НОВИНИ

Мобілізація цигана? На Закарпатті натовп штурмував будівлю ТЦК, лунали постріли
9 ТРА, 2026

Оперативна інформація щодо російського вторгнення станом на 16:00 09.05.2026
9 ТРА, 2026

Лубінець повідомив про госпіталізацію дніпрянина з важкою травмою голови через дії ймовірних представників ТЦК
9 ТРА, 2026

ППО-ШІ-турель для перехоплення ворожих БпЛА пройшла бойове застосування (відео)
9 ТРА, 2026

Нові «покращення» для пацієнтів і лікарів запровадили в Україні: що зміниться від 20 травня
9 ТРА, 2026

Експравоохоронця затримали за новою підозрою у вчиненні злочину під час окупації Чернігівщини
9 ТРА, 2026

Польща запропонувала США посилити східний фланг НАТО – біля кордону з РФ
9 ТРА, 2026

Кроки до трибуналу над російським фашизмом: як Маріуполь документує злочини РФ
9 ТРА, 2026

БРАТВА

Тіньова економіка на стероїдах штучного інтелекту та як Telegram став

У ФОКУСІ

Десять років бігу на місці: як українська прокуратура навчилася змінювати вивіски, не змінюючи звичок

ІНШІ НОВИНИ

ДУМКИ ЧИТАЧІВ

«А МИ ТУТ ПРИ ЧОМУ?». Смертельна відмова за п'ять хвилин від порятунку та ціна байдужості київської підземки

Шантаж дітьми та помаранчеві мітки політв'язнів або історія виживання чернігівчанки в гомельській колонії

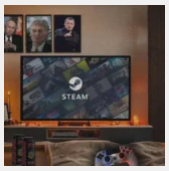
10 КВІ, 2026

Хапаємо по-прокурорськи. Рідня заступника генпрокурора заробляла по обидва боки фронту

10 КВІ, 2026

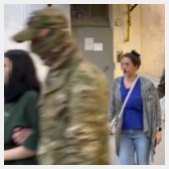
Геноцид під виглядом призову: як Кремль «зачищає» окуповані території від українських чоловіків

11 КВІ, 2026



Пропаганда у бібліотеці Steam: чому ігрові гіганти ігнорують війну та заробляють на російському ринку

11 КВІ, 2026



Конвеєр зникнень або як рашисти перетворили викрадення українців на систему контролю окупованих територій

11 КВІ, 2026

Операція Ходячі або як 81 рік тому чекісти розпочали ліквідацію Греко-католицької церкви в Україні

12 КВІ, 2026

COVID-19 ДТП Донбасс Київ Розшук дітей агрессия России атака дронами-камікадзе вбивство вбивство мирних жителів вимагання война война с Россией воєнні злочини РФ втрати окупантів війна з Росією грабіж державна зрада допомога союзників Україні замах на вбивство зловживання службовим становищем знищення окупантів колабораційна діяльність коронавирус коррупция корупція крадіжка напад Росії на Україну наркозлочини незаконне переправлення осіб через держкордон ножове поранення обстріли цивільної інфраструктури оперативна інформація пособники окупантів привласнення коштів підроблення документів п'яний за кермом ракетні удари окупантів розбій російські воєнні злочинці русский мир смертельна ДТП убийство хабар хуліганство шахрайство

голо вним офіс ом кібе рма фії

PUBLISHED 3 ТРАВНЯ 2026

Забудьте про самотніх геніїв у каптурах — сучасна кіберзлоч виглядає як кремнієва долина, де замість смузі п'ють сльози системни адміністр Глобальни ринок цифровог розбою розрісся до масштабі що перевищу економік

ФОТОРЕПОРТАЖ

Як виглядає українська ТЕЦ, що пережила не одну ракетну атаку російських загарбників

НОВИНИ IT

Технологии

Загрузка...

більшості країн світу, а сервісна модель “Злам як послуга” дозволяє будь-якому дилетанту влаштувати колапс корпорації за ціною підписки на Netflix. У цьому світі Telegram замінив Даркнет, а штучний інтелект пише фішингові листи краще за професійних копірайтерів. Поки ми вибудовуємо стіни, хакери просто купують ключі від наших дверей у “брокерів доступу”, перетворюючи кібервійну на найприбу

бізнес XXI століття.

