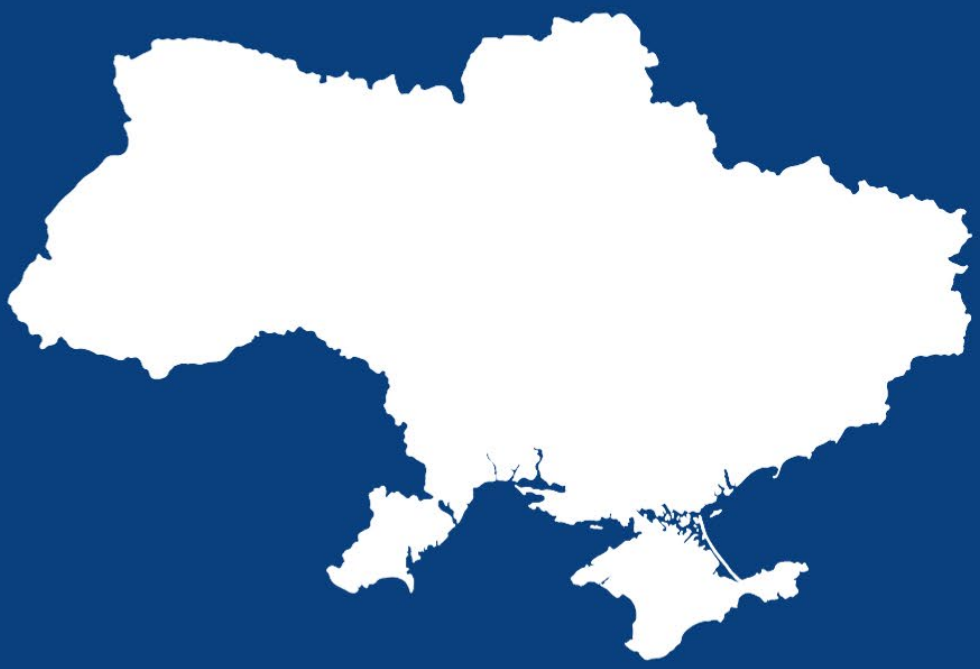
Україна

Ландшафт цифрових загроз: громадянське суспільство та медіа



Internews
Local voices. Global change.

Digital Security Lab

Зміст

Контекст

Вторгнення Росії в Україну поставило під загрозу вільне та безпечне функціонування українських громадських організацій та медіаорганізацій. Не винятком стала і їхня цифрова безпека, а війна загострила й без того серйозну проблему. Цей звіт підготувала команда Свободи та стійкості в Інтернеті організації Internews у рамках діяльності з підтримки здатності громадських організацій (ГО), журналістів та інших правозахисників визначати, аналізувати та розвивати стійкість до цифрових атак за допомогою локалізованої експертизи в аналізі загроз і реагуванні на інциденти. Звіт має на меті зробити огляд цифрових загроз, з якими стикаються громадські та медіаорганізації в Україні та надати поради для фахівців і фахівчинь з цифрової безпеки, які підтримують цю спільноту. Ще одна мета — надати інформацію про цей контекст галузі кібербезпеки, якій може бути потрібно проаналізувати інциденти з безпекою, які впливають на українське громадянське суспільство та медіа. Наприкінці ми запропонуємо заходи зменшення ризиків, які експерти й експертки з цифрової безпеки можуть запропонувати організаціям, з якими працюють, а також громадським і медіаорганізаціям.

Цей звіт було створено в тісній співпраці з Лабораторією цифрової безпеки, українською організацією, яка допомагає українським журналістам / журналісткам, правозахисникам / правозахисницям і громадським активістам і активісткам розв'язувати проблеми з цифровою безпекою, а також підтримує реалізацію прав людини в інтернеті шляхом впливу на політику уряду у сфері цифрових прав.

Загрози, тенденції та тематичні дослідження, висвітлені в цьому звіті, були виявлені шляхом прямої підтримки цифрової безпеки для груп ризику (наданої Internews та Лабораторією цифрової безпеки), кабінетних досліджень і розмов із довіреними членами спільноти Internet Freedom. У цьому звіті зібрано дані з реагування на інциденти та задокументовано моделі атак, характерні для України.

Жовтень 2023 р.

Автор_ки та укладач_ки звіту: Мартейн Грутен, Ешлі Фаулер, Марк Шаффер і Скайлер Саллік
Редагування, дизайн і макет: Скайлер Саллік

Ландшафт цифрових загроз

Політичний контекст, громадянське суспільство та ЗМІ

Хоча Україна — виборна демократія, демократичні інститути в ній слабкі через те, що триває війна з Росією[1]. Чинний президент Володимир Зеленський здобув перемогу на конкурентних виборах у 2019 році та обговорював можливість проведення наступних президентських виборів, визначених Конституцією, у 2024 році в умовах конфлікту[2]. Політики від опозиції та деякі представники громадянського суспільства висловили критику наміру провести вибори, оскільки повноцінній участі громадян могли б перешкоджати логістичні труднощі. Існує також занепокоєння, що вибори сприятимуть укріпленню влади Зеленського без можливості для справжньої опозиції[3]. У 2023 році Індекс демократії Economist відніс Україну до категорії «Гібридний режим» з результатом у 5,42 бала з 10[4]. У звіті Freedom House «Свобода у світі» за 2023 рік країна отримала статус «Частково вільна» з оцінкою 50 зі 100[5]. Freedom House відзначив, що позиція України знизилася на 19 балів порівняно з минулорічним рейтингом, оскільки «повномасштабне вторгнення російських військ в Україну в лютому 2022 року призвело до значного погіршення політичних прав і громадянських свобод, якими користуються українці»[6]. Після початку війни з Росією президент Зеленський запровадив воєнний стан, який дозволяє обмежувати захищені Конституцією права, такі як свобода слова, право обирати та бути обраним, а також право на мирні зібрання та страйк[7]. На момент написання матеріалу в Україні діє воєнний стан.

