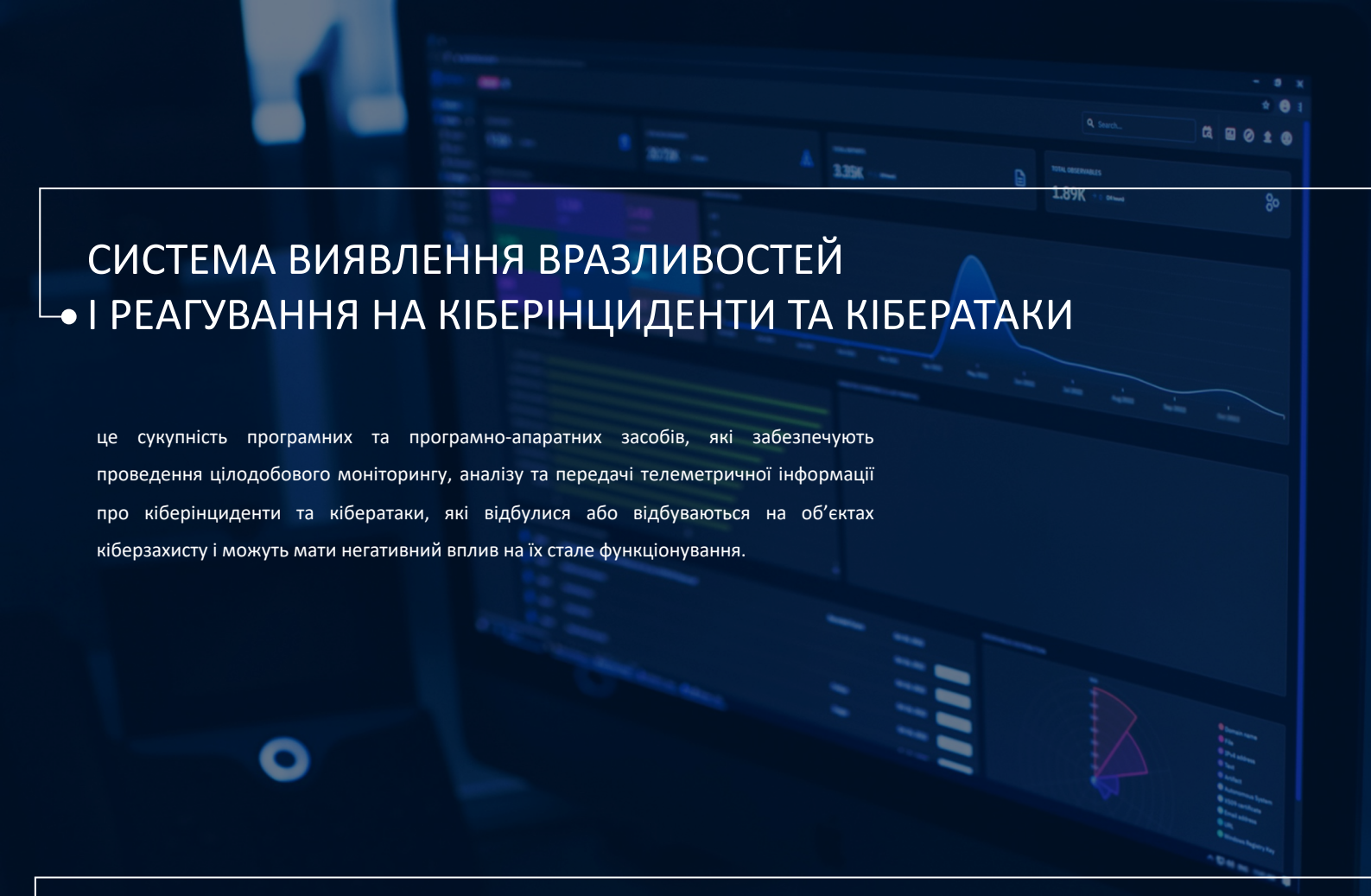
ОПЕРАТИВНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ
ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

2022

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.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