У звітах з кібербезп прийнято описувати хакерські атаки як окремі події — але насправд за кожним успішним зламом стоїть ціла мережа взаємоза постачал послуг, посередн і виконавц Кіберзлоч давно перестал бути справою самітникі і перетвор на повноцін підпільну індустрію з власним ринком праці, ланцюгам постачан та навіть конкурен

між «вендора

За оцінками дослідни у 2025 році глобальні збитки від кіберзлоч сягнули $10,5 трлн на рік — більше, ніж ВВП будь-якої країни світу, крім США та Китаю, зазначає видання (Для порівнянн це вдвічі перевищу ВВП України за всю її незалежн історію, разом узяту. Кіберзлоч як сервісна модель зробила атаки доступни навіть для людей без

технічних знань: купити готовий інструмен для злому можна так само легко, як замовити доставку їжі.

Компанія з кібербезп в 2021 році системат цю екосисте розділив її на три великі категорії: послуги, дистрибу та монетиза Сьогодні ця структура залишає актуальн але кожна з категорій суттєво еволюціо — і доповнил двома новими вимірами яких п’ять років

тому просто не існувало: штучним інтелекто та Telegram як основним майданчи підпільно торгівлі.

Рівень перший: послуги та постачальники

Базова інфрастру кіберзлоч — це набір спеціаліз сервісів, які злочинні угрупован «орендую або купують замість того, щоб розробля самостійн Принцип той самий,

що й у легальної технології бізнесі: навіщо будувати власний дата-центр, якщо можна орендувати хмару?

Брокери початкового доступу (Initial Access Brokers)

Це, мабуть, найпомітніша категорія підпільного ринку останніх років. Брокери доступу — зловмисники, які спеціалізуються на зламі корпоративних мереж і наступному продажі цього доступу

іншим групам. Вони не проводят атаки самостійн — вони постачаю «відчинен двері».

За даними Group-IB, у 2024 році зафіксова понад 3 000 пропозиц продажу доступу до корпорат мереж — на 15% більше порівнянс з 2023 роком. Регіон Північної Америки показав найбільш приріст — 43%. Ціни варіюють від кількох сотень до десятків тисяч доларів залежно від

розміру організац та рівня привілеїв

Ranso mware-as-a-Service та Crime-as-a-Service

Модель «вимагач як сервіс» (RaaS) фактично демократ один із найприбу видів кіберзлоч Розробни програм-вимагачів більше не проводят атаки самостійн — вони створюют платформ й продають або здають в оренду доступ до неї афіліатам отримуюч від 10 до 30% від

кожного виплачен викупу.

У 2024 році Group-IB ідентифік 39 нових RaaS-оголошен і зафіксува 44-відсотков зростанн кількості афіліатів. Кількість атак через спеціаліз сайти витоків збільшил на 10% — до понад 5 000 задокуме випадків. У 2024 році одна компанія зі списку Fortune 50 виплатил рекордни викуп у $75 млн.

Послуг и анонімі зації та «кулен

епроби вний» хостин г

Інфрастру анонімно — ще один ключовий елемент підпільно ринку. Сюди входять резидент проксі-мережі (трафік маршрути через пристрої реальних користува що робить його майже невиявни приватні VPN-сервіси без журналів активнос а також «куленеп хостинг-провайде — компанії, що надають серверну інфрастру і свідомо ігнорують скарги

на
зловжива

Фішинг-набори та Webinject

Фішинг-набори — готові веб-інструмен для автомати фішингов атак — доступні на підпільни ринках за суми від кількох десятків доларів. Більш складні інструмен типу Webinject дозволяк вбудовува шкідливи код безпосер в браузер жертви під час відвідува банківськ сайтів — жертва бачить звичний інтерфейс

але
насправд
взаємодіє
зі
шкідливи
шаром.

