Державна служба спеціального зв'язку
та захисту інформації України

РОСІЙСЬКІ КІБЕР-ОПЕРАЦІЇ

Аналітика за І півріччя 2024 року

ЗМІСТ

Євгенія Наконечна,
начальниця Державного центру
кіберзахисту Держспецзв'язку

Повномасштабне вторгнення рф в Україну стало потужним каталізатором для розвитку кіберзагроз. Війна в кіберпросторі — це поле протистояння, де тактики і технології змінюються щодня.

Російські хакерські угруповання як ті, що працюють у складі спецслужб рф, так і кіберзлочинці та хактивісти, постійно шукають слабкі місця в інформаційних системах України та розробляють нові методи атак як проти нас, так і проти всього цивілізованого світу.

Протягом першого півріччя 2024 року команда CERT-UA у співпраці з іншими підрозділами Сил Оборони зафіксувала суттєву еволюцію в застосуванні кібератак.

У 2022 році ворог робив акцент на операціях знищення IT-інфраструктур організацій сектору критичної інфраструктури, а також отримання баз даних, списків. Проводилися кампанії проти медіа та комерційних організацій, які все ж не призводили до паніки серед цивільного населення та не створювали ефекту на полі бою. Інформаційні приводи для ворожих «кіберперемог» не давали бажаного довготривалого ефекту, а українські IT-системи швидко відновлювалися. Ворожі хакери йшли туди, де були очевидні недоліки, вразливості і можливості, якими вони могли легко скористатися.

У 2023 році їх стратегія поступово змістилася зі знищення інфраструктур організацій, провайдерів послуг Інтернету, міністерств і органів державної влади до закріплення і прихованого

Попередні звіти:

II півріччя 2022

I півріччя 2023

II півріччя 2023

отримання інформації та використання кіберкомпоненту для отримання зворотного зв’язку про результати їхніх кінетичних уражень. ІТ показала себе як галузь, яка швидко відновлювалася після зламів та ставала сильнішою.

У 2024 році спостерігається зміщення фокуса атак на все, що безпосередньо пов’язане з театром бойових дій та атаками на постачальників послуг, з метою якомога довше залишатися непомітними, утримувати присутність в системах, які мають зв’язок з війною та політикою. Хакери йдуть не просто туди, куди можуть, а туди, куди треба для успішної підтримки їхніх військових операцій.

На основі даних, зібраних CERT-UA та іншими кіберпідрозділами Держспецзв’язку, ми проаналізували нові тенденції в кіберзагрозах, виявили слабкі місця в нашій обороні та оцінили ефективність заходів, вжитих для протидії цим загрозам.

У звіті ми детально розглянемо, як змінилися тактика і цілі російських хакерських угруповань, які нові загрози з’явилися та які уроки ми винесли з цього досвіду.

Результати цього дослідження є важливими для розуміння сучасних кіберзагроз та розробки ефективних стратегій протидії.

Ми сподіваємося, що цей звіт стане цінним джерелом інформації як для українських, так і іноземних фахівців у галузі кібербезпеки, а також всіх, хто зацікавлений у вдосконаленні своїх навичок з кіберзахисту.

СТАТИСТИКА ТА ТЕНДЕНЦІЇ

Disclaimer: цей набір даних зібрано на основі аналітики інцидентів, опрацьованих **ВИКЛЮЧНО** Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA та SOC Державного центру кіберзахисту Держспецзв'язку*.

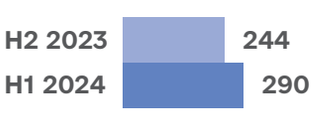
Інциденти за рівнем критичності	H2 2023	H1 2024	Зміна за період
критичні	31	3	-90%
високі	156	45	-71%
середні	1264	1670	32%
низькі	12	21	75%
разом	**1463**	**1739**	**19%**

КІЛЬКІСНІ ПОКАЗНИКИ ПО ОПРАЦЬОВАНИХ ІНЦИДЕНТАХ

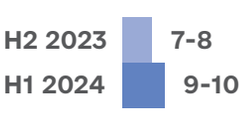
+19%

ЗРОСТАННЯ КІЛЬКОСТІ ЗАРЕЄСТРОВАНИХ ІНЦИДЕНТІВ У І ПІВРІЧЧІ 2024 Р.

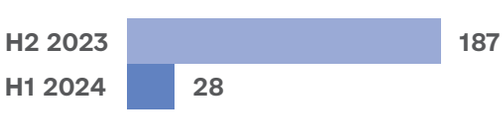
У СЕРЕДНЬОМУ ЗА МІСЯЦЬ



У СЕРЕДНЬОМУ ЗА ДЕНЬ



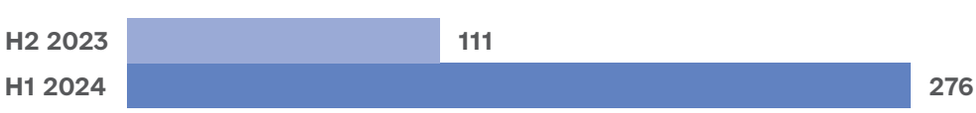
НА 85% МЕНШЕ ІНЦИДЕНТІВ КРИТИЧНОГО ТА ВИСОКОГО РІВНІВ:



НА 40% БІЛЬШЕ КІБЕРІНЦИДЕНТІВ З РОЗПОВСЮДЖЕННЯ ШПЗ

НА 90% БІЛЬШЕ КІБЕРІНЦИДЕНТІВ ІЗ ЗАРАЖЕННЯ ШПЗ*

БІЛЬШ НІЖ УДВІЧІ ЗРОСЛА КІЛЬКІСТЬ АТАК НА СЕКТОР БЕЗПЕКИ ТА ОБОРОНИ



**Зростання кіберінцидентів, пов'язаних із зараженням ШПЗ, меншою мірою пов'язано зі зміною ТТП, а більшою за рахунок підвищення видимості (жертви частіше звертаються за допомогою) **

Як видно з графіків, зберігається тенденція до зростання кількості кіберінцидентів при зменшенні кількості інцидентів високого та критичного рівнів.