Попри виклики війни, українське громадянське суспільство продемонструвало стійкість у своїй здатності залучати волонтерів, збирати кошти для допомоги громадянам і документувати докази російських воєнних злочинів.

За даними Freedom House, громадянське суспільство залишається сильним і ефективним, зміцнюючи свою роль як ключової зацікавленої сторони у процесі реформ в Україні[8]. До війни з Росією значний вплив на політичну сферу мали олігархи, і це явище лише посилювалося через масштабну корупцію[9]. Хоча впливовість олігархів внаслідок війни знизилася, корупція залишається відчутною проблемою, яка сповільнює політичний прогрес[10]. В умовах воєнного стану громадські організації стикаються з законодавчими реформами, які можуть дещо ускладнювати їхню роботу. Зокрема громадським організаціям тепер не дозволяється використовувати іноземні банківські транзакції[11]. Попри виклики війни, українське громадянське суспільство продемонструвало стійкість у своїй здатності залучати волонтерів, збирати кошти для допомоги громадянам і документувати докази російських воєнних злочинів[12].

В умовах війни інформація становить велику цінність, і це зокрема відображено в урядових обмеженнях під час воєнного стану. У березні 2022 року Рада національної безпеки і оборони України (РНБО) випустила пакет положень щодо засобів масової інформації протягом воєнного часу, які спочатку отримали широку підтримку, оскільки такі заходи вважалися доцільними під час війни. Проте з часом ці обмеження почали сприйматися як посягання на демократичні права в Україні[13]. Ситуація з цими обмеженнями, а також Законом України «Про медіа», ще більше ускладнюється отриманням Україною статусу кандидата у члени ЄС, оскільки тепер країна зобов'язана відповідати певним критеріям, щоб зберегти цей статус. Українські законодавці та громадянське суспільство мусять підтримувати тонкий баланс між необхідними обмеженнями воєнного часу та розширенням

демократичних інститутів у процесі законодавчої реформи країни. У цьому контексті Лабораторія цифрової безпеки

Окрім законодавчого тиску через воєнний стан, громадянське суспільство зараз переживає значні загрози фінансовій і фізичній безпеці. Хоча багато українських організацій продовжують працювати у складних обставинах, вони змушені діяти в умовах фінансової нестабільності, і ця загроза лише зростає у міру продовження війни. У 2022 році 82% ГО, які займаються правами жінок, заявили про нестачу фінансових ресурсів[14]. На окупованих територіях активістів переслідують або й арештують російські війська. У більшості випадків російські військові вдавалися до переслідувань за участь у маршах чи протестах проти окупантів[15].

Багато українських громадських організацій змушені діяти в умовах фінансової нестабільності, і ця загроза лише зростає у міру продовження війни.

Кібербезпека в Україні

Україна не перший рік є однією з основних локацій для роботи кіберзлочинців. Попри те, що деяких з них зрештою арештували — наприклад, керівників угруповань, які поширювали шкідливе банківське ПЗ ZuES[16] і Carberp[17], раніше Україна вважалась «безпечною кібергаванню»[18] для злочинної діяльності. Така можливість для кіберзлочинців вільно працювати у країні пояснюється тим, що протягом останнього десятиліття Україна змушена була зосереджуватися на протидії російській агресії. Урядову команду реагування на комп'ютерні надзвичайні події України, CERT-UA, звинуватили в неефективній боротьбі проти кіберзлочинності внаслідок «уваги майже виключно до боротьби з російською агресією на сході України» після анексії Росією Криму у 2014 році[19]. Кар'єра кіберзлочинця, який став політиком, Дмитра Голубова — народного депутата України з 2014 по 2019 рік — ілюструє, наскільки вільно почуваються кіберзлочинці в Україні[20].

Кіберзлочинність в Україні та Росії давно тісно пов'язана між собою, а чимало суб'єктів діють в обох країнах. Зловмисне програмне забезпечення, створене в регіоні, зазвичай перевіряє наявність російської чи української клавіатури (або однієї з розкладок кількох інших країн у регіоні) і зупиняє напад, якщо таку розкладку було виявлено, щоб не наражатися на переслідування з боку місцевої влади[21].

Однак ситуація змінилася після повномасштабного вторгнення в Україну у 2022 році. Кіберзлочинці в обох країнах заявили про лояльність до своїх урядів, що призвело до розпаду кількох злочинних груп. Найбільш публічним прикладом став випадок з угрупованням, яке керувало вірусом-вимагачем Conti — російські члени угруповання публічно заявили про свою підтримку російського вторгнення[22], після чого український учасник опублікував близько 60 000 повідомлень з внутрішньої кореспонденції злочинців, щоб показати, як функціонує угруповання[23]. Група аналізу загроз Google вважає що з того часу деякі з колишніх російських членів угруповання почали працювати на російський уряд[24].

Однак ситуація змінилася після повномасштабного вторгнення в Україну у 2022 році. Кіберзлочинці в обох країнах заявили про лояльність до своїх урядів, що призвело до розпаду кількох злочинних груп.

