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

2022 Q2

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 і 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 обробки 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

Держспецзв'язку постійно фіксує зростання кількості кіберінцидентів та кібератак на державні інформаційні ресурси та об'єкти критичної інформаційної інфраструктури. Від початку війни тренд на зростання кількості кібератак зберігається.

Так, у II кварталі 2022 за допомогою засобів Системи виявлення вразливостей та реагування на кіберінциденти та кібератаки було опрацьовано 19 млрд подій. Кількість зареєстрованих та опрацьованих кіберінцидентів зросла – від 40 до 64.

Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та навіть знищення інформаційних систем за допомогою програм-вайперів. У II кварталі 2022 року ми зафіксували істотне зростання активності хакерських груп щодо розповсюдження шкідливого програмного забезпечення, серед якого є як програми, що викрадають дані, так і ті, які спрямовані на знищення даних. Порівняно зі статистичними даними за I квартал 2022 року, кількість подій ІБ у категорії «Шкідливий програмний код» збільшилась на 38%.

Порівняно з I кварталом 2022 року кількість критичних подій ІБ, джерелом яких є IP-адреси росії, зменшилась у 8,5 разів. Це пов'язано передусім з тим, що постачальники електронних комунікаційних мереж та/або послуг, які забезпечують доступ до інтернету, заблокували IP-адреси, що використовуються рф.
Саме з цих IP здійснювались кібератаки на українські інформаційні ресурси, розповсюджувалась фейкова інформація, що стосується дискредитації державних органів під час російсько-української війни.

Наразі найбільша кількість критичних подій ІБ пов'язана з IP-адресами зі США. Проте автоматично визначена геолокація IP-адрес джерел необов'язково означає атрибуцію кібератак до ідентифікованого місцезнаходження.

Втім, за атрибуцією абсолютна більшість кіберінцидентів пов'язана з хакерськими угрупуваннями, що фінансуються урядом рф. Зокрема, це UAC-0082/UAC-0113 (пов'язано з Sandworm), UAC-0010 (Gamaredon) та інші.

У II кварталі 2022 року основною мішенню хакерів із російської федерації були українські ЗМІ, Уряд та місцеві органи влади. Найбільшу частку подій інформаційної безпеки можна пов'язати з APT-угрупуваннями та хактивістами.

Минулого року Адміністрація Держспецзв'язку ухвалила наказ щодо запровадження в Україні Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури. ДЦКЗ Держспецзв'язку рекомендує установам запроваджувати цей гайдлайн для підвищення кіберстійкості.

СТАТИСТИКА МОНІТОРИНГУ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

6 к
FPS

14.7 к
хостів

183 Gb
отримано вхідних даних

5 Gbit/s
швидкість вхідного трафіку сенсорної мережі

опрацьовано подій
отриманих за допомогою засобів моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки

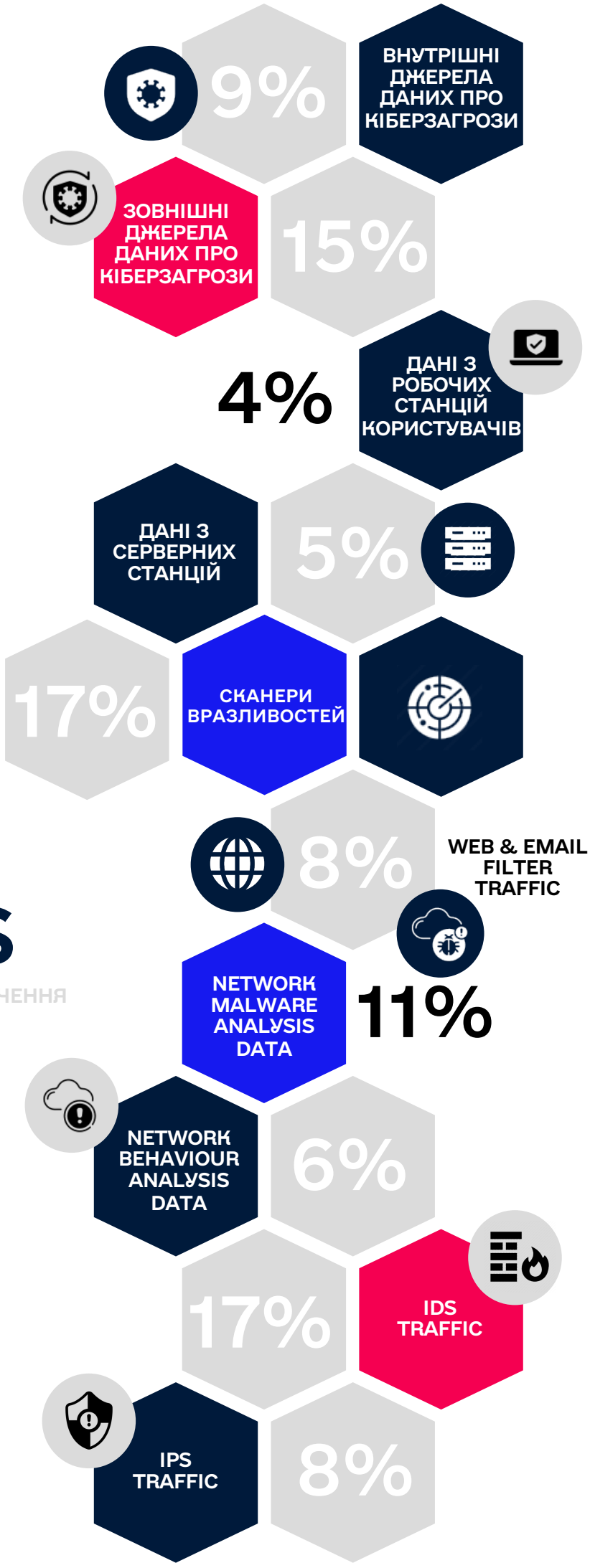
детектовано підозрілих подій ІБ
при первинному аналізі

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

DATA SOURCES

ОСНОВНІ ДЖЕРЕЛА ЗБОРУ ТА ЗБАГАЧЕННЯ КОНТЕКСТОМ ДАНИХ



2022(Q2)