зареєстровано кіберінцидентів

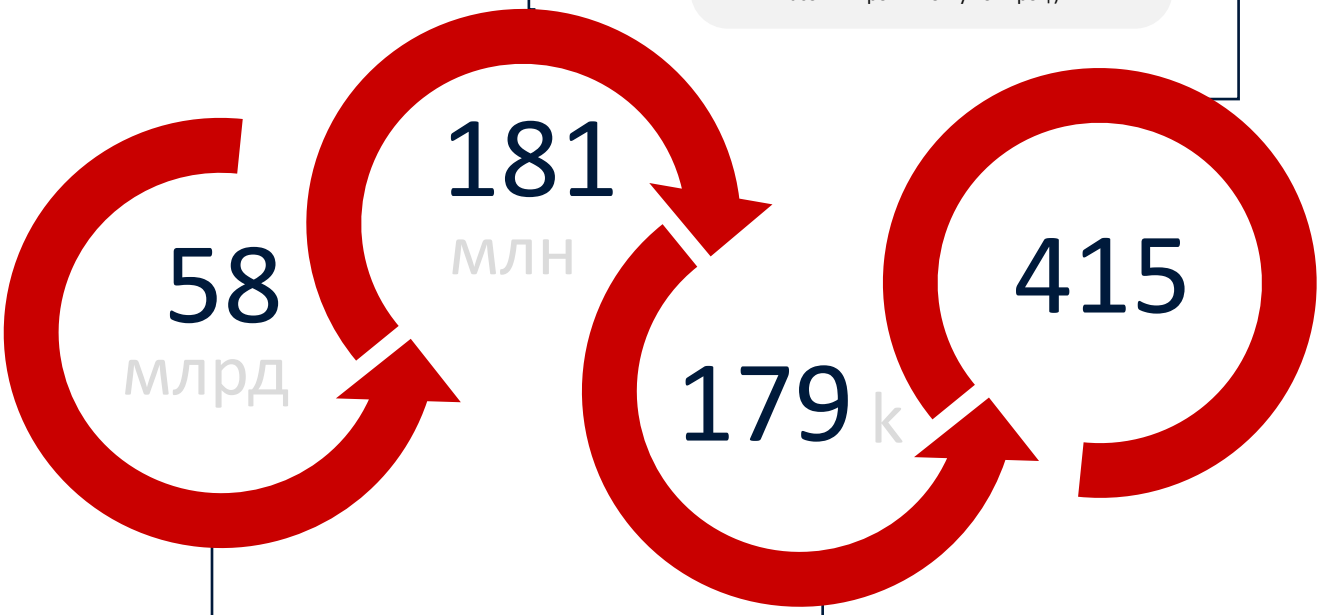
критичних подій ІБ, зафіксованих та оброблених безпосередньо аналітиками безпеки

↑2.8

у стільки разів більше було зареєстровано кіберінцидентів (порівняно з аналогічним часовим проміжком у 2021 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