Переслідування українських користувачів з боку Росії посилилося після вторгнення в Крим. У грудні 2015 року жителі Івано-Франківської області на заході Україні зіткнулися з відключеннями електроенергії від години до шести годин після того, як хакер проник в українську енергомережу — це була перша в історії атака, спрямована конкретно на електропостачання іноземної країни[25]. Вважається, що цей напад — робота групи, яку називають «Піщаним черв'яком», підрозділу кібервійськ ГРУ, військової розвідувальної служби Росії. Також вважається, що «Піщаний черв'як» відповідальний за ще одне, коротше відключення електроенергії в Києві у 2016 році[26] та за невдалу спробу спричинити третє відключення у квітні 2022 року, незабаром після повномасштабного вторгнення[27].

У червні 2017 року хакерам «Піщаного черв'яка» вдалося проникнути в невелику компанію, яка створила широко розповсюджену програму для податкового обліку в Україні, після чого заражене вірусом оновлення потрапило до користувачів у всьому світі. Оновлення містило шкідливу програму NotPetya, яка шифрує всі файли на заражених комп'ютерах. Попри те, що NotPetya діяв як програма-вимагач, цей вірус насправді деструктивний за своєю природою, оскільки не існує методу розшифровки файлів. Оскільки постраждало багато міжнародних компаній, загальний збиток оцінюється в понад 10 мільйонів доларів США[28].

Україну та її прихильників також переслідують різні групи «хактивістів» (хакерів-активістів), таких як КіберБеркут[29], Killnet і NoName057(16)[30]. Серед інших відомих суб'єктів, пов'язаних з Росією, — «Гамаредон», який, схоже, функціонує виняткова для переслідування України, та APT28 (Fancy Bear), ще одне угруповання, пов'язане з ГРУ, яке здійснювало різні напади на українські цілі[31]. У 2022 році APT28 (Fancy Bear) провела фішингову кампанію, націлену на користувачів популярного серед громадських організацій України веб-сервісу UKR.NET[32]. Після анексії Росією Криму у 2014 році пов'язані з Росією суб'єкти дедалі частіше атакують кіберпростір України, через що деякі експерти почали називати країну «ігровим майданчиком Росії» в контексті кібератак[33].

Пазом з тим, Україна створила середовище, яке сприяє експериментальним підходам і багатосторонній співпраці в контексті кібербезпеки та кіберзахисту. Починаючи з російської анексії Криму й особливо після початку повномасштабної війни у 2022 році, Україна отримала велику підтримку у сфері кіберзахисту як від іноземних урядів, так і від приватного сектору. Ця підтримка включала безкоштовне програмне забезпечення та послуги, швидкий обмін інформацією та заходи для забезпечення безперервної роботи бізнесу у разі захоплення[34] фізичних активів.

Стан кібербезпеки громадянського суспільства та ЗМІ

Війна Росії в Україні змінила ландшафт цифрових загроз для громадянського суспільства та незалежних ЗМІ країни. Ще до війни журналістів непокоїли кібератаки на кшталт хакерських зламів та цифрових переслідувань з боку політиків, чиї корупційні дії вони намагалися викрити. Після військового вторгнення кількість подібних загроз зменшилася, адже боротьба проти спільного ворога об'єднала суспільство. Однак тепер місцеві експерти з цифрової безпеки повідомляють про відновлення дрібномасштабних внутрішніх хакерських атак на тлі війни, що триває і досі.

Відомі випадки явного цифрового переслідування українського громадянського суспільства з боку російських або пов'язаних з Росією суб'єктів є нечисленними. Звісно, деякі атаки можуть залишатися непоміченими, але правда й те, що російські злочинні суб'єкти наразі більше зосереджені на українських урядових і військових об'єктах[35]. Проте громадянське суспільство теж може

постраждати — так би мовити, в якості «побічних втрат» — через цифрові загрози, з якими стикаються державні установи, адже межа між громадянським суспільством та урядом не завжди є чіткою. Попри поточну геополітичну ситуацію в країні, кіберзлочинці продовжують атакувати користувачів за допомогою фішингу та шкідливого програмного забезпечення, і через їхню невибірковість жертвами таких атак іноді стають члени громадянського суспільства.

Багато журналістів та керівників відділів безпеки пересилають отримані підозрілі електронні листи до відповідних організацій, наприклад до Лабораторії цифрової безпеки (DSLU), для аналізу, оскільки добре усвідомлюють їхню небезпечність. Але в цілому кібергігієна серед українського громадянського суспільства далека від ідеальної, оскільки дуже велика кількість людей використовує зламані версії легального програмного забезпечення, які часто містять шкідливі програми[36]. Декому така популярність зламаного програмного забезпечення може здатися дивною, зважаючи на кількість ліцензій на вільне програмне забезпечення, які надаються українським організаціям та компаніям. Але річ у тім, що, як повідомляють IT-адміністратори державних установ та організацій громадянського суспільства, часто буває простіше встановити зламане програмне забезпечення, ніж подолати бюрократичні перепони, пов'язані з доступом до безкоштовних ліцензій.

Україна щонайменше з 2019 року намагається придбати Pegasus для власного використання, але ізраїльський уряд забороняє компанії NSO Group продавати її програмне забезпечення Україні.

В Україні не зафіксовано жодного випадку розповсюдження сучасного мобільного шкідливого програмного забезпечення, такого як Pegasus. Україна щонайменше з 2019 року намагається придбати Pegasus для власного використання, але ізраїльський уряд забороняє компанії NSO Group продавати її програмне забезпечення Україні. Офіційних заяв щодо причини заборони продажу не було, але експерти вважають, що вона пов'язана з тісними зв'язками між розвідувальними службами Ізраїлю і Росії. Вочевидь, уряд Ізраїлю побоюється, що Україна використовуватиме Pegasus проти російських чиновників, і не хоче дратувати Росію. Таке рішення не є чимось новим: наприклад, умовами продажу Pegasus уряду Естонії чітко заборонялося використання цього програмного забезпечення для впливу на російських посадовців[37].