Послуг
и з
вербув
ання та
«грошо
ві
мули»

Вербуван
звичайни
людей
для
участі у
злочинни
схемах —
окрема
спеціаліз
Так звані
«грошові
мули»
фізично
знімають
готівку із
зламаних
рахунків
або
отримуют
переказ
на
власний
рахунок,
а потім
пересила
кошти
далі по
ланцюжк
відмиван
Частину
цих
людей

свідомо вербують на підпільни форумах; інші стають жертвами шахраїв, які пропонук «легкий заробіток

Рівень другий: дистрибуція та доставка атак

Навіть найдоско шкідливе програмн забезпеч марне без механізм доставки Саме тому дистрибу — окремий сегмент підпільно ринку з власними спеціаліс

та
сервісами

**Спам- та
фішингов
кампанії**
найпоши
інструме
початков
проникне
За
даними
ENISA,
фішинг є
домінуюч
вектором
злому в
60%
задокуме
інциденті
у
Євросою
Окремі
групи
спеціаліз
виключно
на
масових
розсилка
— вони
не
розробля
шкідливе
ПЗ і не
монетизу
дані,
їхній
«продукт»
— це
охоплення
аудиторії.

Ще одна
ключова
категорія
— **заванта
або
«лоадери**
Це

угрупован
які вже
контролю
заражені
пристрої
і
пропонує
«встанови
шкідливе
ПЗ іншої
групи у
вже
скомпром
мережі.
Фактично
це
послуга
субпідряд
одна
група
будує
плацдарм
інша —
його
використ
для
власних
цілей.

Exploit-кити — набори для автомати експлуата вразливо у браузера та плагінах — дозволяю заражати пристрої жертв без будь-якої взаємодії

з їхнього боку: достатньо просто відвідати скомпром сайт. Трафік на такі сайти перенапр через зламані легітимні веб-ресурси, що ускладню виявленн

Рівень третій: монетизація — перетворення злому на гроші

Зламати мережу — лише половина справи. Наступна задача — конверту

здобуті дані чи доступ у реальні кошти, залишаю при цьому невиявле Монетиза — найрізном сегмент кіберзлоч екосисте

Кардинго форуми з основним ринком збуту викраден платіжни даних. Ціна залежить від типу картки, країни та наявност повного «дампу» з CVV-кодом. Окремі сервіси перевірки карток дозволяю автомати верифікує дійсність тисяч номерів за лічені хвилини.

Відмиван грошей

еволюціо
разом із
криптова
та
«тумблер
сервіси,
що
перемішу
криптотра
для
приховува
їхнього
походжен
— стали
стандарті
інструмен
За
даними
Chainalysi
загальний
обсяг
криптозл
у 2024
році
перевищи
$51
млрд.
Паралель
існують
мережі
підставни
компаній
для
відмиван
коштів
через
легальні
банківськ
канали.

«Шахрайс
перепрод
схема, за
якої
викраден
кошти
конверту
в реальні

товари (зазвичай електроні ювелірні вироби або автомобіл які потім перепрод за готівку. Це ускладню відстежен гроші «очищаю через легальний товарний ринок.

Вимаганн — ще одна форма монетиза що вийшла далеко за межі класично ransomwa Сьогодні поширена **атака»**: зашифру дані і водночас погрожув їх публікаці Деякі угрупован повністю відмовил від шифруван й

займають
виключно
крадіжкою
та
шантажем
— це
простіше
й так
само
прибутков

Новий вимір: штучний інтелект як підсилювач злочинності

П’ять років
тому ШІ у
кіберзлоч
був
екзотикою
Сьогодні
він
вбудован
у
підпільну
екосисте
як
стандарт

інструмен
Дослідни
Trend
Micro
зафіксува
принципо
зміну:
злочинці
більше
не
будують
ШІ-
інструмен
самостійн
— вони
купують
готові
сервіси
або
зламують
легальні
платформ

Jailbreak-as-a-Service — окремий сегмент ринку: постачал продають методи обходу захисту комерційн мовних моделей (ChatGPT, Claude, Gemini) для генерації фішингов листів, сценаріїв соціальнс інженерії та

шкідливо
коду. На
підпільни
маркетпл
також
продають
скомпром
акаунти
ChatGPT і
Claude —
для
масової
автомати
або
обходу
санкційни
обмежень
(актуальн
для росії,
Ірану та
Північної
Кореї, де
доступ
до цих
сервісів
заблокова

Дипфейк-
технології
із
курйозу
на
інструмен
корпорат
шахрайст
Зафіксова
випадки,
коли
зловмисн
підробля
відео- та
аудіозвер
керівникі
компаній,
щоб
змусити
фінансові
співробіт

здійснити
великі
перекази.
загроз
Europol
за 2025
рік прямо
попередж
злочинні
угрупован
дедалі
активніш
використ
генератив
ШІ для
масштабу
фішингу
та
шахрайсь
операцій.