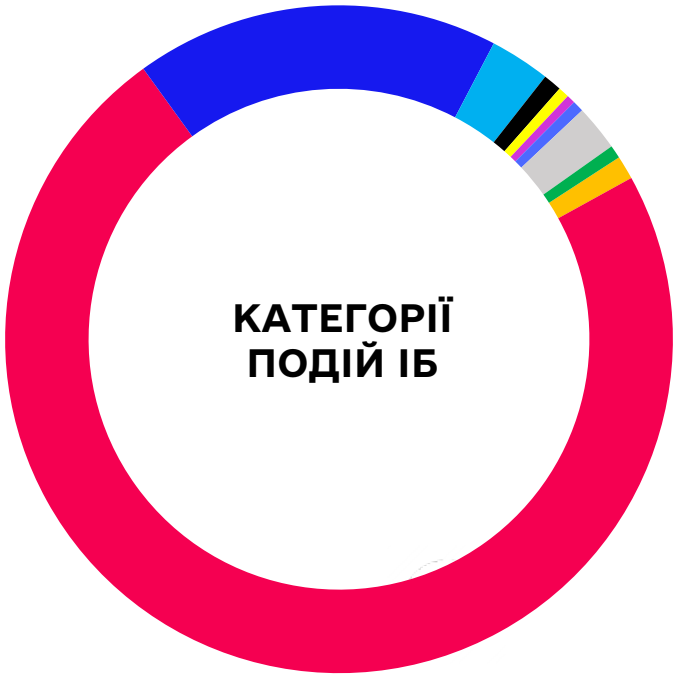
СТАТИСТИКА ПОДІЙ ІБ

КІЛЬКІСНІ ПОКАЗНИКИ ЗІБРАНИХ ТА ОПРАЦЬОВАНИХ ДАНИХ

представлена згідно

Переліку категорій кіберінцидентів

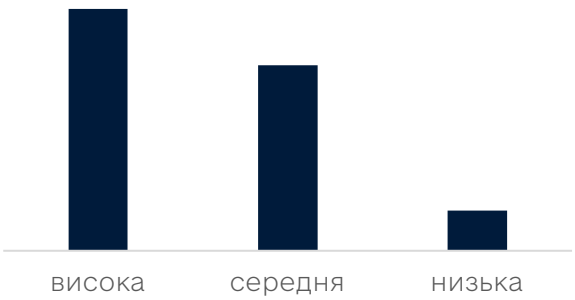
схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України



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

критичність кіберінцидентів

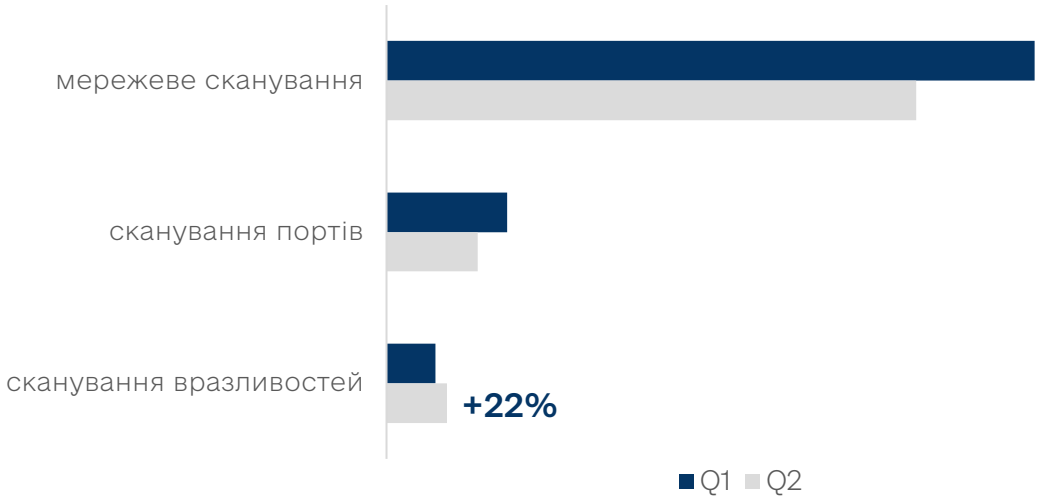
Графік відображає статистичну інформацію за звітний період, отриману шляхом аналізу зареєстрованих інцидентів кібербезпеки згідно внутрішньої системи оцінювання рівня критичності, відповідно до якої інциденти можна класифікувати за цим параметром

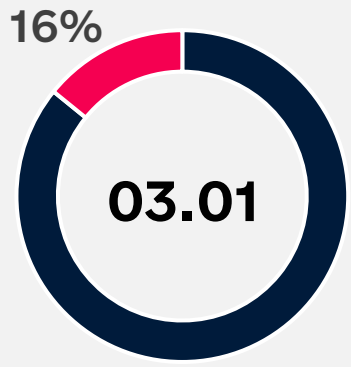


РОЗГЛЯНЕМО СТАТИСТИКУ ТИПІВ ПОДІЙ ІБ

які протягом II кварталу 2022 року домінують у відсотковому відношенні над іншими типами подій ІБ

за типом сканування





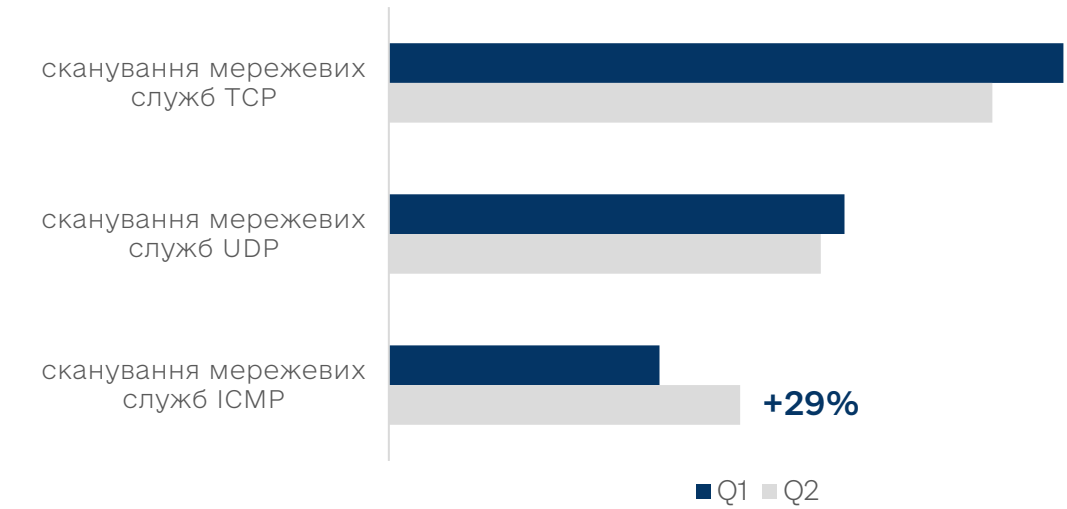
сканування

збір інформації про системи або мережі

за геолокацією IP-адрес джерел

**автоматично визначена геолокація IP-адреси не обов'язково означає атрибуцію подій ІБ в категорії 03.01 до ідентифікованого місцезнаходження*