Постійна та ефективна кооперація підрозділів Держспецзв'язку, основним завданням яких є забезпечення кібербезпеки та кіберзахисту в Україні, суттєво вплинула на цю статистику.

Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Держспецзв'язку (SOC ДЦКЗ) використовує індикатори кіберзагроз, отримані CERT-UA за результатами дослідження кіберінцидентів та кібератак, а також додаткові індикатори компрометації, отримані від партнерів та збагачені фахівцями обох підрозділів.

На основі цих індикаторів SIEM автоматично аналізує дані, зібрані з різних джерел, таких як NDR (Network Detection & Response), EDR (Endpoint Detection & Response), потоків мережевих сесій, опрацьовує мільярди та виявляє мільйони подій безпеки різного рівня критичності. За результатами ручного аналізу підозрілих подій, виявлених SIEM, фахівці SOC виявили 525 кіберінцидентів. До того ж більшість цих подій були заблоковані засобами захисту, наданими Оперативним центром реагування на кіберінциденти ДЦКЗ більше ніж 70 організаціям, і не мали впливу на кінцеві системи.

Як свідчить статистика, значно зросла кількість атак на урядові організації та місцеві органи влади. Кількість опрацьованих кіберінцидентів, націлених на сектор безпеки та оборони та на енергетичний сектор, зросла більше ніж вдвічі.

Проте доречно зауважити, що ці статистичні дані відносні і залежать від різних факторів. Окрім зміни тенденцій атак в кіберпросторі, на ці цифри також впливає збільшення видимості (можливостей виявлення інфікувань), зростання усвідомленості (дедалі більше організацій звертаються до нас за консультацією/допомогою) тощо.

КЛЮЧОВІ ВИСНОВКИ ТА ІНСАЙТИ ЗА І ПІВРІЧЧЯ 2024 РОКУ

НОВІ ГРУПИ І ВАРІАНТИ АТАК ЧЕРЕЗ ПОШТУ, АРХІВИ І ВІРУСИ

На початку першого півріччя 2024 року, як і в другому півріччі 2023 року, кібератаки з метою шпигунства мали вигляд таргетованих розсилок шкідливого програмного забезпечення.

Еволюцію та трансформацію ключових підходів старих груп ми продемонстрували на такій візуалізації.

Також за Н1 2024 ми фіксуємо значну активність 8 кластерів кіберзагроз, які відслідковуємо з початку цього чи кінця минулого року. Деякі з них відомі давно, але з тих чи інших причин ми не фіксували їх операцій протягом тривалого часу:

1. **UAC-0184** (кібершпіонаж, рф)
2. **UAC-0027** (кібершпіонаж, Китай)
3. **UAC-0195** (викрадення акаунтів месенджерів)
4. **UAC-0020** (кібершпіонаж, т.о. Луганськ)
5. **UAC-0149** (кібершпіонаж, рф)
6. **UAC-0188** (атаки на фінансові та страхові установи ЄС, США та України)
7. **UAC-0063** (кібершпіонаж, можливо, підкластер UAC-0001)
8. **UAC-0180** (кібершпіонаж)

На початку H1 2024 найбільше розсилок електронних листів зі шкідливим вкладенням було зафіксовано від російського хакерського угруповання **UAC-0050**. Ми фіксували до 5 таких інцидентів щотижня.

Проте з березня ця активність знизилася, і вже в квітні не було зафіксовано жодної такої розсилки. У цей же період їм на заміну прийшли угруповання **UAC-0149** та **UAC-0184**. Їх підхід більш витончений, атаки таргетовані на конкретних осіб Сил Оборони України.

Натомість атаки **UAC-0010** ФСБ рф продовжуються з 2014 року і донині.

Варто зазначити, що хакерські групи, які здійснюють атаки проти України в рамках так званої «СВО», щодо яких нами ще не здійснено підтверджену атрибуцію, можуть належати до кластерів загроз:

- **росгвардія**
- **мвд рф**
- **спецзв'язок фсо рф**
- **генштаб рф**

АНОМАЛЬНІ ЗМІНИ В АКТИВНОСТІ ФІНАНСОВИХ ХАКЕРСЬКИХ ГРУП

Так само, як і **UAC-0050**, угруповання **UAC-0006**, яке займалося викраденням коштів українських компаній, зникло з нашого поля зору в березні 2024 року аж до травня.

За час їх відсутності відбулося кілька кібератак з використанням вірусів-шифрувальників, при цьому хакерам вдалося зашифровувати дані в мережах комерційних компаній, включаючи резервні копії. Єдиним варіантом їх відновлення для компаній було погодитися на умови зловмисників та придбати у них «розшифрувальник». У таких випадках важливо мати резервні копії критичних систем на зовнішніх носіях, не підключених до ІКС.

Починаючи з травня 2024 року, **UAC-0006** відновили свою діяльність, розсилаючи ШПЗ новим жертвам та відновлюючи доступ до комп'ютерів, які були інфіковані раніше.

