Держспецзв’язку фіксує зміну тактики хакерів: від стілерів до довгострокової компрометації

Держспецзв’язку фіксує зміну тактики хакерів: від стілерів до довгострокової компрометації

Є в Україні один документ, який виходить двічі на рік, якого ніхто не чекає з нетерпінням, але який варто читати уважніше за гороскоп. Це аналітичний звіт CERT-UA — Національної команди реагування на кіберінциденти при Державній службі спеціального зв’язку та захисту інформації.

Свіжий випуск за друге півріччя 2025 року написаний мовою, якою зазвичай пишуть інструкції до пральних машин — сухо, точно, без емоцій. Але якщо перевести його з бюрократичної на людську, виходить доволі моторошна історія про те, як ціла країна щодня живе під цифровим обстрілом, і чому навіть зменшення кількості «прильотів» — не привід розслаблятися.

Розбір звіту CERT-UA за друге півріччя 2025 року для тих, хто не читає PDF-ки від Держспецзв’язку, але, мабуть, мав би.

Менше інцидентів, більше тривоги

Головна новина звіту звучить майже оптимістично: вперше з початку повномасштабного вторгнення кількість кіберінцидентів у півріччі зменшилась. Було 3 018 — стало 2 909, мінус чотири відсотки. Жодного критичного інциденту. Інцидентів високого рівня — п’ять замість шести. Здавалось би, відкривай шампанське.

Читайте по темі: Онлайн-сервіс «BitCapital» викрили у схемі з погрозами боржникам на понад 5 мільйонів гривень

Але CERT-UA — люди, які шампанське відкривають рідко і з підозрою дивляться на будь-яку пляшку, що шипить. Тому вони одразу пояснюють: зменшення кількості не означає зменшення загрози. Противник не став добрішим і не пішов у відпустку. Він змінив тактику. І ця нова тактика — значно неприємніша за стару.

У першому півріччі 2025-го серед хакерських угруповань була популярна модель, яку аналітики охрестили «Steal & Go» — вкради й тікай. Зловмисник закидав жертві стілер (програму для крадіжки даних), вичавлював з комп’ютера все цінне за кілька хвилин і зникав, не залишаючи слідів. Швидко, ефективно, мінімальний ризик виявлення. Щось на кшталт кишенькової крадіжки в метро: поки ви помітили — злодій уже на іншій станції.

У другому півріччі модель змінилась. Тепер хакери не тікають. Вони заходять, озираються, знаходять зручне місце і залишаються. CERT-UA фіксує зміщення акценту з одноразового викрадення інформації на отримання стійкого несанкціонованого доступу. Іншими словами, замість «вкради й тікай» — «зайди й живи». Компрометація перестала бути подією і стала початком тривалих стосунків. Без згоди другої сторони, зрозуміло.

