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

2024

РІЧНИЙ ЗВІТ

СИСТЕМИ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ І РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

TLP: CLEAR

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 всіма 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 й 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.

ЗМІСТ

ВСТУП

Звіт за 2024 рік є деталізованим описом результатів функціонування Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки (далі - СВВ) на виконання Постанови Кабінету Міністрів України від 23 грудня 2020 року № 1295, якою була визначена необхідність створення та функціонування такої системи в рамках захисту країни від кібернетичних загроз.

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки є важливим інструментом для забезпечення безпеки і стабільності інформаційного простору України. Протягом 2024 року, в рамках функціонування СВВ здійснювався постійний моніторинг кіберпростору, як результат – було виявлено низку кіберінцидентів та кібератак, а також було здійснено відповідні заходи щодо реагування на виявлені кіберінциденти та кібератаки фахівцями Оперативного центру реагування на кіберінциденти (далі - ОЦРК).

В рамках звіту будуть представлені статистичні дані та ключові події, які відбулися протягом 2024 року, а також описані кластери кіберзагроз та заходи, що були вжиті для протидії кіберінцидентам та кібератакам.

💡 **ПРИМІТКА**

Цей звіт ґрунтується на статистичних даних Оперативного центру реагування на кіберінциденти Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки з 1 січня 2024 року по 31 грудня 2024 року включно.

КЛЮЧОВІ ВИСНОВКИ

КЛЮЧОВІ ВИСНОВКИ

У 2024 році за допомогою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було оброблено сотні мільярдів подій телеметрії та зафіксовано майже 3 мільйони подій інформаційної безпеки. Цього вдалося досягти завдяки постійному моніторингу активності в ІКС із використанням засобів виявлення загроз у мережі, аналізу даних засобів захисту кінцевих точок та інтеграції даних розвідки загроз для виявлення потенційних кіберінцидентів та кібератак на об’єкти кіберзахисту.

Особливу увагу було приділено 28 тисячам критичних подій інформаційної безпеки, які потребували негайного втручання аналітиків Оперативного центру реагування на кіберінциденти.

У процесі аналізу цих подій було виявлено та опрацьовано 1042 кіберінциденти. Переважна більшість з них стосувалася поширення шкідливого програмного забезпечення. Основною ціллю таких атак було отримання віддаленого доступу до інформаційних систем із метою кібершпигунства або викрадення грошових коштів.

1 Зловмисники використовують дедалі складніші методи атак, застосовуючи легітимні сервіси та інструменти, що ускладнює їх виявлення та нейтралізацію на рівні мережі та кінцевих точок.

2 Використання скомпрометованих облікових записів та розповсюдження ШПЗ засобами електронної пошти є одними із найпоширеніших методів, які використовують зловмисники для отримання первинного доступу.

3 Найбільш активними у 2024 році були кластери кіберзагроз UAC-0010, UAC-0006 та UAC-0050 згідно з класифікацією Урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA.

ОГЛЯД МОНІТОРИНГУ

СТАТИСТИКА МОНІТОРИНГУ

ОПИС ОРГАНІЗАЦІЙНОЇ СТРУКТУРИ, КОМАНД, ТЕХНОЛОГІЙ ТА ІНСТРУМЕНТІВ

Протягом 2024 року до підсистеми збору телеметрії ІКС (NDR) було підключено 9 нових організацій, які отримали 10 комплектів обладнання сенсорів для моніторингу мережі. До підсистеми захисту кінцевих точок (EDR) підключено 35 організацій, таким чином на моніторингу СВВ перебуває понад 28000 робочих станцій і серверів. До сервісу управління поверхнею атаки (ASM) підключено 38 організацій, що на 10 організацій більше ніж попереднього року.

Загалом у 2024 році до СВВ було підключено 13 нових організацій, з яких 9 належать до урядового сектору та 4 - до оборонного.

Технології та інструменти

Засоби кіберзахисту

Підсистема збору телеметрії	Підсистема захисту кінцевих точок	Управління поверхнею атаки
NDR	**EDR**	**ASM**
Підключено організацій: **67+9**	Підключено організацій: **58+35**	Підключено організацій: **38+10**
Встановлено сенсорів: **69+10**	Захищено хостів: **28000+**	Скановано активів: **1200+**

Сектори та організації

Об'єкти кіберзахисту

81+9	**2**	**7+4**
Урядовий	Енергетичний	Оборонний

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

За допомогою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було оброблено сотні мільярдів подій телеметрії та зафіксовано майже 3 мільйони подій інформаційної безпеки.

Основними джерелами даних є засоби захисту ІКС об'єктів кіберзахисту, а саме: інструменти для виявлення загроз у мережі (NDR) - сенсори підсистеми збору телеметрії, інструменти для аналізу даних із робочих станцій та серверів (EDR) - сенсори підсистеми захисту кінцевих точок, а також дані розвідки загроз щодо скомпрометованих облікових записів та інших індикаторів компрометації (TI).