Заходи зі зменшення ризиків

Безпека облікових записів важлива для всіх людей в Україні, надто для членів громадянського суспільства. **Двофакторна автентифікація абсолютно необхідна**, адже вона зменшує ризики, пов'язані з використанням слабких та повторюваних паролів. Двофакторна автентифікація за допомогою SMS-повідомлень — це, звісно, краще, ніж її цілковита відсутність, проте цей спосіб не можна вважати надійним, особливо для користувачів з груп ризику. Додаток для автентифікації є безпечнішим за SMS, але найвищий рівень захисту забезпечує все ж таки використання апаратного токена — щоправда, для цього потрібне додаткове обладнання.

В деяких додатках для обміну повідомленнями, наприклад Telegram, WhatsApp і Signal, для активації облікового запису використовується номер телефону. Двофакторна автентифікація передбачає доступ до облікового запису з використанням **пароля** на додаток до SMS, що забезпечує захист на випадок

перехоплення SMS. Якщо ця функція увімкнена, програма періодично вимагає від користувача ввести пароль, щоб переконатися, що ніхто крім власника облікового запису не має доступу до повідомлень. Це запобігає заволодінню обліковими записами шляхом перехоплення SMS, що є поширеним явищем в Україні.

Програмне забезпечення кінцевих пристроїв — ноутбуків та мобільних телефонів — слід оновлювати, встановлюючи патчі безпеки для операційних систем та іншого програмного забезпечення щоразу, коли вони стають доступними. **Для придбання програмного забезпечення слід користуватися лише офіційними джерелами.** У багатьох випадках це передбачає оплату. Неурядові організації не повинні соромитися обговорювати це питання з донорами або шукати безкоштовні альтернативи у вигляді програмного забезпечення з відкритим вихідним кодом або акційних програм з надання програмного забезпечення неурядовим організаціям, які відповідають певним критеріям, безкоштовно або за зниженими цінами.

Немає жодних свідчень щодо використання сучасного шпигунського або шкідливого програмного забезпечення для цілеспрямованих атак на громадянське суспільство або ЗМІ в Україні, але таку можливість не можна виключати з огляду на війну з Росією, однією з найпотужніших «кібердержав» у світі. Це особливо стосується людей, які живуть і працюють на підконтрольних Росії територіях.

Члени громадянського суспільства та журналісти мають бути пильними та застосовувати загальноприйняті практики для зменшення ризику атак сучасних шпигунських програм, наприклад **регулярно перезавантажувати телефон** і **використовувати програми додаткового захисту облікових записів Google та режим блокування на iPhone та iPad**. Не слід відкривати підозрілі електронні вкладення та переходити за підозрілими посиланнями, натомість їх рекомендується пересилати на перевірку довіреним експертам, таким як DSLU.

Громадяни, які проживають на окупованих Росією територіях країни, можуть **використовувати VPN, щоб уникнути цензури** та втручання окупаційної влади. Однак особи, діяльність яких пов'язана з ризиком арешту або переслідування, мають знати: при використанні VPN (або Tor) їхній трафік виділятиметься серед спільноти й сам по собі може привернути до них небажану увагу.

В Україні поширені пристрої російського виробництва, які підключаються до російських серверів. Хоча ризики, пов'язані з цими з'єднаннями, залежать від пристрою, їх краще уникати. На момент написання цього звіту інтернет-з'єднання з Росією в Україні заблоковано, і пристрої російського виробництва потребують VPN для підключення до російських серверів. Тож хоча використання VPN задля уникнення урядової цензури, як правило, є хорошою ідеєю і рекомендується на територіях, контрольованих Росією, слід пам'ятати, що необхідність використання VPN для підключення може бути ознакою того, що пристрій з'єднується з сервером, розташованим у Росії.

Розгляд кейсів

Україна стала мішенню троянської програми Remcos

У лютому 2023 року дві окремі неурядові організації в Україні отримали фішинговий електронний лист з однаковим захищеним паролем архівом у вкладенні. Не відкриваючи вкладення, адресати

перенаправили листа Лабораторії цифрової безпеки — організації, яка допомагає українським журналістам, правозахисникам та громадським активістам розв'язувати проблеми з цифровою безпекою.

Хоча архів був відносно малий, розпакований файл містив великий виконуваний файл Windows (.exe) (657 МБ). Розмір файлу не дозволив Лабораторії цифрової безпеки завантажити його на VirusTotal, популярний сайт Google для аналізу загроз, оскільки там встановлено обмеження 650 МБ. Великий розмір архіву та захищеність паролем призначені для обходу файлом таких перших рівнів захисту як антивірус або захист електронної пошти під час відкриття користувачем. Розмір інфікованого файлу та використання захищеного паролем архіву — поширені способи обійти перевірку під час таргетованих чи нетаргетованих атак шкідливого ПЗ.