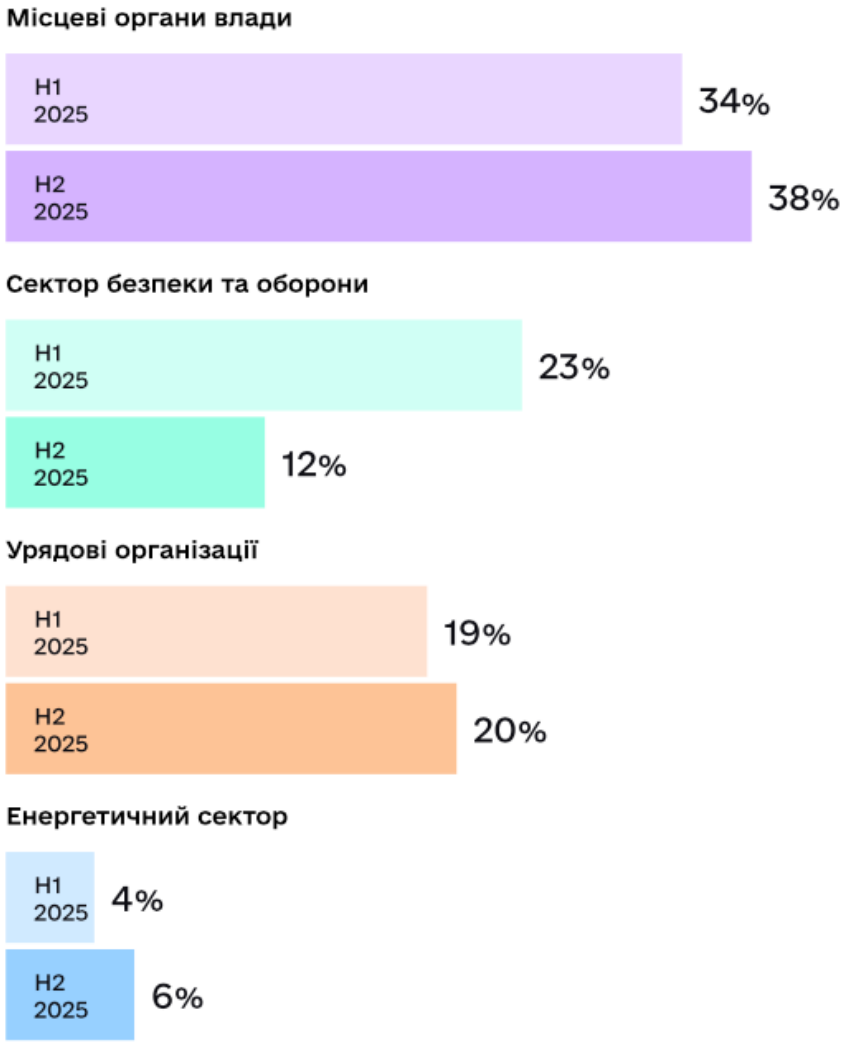
Вони повертаються

Окремий розділ звіту присвячений явищу, яке будь-який IT-фахівець зустріне з нервовим посмикуванням ока. Зловмисники повертаються до раніше скомпрометованих систем. Не тому, що забули щось вкрасти. А тому, що хочуть перевірити: чи ви усунули причину зламу, чи просто перезавантажили сервер і помолились?

І часто з’ясовується, що помолились. CERT-UA делікатно формулює це як «неповне усунення причин попереднього інциденту». Менш делікатно це звучить так: організація пережила кібератаку, відновила працездатність системи, видихнула і вирішила, що все минулося. А через місяць ті самі хакери зайшли через ту саму діру, яку ніхто не залатав. Це не гіпотетичний сценарій — це реальні випадки з українського кіберпростору другого півріччя 2025 року.

Хто по кого приходить

Четвірка головних мішеней залишається незмінною і виглядає саме так, як ви очікуєте від країни, що перебуває у стані війни. Урядові організації — 38 відсотків усіх інцидентів (було 34). Місцеві органи влади — 23 відсотки (було 20). Сектор безпеки та оборони — 6 відсотків у статистиці CERT-UA, але ця цифра — лукава, бо значна частина атак на військових опрацьовується кіберпідрозділами ЗСУ і в цю статистику просто не потрапляє. Енергетичний сектор тримається на четвертому місці з 4 відсотками.