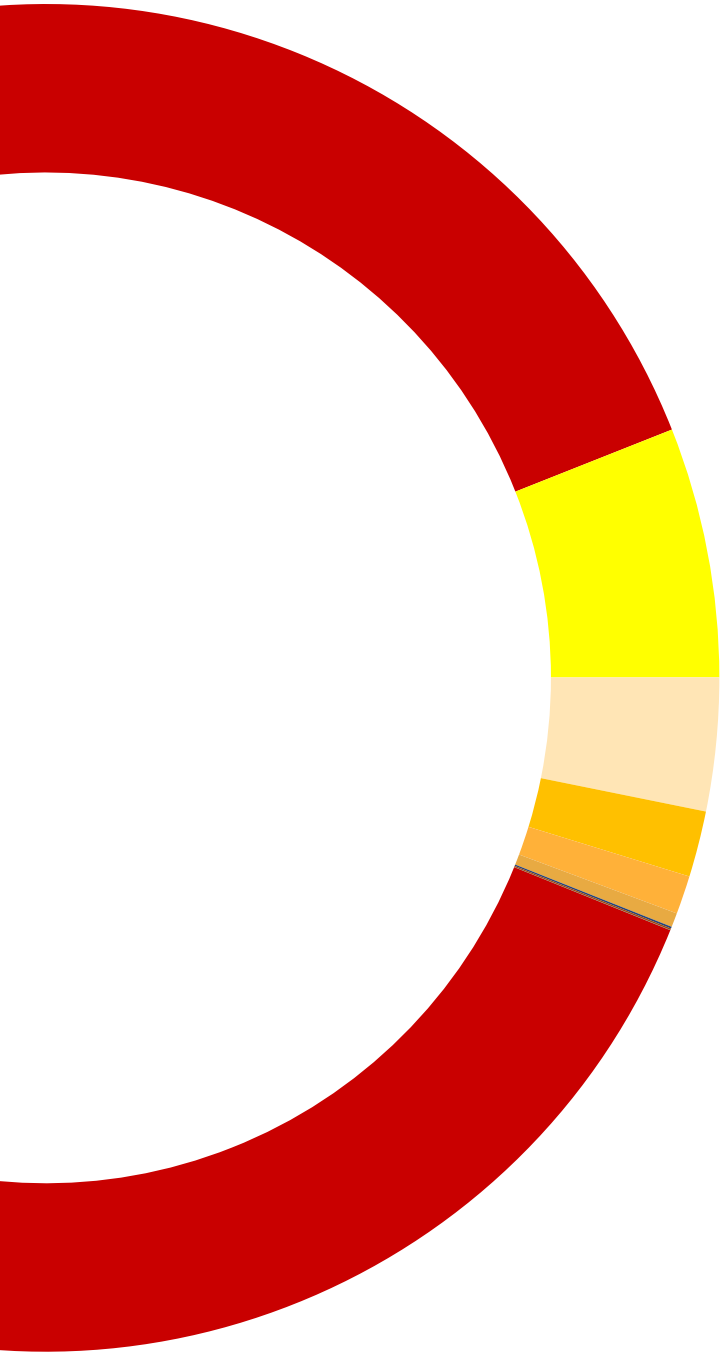
СТАТИСТИКА ПОДІЙ ІБ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