За допомогою інструмента Detect-It-Easy, що допомагає аналітикам визначати типи файлів, у Лабораторії цифрової безпеки встановили, що файл був замаскований за допомогою обфускатора SmartAssembly — ще одного поширеного способу протидії аналізу. Однак за допомогою деобфускатора .NET de4dot Лабораторії цифрової безпеки вдалося створити версію файлу, на 0,1% меншу від початкового розміру з таким самим функціоналом. Файл був завантажений на VirusTotal. Лабораторія цифрової безпеки також проаналізувала файл у Flare VM — дистрибутиві безпеки на базі Windows, під управлінням безпекової компанії Mandiant.[38]

Завдяки цьому аналізу Лабораторія цифрової безпеки встановила, що файл був створений 20 лютого 2023 року, безпосередньо перед відправленням електронного листа. Динамічний аналіз у Flare VM показав, що файл був налаштований для зберігання його копії на диску та запуску під час додавання ключа до реєстру Windows, забезпечуючи роботу файлу .exe під час кожного запуску комп’ютера. Оскільки цей метод використовується у легальних програмах, це дуже поширена стратегія забезпечення присутності шкідливих програм на заражених комп’ютерах з Windows після перезавантаження.

Під час аналізу Лабораторія цифрової безпеки також знайшла програму, яка підключається до двох IP-адрес в інтернеті. Результати аналізу IP-адрес, до яких підключається шкідливе ПЗ можна використати для визначення вже проведених кампаній, що допомагає краще зрозуміти таке ПЗ. За допомогою інструмента Process Hacker, що використовується для моніторингу системних ресурсів та пошуку шкідливих програм, аналітики змогли виявити ще 12 IP-адрес, до яких підключалася шкідлива програма. Вони також помітили рядок «Remcos Agent initialized» та інші згадки Remcos.

За результатами використання інструментів, що вже обговорювалися та різних «пісочниць» шкідливого ПЗ, аналітики дійшли висновку, що ця атака могла бути різновидом троянської програми віддаленого доступу Remcos (Remcos Remote Access Trojan, RAT). Ця програма надає повний віддалений доступ до зараженого комп’ютера та слугує ідеальним інструментом шпіонажу та фінансового шахрайства. Remcos вперше вдалося проаналізувати в лютому 2017 року — це одна з троянських програм віддаленого доступу, яку виявляють найчастіше[39]. Чимало троянських програм віддаленого доступу продаються на чорних кіберринках, причому деякі з них, зокрема й Remcos, спершу розроблялися як *Інструменти* віддаленого доступу для підтримки.

Незрозуміло чому ці дві ГО стали мішенню Remcos. Можливо це була опортуністична спроба невибіркового кіберзлочину або цілеспрямована загроза з боку суб’єкта, зацікавленого в їхній

діяльності. Відносно досвідчені користувачі, що діють від імені держав, іноді купують інструменти нападу у кіберзлочинців, а не розробляють власні.

У будь-якому випадку, оскільки вкладення не було відкрите, атака не вдалася, а електронний лист, надісланий Лабораторії цифрової безпеки, допоміг спільноті краще зрозуміти загрозу. Цей кейс демонструє, чому такій місцевій організації як Лабораторія цифрової безпеки варто вміти аналізувати загрози. Приклади, наведені у цьому розслідуванні, можна використовувати під час тренінгів та постійної підтримки спільнот, що перебувають під загрозою, допомагаючи фахівцям точніше налаштовувати заходи запобігання та надавати кращі рекомендації щодо мінливих ландшафтів загроз.

Працівник органів місцевого самоврядування міг стати мішенню шкідливої програми Gamaredon

Український чиновник, який має попередній досвід роботи в громадській організації, отримав електронний лист із вкладенням, відправлений зі зламаного облікового запису місцевого державного органу. Не відкриваючи вкладення, одержувач перенаправив листа на аналіз Лабораторії цифрової безпеки — організації, яка допомагає українським журналістам, правозахисникам та громадським активістам розв'язувати проблеми з цифровою безпекою.

Електронний лист містив вкладення у форматі HTML з технологією «HTML smuggling» для відкриття якісно стисненого архіву Roshal Archive (RAR)[40]. Цей архів містив файл .hta — поширене розширення для застосунку HTML[41]. Застосунки HTML використовуються для різноманітних законних завдань на комп’ютерах з Windows, однак через здатність запускати коди вони популярні й серед авторів шкідливих програм. Ці інструменти особливо привабливі, оскільки працюють всередині законної програми mshta.exe, дозволяючи шкідливому ПЗ уникнути виявлення засобами безпеки. Використання законних програм для шкідливих цілей називається living-off-the-land або LOLbin.

З файлом .hta в архіві RAR завантажуються корисні дані з адреси http://80.90.181[.]243/sb.12.05.gif/query/heal.jpeg. Попри зміст URL-адреси, в результаті завантажується не файл у форматі GIF або JPEG, а сценарій PowerShell, що виконується локально. Оскільки URL-адреси на основі IP нечасто використовуються для законної мети, це була не надто продумана спроба ввести користувача в оману. Однак середньостатистичний користувач може подумати, що за цією URL-адресою можна завантажити зображення. Для інших електронних листів, що, як виявилося пізніше, належали до тієї самої кампанії, використовувалися інші шляхи, однак завантажувалися ті самі дані.

Цікаво те, що дані завантажувалися лише у разі використання української IP-адреси, отже можна припустити географічний таргетинг електронних листів. Тобто відкриття вкладення у «пісочниці» не призвело б до подальших дій. Для завершення аналізу аналітикам Лабораторії цифрової безпеки довелося запустити файл локально на віртуальній машині.

PowerShell — мова сценаріїв Windows та потужний інструмент як для законних, так і шкідливих завдань. У цьому випадку сценарій передбачав встановлення ключа запуску, відкриття порожнього документа Word та створення локального файлу під назвою «junior». Відкриття документа Word може бути інструментом захисту, оскільки шкідливе ПЗ не могло б працювати без встановлення Microsoft Word, а в деяких середовищах аналізу це б могло статися.