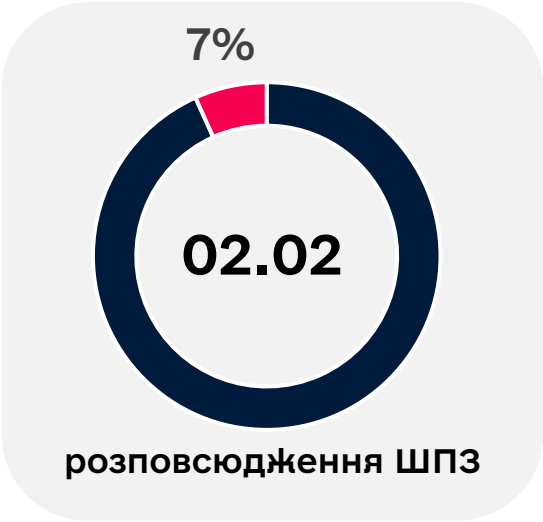
за методом сканування



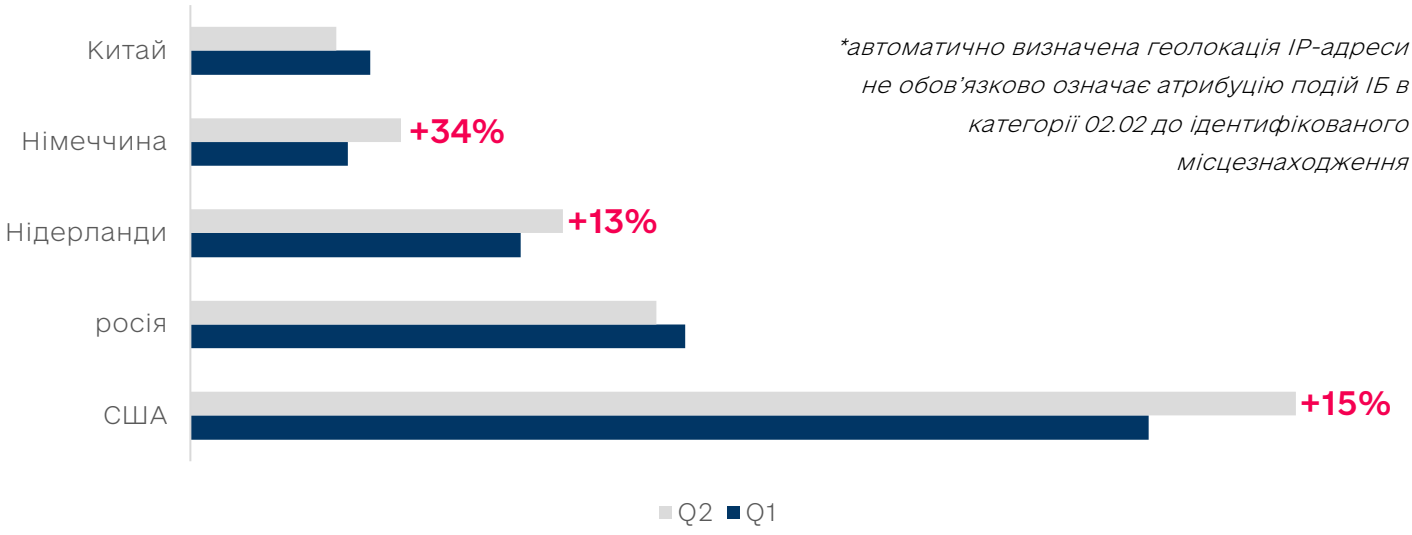
Порівняно зі статистичними даними за I квартал 2022 року, **протягом II кварталу 2022 року на 38% зросла кількість подій ІБ в категорії «Шкідливий програмний код»,** що свідчить про значне підвищення рівня шкідливої мережевої активності, пов'язаної з розповсюдженням ШПЗ і спробами його використання з метою залучення нових / експлуатації раніше інфікованих пристроїв бот-мереж.

408

підозрілих унікальних файлів було детектовано в автоматичному режимі підсистемою збору телеметрії Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки та оброблено безпосередньо аналітиками безпеки на предмет критичності протягом звітного періоду

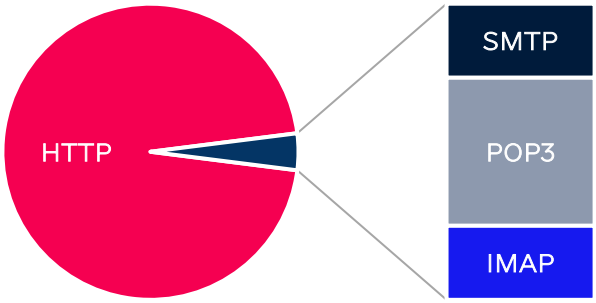


за геолокацією IP-адрес джерел

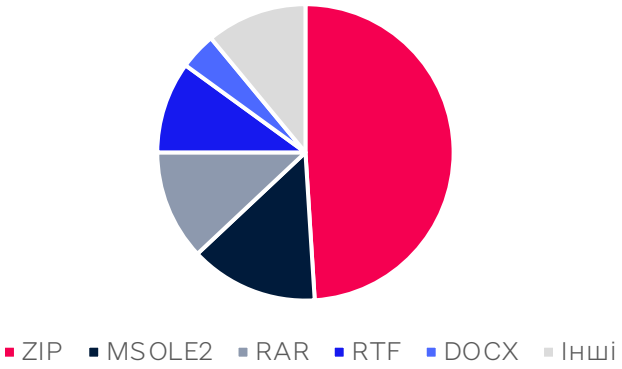


**автоматично визначена геолокація IP-адреси не обов'язково означає атрибуцію подій ІБ в категорії 02.02 до ідентифікованого місцезнаходження*