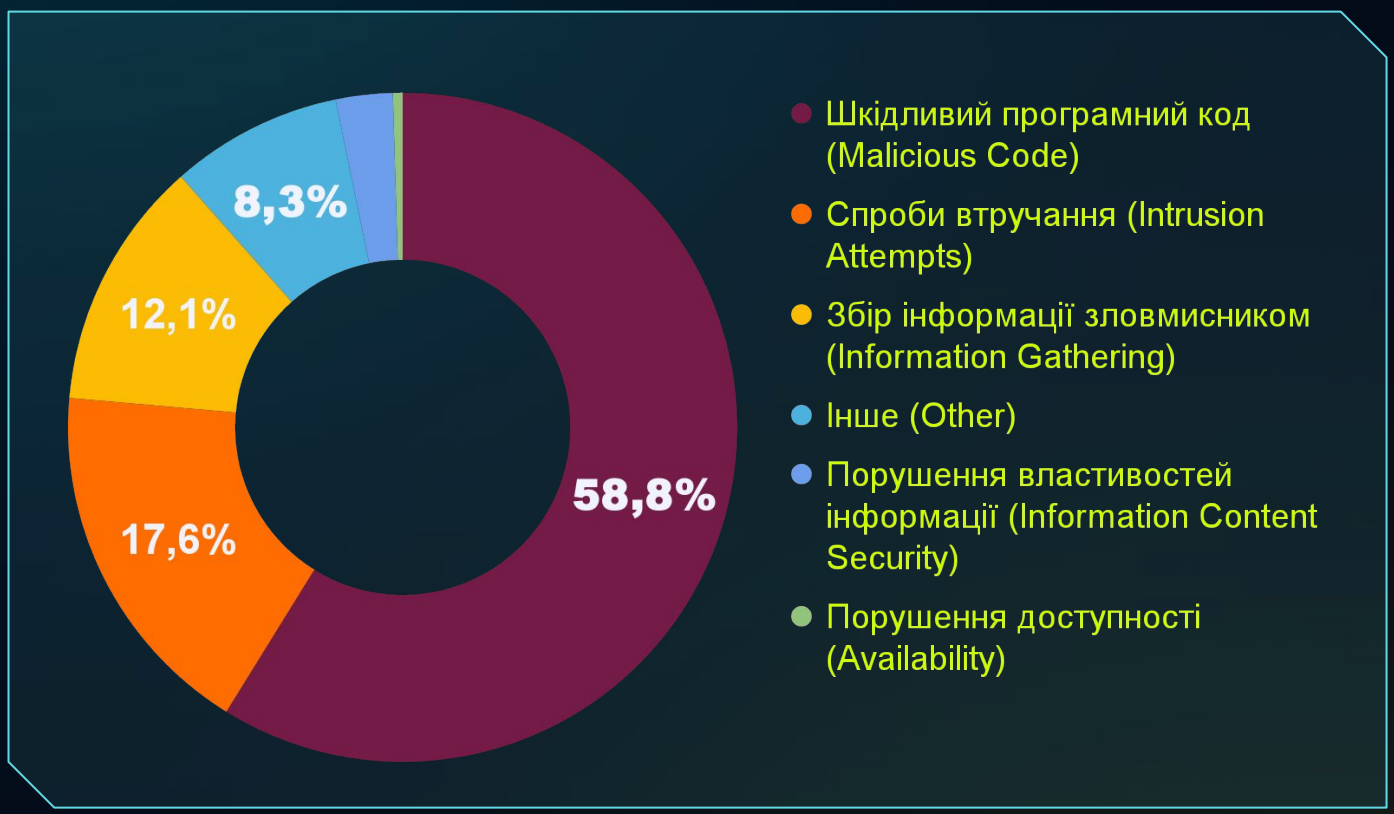
💡 ПРИМІТКА

Варто зауважити, що показники моніторингу суттєво відрізняються порівняно з минулим роком, оскільки в системі було здійснено модернізацію засобів збору мережевої телеметрії, а також впроваджено SOAR систему та застосовано генеративний штучний інтелект для автоматизації виявлення та опрацювання потенційних кіберінцидентів та кібератак. Це дозволило знизити навантаження на SIEM систему та аналітиків ОЦРК, проте кількість виявлених кіберінцидентів та кібератак залишається майже на тому ж рівні, що й минулого року.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

Статистика представлена згідно з Переліком категорій кіберінцидентів, схваленим Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України



Серед виявлених подій інформаційної безпеки основну частину, а саме 58.8%, становлять події, пов'язані зі шкідливим програмним кодом (Malicious Code). Спроби втручання (Intrusion Attempts) займають 17,6%, тоді як збір інформації зловмисником (Information Gathering) становить 12,1%. Інші події (Other) складають 8,3%, порушення властивостей інформації (Information Content Security) та порушення доступності (Availability) займають 2,7% та 0,5% відповідно.