представлена згідно Переліку категорій кіберінцидентів

Схваленого Національним координаційним центром кібербезпеки

при Раді національної безпеки та оборони України



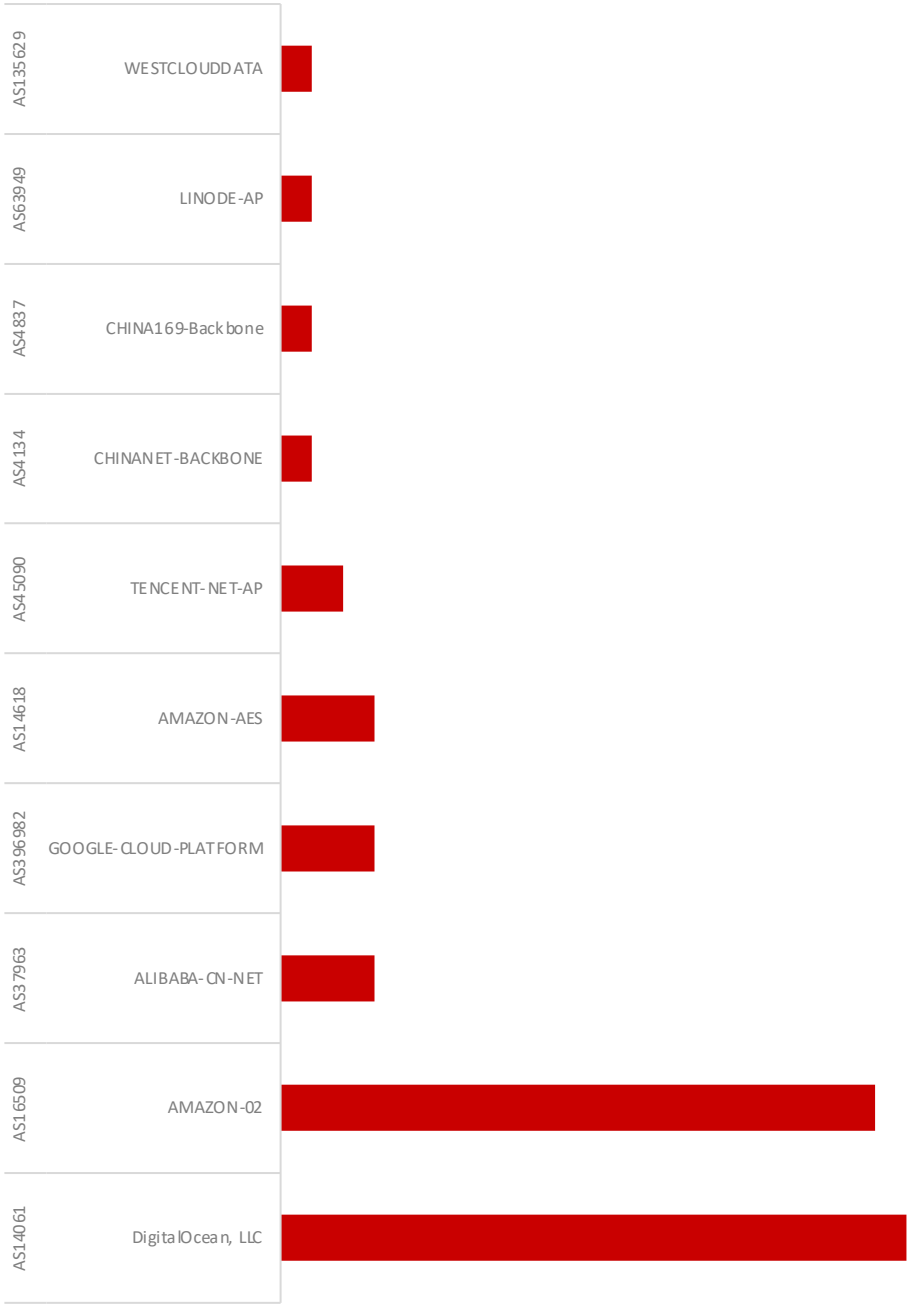
- 02 Шкідливий програмний код
- 03 Збір інформації зловмисником
- 04 Спроби втручання
- 10 Інше
- 08 Шахрайство
- 07 Порушення властивостей інформації
- 06 Порушення доступності
- 09 Відома вразливість
- 05 Втручання
- 01 Шкідливий (образливий) вміст

↑18.3 та ↑2.2

у стільки разів відповідно зросла кількість подій ІБ категорій «02 Шкідливий програмний код», «03 Збір інформації зловмисником»
(порівняно з аналогічним часовим проміжком у 2021 році)

Топ 10 джерел - ASN

графік відображає топ 10 ASN (у відсотковому відношенні), домінантна кількість IP-адрес яких була ідентифікована як джерело активного сканування під час звітного періоду