МАСОВІ КАМПАНІЇ З ВИКРАДЕННЯ ДОСТУПУ ДО МЕСЕНДЖЕРІВ

Хакери викрадають акаунти в месенджерах для подальшого розповсюдження ШПЗ та фішингу з метою скомпрометувати якнайбільше користувачів. Серед контактів жертви можуть бути «важливі» для них цілі, листування яких цікаве для співробітників різних спецслужб країни-агресора.

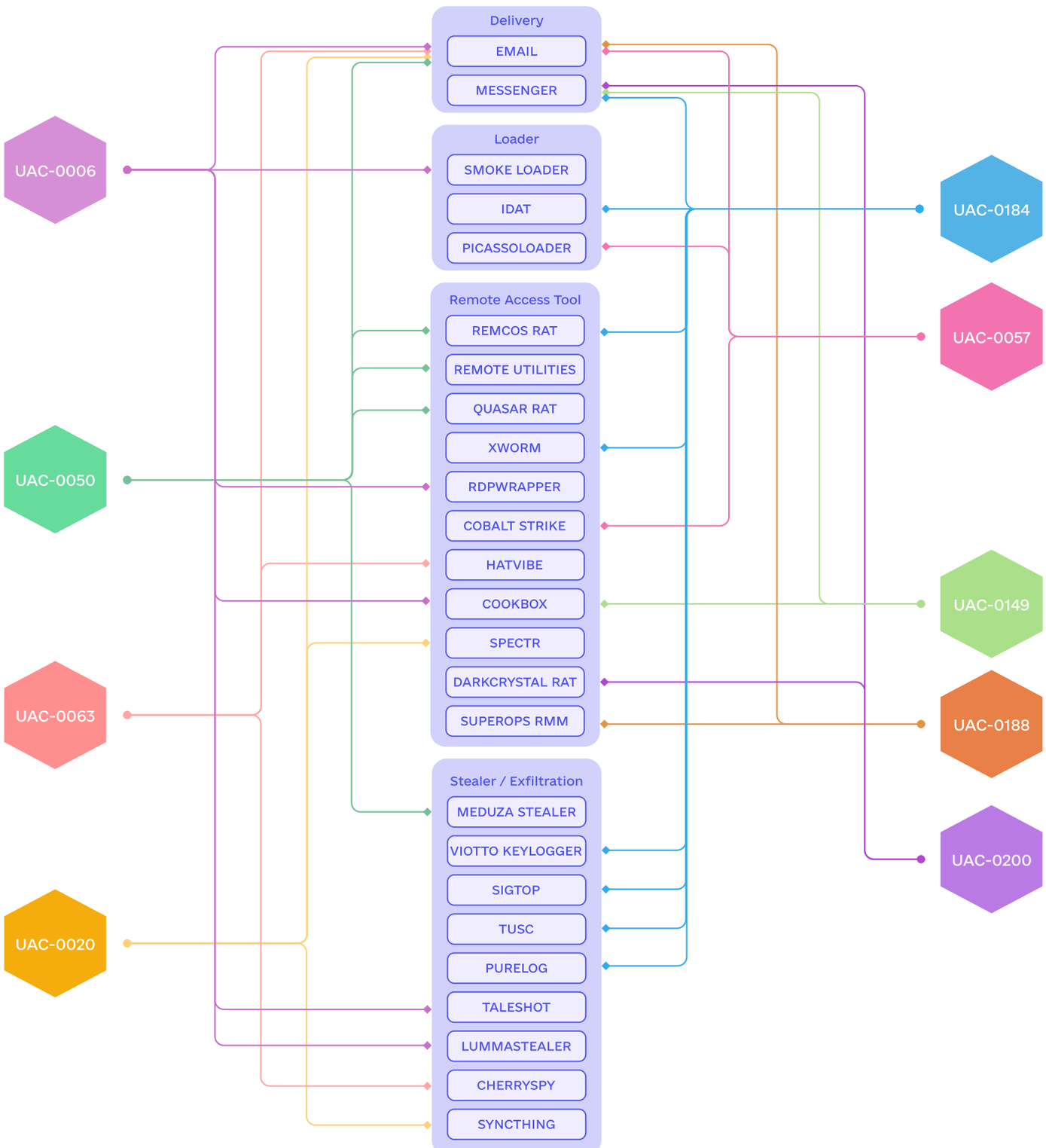
Компрометацію облікових записів використовують не лише для шпигунства, але й для отримання фінансової вигоди.

РОЗПОВСЮДЖЕННЯ ШПЗ ЗА ДОПОМОГОЮ «ПІРАТСЬКОГО» ПЗ

Доволі значна частина «піратського» програмного забезпечення постачається відразу з «бекдорами», що призводить до інфікування системи. Слід зазначити, що мінімізації цього ризику та й підвищенню рівня захисту в цілому суттєво сприяє допомога закордонних партнерів, що надають ліцензійне програмне забезпечення та засоби захисту, доступ до хмарних сервісів, але цього все ж недостатньо. Також мусимо зазначити, що надання ліцензованого ПЗ Windows, Office, EDR, MDM, SIEM, IDM є критично важливим для українських військових і цивільних організацій, щоб не залишатися вразливими до інфікування шкідливим програмним забезпеченням через неліцензоване ПЗ.

ІНСТРУМЕНТАРІЙ

Аналіз інструментарію противника дозволяє виявити схожості по TTP та кластеризувати угруповання, виявити, які групи закуповують та використовують ШПЗ.



КЕЙСИ

Нижче представлено огляд активностей **UAC-0184**, **UAC-0020**,**UAC-0149**, **UAC-0200**, **UAC-0180**, які в Н1’2024 фокусувалися саме на атаках проти військових із застосуванням різних варіацій RAT та іншого ШПЗ для утримання та віддаленого контролю скомпрометованих Windows комп'ютерів військовослужбовців Сил Оборони України.