Ці дані про типи подій, що були опрацьовані ОЦРК протягом звітного періоду, допомагають визначити пріоритетні напрямки для посилення заходів кіберзахисту.

ОГЛЯД КІБЕРІНЦИДЕНТІВ

КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

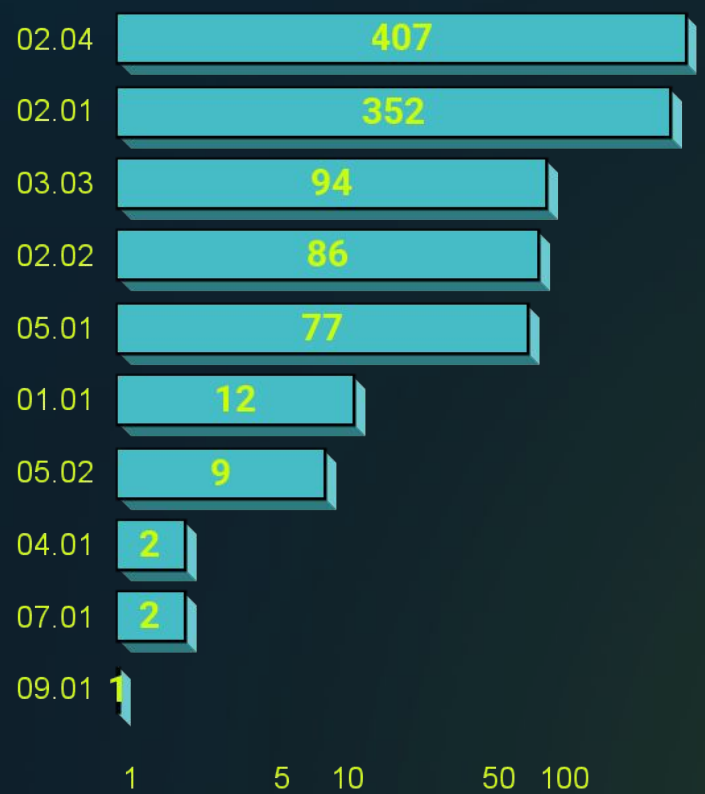
КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ

Розподіл за типами джерел

1042 Протягом 2024 року аналітиками ОЦРК зареєстровано та опрацьовано кіберінцидентів

EDR	NDR	TI
249	739	54

Розподіл за типами кіберінцидентів



Понад **90%** опрацьованих кіберінцидентів стосуються організацій урядового сектору.

За класифікацією, найбільше кіберінцидентів належать до типу **«02.04 Шкідливе підключення»** – спроби з'єднання від/до URL або IP-адреси, пов'язаної з відомим ШПЗ, наприклад C&C, або ресурсом розповсюдження компонентів, пов' язаних з активністю певної бот-мережі.