Топ 10 IP-адрес джерел

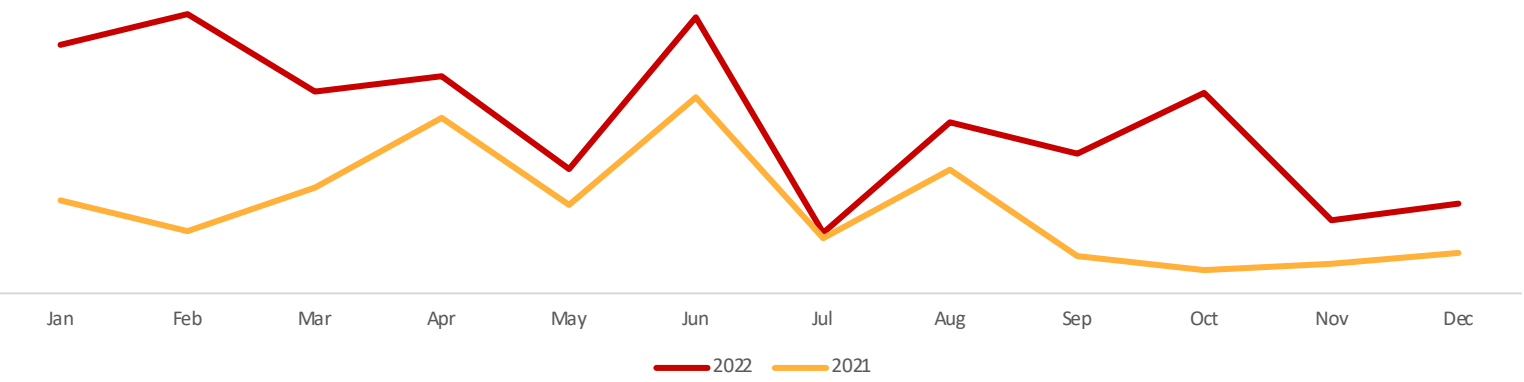
графік відображає топ 10 IP-адрес джерел (у відсотковому відношенні), що були ідентифіковані як джерела активного сканування під час звітного періоду

src	src country	AS NUMBER	AS NAME	%
45.93.16.71	Germany	AS23470	ReliableSite	0,40
206.189.5.99	Netherlands	AS14061	DIGITALOCEAN-ASN	0,38
89.248.165.199	Netherlands	AS202425	IP Volume inc	0,32
72.167.32.184	United States	AS398101	GoDaddy	0,31
185.156.73.91	russian federation	AS44446	OOO SibirInvest	0,30
97.74.81.123	Singapore	AS26496	GoDaddy	0,29
60.161.81.116	China	AS4134	Chinanet	0,26
93.174.93.227	Netherlands	AS202425	IP Volume inc	0,23
146.88.240.4	United States	AS20052	NETSCOUT Arbor	0,22
45.143.200.114	russian federation	AS212283	Roza Holidays Eood	0,21

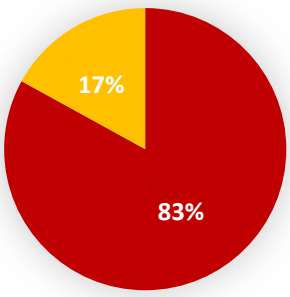
87 389

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»



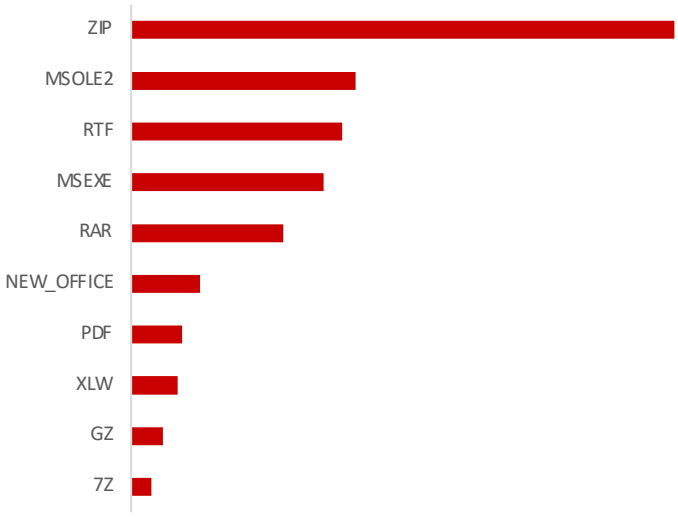
Категорії джерел подій ІБ категорії «02 Шкідливий програмний код»