SIGNAL І ТАРГЕТОВАНІ РОЗВІДУВАЛЬНІ ОПЕРАЦІЇ ГРУПИ UAC-0184 ПРОТИ ВІЙСЬКОВИХ

За час повномасштабного вторгнення хакери активно збирали персональні дані громадян України, в тому числі військовослужбовців. Прізвище та ім’я, паспортні дані, а найголовніше — місце їх служби та посада. Саме ці дані надають змогу хакерам сконцентруватися на конкретних особах, на комп’ютерах яких з високою ймовірністю є важливі документи.

На більшості корпоративних поштових серверів використовуються засоби захисту, тому хакери дедалі частіше відмовляються від надсилання шкідливих програм на поштові скриньки жертв та віддають перевагу атакам через інші засоби комунікації. Тут в нагоді стають месенджери, якими також користується велика кількість військових. Маючи вдосталь даних про особу та контактний телефон, хакери з угруповання **UAC-0184** видають себе за інших та розпочинають спілкування з майбутньою жертвою, зазвичай за допомогою Signal. Слід відмітити, що для «обробки» жертви використовуються будь-які доступні ресурси, навіть платформи для знайомств.

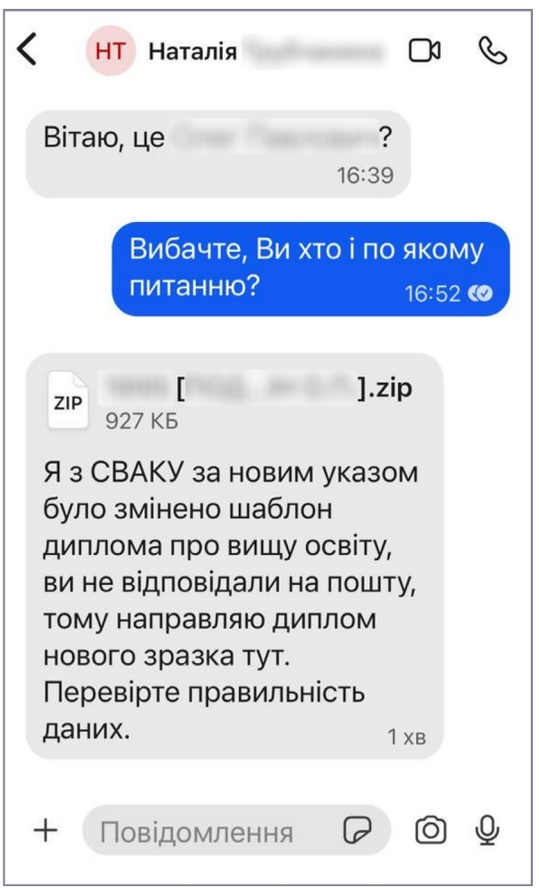
Отже, «втершись в довіру», під виглядом документів на нагородження, відео бойових дій, рекрутингу до інших підрозділів жертві надсилають архів з файлом-ярликом. Це не вичерпний список тем, на які зловмисники спілкуються зі своїми жертвами. Особлива увага приділяється тому, що зазначені файли необхідно відкрити саме на комп’ютері.

Відкриття файлу-ярлика на комп'ютері відобразить релевантний до тематики спілкування файл-приманку, а також інфікує систему шкідливою програмою — завантажувачем, який в свою чергу встановить програму для віддаленого управління ЕОМ. Таким чином, угруповання **UAC-0184** отримує повний доступ до комп'ютера.

НАЙТИПОВІШІ СЦЕНАРІЇ

Запит інформації

- «скиньте контакт»
- підтвердіть
- повідомте
- ви з'явилися у списку на отримання, а ми наказ знайти не можемо
- ви якісь документи з цього приводу не отримували?



Залякування

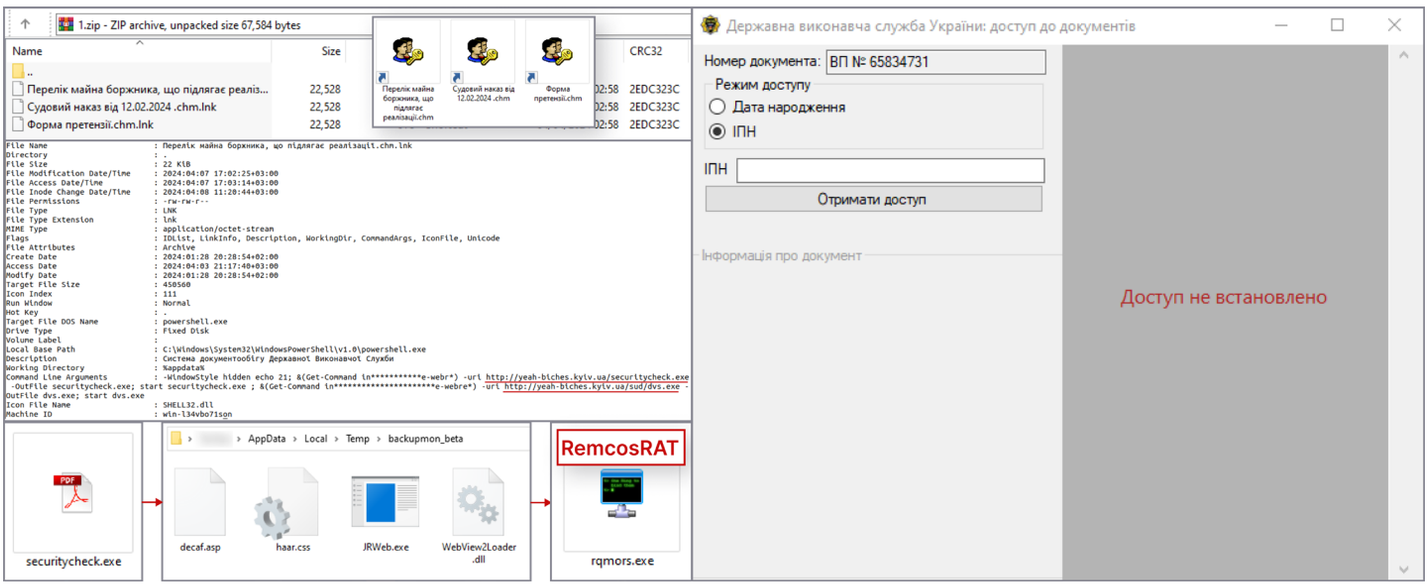
- відкриття провадження проти військовослужбовця
- «є проблема з»
- «ви з'явилися у списку»
- «до вас є питання щодо діяльності»