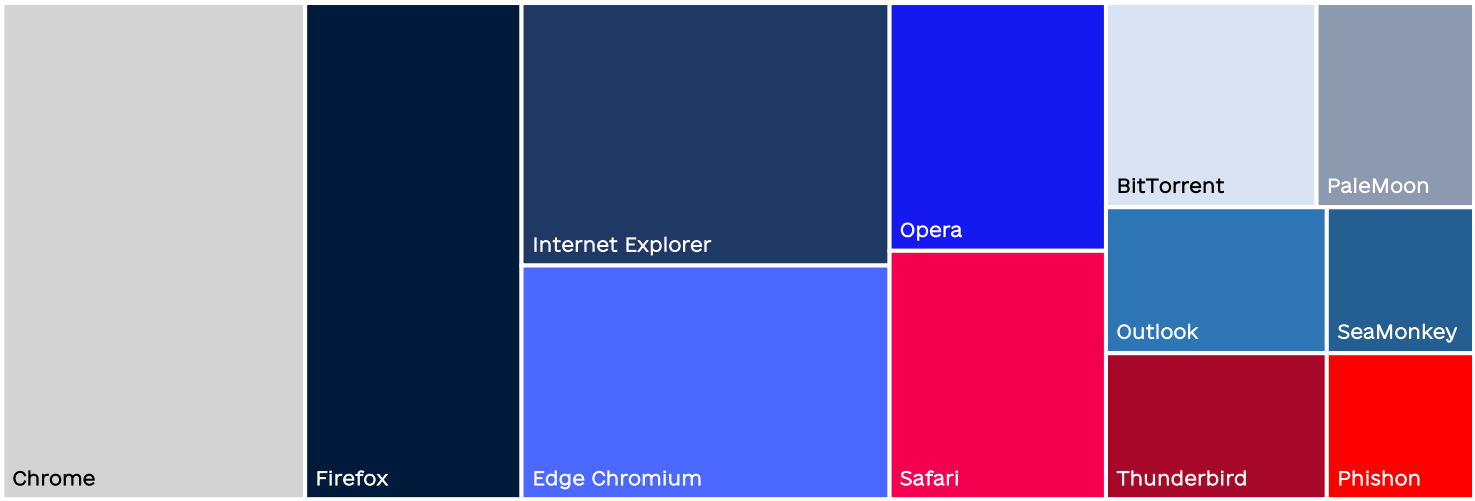
за протоколом розповсюдження ШПЗ



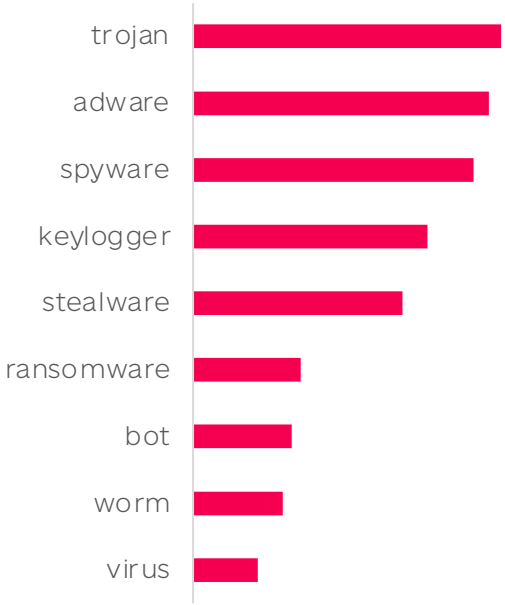
за форматом розповсюджуваного ШПЗ



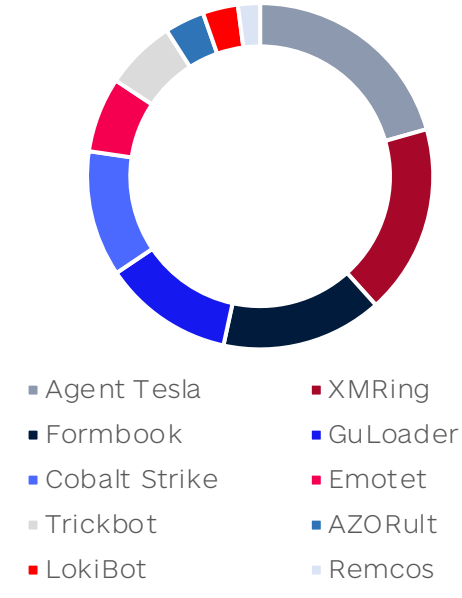
за асоційованим ПЗ клієнтів



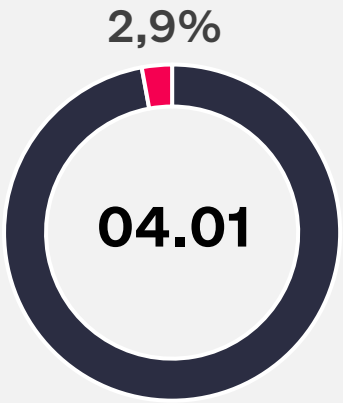
за типом ШПЗ



за сімейством ШПЗ



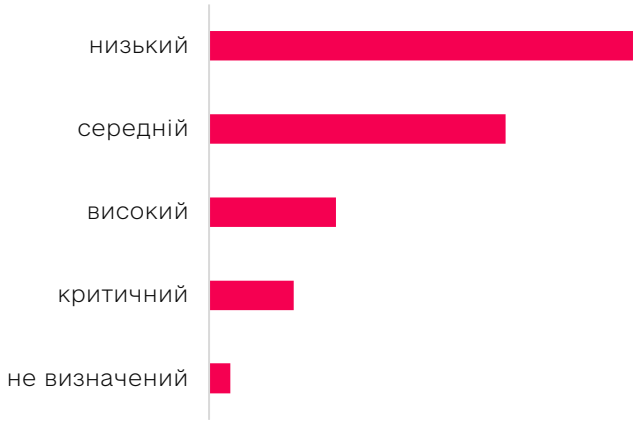
Графіки відображають статистичну інформацію за звітний період, отриману шляхом аналізу подій ІБ, джерелом яких є спроби вторгнення до мереж об'єктів кіберзахисту і реалізація кіберзагроз із метою виявлення вразливостей у програмному забезпеченні, знаходження проблемних конфігурацій сервісів і активних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