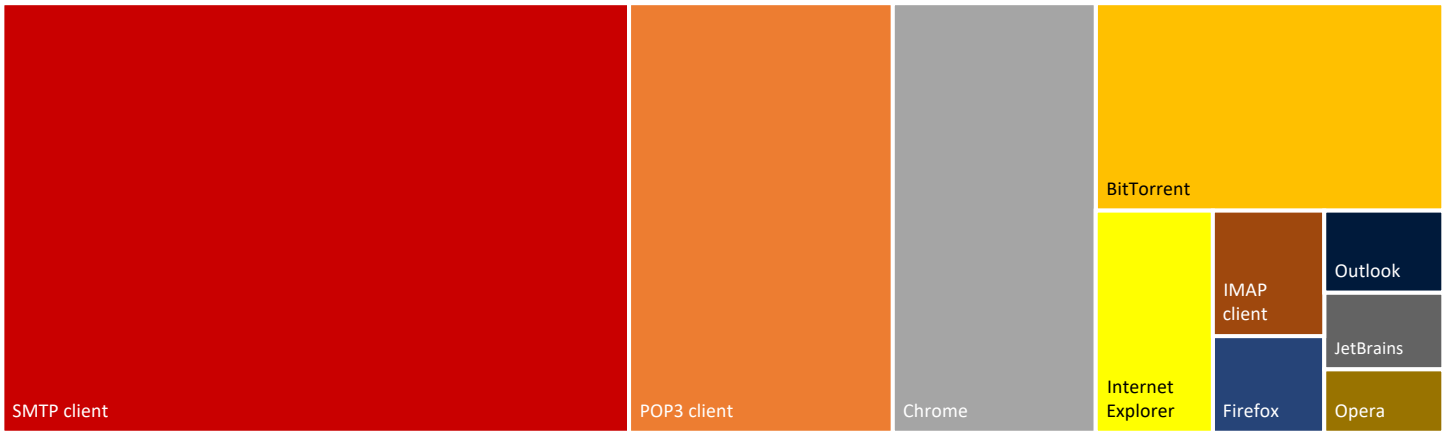
network — мережеві події з підсистеми збору телеметрії інформаційно-комунікаційних систем, що ідентифікують розповсюдження ШПЗ за протоколами HTTP, SMTP, POP3, IMAP

endpoint — сповіщення з підсистеми виявлення та реагування на кібератаки на рівні робочих та серверних станцій (EDR) про виявлення шкідливої активності на них