КІБЕРІНЦИДЕНТИ ТА КІБЕРАТАКИ

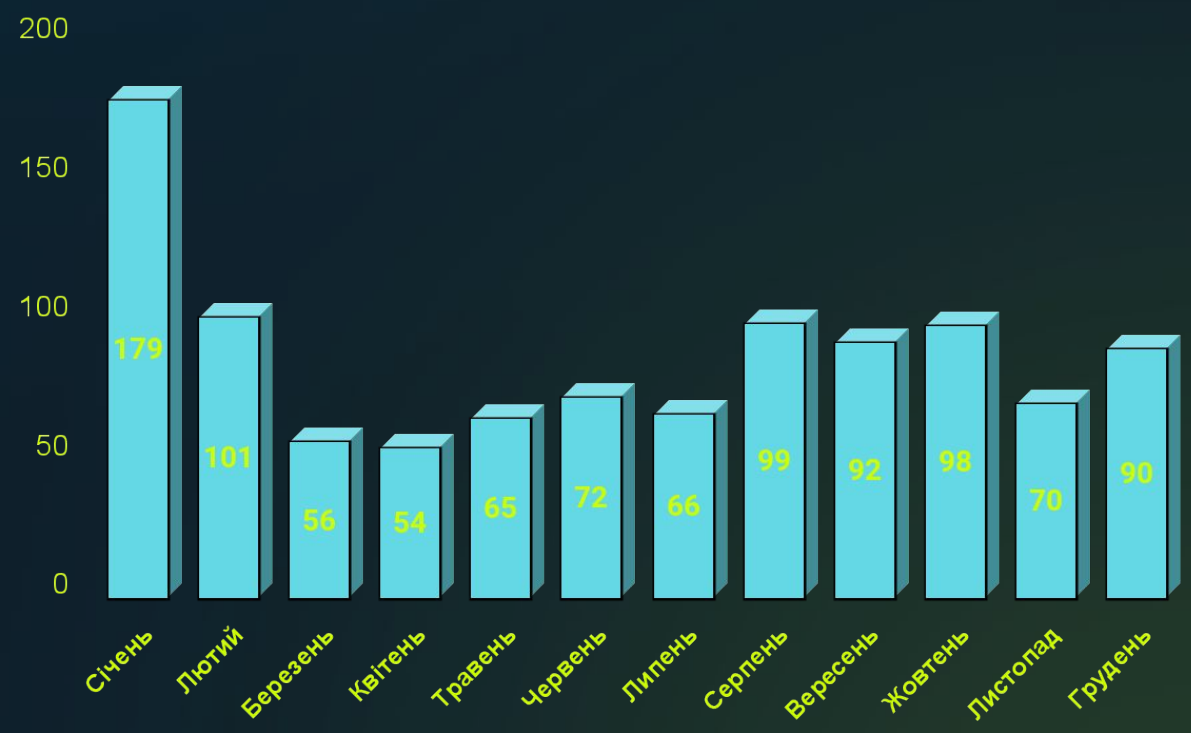
КІЛЬКІСНІ ПОКАЗНИКИ ОПРАЦЬОВАНИХ КІБЕРІНЦИДЕНТІВ

Розподіл кіберінцидентів за секторами

71 Протягом 2024 року така кількість об'єктів кіберзахисту зазнала кібератак і/або кіберінцидентів