спроба експлуатації вразливості

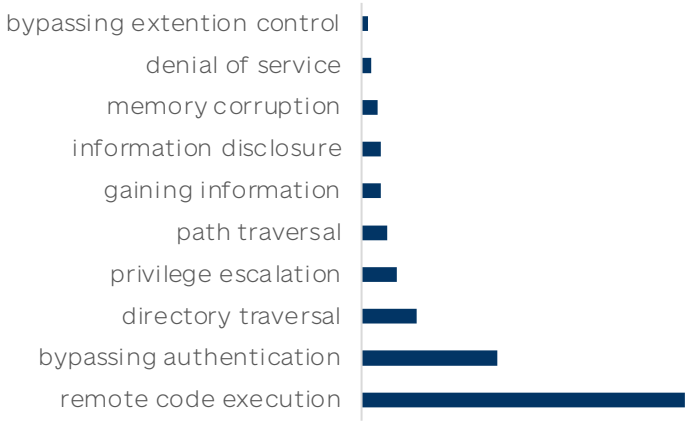
спроба вторгнення з використанням вразливості у системі, компоненті чи мережі

якісна оцінка за CVSS Base Score

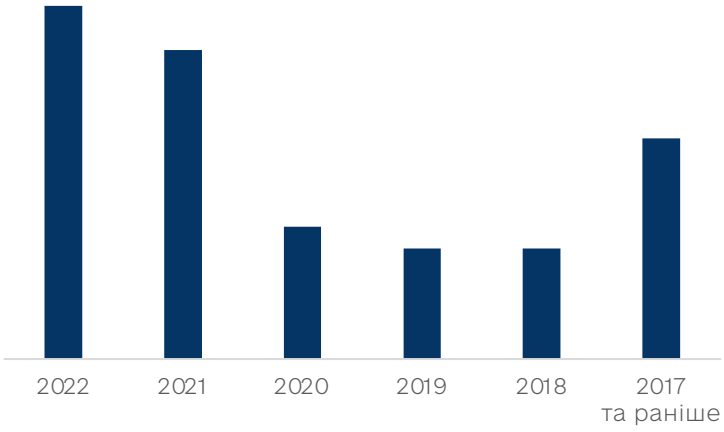


згідно з визначеним специфікацією CVSSv3.1 підходом до співставлення оцінок CVSS Base Score (1-10) до якісної шкали оцінювання

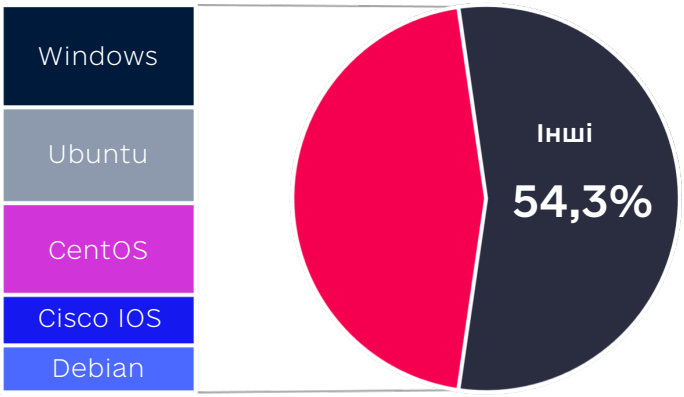
категорії експлуатованих CVE



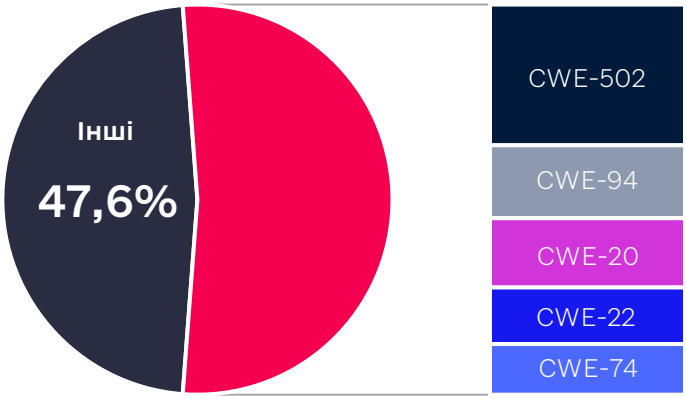
експлуатовані CVE за роком реєстрації



найбільш таргетовані ОС



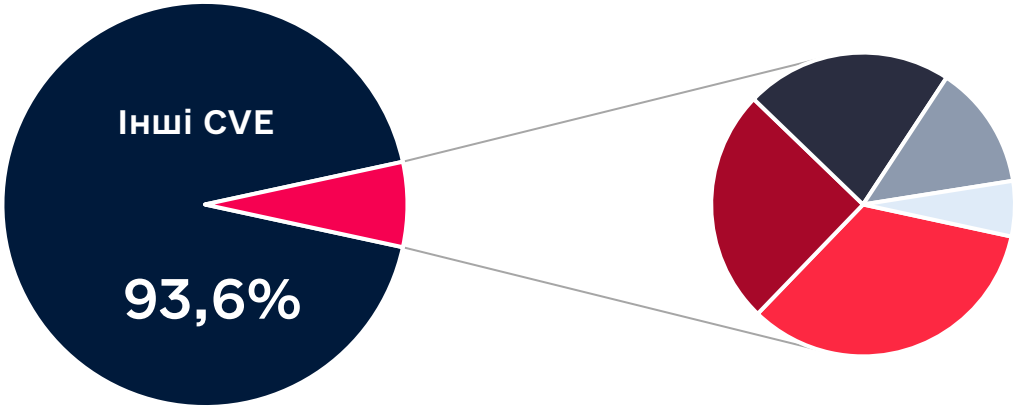
найбільш експлуатовані CWE



актуальні вразливості

Нижченаведений перелік актуальних вразливостей програмного забезпечення не є вичерпним та відображає CVE, що були задокументовані експертними групами кіберрозвідки і які продовжують активно експлуатуватись із метою отримання неавторизованого доступу або привілейованого контролю.