Файл «junior» міг отримати IP-адресу командно-контрольного сервера двома способами: або шляхом підключення до публічного Telegram-каналу, або за допомогою доменного імені як запасного варіанту. Хмарні сервіси та Telegram часто використовуються шкідливим ПЗ для доступу до командно-контрольних серверів, оскільки вони можуть забезпечити більшу стійкість ніж використання доменних імен або статичних IP-адрес. Цей метод означає, що учасники не повинні заздалегідь мати або реєструвати сервери й можуть їх отримати вже після початку кампанії.

Після отримання адреси командно-контрольного сервера, на нього надсилається запит HTTP GET з ім'ям комп'ютера та серійного номера жорсткого диска у полі заголовка «Користувач-Агент». Хоча програма повинна очікувати відповіді, під час аналізу жодних відповідей, окрім 404 не спостерігалося. Можливо сервером якимось чином було виявлено, що запит надійшов з аналітичного комп'ютера.

Хоча аналіз і не виявив шкідливої активності, багато аспектів вказувало на шкідливість цього ПЗ. Така невелика організація, як Лабораторія цифрової безпеки, часто не має змоги достовірно встановити взаємозв'язок кампанії та конкретного учасника, адже для цього потрібно багато телеметричних даних. Однак чимало артефактів цього ПЗ — використання файлів .hta, PowerScript та Telegram для доступу до командно-контрольного сервера та таргетування на Україну наводять на думку про причетність суб'єкта загроз, якого безпекові компанії називають Gamaredon (інші назви цієї групи — Primitive Bear та Shuckworm)[42].

Gamaredon — пов'язана з Росією група кібершпигунів, що виявляє особливу увагу Україні з моменту її виявлення у 2013 році. Її мішенями ставали урядові організації, правоохоронні органи та ГО.

Додаткові джерела

Цей звіт доводить, що організації громадянського суспільства та журналісти часто стикаються з унікальними продуманими загрозами, не маючи при цьому ресурсів для виявлення, аналізу та протидії. Глибоке розуміння громадянським суспільством та медіа можливих загроз дозволяє спеціалістам з цифрової безпеки адаптувати методи роботи та надавати якіснішу підтримку організаціям, з якими вони працюють, тобто кастомізувати заходи протидії загрозам, робити їх ефективнішими та простішими для застосування представниками громадянського суспільства та медійних організацій. Детальніше про загрози для громадянського суспільства та журналістів — у звіті Internews та партнерів «Global Trends in Digital Threats: Civil Society & Media» («Глобальні тенденції цифрових загроз: громадянське суспільство та медіа») та цифровій версії для Вірменії, Бразилії, Сербії та України. Ці матеріали можна знайти та сторінці Internews «Технологічні ресурси».

Історія України

Україна — друга за величиною країна в Європі, що межує з Росією, Білоруссю, Польщею, Словаччиною, Угорщиною, Румунією та Молдовою. Україна має берегову лінію вздовж Чорного та Азовського морів. Це унітарна республіка з одним законодавчим органом, член Організації Об'єднаних Націй[43], Світової організації торгівлі[44], Ради Європи[45] та Організації з безпеки і співробітництва в Європі[46]. У лютому 2022 року Росія вторглася в Україну, і на момент написання цього звіту війна ще триває.

Слов'янські народи оселилися на території, яка зараз є Україною, у четвертому столітті нашої ери, а Київ став головним містом[47]. У дев'ятому столітті територія навколо Києва була об'єднана в державу під назвою Київська Русь. Київська Русь стала основним джерелом влади, досягнувши свого піку в XI столітті[48]. Київська Русь є важливим аспектом східноєвропейської історії, оскільки Росія, Україна та Білорусь пов'язують свою національну ідентичність із державою раннього середньовіччя. В українській націоналістичній історіографії Київська Русь є «Українською державою по своїй суті, а відмінності між росіянами та українцями були очевидні і досить глибокі вже тоді»[49]. На противагу цьому російські імперіалістичні історики використовували Київську Русь як обґрунтування тези, що українці і білоруси — це «лише підгрупи»[50]. Це протистояння продовжує впливати на відносини між країнами, про що свідчать неодноразові згадки Путіним Київської Русі і донині[51].

Після розпаду держави Київська Русь контроль над територією України почергово отримували Литва, Польща, Росія та Гетьманщина — Козацьке самоврядування. У XVIII столітті Російська імперія зміцнила контроль над Україною і значною мірою зберігала це панування аж до розпаду Радянського Союзу[52]. У XIX столітті в українців, як і в багатьох інших регіонів Європи, почало розвиватися почуття націоналізму і віра в самовизначення. У той час Батьківщина українця була розділена між Росією на сході та Австро-Угорською імперією на заході. Ці дві імперії по-різному реагували на рух, причому під Австрією визнання меншин зростало, а під росією українська ідентичність придушувалася. Після повалення російської монархії Україна ненадовго проголосила незалежність, перш ніж громадянська війна в Росії призвела до включення України до складу Радянського Союзу як Української Радянської Соціалістичної Республіки без політичної автономії[53]. В рамках політики колективізації Йосипа Сталіна радянські лідери спровокували голод в Україні, що отримав назву «Голодомор», який призвів до загибелі мільйонів українців[54].