- **5** Оборонний
- **65** Урядовий
- **1** Енергетичний

Розподіл кіберінцидентів за місяцями

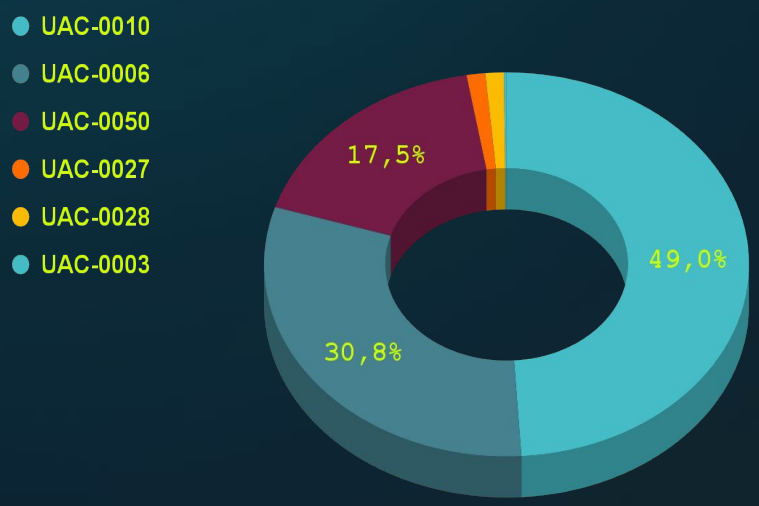


ОГЛЯД КІБЕРЗАГРОЗ

КІБЕРЗАГРОЗИ

КІЛЬКІСНІ ПОКАЗНИКИ КІБЕРЗАГРОЗ

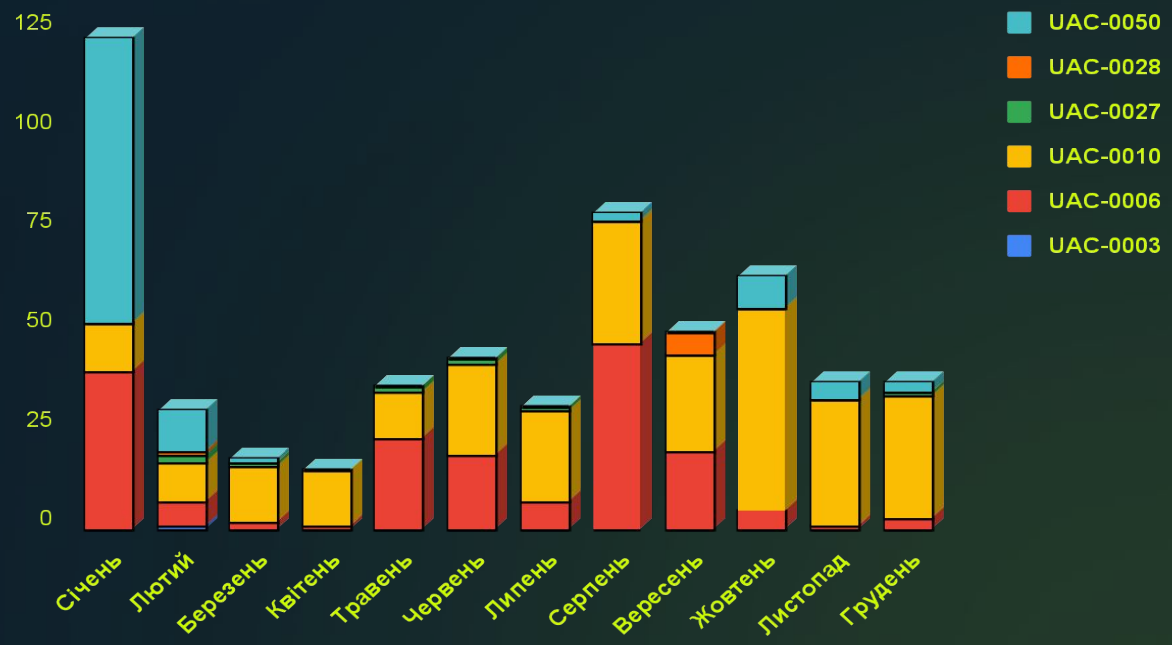
Розподіл кіберінцидентів



Найактивнішими кластерами кіберзагроз, які були виявлені Оперативним центром реагування на кіберінциденти, у 2024 році стали **UAC-0010**, **UAC-0006** та **UAC-0050** (за класифікацією CERT-UA).

Основним початковим вектором кібератак було розповсюдження ШПЗ засобами електронної пошти – **T1566.001** Phishing: Spearphishing Attachment (за класифікацією MITRE ATT&CK).

Часовий розподіл кіберінцидентів, що були атрибутовані до кіберзагроз



КІБЕРЗАГРОЗИ

КІЛЬКІСНІ ПОКАЗНИКИ КІБЕРЗАГРОЗ

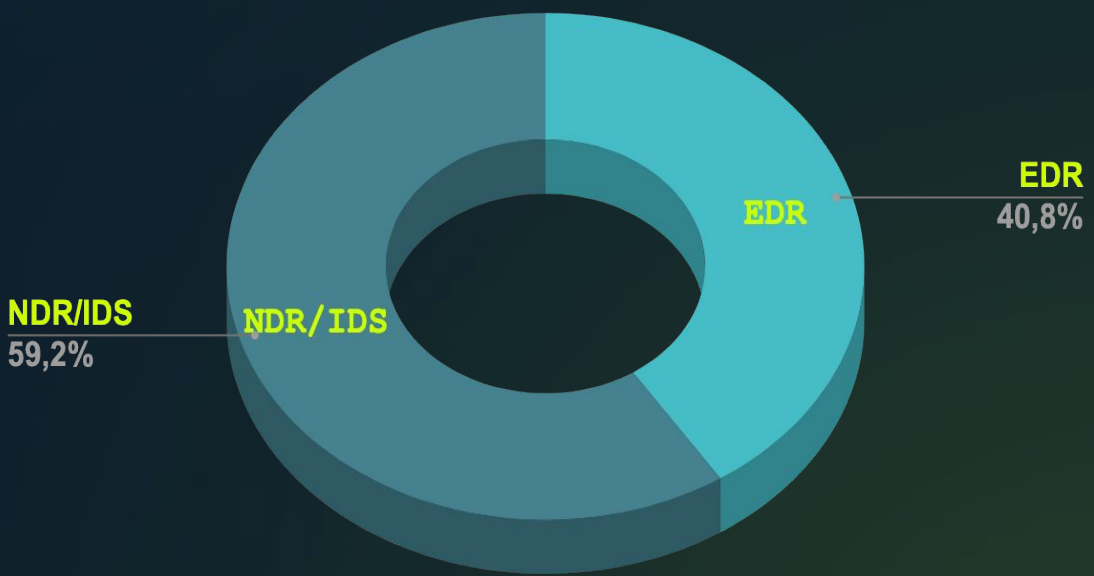
Розподіл кіберінцидентів за секторами

61

Протягом 2024 року така кількість об'єктів кіберзахисту зазнали кібератак чи кіберінцидентів, що були пов’язані з відомими кластерами кіберзагроз