Паралель
з’являють
перші
зразки
шкідливо
ПЗ, що
динамічн
генеруют
власний
код за
допомого
вбудован
мовних
моделей
—
адаптуюч
до
конкретн
середови
та
ускладню
виявленн
Поки що
ці
техніки
залишаю
нішевими

через нестабіль і залежніст від зовнішніх API, але тенденція зафіксова

Нова інфраструктура: Telegram замінив даркнет

Якщо п’ять років тому основним майданчи підпільно торгівлі були анонімні форуми в мережі Tor та даркнет-маркетпл то сьогодні центр ваги змістився в бік Telegram. Дослідже

компанії Cyfirma підтверд
став основно
платфор
для хакерів.

Масштаб
вражают
Лише через одну групу в Telegram — Huione Guarantee — з 2021 по 2025 рік пройшло $27 млрд транзакці пов’язан із незаконн діяльніст Це перевищу обіг найвідом даркнет-маркетпл за всю їхню історію. Коли в травні 2025 року Telegram заблокув цей канал, його місце миттєво

зайняли клони — і за лічені місяці новий канал досяг обігу в $1,1 млрд.

Telegram приваблю злочинціе з кількох причин: відносна анонімніс можливіс створюва великі закриті групи, зручна інтеграція з криптова. ботами та значно нижча технічна складніст порівнянс з Tor. Продаж зламаних баз даних, кредитни карток, інструмен для кіберзлоч вербуван «грошови мулів» — все це

відбувает
у
відкритих
і
закритих
каналах
із
мінімальн
модераці

*Після
арешту
Павла
Дурова у
Франції в
серпні
2024
року
Telegram
оголосив
про
передачу
правоохо
органам
даних
користува
які
займають
незаконн
діяльніст
У 2024
році
платформ
заблокува
понад
15,3 млн
каналів і
груп.
Попри це,
за
спостереж
дослідник
кіберзлоч
активніст
у
Telegram
продовжу
зростати.*

Чому таргетування постачальників ефективніше, ніж переслідування виконавців

Відстежит
всі
зв’язки
між
угрупован
та їхніми
постачал
—
завдання
надсклад
через
широке
використ
зашифро
каналів
зв’язку
та
криптова
Однак
аналітичн
компанія
Chainalysi
ще в
2021 році
сформулю

принцип, який залишає актуальни правоохо органи досягают кращих результат якщо атакують спільну інфрастру а не кінцевих виконавц

Логіка проста: знищити один RaaS-сервіс означає одночасн вивести з ладу десятки угрупован які ним користува Зламати мережу «куленеп хостингу — позбавит інфрастру цілий кластер злочинни операцій. Цей підхід показав реальні результат операції

проти
інфрастру
та
ALPHV/Bl
(2024)
завдали
значно
більших
збитків
кіберзлоч
екосисте
ніж
точкові
арешти
окремих
хакерів.

Є й інша
перевага:
постачал
підпільни
послуг
зазвичай
мають
слабшу
операційн
безпеку,
ніж
найбільш
злочинні
угрупован
Їхні
«сліди»
залишаю
в даних,
які потім
допомага
ідентифік
клієнтів
вищого
рівня.

Конте
кст
для

Украї
ни

Україна
перебуває
в
специфічн
положенн
вона є
одночасн
і
мішенню
найактив
у світі
державни
хакерів, і
країною,
де
кіберзахи
перетворі
на
питання
національ
безпеки.
Важливо
розуміти:
між
«комерції
кіберзлоч
та
державни
кібератак
—
насампер
з боку
росії —
межа
часто
розмита.

Дослідже
Trend
Micro
характери
російськ
кіберзлоч
екосисте
як

«найсофіс
та
найстійкіі
у світі».
Частина
угрупован
що
формальн
є
«комерції
фактично
діє в
інтересах
або за
замовлен
спецслуж
—
особливо
в
контексті
повномас
вторгнен
в
Україну. C
UA регуля
фіксує
атаки з
використ
тих
самих
інструмен
і
інфрастру
що їх
продають
на
підпільни
маркетпл

Джерело:
CybercalM

Like
Tweet

Tags:

Telegram

кіберзлочинність

хакери

YOU MAY ALSO LIKE...

Миллионные штрафы и конфискация: к

Реформа тюремної медицини: добрі

Как «воры в законе» скрываются от пр

Новини

Процеси