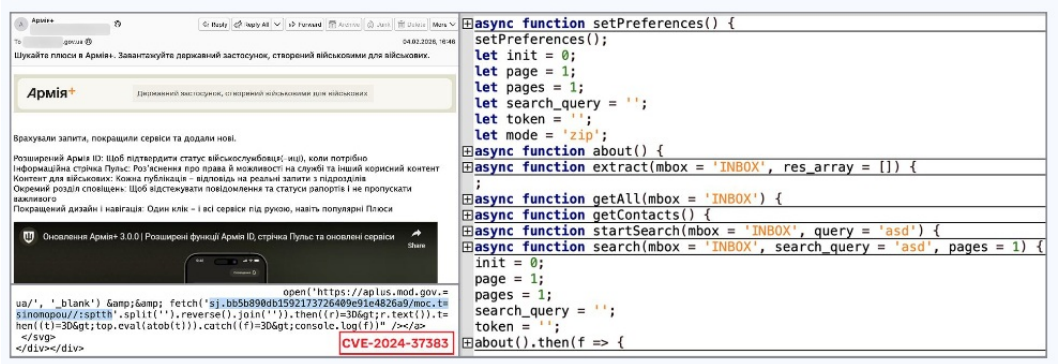
Цікаво інше: попри те, що розсилок шкідливого програмного забезпечення стало більше, кількість реальних заражень зменшилась. Люди, виявляється, поступово вчаться не клікати на все, що блимає. Три з половиною роки війни — непоганий курс цифрової грамотності, хоча й дещо дорогий.

Читайте по темі: Поліція “на абонементі”: як Руслан Герасимчук і Андрій Чайковський закривають очі на шахрайські кол-центри Миколайчика

Нові обличчя, старі наміри

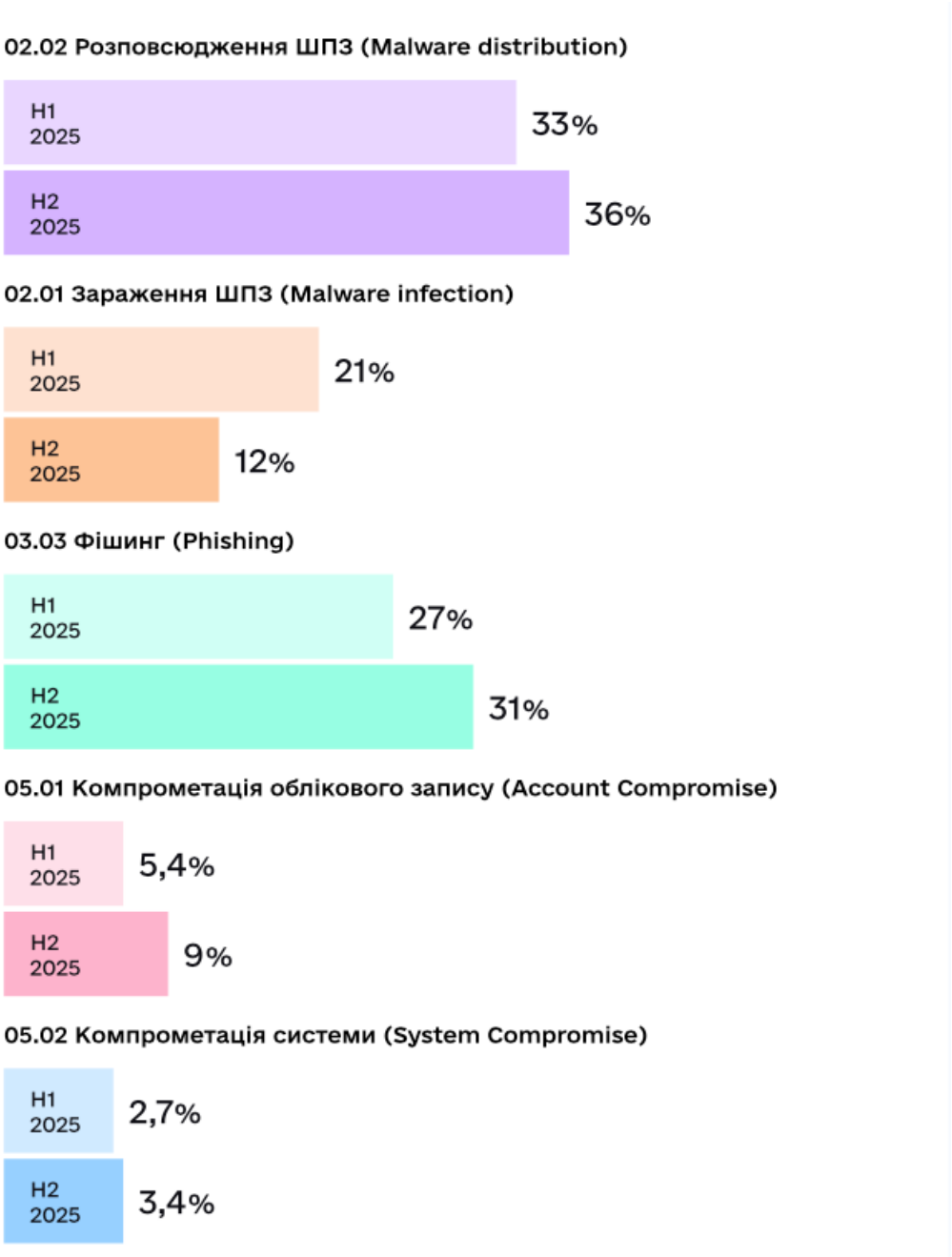
Звіт фіксує появу нових кластерів кіберзагроз — у класифікації CERT-UA кожне хакерське угруповання отримує код UAC з порядковим номером. У другому півріччі з’явилися кілька «новачків», хоча слово «новачок» тут звучить так само недоречно, як «початківець» стосовно кишенькового злодія з двадцятирічним стажем.