5	55	1
Оборонний	Урядовий	Енергетичний

Розподіл за джерелом виявлення



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0010

Псевдоніми:
Gamaredon, Primitive Bear, Trident Ursa, Aqua Blizzard

Відслідковується з:
2013 року

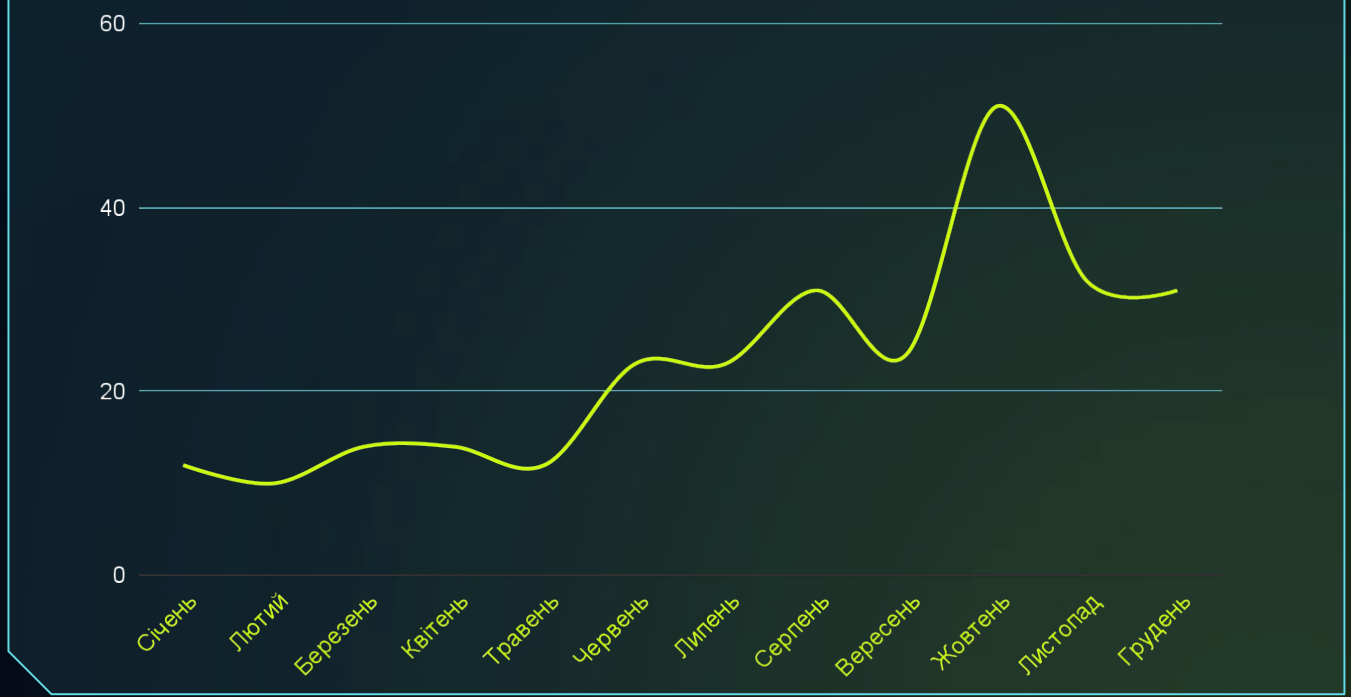
Мотивація:
кібершпигунство

Цілі кібератак:
державні органи, сили оборони

Протягом року фахівці ОЦРК було виявлено 277 кіберінцидентів, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0010. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти та за допомогою флеш-носіїв.

Зведена інформація щодо діяльності угрупування UAC-0010 за посиланням: **https://cert.gov.ua/article/5160737**.