Україна має потужну історію опору російському контролю у минулому столітті, що продовжилася під час великої війни. У 1991 році Україна здобула незалежність, а у 1996 — затвердила чинну Конституцію. У 1991-1999 роках відбувся спад під час переходу до ринкової економіки із втратою 60% ВВП та гіперінфляцією, що досягла піку 100 000% у 1993 році. З 1990-х років українці двічі бунтували проти уряду: під час Помаранчевої революції проти спірних виборів 2004 року та під час протестів на київському Майдані, які повалили проросійський уряд у 2014 році. За тимчасового уряду російські війська вторглися на Кримський півострів і анексували його. Після цього підтримувані росією ополченці-сепаратисти на сході України виступили проти державної армії і проголосили незалежність[55]. Напруженість досягла кульмінації з російським вторгненням у 2022 році[56].

Подяки

З 2021 року Internews працює з сімома лабораторіями Threat Labs (*місцевими організаціями, що мають технічні можливості та належні інструменти для аналізу зразків фішингу та шкідливого ПЗ для надання спільнотам даних про тенденції загроз, нові загрози та заходи протидії*) для реагування на інциденти, що впливають на цифрову безпеку громадянського суспільства та медійних організацій у всьому світі. Дані, зібрані в рамках програми реагування на інциденти, допомогли сформувати заходи пом'якшення наслідків та підходи до реагування для спільнот, що перебувають під загрозою, і стали основою цього звіту.

Internews висловлює вдячність членам спільноти Threat Labs, що працювали з нами над цим проектом. Вони допомагають тим, хто цього потребує та сприяють виконанню завдань партнерами з громадянського суспільства та медіа-організацій. Загалом у межах проекту Threat Labs отримали підтримку під час роботи з понад 200 інцидентами цифрової безпеки та опублікування понад 60 освітніх ресурсів на власних веб-сайтах та платформах соцмереж.

Особлива подяка Лабораторії цифрової безпеки України за надання інформації, документів і кейсів на розгляд, а також за цінні коментарі до цього звіту. Цей звіт не був би можливим без їхньої підтримки.

Примітки

[1] Методологія «Nations in Transit». Freedom House. Переглянуто: серпень 2023 р. https://freedomhouse.org/reports/nations-transit/nations-transit-methodology.; «Nations in Transit 2023: Україна». Freedom House. Переглянуто: серпень 2023 р. https://freedomhouse.org/country/ukraine/nations-transit/2023.

[2] Старков, Нік. «Zelenskiy says elections could happen under fire if West helps». *Reuters*. Змінено 27 серпня 2023 р. https://www.reuters.com/world/europe/zelenskiy-says-elections-could-happen-under-fire-if-west-helps-2023-08-27/.

[3] Крамер, Ендрю Е. «Zelensky's First Term Is Almost Up. No One's Sure What Happens Next». The New York Times. 5 жовтня 2023 р. https://www.nytimes.com/2023/10/05/world/europe/ukraine-zelensky-elections-war.html

[4] «Індекс демократії 2022: Frontline democracy and the battle for Ukraine», Economist Intelligence. С. 9.

[5] «Freedom in the World 2023: Ukraine». Freedom House. Переглянуто: серпень 2023 р. https://freedomhouse.org/country/ukraine/freedom-world/2023.

[6] «Freedom in the World 2023: Ukraine», Freedom House.

[7] «Nations in Transit 2023: Ukraine», Freedom House.

[8] «Freedom in the World 2023: Ukraine», Freedom House; «Nations in Transit 2023: Ukraine», Freedom House.

[9] «Freedom in the World 2023: Ukraine», Freedom House.

[10] «Freedom in the World 2023: Ukraine», Freedom House.

[11] «Freedom in the World 2023: Ukraine», Freedom House.

[12] «One year into Russia's war on Ukraine: Civil society in the crossfire». Civicus Lens. Змінено 24 лютого 2023 р. https://lens.civicus.org/one-year-into-russias-war-on-ukraine-civil-society-in-the-crossfire/.

[13] «Nations in Transit 2023: Ukraine», Freedom House.

[14] «Nations in Transit 2023: Ukraine», Freedom House.

[15] «Nations in Transit 2023: Ukraine», Freedom House.

[16] Gallagher, Sean. «Alleged botnet mastermind and his coders busted by Russian, Ukrainian security". ARS Technica. 4 квітня 2013 р. https://arstechnica.com/tech-policy/2013/04/alleged-botnet-mastermind-and-his-coders-busted-by-russian-ukranian-security/.

[17] Gallagher, «Alleged botnet mastermind and his coders busted by Russian, Ukrainian security".

[18] Kostyuk, Nadiya. «Ukraine: A Cyber Safe Haven?» In *Cyber War in Perspective: Russian Aggression Against Ukraine*, edited by Kenneth Geers, 113 — 122. Tallinn, Estonia: NATO CCD COE Publications, 2015. https://www.ccdcoe.org/uploads/2018/10/Ch13_CyberWarinPerspective_Kostyuk.pdf.

[19] Kostyuk, «Ukraine: A Cyber Safe Haven?»

[20] «Dmitri Golubov (politician)". *Wikipedia*. Переглянуто: вересень 2023 р. https://en.wikipedia.org/wiki/Dmitri_Golubov_(politician)

[21] «Try This One Weird Trick Russian Hackers Hate". KrebsonSecurity. 17 травня 2021 р. https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/.

[22] Abrams, Lawrence. «Conti ransomware's internal chats leaked after siding with Russia». *Bleeping Computer*. 27 лютого 2022 р. https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/.