Особливу тривогу викликають так звані zero-click атаки — ті, де жертві навіть не треба нічого натискати. Достатньо просто отримати листа. Угруповання UAC-0233 та UAC-0250 експлуатували вразливості поштових серверів Roundcube та Zimbra, які дозволяли виконувати шкідливий код без будь-якої взаємодії з боку користувача.



Приклад активності UAC-0233

Лист приходить, код виконується, поштова скринька — включно з листуванням, резервними кодами двофакторної автентифікації та паролями застосунків — пакується в архів і відправляється зловмисникам. Жертва при цьому навіть не підозрює, що щось відбулося. Це як обікрасти квартиру, поки господар сидить у вітальні і дивиться серіал.



Повернулись і кібервимагачі — ті, хто шифрує ваші файли і вимагає гроші за розшифрування. UAC-0238 з липня 2025 року атакував органи місцевого

самоврядування за допомогою програм-вимагачів сімейства Proton. Точкою входу слугував старий добрий RDP, виставлений в інтернет — те, про що кібербезпековці кричать останні десять років, але що й досі стирчить назовні в половині українських держустанов, як незачинені двері підвалу.

Друге угруповання вимагачів, UAC-0243, використовувало варіацію сумнозвісного LockBit 3.0 під назвою X2anylock (або Warlock). Заходили через вразливі сервери Microsoft SharePoint, а для горизонтального переміщення мережею використовували абсолютно легітимні інструменти — Cloudflare Tunnel, Velociraptor та RClone. Тобто зламували вас за допомогою тих самих програм, якими ви, можливо, й самі користуєтесь. Аналогічні атаки CERT-UA фіксує проти держорганів Португалії, Хорватії та Туреччини — Україна в цьому клубі потрапила не за власним бажанням, а за географічним принципом: якщо ви в зоні інтересів російських спецслужб, вам рано чи пізно прийдуть.

WinRAR, яким б’ють двічі в одну воронку

Є в цьому звіті деталь, від якої хочеться одночасно сміятись і плакати. Одна з найпоширеніших технік другого півріччя — експлуатація вразливості WinRAR з кодом CVE-2025-8088. Для тих, хто не стежить за кібербезпекою щоденно: WinRAR — це програма для розпакування архівів, якою в Україні користуються приблизно всі, і яка вже котрий рік є улюбленою «дверима» для хакерів.