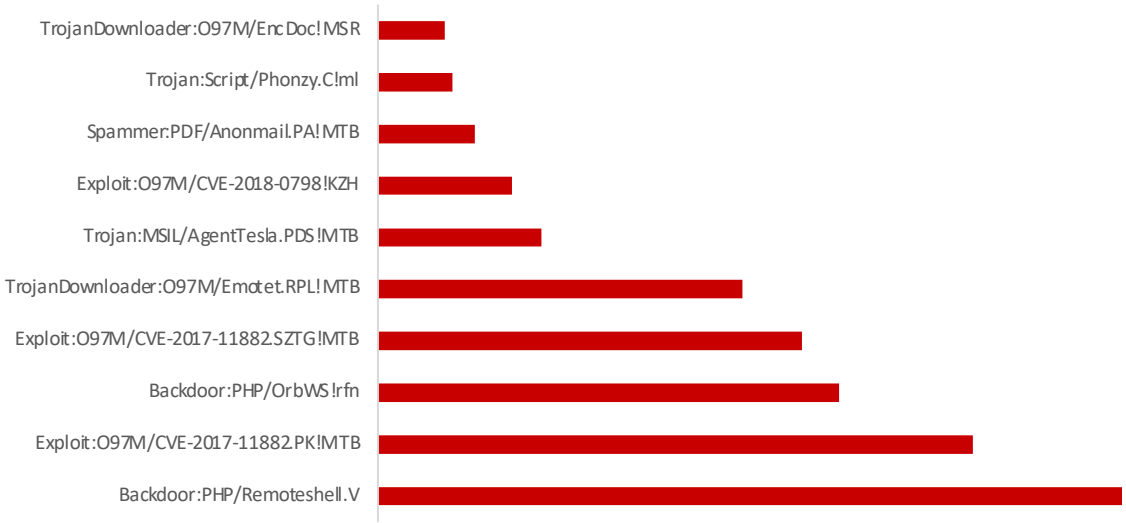
За форматом розповсюджуваного ШПЗ



За асоційованим ПЗ клієнтів



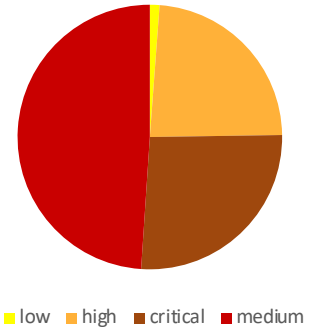
За сигнатурами ШПЗ



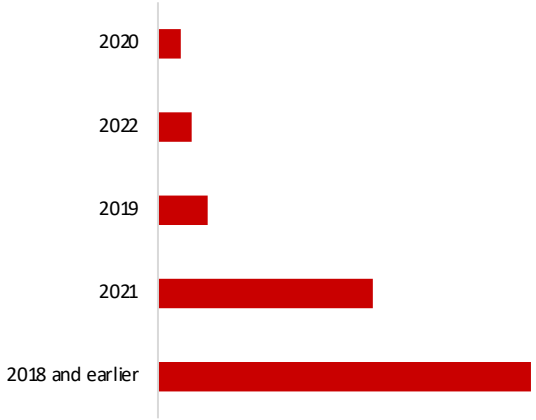
графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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

Якісна оцінка за CVSS Base Score

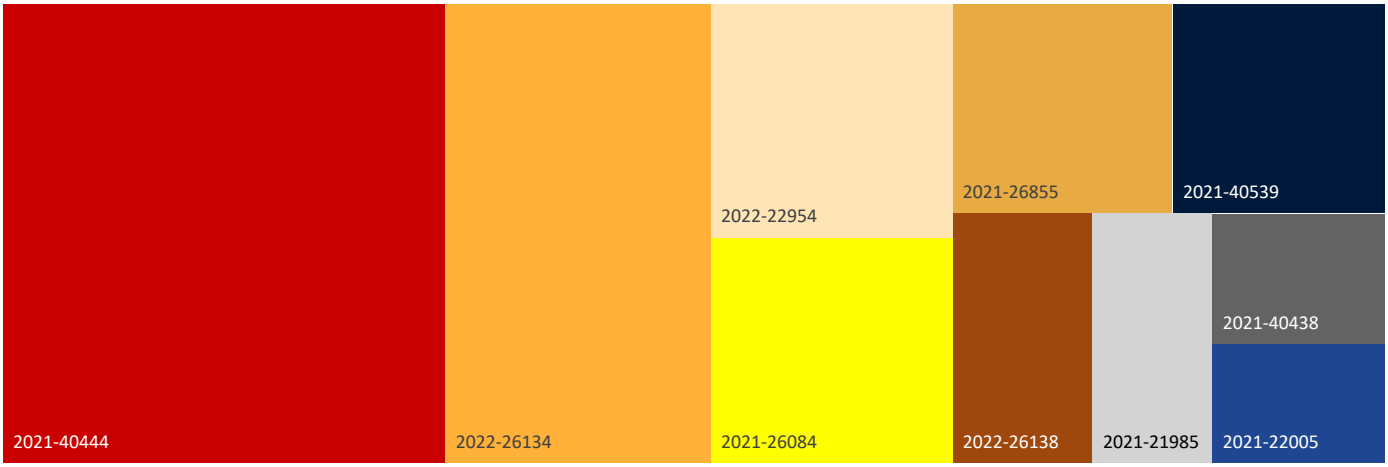
згідно з визначеним специфікацією CVSSv3.1 підходом до співставлення оцінок CVSS Base Score (1-10) до якісної шкали оцінювання