[23] Bing, Christopher. «Russia-based ransomware group Conti issues warning to Kremlin foes». *Reuters*. 25 лютого 2022 р. https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

[24] Huntley, Shane. «Fog of war: how the Ukraine conflict transformed the cyber threat landscape». Google, оновлення від Групи аналізу загроз. 16 лютого 2023 р. https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

[25] Zetter, Kim. «Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid». *Wired*. 3 березня 2016 р. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[26] Greenberg, Andy. «How an Entire Nation Became Russia's Test Lab for Cyberwar». *Wired*. 20 червня 2017 р. https://www.wired.com/story/russian-hackers-attack-ukraine/.

[27] Greenberg, Andy. «Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine». *Wired*. 17 квітня 2022 р. https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/.

[28] Greenberg, Andy. «The Untold Story of NotPetya, the Most Devastating Cyberattack in History». *Wired*. 22 серпня 2018 р. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[29] Rodrigo, «Cyber Berkut Graduates From DDoS Stunts to Purveyor of Cyber Attack Tools». Recorded Future. 8 червня 2015 р. https://www.recordedfuture.com/cyber-berkut-analysis.

[30] «Pro-Russian Hacktivist Groups Target Ukraine Supporters». Intel471. 14 вересня 2022 р. https://intel471.com/blog/pro-russian-hacktivist-groups-target-ukraine-supporters.

[31] Kremez, Vitali. «Pro-Russian CyberSpy Gmaredon Intensifies Ukrainian Security Targeting». SentinelLABS. 5 лютого 2020 р. https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/.

[32] Aimé, Felix. «APT28 leverages multiple phishing techniques to target Ukrainian civil society». Sekoia blog. 17 травня 2023 р. https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/.

[33] Cerulus, Laurens. «How Ukraine became a test bed for cyberweaponry». *Politico*. 14 лютого 2019 р. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/.

[34] Beecroft, Ben. «Evaluating the International Support to Ukraine Cyber Defense». Carnegie Endowment for International Peace. 3 листопада 2022 р. https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322.

[35] Nimmo, Ben and David Agranovich. «Meta's Adversarial Threat Report, Second Quarter 2022». Meta. 4 серпня 2022 р. https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.

[36] Abrams, Lawrence. «Pirated Software is All Fund and Games Until Your Data is Stolen». *Bleeping Computer.* 2 лютого 2020 р. https://www.bleepingcomputer.com/news/security/pirated-software-is-all-fun-and-games-until-your-data-s-stolen/.

[37] Kirchgaessner, Stephanie. «Israel blocked Ukraine from buying Pegasus spyware, fearing Russia's anger». *The Guardian*. 23 березня 2022 р. https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia.

[38] Kacherginsky, Peter. «FLARE VM: The Windows Malware Analysis Distribution You've Always Needed!» Mandiant. 26 липня 2017 р. https://www.mandiant.com/resources/blog/flare-vm-the-windows-malware.

[39] Bacurio, Floser та Joie Salvio. «REMCOS: A New RAT In The Wild". FORTINET. 14 лютого 2017 р. https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2.

[40] Microsoft Threat Intelligence. «HTML smuggling surges: Highly evasive loader technique increasingly used in banking malware, targeted attacks». Microsoft. 11 листопада 2021 р. https://www.microsoft.com/en-us/security/blog/2021/11/11/html-smuggling-surges-highly-evasive-loader-technique-increasingly-used-in-banking-malware-targeted-attacks/.

[41] «HTML Application». *Wikipedia*. Переглянуто: вересень 2023 р. https://en.wikipedia.org/wiki/HTML_Application.

[42] «Gamaredon Group». MITRE. Змінено 22 березня 2023 р. https://attack.mitre.org/groups/G0047/.

[43] «Member States». United Nations. Переглянуто: вересень 2023. https://www.un.org/en/about-us/member-states.

[44] «Members and Observers». World Trade Organization. Переглянуто: вересень 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[45] «46 Member States». Council of Europe. Переглянуто: вересень 2023. https://www.coe.int/en/web/portal/46-members-states.

[46] «Participating States». Organization for Security and Co-operation in Europe». Переглянуто: вересень 2023. https://www.osce.org/participating-states.

[47] «Ukraine summary». *Britannica*. Переглянуто: вересень 2023. https://www.britannica.com/summary/Ukraine.

[48] «Kievan Rus». *Britannica*. Змінено 11 серпня 2023 р. https://www.britannica.com/topic/Kyivan-Rus.

[49] Polkhy, Serhii. *The Origins of the Slavic Nations: Premodern Identities in Russia, Ukraine, and Belarus.* Camridge University Press. с. 65. http://assets.cambridge.org/97805218/64039/excerpt/9780521864039_excerpt.pdf

[50] Ibid.

[51] Andrejsons, Kristaps. «Russia and Ukraine Are Trapped in Medieval Myths». *Foreign Policy*. 6 лютого 2022 р. https://foreignpolicy.com/2022/02/06/russia-and-ukraine-are-trapped-in-medieval-myths/.

[52] «Ukraine summary», *Britannica*.

[53] «A short history of Ukrainian nationalist—and its tumultuous relationship with Russia». *The Conversation.* 17 березня 2022 р. https://theconversation.com/a-short-history-of-ukrainian-nationalism-and-its-tumultuous-relationship-with-russia-179346.

[54] «Ukraine summary», *Britannica*.

[55] Vorobyov, Niko. «Ukraine crisis: Who are the Russia-backed separatists?» Al Jazeera. 4 лютого 2022 р. https://www.aljazeera.com/news/2022/2/4/ukraine-crisis-who-are-the-russia-backed-separatists

[56] «Ukraine summary", *Britannica*.