Вразливість дозволяє при розпакуванні архіву непомітно створити додатковий файл у директорії автозавантаження Windows. Тобто ви розпаковуєте нібито нешкідливий архів з документом, а десь у надрах системи тихенько з’являється файл, який запуститься при наступному включенні комп’ютера. Інформацію про вразливість оприлюднили в серпні, а вже з вересня почались масові розсилки з експлойтами. Першим цю діру використало угруповання UAC-0010 (воно ж Gamaredon, воно ж — структурний підрозділ ФСБ Росії, розташований у тимчасово окупованому Криму). Потім підтягнулись UAC-0002, UAC-0226 та інші. Ефективна вразливість в екосистемі російських хакерських груп поширюється зі швидкістю вірусного відео — хтось знайшов, усі скопіювали.

Той самий UAC-0010, відомий своєю параноїдальною наполегливістю — на одному зараженому комп’ютері він створює більше сотні шкідливих файлів у різних директоріях — у 2025 році освоїв ще й альтернативні потоки даних (Alternate Data Streams, ADS). Це штатна функція файлової системи NTFS, яка дозволяє зберігати додаткові дані, прив’язані до файлу. Фішка в тому, що ці потоки не видно у звичайному провіднику Windows. Файл може мати розмір 0 байт і виглядати абсолютно порожнім, але в його альтернативному потоці буде сидіти повноцінний шкідливий код. Це як подвійне дно у валізі, тільки цифрове.

Коли хакер дзвонить по телефону

Але найелегантнішою — і найнебезпечнішою — зміною другого півріччя стала еволюція соціальної інженерії. Тут варто процитувати звіт дослівно в одному реченні, бо воно заслуговує на те, щоб його повісити на стіну кожного кібербезпековця: «Первинна взаємодія з об’єктами атак дедалі частіше здійснюється з використанням телефонних номерів українських мобільних операторів і легітимних облікових записів».

Розшифровую. Російські хакери — зокрема APT28 (вони ж UAC-0001, вони ж підрозділ ГУ Генштабу ЗС РФ, тобто військова розвідка) та Void Blizzard (UAC-0190) — тепер не просто надсилають фішинговий лист з вкладенням. Вони спершу дзвонять. З українського номера. Розмовляють українською. Використовують аудіо- та відеозв’язок. Демонструють знання про конкретну людину та організацію. Встановлюють довіру. І лише потім, після живого спілкування, надсилають у месенджер «службовий документ» — XLS-файл

із макросом, який відкриває двері у вашу систему.

APT28 провело таким чином масштабну кібероперацію проти українських військовослужбовців та працівників підприємств оборонно-промислового комплексу. Файл був замаскований під службову документацію. Жертва отримувала його не від невідомого відправника, а від «колеги», з яким щойно розмовляла по телефону. Рівень довіри — максимальний. Рівень підозри — нульовий.

Це якісний стрибок. Від масових фішингових розсилок, де один лист з тисячі «вистрілить», — до точкових операцій, де кожна атака підготовлена індивідуально, з розвідкою, легендою та акторською грою. Кіберспецоперації дедалі більше нагадують класичну розвідку: вербувальний підхід, встановлення контакту, формування довіри, отримання доступу.

Скомпрометовані роутери як зброя

Ще один тривожний тренд — використання скомпрометованих українських пристроїв як проміжних вузлів для атак. Угруповання UAC-0002 (Sandworm, він же підрозділ ГРУ, відповідальний за найбільш деструктивні кібератаки в історії України) після компрометації об’єкта критичної інфраструктури було виявлено завдяки моніторингу спроб повторної автентифікації у вже змінені облікові дані. Спроби підключення йшли з українських IP-адрес, і всі ці адреси мали спільну рису — публічно доступну панель адміністрування мережевого пристрою.

Тобто ваш роутер з паролем admin/admin або з незакритою адмін-панеллю може прямо зараз працювати як проміжний вузол у ланцюзі атаки російської військової розвідки на українську критичну інфраструктуру. Хакери вмикали на таких пристроях SOCKS-проксі та SSH-тунелювання, перетворюючи побутовий роутер на елемент наступальної кіберінфраструктури. Щоб ускладнити відстеження, використовувались ланцюги з кількох таких пристроїв — щось на кшталт цифрової версії «естафети», де кожен вузол знає лише попередній і наступний.