Винагорода

- годинник
- виплата
- відпустка

Переведення

- в нову частину
- відрядження за кордон



Приклад ланцюга ураження

MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.001] Command and Scripting Interpreter: PowerShell
- [T1059.003] Command and Scripting Interpreter: Windows Command Shell
- [T1059.005] Command and Scripting Interpreter: Visual Basic
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Defense Evasion [TA0005]
- [T1140] Deobfuscate/Decode Files or Information
- [T1564.003] Hide Artifacts: Hidden Window
- [T1036] Masquerading
- [T1553.005] Subvert Trust Controls: Mark-of-the-Web Bypass

Collection [TA0009]
- [T1560.001] Archive Collected Data: Archive via Utility
- [T1119] Automated Collection

Command and Control [TA0011]
- [T1071.001] Application Layer Protocol: Web Protocols
- [T1105] Ingress Tool Transfer
- [T1095] Non-Application Layer Protocol

https://cert.gov.ua/article/6278521

UAC-0020

Діяльність угруповання ведеться співробітниками силових відомств тимчасово окупованого Луганська. Фактично це зрадники, які перейшли на сторону окупанта, як і **UAC-0010**. Востаннє активність цієї групи була зафіксована нами в березні 2022 року.

Жертвам надсилався електронний лист нібито з технічними характеристиками нової версії озброєння та вкладенням у вигляді архіву «туррель.фоп.вовчок.rar», захищеного паролем. В архіві знаходився RARSFX-архів «туррель.фоп.вовчок.sfx.rar.scr», що містив файл-приманку «Wowchok.pdf», EXE-інсталятор «sync.exe» та BAT-файл «run_user.bat».

Як і раніше для збору даних (документів, файлів, паролів та іншої інформації) вони скористалися шкідливим програмним забезпеченням SPECTR, а для їх ексфільтрації цього разу використали штатний функціонал синхронізації легітимного програмного забезпечення SyncThing.

MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.007] Command and Scripting Interpreter: JavaScript
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1053.005] Scheduled Task/Job: Scheduled Task

Defense Evasion [TA0005]
- [T1036.007] Masquerading: Double File Extension

Credential Access [TA0006]
- [T1528] Steal Application Access Token
- [T1539] Steal Web Session Cookie

Collection [TA0009]
- [T1119] Automated Collection
- [T1074.001] Data Staged: Local Data Staging
- [T1005] Data from Local System
- [T1025] Data from Removable Media
- [T1113] Screen Capture

Command and Control [TA0011]

https://cert.gov.ua/article/6279600

- [T1071.001] Application Layer Protocol: Web Protocols
- [T1090.003] Proxy: Multi-hop Proxy
- [T1090.004] Proxy: Domain Fronting

Exfiltration [TA0010]
- [T1020] Automated Exfiltration
- [T1048] Exfiltration Over Alternative Protocol

UAC-0006. PLAY, PAUSE, REPLAY

На початку першого півріччя 2024 року продовжувалися масові розсилки від фінансово вмотивованого угруповання **UAC-0006**, які почались ще в травні 2023 року. Розсилки були направлені на працівників фінансових підрозділів організацій.

Використовуючи архіви-поліглоти (які мали різний вміст залежно від програмного забезпечення, яким їх відкривали), зловмисники доставляли на ЕОМ бухгалтерів шкідливу програму-завантажувач SmokeLoader. Слід зауважити, що в конфігурації цього завантажувача було вказано кілька доменних імен, більшість з яких не мали А-запису, тобто були не зареєстровані.

За допомогою SmokeLoader хакери встановлювали інше ШПЗ зі свого арсеналу, наприклад шкідливе програмне забезпечення TALESHOT, яке робить знімки екрана, якщо на ньому відкрито вікно з назвою банківського додатка, в тому числі браузер з відкритою його вебверсією, та передає ці знімки хакерам. Залежно від зацікавленості конкретним комп'ютером, за результатом аналізу отриманих даних **UAC-0006** встановлювали збірку RMS + LOADERX3 + RDPWRAPPER, що надає інтерактивний доступ до комп'ютера (паралельно з легітимним користувачем), а відповідно і можливість провести детальніший аналіз жертви. Фінальним етапом було створення платежу або редагування наявного.

Ця хвиля кібератак, що тягнулася з 2023 року, закінчилася в березні цього року.

Вже через два місяці відпочинку, як і минулого року, в травні, **UAC-0006** повернулися. Окрім нових розсилок, з метою «отримання» нових жертв, вони зареєстрували домени, які були в минулих конфігураціях SmokeLoader, щоб повернути контроль над ЕОМ, які були інфіковані раніше.