На графіку відображено % відношення виявленої активності в мережах клієнтів, потенційно пов'язаної з експлуатацією нижчеописаного переліку CVE, до загальної кількості детектувань активності, пов'язаної з усіма виявленими ідентифікаторами вразливостей за звітний період.



CVE-2022-26134

Вразливість компоненти *OGNL Handler* дозволяє реалізувати **віддалений неавторизований доступ до файлів і виконання довільного коду** у вразливих версіях продуктів Atlassian Confluence (Confluence Server і Data Center)

CVE-2022-30190

Вразливість інструменту *Microsoft Windows Support Diagnostic Tool (MSDT)*, більш відома як **Follina**, дозволяє реалізувати **виконання довільного коду** з привілеями викликаючого MSDT додатку у всіх ОС сімейства Windows (як звичайних, так і серверних)

CVE-2022-26809

Вразливість протоколу *Microsoft Remote Procedure Call (RPC)* дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду** з рівнем привілеїв служби RPC. Потенційно припускають активну експлуатацію цієї вразливості в майбутніх широкомасштабних кібератаках через можливість автономного запуску (незалежність від користувацької взаємодії)

CVE-2022-26925

Вразливість, пов'язана зі спуфінгом *Windows Local Security Authority (LSA)* при її застосуванні в атаках NTLM Relay на службу сертифікатів Active Directory дозволяє **автентифікуватись на контролері домену.** Актуальна для користувачів ОС, починаючи з Windows 7 (для серверних систем – з Windows Server 2008)

CVE-2022-26937

Вразливість у мережевій файловій системі *Windows Network File System (NFS)* дозволяє реалізовувати **віддалене неавторизоване виконання довільного коду** в контексті служби NFS

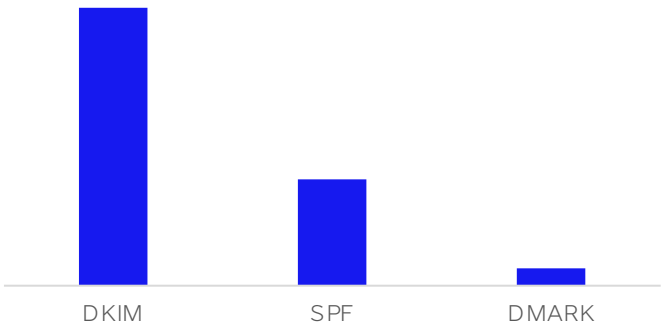
EMAIL SECURITY GATEWAY

з яких **21%**
заблокованих в автоматичному режимі

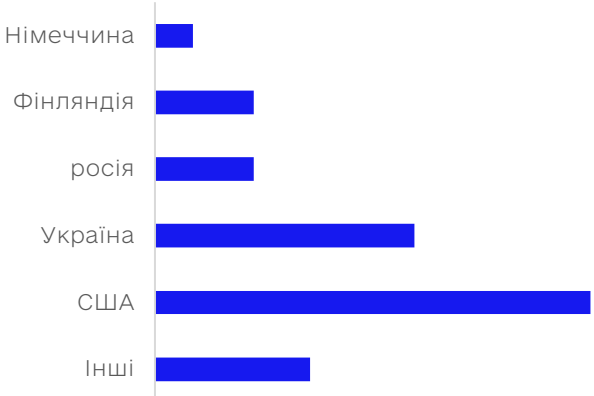
120 к
листів отримано та проаналізовано
за звітний період

Sender Validation failure reason

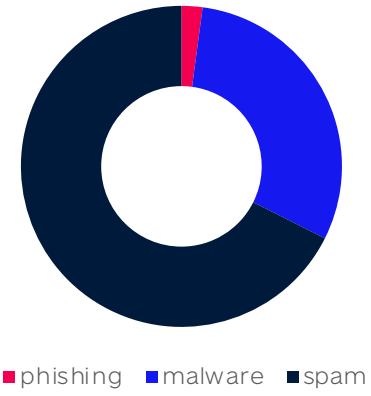
Sender Authentication failure reason



Sender Threat category (by country)