Що з усього цього випливає

Звіт CERT-UA — це не паніка і не алармізм. Це холодна фіксація реальності, в якій Україна живе вже четвертий рік. Кіберпростір залишається повноцінним театром воєнних дій, де щодня відбуваються тисячі зіткнень, про які не пишуть у зведеннях Генштабу, але які можуть мати наслідки не менш серйозні, ніж ракетний удар по енергоінфраструктурі.

Позитив є: кількість інцидентів вперше знизилась, заражень стало менше при більшій кількості розсилок, критичних інцидентів не було. Українські організації поступово адаптуються — десь краще налаштували захист, десь працівники нарешті навчились не відкривати підозрілі файли.

Але негатив переважає. Противник стає розумнішим, терплячішим і винахідливішим. Він більше не б’є навмання — він цілиться. Він більше не тікає після крадіжки — він оселяється. Він більше не пише корявих фішингових листів з помилками — він телефонує вам особисто, називає по імені і знає, в якому підрозділі ви служите.

І поки WinRAR залишається на кожному другому комп’ютері держслужбовця, поки RDP стирчить в інтернет з паролем «qwerty123», поки після кіберінциденту обмежуються перезавантаженням замість повноцінного розслідування — ці 2 909 інцидентів за півріччя будуть не зменшуватись, а зростати. Бо противник вчиться швидше, ніж ми латаємо діри.

А якщо вам здається, що все це вас не стосується, бо ви не працюєте ні в уряді, ні в армії, — перечитайте абзац про роутери. Той сірий прямокутник з антеною, що стоїть у вас під телевізором, прямо зараз може працювати на

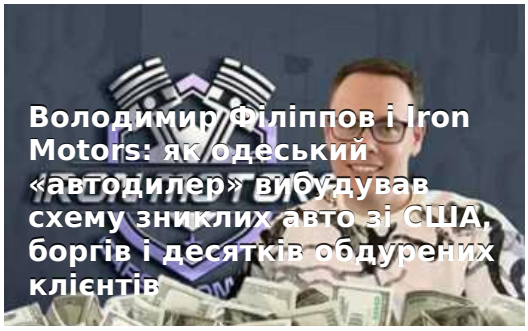
ворога. І він, на відміну від WinRAR, навіть ліцензії не потребує.

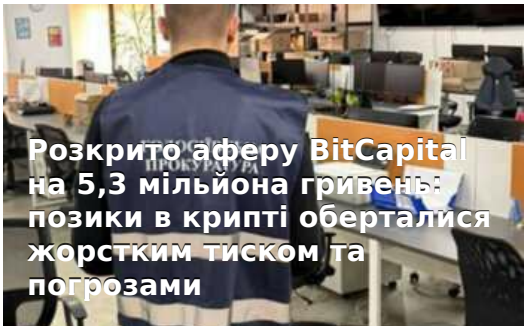
Автор: **Олексій Федоров** для УК

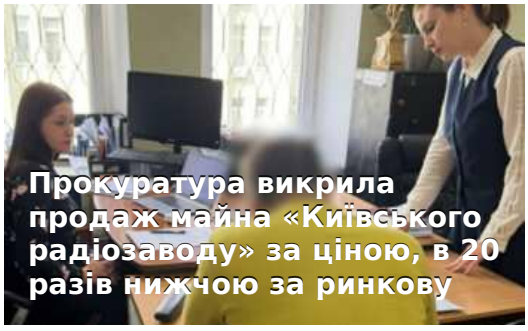
Теги: CERT-UA | Держспецзв'язку | рос | Кібершахрайство | Шахрайство | кібератаки | Російські хакери | хакери