За звітний період у співпраці з Оперативним центром реагування на кіберінциденти ДЦКЗ Держспецзв'язку опрацьовано 251 кіберінцидент, пов'язаний з діяльністю цього угруповання. При цьому 36% цих інцидентів зафіксовано засобами SOC ДЦКЗ.

https://cert.gov.ua/article/6279366

MITRE ATT&CK

Initial Access [TA0001]
- [T1566.001] Phishing: Spearphishing Attachment

Execution [TA0002]
- [T1059.001] Command and Scripting Interpreter: PowerShell
- [T1059.003] Command and Scripting Interpreter: Windows Command Shell
- [T1059.005] Scheduled Task/Job: Scheduled Task
- [T1204.002] User Execution: Malicious File

Persistence [TA0003]
- [T1547.001] Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

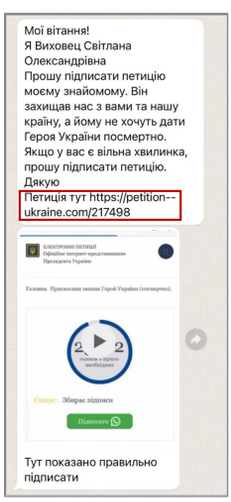
Defense Evasion [TA0005]
- [T1562.004] Impair Defenses: Disable or Modify System Firewall
- [T1036] Masquerading
- [T1036.007] Masquerading: Double File Extension
- [T1027.010] Obfuscated Files or Information: Command Obfuscation
- [T1553.005] Subvert Trust Controls: Mark-of-the-Web Bypass

Command and Control [TA0011]
- [T1071.001] Application Layer Protocol: Web Protocols
- [T1105] Ingress Tool Transfer
- [T1095] Non-Application Layer Protocol

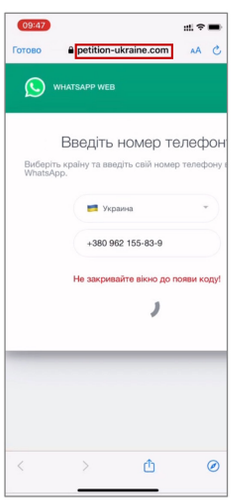
ГОЛОСУВАННЯ В МЕСЕНДЖЕРАХ — НОВИЙ СПОСІБ ВИКРАДЕННЯ АКАУНТІВ

Месенджери WhatsApp та Telegram користуються великою популярністю серед українців. Їх використовують як засоби зв'язку, спосіб швидко дізнатися останні новини чи поширити певну інформацію. Саме тому ці месенджери опинилися під прицілом російських хакерів цієї весни.

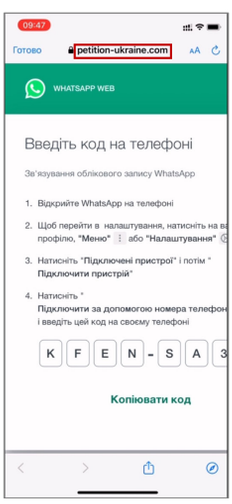
Атаки угруповання **UAC-0195** направлені на отримання доступу до месенджерів громадян України з метою максимального поширення і зараження (spray & pray). Метою цих атак є шпигунство (викрадення даних з чатів), подальше розповсюдження фішингових посилань (для збільшення кількості жертв) та фінансова складова (виманювання грошей).



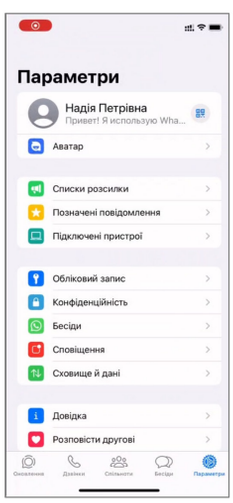
Зловмисник надсилає повідомлення з посиланням та відеоінструкцією



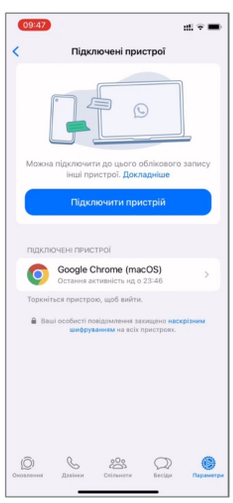
Жертва **переходить** за посиланням та вводить номер телефону



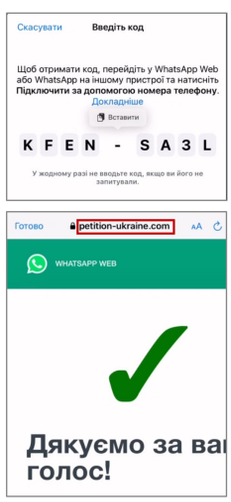
Вебсайт зловмисника ініціює запит до WhatsApp та отримує код



Жертва **відкриває** налаштування WhatsApp «Підключені пристрої»



Жертва **натискає** «Підключити пристрій»



Жертва **вводить** раніше отриманий код. Аккаунт WhatsApp скомпрометовано

Першою хвилею було викрадення облікових записів WhatsApp. Хакери використали як прикриття підписання петиції на сайті Президента за надання звання «Героя України» полеглому захиснику. Таким чином вони намагались направити людей на сайт, що мав вигляд офіційного сайту Президента України, де для «підписання петиції», потрібно було «автентифікуватись» за допомогою WhatsApp, що призводило до додавання стороннього пристрою до облікового запису. До повідомлення додавалася відеоінструкція необхідних дій.