Таймлайн кібератак UAC-0010



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0006

Псевдоніми:
Відсутні

Відслідковується з:
2013 року

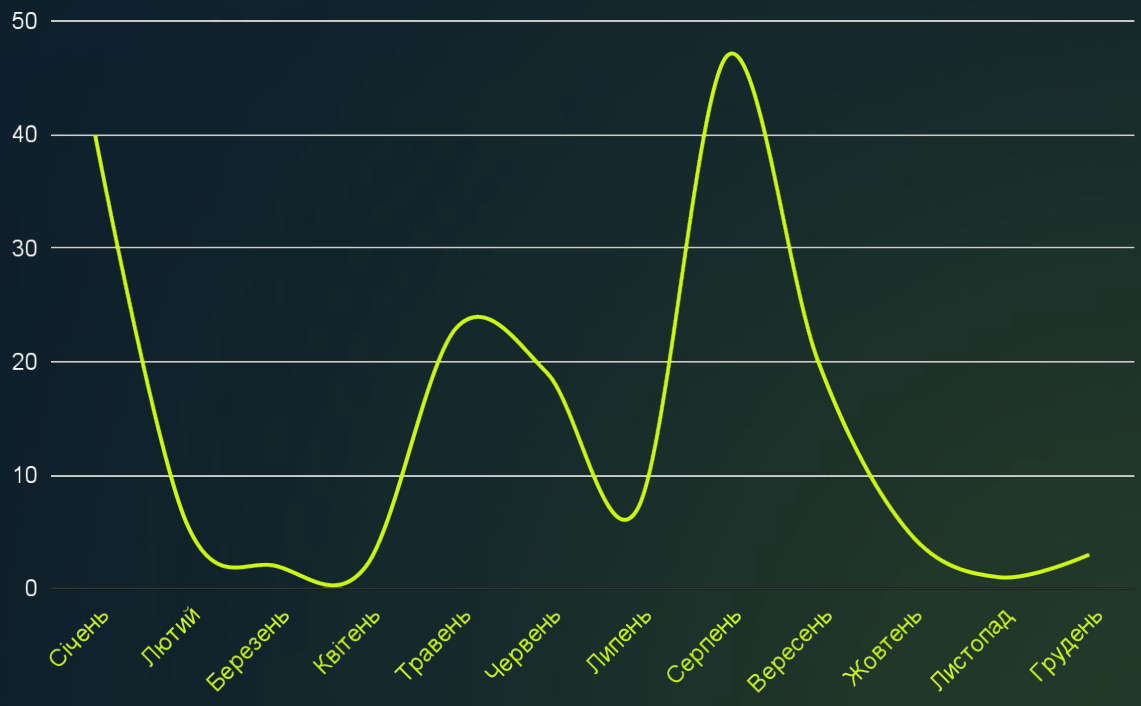
Мотивація:
викрадення коштів

Цілі кібератак:
фінансові підрозділи організацій

У 2024 році фахівці ОЦРК виявили 174 кіберінциденти, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0006. Серед досліджених кіберінцидентів найчастіше первинним вектором ураження було розповсюдження ШПЗ SmokeLoader засобами електронної пошти.

Зведена інформація щодо діяльності угрупування UAC-0006 за посиланням: **https://cert.gov.ua/article/6276584**.

Таймлайн кібератак UAC-0006



КІБЕРЗАГРОЗИ

АКТИВНІСТЬ КЛАСТЕРІВ КІБЕРЗАГРОЗ

Опис кластеру UAC-0050

Псевдоніми:
Відсутні

Відслідковується з:
2020 року

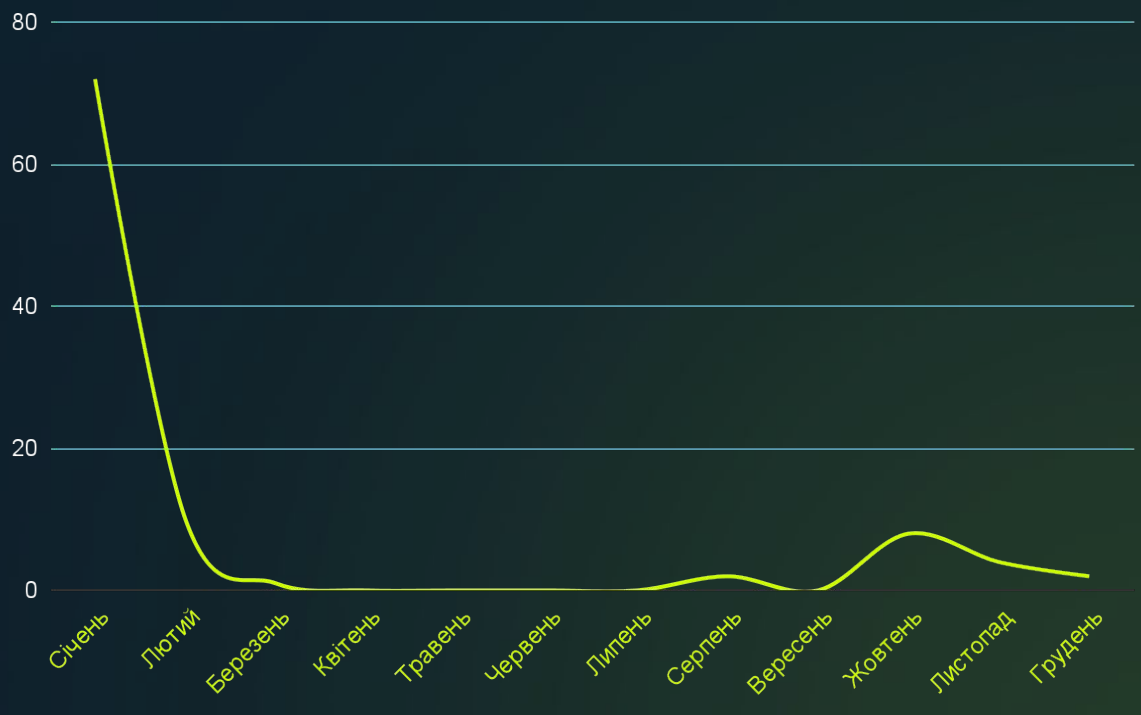
Мотивація:
кібершпигунство, викрадення коштів, ІПСО

Цілі кібератак:
державні органи, сили оборони, фінансові установи

Упродовж року фахівці ОЦРК виявили 99 кіберінцидентів, що атрибутуються до активності, яка відслідковується CERT-UA за ідентифікатором UAC-0050. Серед досліджених кіберінцидентів первинним вектором ураження було розповсюдження ШПЗ засобами електронної пошти.

Зведена інформація щодо діяльності угрупування UAC-0050 за посиланням: **https://cert.gov.ua/article/6281009**.