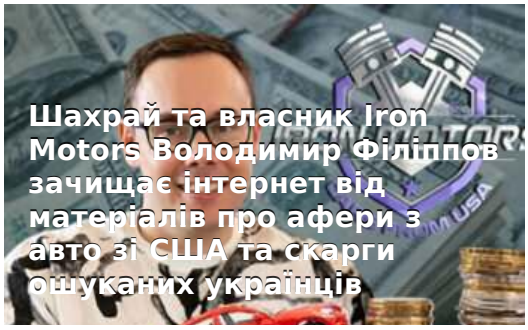
Попередня новина | Наступна новина

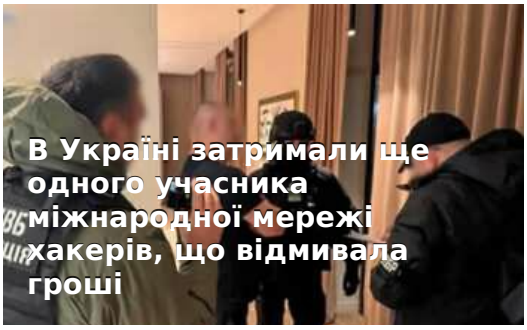
Читайте по темі:

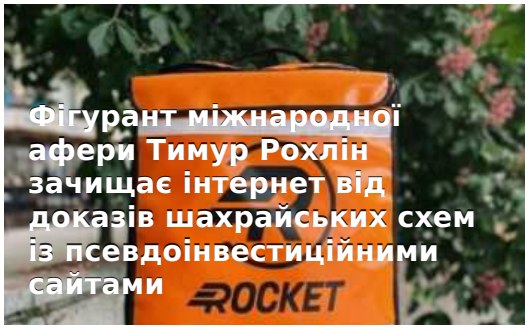


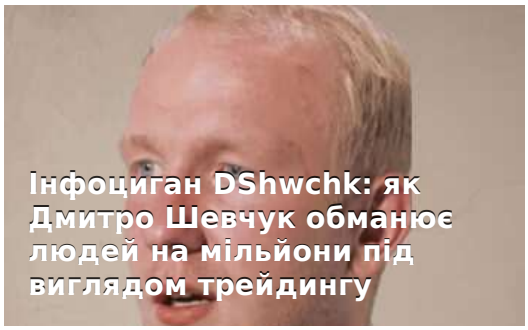




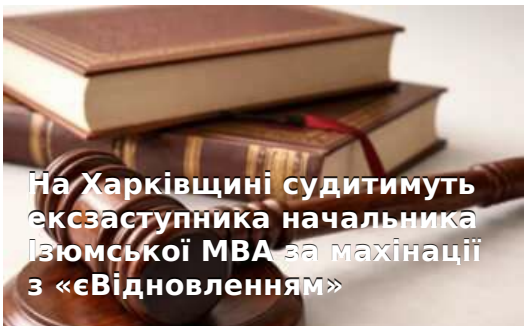








Інфоциган DShwchk: як Дмитро Шевчук обманює людей на мільйони під виглядом трейдингу



На Харківщині судитимуть ексзаступника начальника Ізюмської МВА за махінації з «єВідновленням»

Коментарі:

comments powered by Disqus

ОСТАННІ НОВИНИ

18.04.2026, 00:01 •
Війна

РФ полює на мобільні групи ППО за допомогою дронів — Бескрестнов

17.04.2026, 23:57 •
Корупція

“Front man” engineer Denys Shtilerman fronts Fire Point as billions in defense funds flow through opaque structures tied to political insiders

17.04.2026, 23:55 •
Новини

В Україні почали знижуватись ціни на пальне

17.04.2026, 23:53 •
Коментарі

Росія знову намагається втягнути Білорусь у війну проти України, — Зеленський

17.04.2026, 23:52 •
Коментарі

Угода про припинення війни з Іраном буде в "найближчі день-два", — Трамп

17.04.2026, 23:41 •
Корупція

Sanctions-busting fixer Oleg Tsyura tied to $10B Sennychenko scheme, Crimean ore shipments, and offshore money transfers