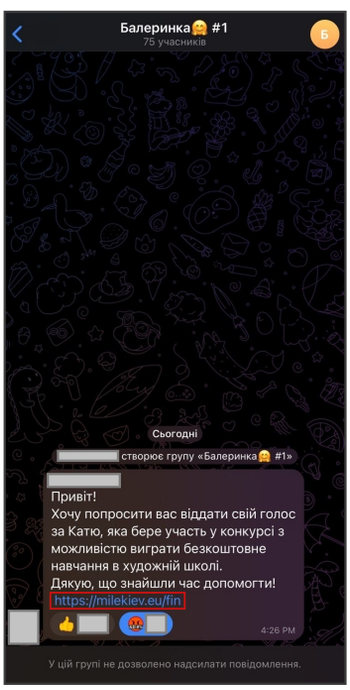
https://cert.gov.ua/article/6278735

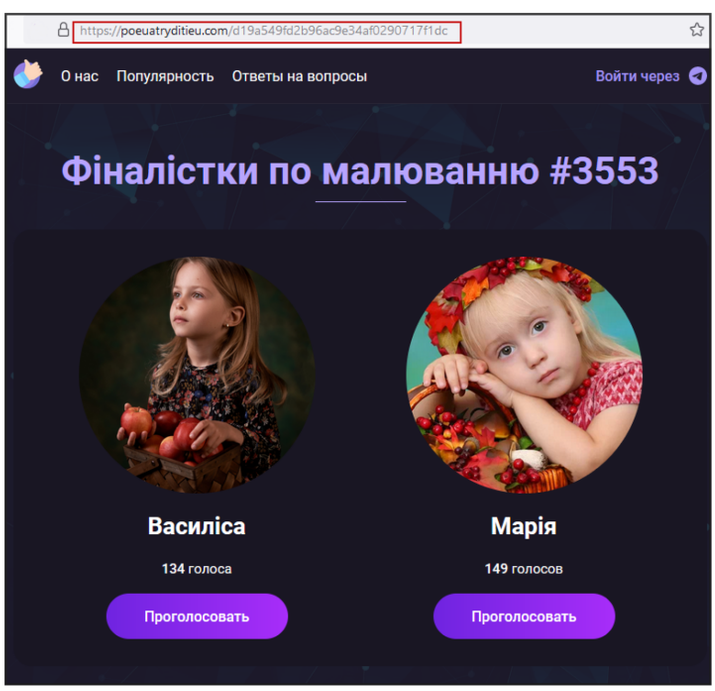
Інша хвиля була націлена на користувачів Telegram. Цього разу прикриттям була тематика голосувань за дитину, що бере участь в конкурсі мистецької діяльності.

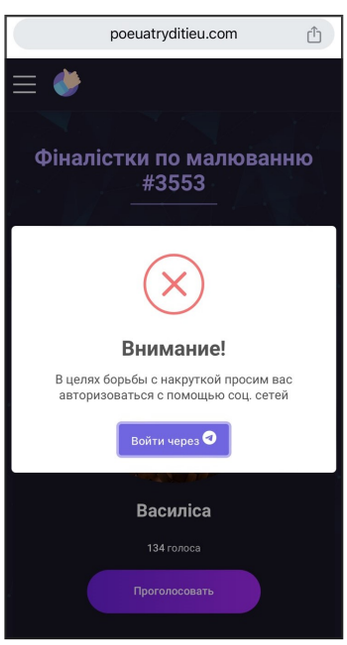
Знову ж таки, для голосування необхідно було «автентифікуватися» за допомогою месенджера, що так само призводило до додавання стороннього пристрою.

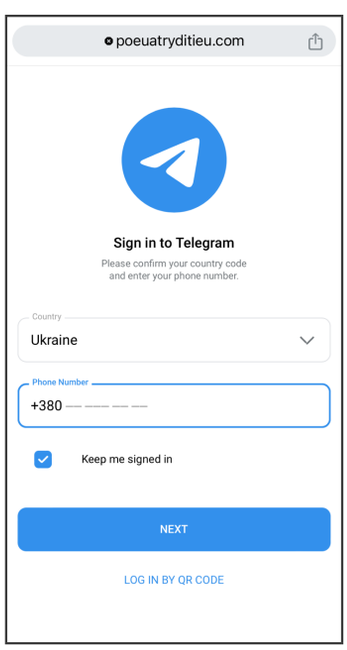
Враховуючи кількість зареєстрованих доменних імен для використання в кібератаках, а також кількість відомих нам жертв, ця загроза є надзвичайно поширеною та активною і досі.

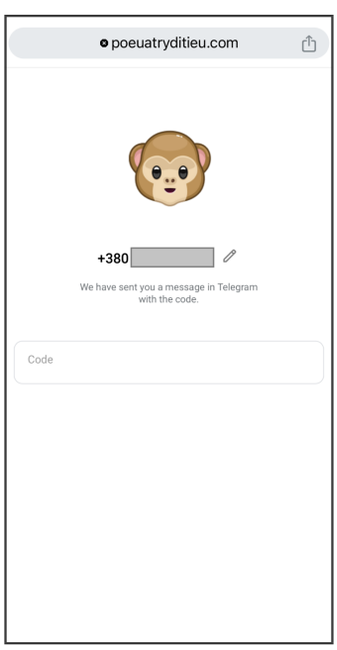
https://cert.gov.ua/article/6279491











MITRE ATT&CK

Resource Development [TA0042]
- [T1583.001] Acquire Infrastructure: Domains
- [T1586.001] Compromise Accounts: Social Media Accounts

Initial Access [TA0001]
- [T1566.002] Phishing: Spearphishing Link

Persistence [TA0003]
- [T1098.005] Account Manipulation: Device Registration

ВИКОРИСТАННЯ SUPPLY CHAIN ДЛЯ ПОВЕРНЕННЯ В ЕНЕРГЕТИЧНІ МЕРЕЖІ ВІД UAC-0002

У березні 2024 року ми виявили зараження в одній з енергетичних компаній. Детальний аналіз цього кіберінциденту дав нам індикатори та зачіпки для пошуку інших жертв, оскільки первинне інфікування відбулося через спільного постачальника послуг (комерційну компанію).