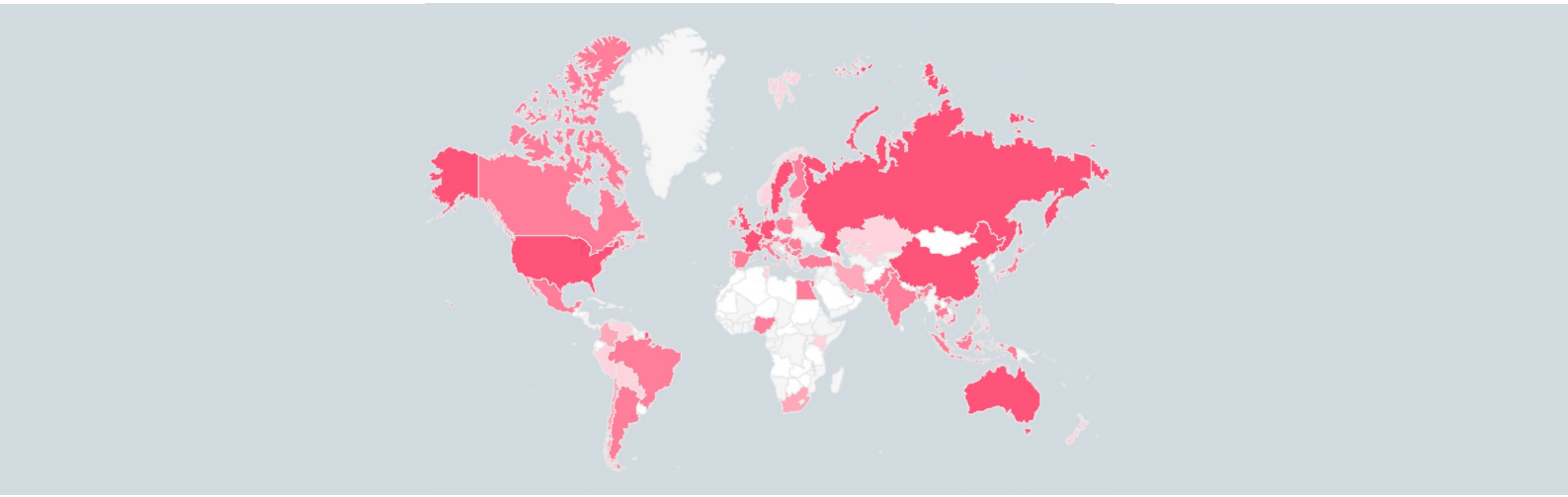
Sender Threat category

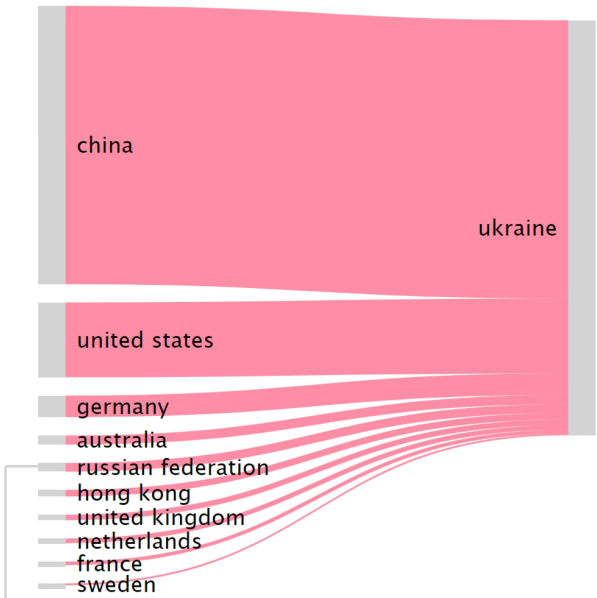


ГЕОГРАФІЯ ДЕТЕКТУВАНЬ

КРИТИЧНИХ ПОДІЙ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ*

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





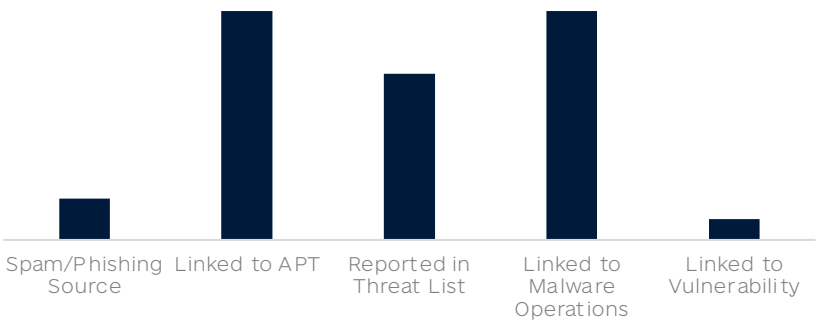
8,5 разів

настільки зменшилась кількість критичних подій ІБ, джерелом яких є IP-адреси росії (порівняно з I кварталом 2022 року). Це пов'язано більшою мірою з блокуванням AS, які використовуються рф, (з яких здійснюються кібератаки на українські інформаційні ресурси, розповсюджується фейкова інформація, що стосується дискредитації державних органів, ходу російсько-Української війни, тощо), постачальниками електронних комунікаційних мереж та/або послуг, що забезпечують доступ до інтернету

активність російських хакерських угрупувань

за секторами

за категоріями детектувань



THREAT ACTORS ACTIVITY

нижченаведений перелік відображає актуальні хакерські угрупування, таргетовані на інформаційні ресурси України, ідентифікатори активності яких були детектовані в мережах об'єктів кіберзахисту за звітний період

UAC-0010

Related names: Gamaredon, Armageddon, PrimitiveBear
Category: Nation State Sponsored
Location: russia
First Reference: 2013-2014

Детальніше: Кібератаки групи UAC-0010 (CERT-UA#4634,4648)
Кібератака групи UAC-0010 (CERT-UA#4434)

UAC-0056

Related names: Lorec53, SaintBear, GraphSteal, GrimPlant
Potential Category: Nation State Sponsored
Potential Location: russia
First Reference: Jul, 2021

Детальніше: Кібератака групи UAC-0056 (CERT-UA#4545)
Кібератака групи UAC-0056 (CERT-UA#4293)

UAC-0028

Related names: APT28, Fancy Bear, Iron Twilight, Sednit
Category: Nation State Sponsored
Location: russia
First Reference: Apr, 2013

Детальніше: Кібератака групи APT28 (CERT-UA#4843)
Кібератака групи APT28 (CERT-UA#4622)

UAC-0098

Related Malware: GzipLoader, IcelD, Cobalt Strike Beacon
Potential Related Threat Group: Trickbot/IcelD
Potential Location: russia
First Reference: Apr, 2022

Детальніше: Кібератака групи UAC-0098 (CERT-UA#4842)
Кібератака групи UAC-0098 (CERT-UA#4560)