Експлуатовані CVE за роком реєстрації



Топ 10 експлуатованих CVE

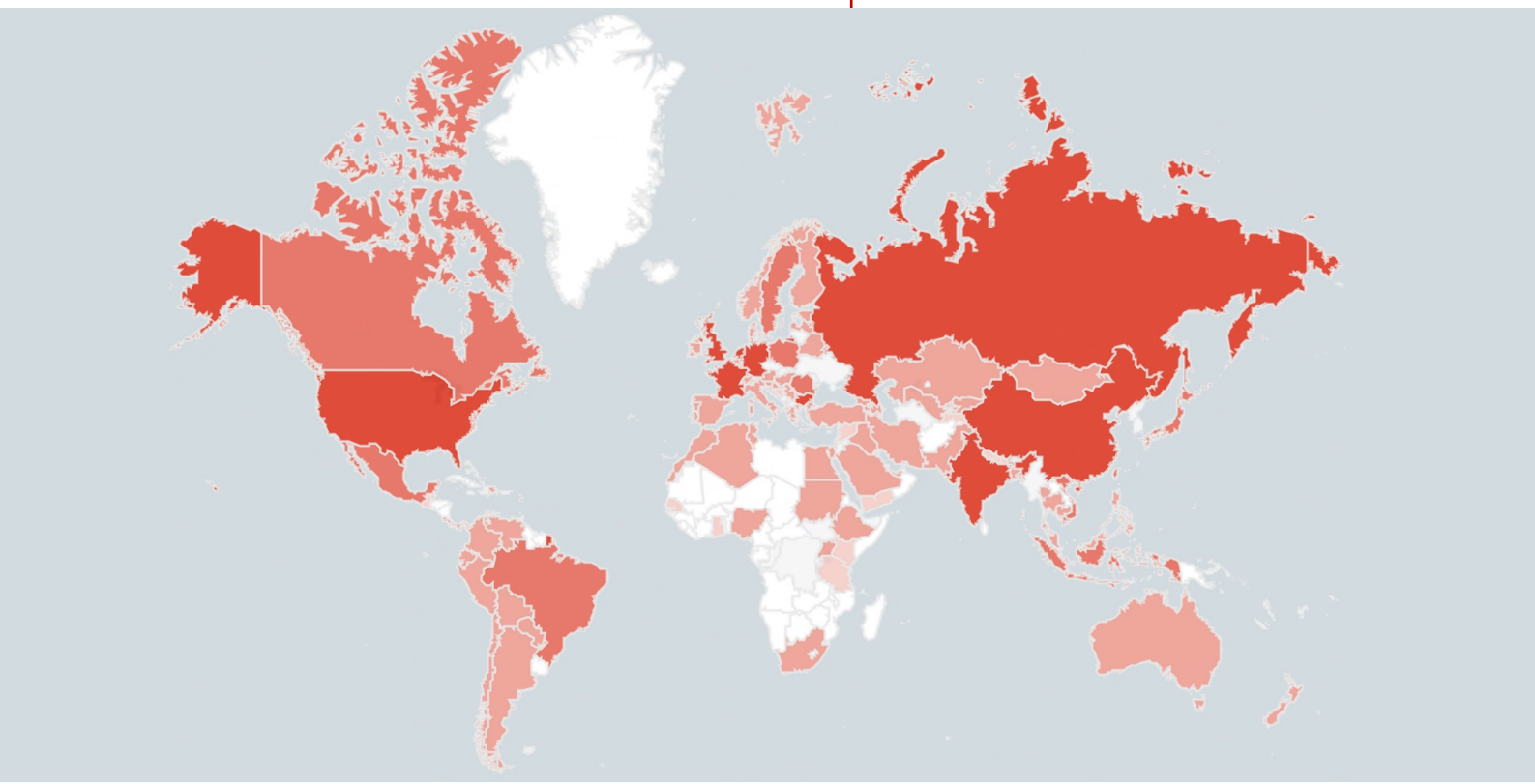


ГЕОГРАФІЯ ДЕТЕКТУВАНЬ

КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*

↑26%

на стільки % зросла кількість критичних подій ІБ, джерелом яких є IP-адреси росії (порівняно з аналогічним часовим проміжком у 2021 році)



*автоматично визначена геолокація IP-адрес джерел критичних подій ІБ не обов'язково означає їх атрибуцію до ідентифікованого місцерозташування

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