Як виявилося, угруповання **UAC-0002** вчергове здійснювало спробу деструктивної атаки проти майже 20 об'єктів енергетичної інфраструктури України (енерго-, тепло- та водопостачання).

Ураження такої кількості організацій поодинці — складне завдання, тому цього разу вони здійснили атаку на ланцюги поставки, точніше відразу на мінімум три ланцюга поставки. До такого висновку дійшли через те, що в одних випадках первинний несанкціонований доступ корелює встановлення спеціалізованого програмного забезпечення (далі — СПЗ), що містило програмні закладки та вразливості, а в інших — скомпрометовано облікові записи співробітників постачальника, які штатно мали доступ до ІКС організацій для супроводження та технічної підтримки.

Під час дослідження цього кіберінциденту на ЕОМ з ОС Linux, на яких було встановлено СПЗ, ми виявили шкідливі програми LOADGRIP та BIASBOAT. Остання є аналогом бекдору QUEUESEED (KNUCKLETOUCH, ICYWELL, WRONGSENS, KAPEKA), який було виявлено при дослідженні деструктивних кібератак угруповання **UAC-0133** (підкластер **UAC-0002**) на об'єкти водопостачання, зокрема з використанням SDELETE. Усіх жертв поєднувало використання однакового програмного забезпечення, що й було початковим вектором компрометації.

Зважаючи на функціонування ЕОМ з СПЗ в межах ІКС об'єктів кібератаки, зловмисники використовували їх для горизонтального переміщення та розвитку кібератаки у відношенні корпоративних мереж підприємств. Для прикладу, на таких ЕОМ в каталогах з СПЗ було виявлено заздалегідь створені PHP-вебшелли WEEVELY, PHP-тунель REGEORG.NEO або PIVOTNACCI.

Можна припустити, що несанкціонований доступ до ІКС значної кількості об'єктів енерго-, тепло- та водопостачання мав бути використаний для підсилення ефекту від ракетних ударів по інфраструктурних об'єктах України навесні 2024 року.

ВИСНОВКИ

Тенденція, яку ми спостерігали в минулому півріччі, а саме збільшення загальної кількості кіберінцидентів при зменшенні інцидентів високого та критичного рівня, прослідковується і зараз. Завдяки плідній роботі суб'єктів забезпечення кібербезпеки України, а також співпраці з вендорами та партнерами, розгортанню сучасних технологій та зменшенню поверхні атаки вдалося суттєво мінімізувати ризики та підвищити захищеність багатьох ключових систем.

Проте спроможності хакерів постійно зростають і нам також необхідно вдосконалюватися. Збільшення рівня захищеності ІКС, обізнаності усіх без винятку громадян — ключові аспекти, над якими потрібно безперервно працювати.

Війна триває і кіберпростір також є своєрідним полем бою. Ворог намагається розвідати інформацію будь-яким способом, тому вважаємо що кібератаки на військових та державні органи залишаться в тренді і надалі. Основними інструментами кібершпіонажу є фішинг та інфікування шкідливим програмним забезпеченням і найслабшою ланкою в цьому випадку є людина. Саме тому основним засобом кіберзахисту, в першу чергу, є постійне підвищення обізнаності громадян з основними правилами кібергігієни та актуальними кіберзагрозами.

Інший напрям ворога — дестабілізація ситуації в країні. Для знищення цивільної критичної інфраструктури (зокрема енергетичних об'єктів) застосовуються не лише кінетичні, а й деструктивні кібератаки, які дешевші за пуск балістичної ракети, але можуть призвести до таких самих руйнівних наслідків. Тому терористичні кібероперації стосовно критичної інфраструктури також не закінчаться. Виконання типових вимог, опублікованих на сайті CERT-UA (https://cert.gov.ua/article/5436463) та в звіті за друге півріччя 2023 року, — мінімально необхідна база забезпечення захисту ІКС від кібератак.

І наостанок, кібермародери — ті шахраї, які будуть завжди. Важко передбачити, яку тематику та платформу для розповсюдження вони виберуть наступного разу, щоб виманити в людей гроші чи дані банківської картки, але точно відомо, що ми про них будемо чути ще дуже довго.

Давайте будемо свідомими та відповідальними. Разом до Перемоги. Слава Україні!

ПОПЕРЕДНІ ЗВІТИ

Для повноти картини і трансформацій у застосуванні кіберможливостей під час повномасштабної війни доступні попередні аналітичні звіти за такими посиланнями:

1. Russia's Cyber Tactics: H2'2022-UA

2. Russia's Cyber Tactics H1'2023-UA

3. Russia's Cyber Tactics H2'2023-UA

Щоб дізнатися більше, підпишіться за цим посиланням:
Контакт-центр для ЗМІ
press@cip.gov.ua

STAY CONNECTED:

https://twitter.com/SSSCIP

https://twitter.com/_CERT_UA

Requests for public information, statements, complaints and suggestions:
press@cip.gov.ua

РОСІЙСЬКІ КІБЕРОПЕРАЦІЇ

Аналітика за І півріччя 2024 року

Державна служба спеціального зв'язку та захисту інформації України