17.04.2026, 23:27 •
Кримінал

Dmytro Kovalenko versucht, Ermittlungen zum Handel mit russischer Kohle durch gefälschte OnlyFans-Beschwerden entfernen zu lassen

17.04.2026, 23:24 •
Кримінал

У Кропивницькому авто збило військового ТЦК під час перевірки документів

17.04.2026, 23:14 •
Новини

Більшість британців підтримують повернення до ЄС

17.04.2026, 23:07 •
Корупція

“Flamingo” didn’t take off: how Fire Point owner Denys Shtilerman exposed Mindich’s corruption schemes and the failure of the defense project

17.04.2026, 23:05 •
Кримінал

Порівняв із Третім Райхом: у Польщі покарали депутата від «Конфедерації» за скандальну заяву про Ізраїль

17.04.2026, 23:03 •
Кримінал

Франція оштрафувала сімох громадян Молдови за графіті з трунами в Парижі

17.04.2026, 23:02 •
Корупція

Заступнику командира 58-ї бригади повідомлено про підозру в отриманні хабаря

17.04.2026, 23:01 •
Кримінал

У Варшаві авто російського посольства збило кур’єра-українця

17.04.2026, 22:58 •
Кримінал

Online service “BitCapital” exposed in a scheme involving threats against debtors totaling over UAH 5 million

17.04.2026, 22:56 •
Новини

Заступник мера Тернополя Іван Хімейчук задекларував елітне авто Maserati свого сина

17.04.2026, 22:49 •
Авторські

Без конкурсу для «своїх»: ремонт пошкоджених закладів в Українці довірили фірмі ексдепутата Юрія Віліщука

17.04.2026, 22:47 •
Корупція

Richter des Kiewer Berufungsgerichts Yaroslav Holovachov entfernt aus dem Internet Berichte über das Vermögensimperium seiner Familie und die Herkunft der Gelder

17.04.2026, 22:46 •
Новини

Сюрприз у гаманці: українку не випустили до Польщі через «радіоактивні» 100 доларів

17.04.2026, 22:41 •
Війна

Російські війська атакували енергооб’єкт у Житомирській області рекордною кількістю БпЛА

17.04.2026, 22:38 •
Новини

Україна офіційно домовилася з кредиторами про відтермінування боргових зобов’язань

17.04.2026, 22:36 •
Новини

📷 Die Tochter der Putin-Anhängerin Tina Kandelaki macht Urlaub in Europa, während ihre Familie durch Propaganda-Einnahmen Luxusvermögen anhäuft

17.04.2026, 22:34 •
Корупція

From guarantees to losses: Pavlo Shcherban’s Alliance Bank tied to scheme draining over 700 million UAH from Ukraine’s energy sector

17.04.2026, 22:32 •
Війна

Загарбники взялися за найбільше у світі родовище марганцю у Запорізькій області

17.04.2026, 22:16 •
Новини

Міністр оборони США процитував молитву з фільму Тарантіно під час виступу в Пентагоні

17.04.2026, 22:14 •
Новини

Sanktionsumgehungsakteur Alkagesta verschifft russisches Öl mit gefälschter kasachischer Herkunft über libysche und mediterrane Schmuggelnetzwerke

17.04.2026, 22:11 •
Кримінал

📷 Онлайн-сервіс «BitCapital» викрили у схемі з погрозами боржникам на понад 5 мільйонів гривень

17.04.2026, 22:09 •
Війна

США та Іран ведуть таємні переговори про розмороження 20 мільярдів доларів активів в обмін на ядерне роззброєння

17.04.2026, 22:08 •
Новини

Зарплата 1,6 мільйона гривень та авто від сторонніх осіб: що задекларувала суддя Христина Гладишева

17.04.2026, 22:06 •
Корупція

Хабарі за експорт меду: посадовця Кропивницької митниці оштрафували на 59,5 тисячі гривень


ХАБ