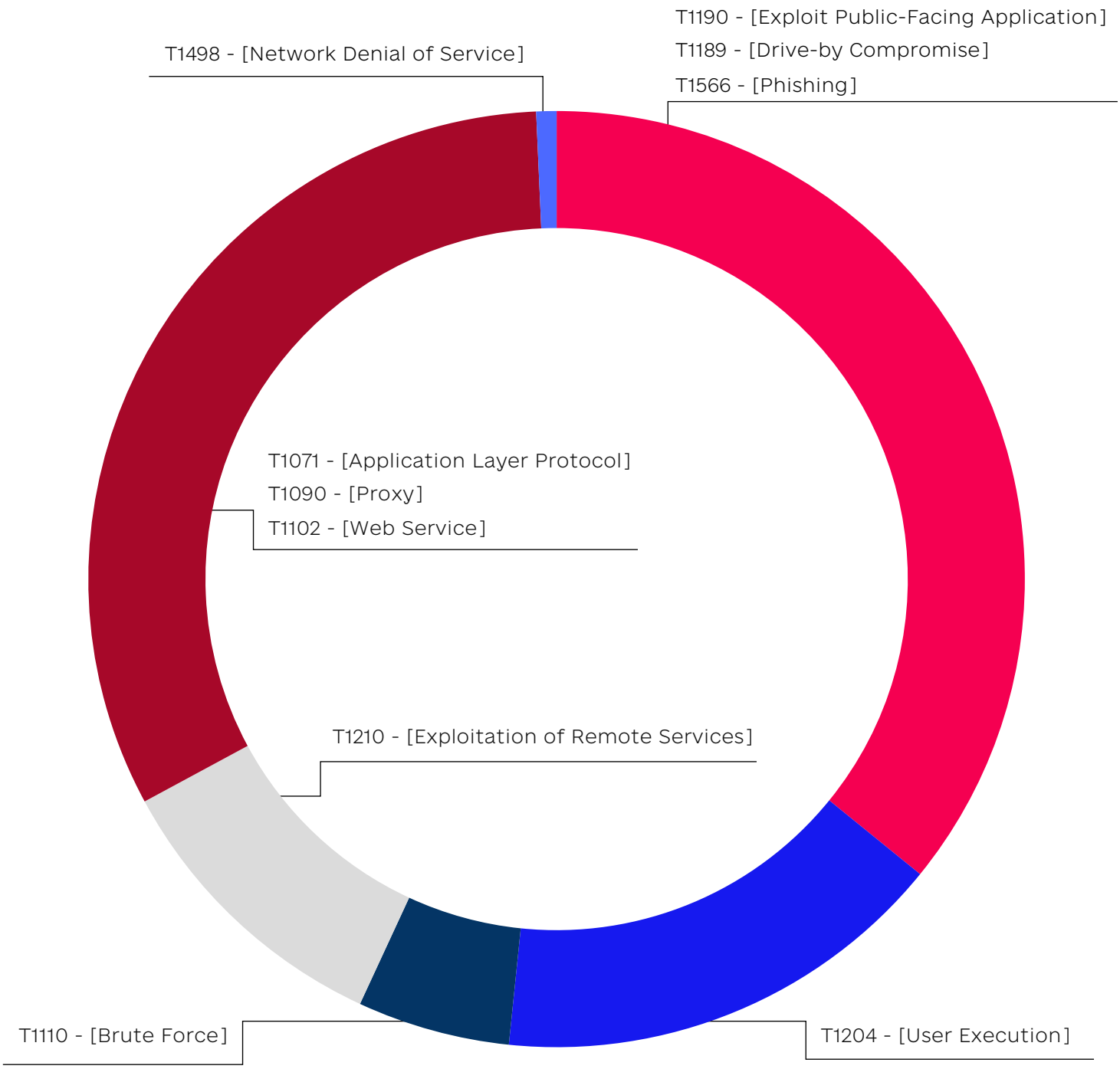
UAC-0082, UAC-0113

Related Malware: CrescentImp, DarkCrystal RAT
Potential Related Threat Group: Sandworm
Potential Location: russia
First Reference: Jun, 2022

Детальніше: Атака з використанням CrescentImp (CERT-UA#4797)
Атака з використанням DarkCrystal RAT (CERT-UA#4874)

MITRE ATT&CK MAPPING

статистика детектованих тактик/технік (відповідно до бази знань MITRE ATT&CK), асоційованих із набором виявлених та оброблених індикаторів, що використовувались на різних етапах життєвого циклу атак, які відбувались протягом звітного періоду



МЕТОДИЧНІ РЕКОМЕНДАЦІЇ

ЩОДО ПІДВИЩЕННЯ РІВНЯ КІБЕРЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Методичні рекомендації щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури розроблені відповідно до підпункту 1 частини другої та пункту 3 частини третьої статті 8 Закону України «Про основні засади забезпечення кібербезпеки України», абзацу другого частини першої статті 3, пунктів 85, 86 і 88 частини першої статті 14 Закону України «Про Державну службу спеціального зв'язку та захисту інформації України», абзацу другого підпункту 1 пункту 3 Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України, затвердженого постановою Кабінету Міністрів України від 3 вересня 2014 року № 411, та Загальних вимог до кіберзахисту об'єктів критичної інфраструктури, затверджених постановою Кабінету Міністрів України від 19 червня 2019 року № 518, з метою підвищення рівня кіберзахисту критичної інформаційної інфраструктури.

Рекомендації **розроблені з урахуванням Настанови для підвищення кібербезпеки критичної інфраструктури (Framework for Improving Critical Infrastructure Cybersecurity)**, виданої у 2014 році та оновленої у 2018 році Національним інститутом стандартів та технології Сполучених Штатів Америки (National Institute of Standards and Technology).

Рекомендації **не є нормативно-правовим актом, мають інформаційний та рекомендаційний характер, не встановлюють правових норм і є добровільними для використання**.

Рекомендації **описують загальний підхід до забезпечення кібербезпеки**, що дозволяє:

- здійснити аналіз та надати характеристику поточного стану кібербезпеки ОКІІ;
- описати цільовий стан кібербезпеки ОКІІ;
- ідентифікувати та визначити пріоритети, рівень упровадження заходів кіберзахисту в контексті безперервного та повторюваного процесу управління ризиками у сфері кібербезпеки ОКІІ;
- оцінити прогрес у досягненні цільового стану кібербезпеки ОКІІ;
- забезпечити комунікацію між суб'єктами, які безпосередньо перебувають на ОКІ, та із суб'єктами, які є партнерами організації щодо управління ризиками у сфері кібербезпеки.

Рекомендації **складаються з трьох основних частин**:

- системи (таксономії) заходів кіберзахисту;
- рівнів упровадження заходів кіберзахисту;
- профілю кіберзахисту.

Підхід, що визначається у Рекомендаціях, **не є єдиним підходом для управління ризиком кібербезпеки**, оскільки ОКІ, що належать різним секторам такої інфраструктури, можуть мати як однакові ризики, так і різні унікальні ризики – унікальні загрози, різні вразливості, різні допустимі рівні ризику. Підхід до забезпечення кібербезпеки залежить від того, яким чином організація впроваджуватиме заходи кіберзахисту, що наведені у цих Рекомендаціях.

Ознайомитись з Наказом Адміністрації Держспецзв'язку Про затвердження Методичних рекомендацій щодо підвищення рівня кіберзахисту критичної інформаційної інфраструктури

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