Таймлайн кібератак UAC-0050



РЕКОМЕНДАЦІЇ

РЕКОМЕНДАЦІЇ

Вчасно оновлюйте програмне та апаратне забезпечення	Регулярно оновлюйте своє програмне забезпечення та встановлюйте патчі безпеки. Також переконайтеся, що ваше апаратне забезпечення не є застарілим. Слідкуйте за поверхнею атаки, яка доступна з мережі Інтернет.
Використовуйте засоби захисту електронної пошти	Будьте обережні з електронними листами, особливо з незнайомими або підозрілими вкладеннями чи посиланнями. Ніколи не вводьте свої особисті дані на підозрілих вебсайтах.
Використовуйте засоби захисту кінцевої точки	Використовуйте антивірусне програмне забезпечення, регулярно його оновлюйте, періодично скануйте систему. Захист в реальному часі допоможе уникнути ураження системи. Також уникайте встановлення небажаних програм, які можуть стати джерелом загроз.
Здійснюйте інвентаризацію активів та моніторинг мережі	Забезпечте повну інвентаризацію всіх активів, включаючи сервери, робочі станції, мобільні пристрої та мережеве обладнання. Регулярно оновлюйте інформацію про корпоративні мережі, гостьові WiFi мережі, DNS-записи та IP-адреси. Це дозволить швидко ідентифікувати та локалізувати активи у разі кіберінциденту.
Використовуйте багатофакторну автентифікацію	Використовуйте довгі та складні паролі, які складаються з комбінації різних символів. Активуйте багатофакторну автентифікацію для додаткового захисту вашого облікового запису.
Налаштуйте логування	Забезпечте максимальне логування подій у вашій інфраструктурі, включаючи активність користувачів, мережеві підключення, зміни в конфігураційних файлах та доступ до критично важливих даних. Повний обсяг логів дозволяє своєчасно виявляти та реагувати на кіберінциденти та кібератаки.

Також ознайомтеся з рекомендаціями, що були підготовлені Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, за посиланням: https://cert.gov.ua/article/5436463

РЕКОМЕНДАЦІЇ

Для підвищення рівня кіберзахисту ІКС вашої організації пропонуємо скористатися сервісами кіберзахисту, що функціонують в межах "Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки", щодо виявлення кіберзагроз в реальному часі й управління кіберінцидентами.

NDR	Сервіс передбачає встановлення та налаштування мережевого сенсора для моніторингу мережевого трафіку і виявлення кіберінцидентів та кібератак. Сенсор може бути встановлений як всередині мережі, так і на її периметрі.
EDR	Сервіс передбачає комплексний захист кінцевих точок вашої організації (персональні комп'ютери, сервери, віртуальні машини) за допомогою встановлення та налаштування на них технології EDR.
ASM	Сервіс передбачає сканування публічних інформаційних ресурсів, та охоплює перевірку наявних вразливостей, ідентифікацію потенційних ризиків та векторів атак, надання детальних звітів з описом вразливостей тощо.

Для зв'язку з Державним центром кіберзахисту щодо підключення вищезгаданих сервісів:

Email: info_scpc@cip.gov.ua

Телефон: +38 (044) 281 87 37

РЕКОМЕНДАЦІЇ

Перелік призначений для впровадження таксономії як інструменту для обміну інформацією щодо кіберінцидентів.

Код xx	Категорія інциденту	Код xx	Тип інциденту	Тип інциденту англійською
01.	Шкідливий вміст (Abusive content)	01	Спам	Spam
02.	Шкідливий програмний код (Malicious Code)	01	Зараження шкідливим програмним забезпеченням (далі – ШПЗ)	Malware infection
		02	Розповсюдження ШПЗ	Malware distribution
		03	Командно-контрольний центр (C2)	Command & Control (C2)
		04	Шкідливе підключення	Malicious connection
03.	Збір інформації зловмисником (Information Gathering)	01	Сканування	Scanning
		02	Снiфінг	Sniffing
		03	Фішинг	Phishing
04.	Спроби втручання (Intrusion Attempts)	01	Спроба експлуатації вразливості	Vulnerability exploitation attempt
		02	Спроби авторизації/входу в систему	Login attempts
05.	Втручання (Intrusion)	01	Компрометація облікового запису	Account compromise
		02	Компрометація системи	System compromise
06.	Порушення доступності (Availability)	01	Атака на відмову в обслуговуванні	DoS/DDoS
		02	Саботаж / шкідливі дії	Sabotage
		03	Збій	Outage, no malice
07.	Порушення властивостей інформації (Information Content Security)	01	Несанкціонований доступ до інформації	Unauthorised access to information
		02	Несанкціонована модифікація	Unauthorised modification of info
08.	Шахрайство (Fraud)	01	Шахрайський сайт	Fraudulent site
09.	Відома вразливість (Vulnerable)	01	Вразливість	Vulnerability
		02	Некоректна конфігурація	Misconfiguration
10	Інше (Other)	01	Невизначений інцидент	Undetermined incident

Оперативний центр реагування на кіберінциденти

Державний центр кіберзахисту

Державна служба спеціального зв'язку та захисту інформації України

e-mail: soc@cip.gov.ua

тел.: +38 (044) 281 87 37