РОСІЙСЬКІ КІБЕРОПЕРАЦІЇ

АНАЛІТИКА ЗА ПЕРШЕ ПІВРІЧЧЯ 2023 РОКУ

Зміна тактик, цілей і спроможностей хакерських груп уряду рф та контрольованих ним угруповань

Аналітичний звіт Держспецзв'язку
за результатами дослідження загроз

Вересень 2023 р.

Державна служба спеціального зв'язку та захисту інформації України

ВСТУП

Від середини 2021 року відбувається новий стрімкий розвиток методів застосування кіберспроможностей для підтримки російських військових операцій як на полі бою, так і для гібридних атак проти цивільного населення. Детальний аналіз і вивчення їхніх тактик, змін та спроможностей є важливим для адаптації та вдосконалення українських підходів реалізації кіберзахисту та унікальним досвідом, який наші західні партнери зможуть адаптувати в своїх країнах.

Це дослідження ґрунтується на даних, зібраних Державною службою спеціального зв'язку та захисту інформації України (Держспецзв'язку) в процесі роботи над ліквідацією наслідків успішних російських кібероперацій, а також над тими, яким вдалося запобігти завдяки вчасній взаємодії. Держспецзв'язку постійно аналізує інновації в інструментах, інфраструктурі, поведінці, цілях та методиках, шаблонах та спроможностях нападників.

У цьому звіті підсумовані знання та спостереження, здобуті в процесі постійного обміну досвідом Держспецзв'язку та CERT-UA з міжнародною експертною спільнотою, журналістами та IT-фахівцями. Ви також можете переглянути Підсумковий звіт за 2022 рік (https://cip.gov.ua/ua/news/u-2022-roci-kilkist-zareyestrovanikh-kiberincidentiv-virosla-maizhe-vtrichi-zvit) та підписатися (https://share-eu1.hsforms.com/1SNVq2857Q82uZWUfbxCyhw2b2xj0) на розсилку іншої аналітичної документації Держспецзв'язку.

Ми невпинно розвиваємося і кожну кібератаку, описану в цьому звіті, аналізуємо щодо контексту (часові межі, завдання, наслідки), віктимології (атаковані сектори, країни), основних тактик, методик і процедур (ТМП), а також атрибуції на підставі власного досвіду, маркерів і спостережень.

Це наш другий аналіз активної фази кіберскладової нинішньої війни. Він є спробою абстрагуватися від повсякденних подій, роздивитися ситуацію крізь туман війни і побачити загальну картину. Картину, яка могла би дати змогу нашим партнерам більше дізнатися і пристосуватися до нової епохи гіперактивної кіберагресії. Враховуючи знання, здобуті в процесі моніторингу змін у тактиці російської кіберагресії протягом найактивнішої фази проведення кібер- і кінетичних операцій, кіберспільнота отримує цінний матеріал для прогнозування / моделювання:

1. **Вибору майбутніх цілей:** Аналіз еволюції російських тактик ведення кібервійни з погляду вибору цілей може дати уявлення про потенційні майбутні цілі. До них можуть належати критична інфраструктура, державні органи або конкретні галузі.
2. **Атрибуції та звичок:** Розуміння звичок та можливостей / навиків ворожих команд, які російські угруповання та інституції реалізовують ті чи інші тактики майбутніх операцій, як розуміти їхні цілі і мотиви, наслідки та способи закріплення.
3. **Стратегій гібридної війни:** Вивчення того, як було інтегровано кіберкомпонент в російські стратегії гібридної війни, може дати корисні підказки щодо їхніх намірів і можливих способів використання кіберможливостей у майбутніх геополітичних конфліктах.

4. **Розвитку сучасного шкідливого ПЗ та методів його застосування:** Виявлення передового ШПЗ і методів його застосування російськими суб'єктами кіберагресії може стати в пригоді для прогнозування нових інструментів та необхідних методів виявлення та протидії.
5. **Взаємодії та зв'язків груп всередині країни, що воює:** Вивчення відносин між російськими групами та інституціями (військовими, правоохоронними, розвідувальними) і їхньої співпраці з іншими організаціями — як недержавними, так і спонсорованими державою — може пролити світло на можливі загрози, альянси та кооперaційні стратегії в майбутніх конфліктах.

Для кращого розуміння історичних змін у завданнях, що стоять перед російськими державними хакерськими угрупованнями (APT) та іншими командами, що беруть безпосередню участь у кампаніях атак проти України, пропонуємо ознайомитися з нашим попереднім звітом — https://cip.gov.ua/ua/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

«ПЕРЕД НАМИ — ВЕЛИЧЕЗНА СТОРІНКА З ХРОНІКИ ПОДІЙ В УКРАЇНІ. МАБУТЬ, ВІД ВАС МИ ДІЗНАЄМОСЯ НЕ МЕНШЕ, НІЖ ВИ ВІД НАС»

Джен Істерлі
директорка Агентства з питань кібербезпеки
і захисту інфраструктури США

https://www.ft.com/content/c7038f7e-48fb-4d76-a608-96eec217a654

«СПІЛЬНОТА ЗАХИСНИКІВ УКРАЇНИ ЩИРО ВДЯЧНА ЗА ПІДТРИМКУ, НАДАНУ НАШИМИ СОЮЗНИКАМИ. МИ ВДЯЧНІ ЗА НАВЧАННЯ, ТЕХНОЛОГІЇ ТА СПІВПРАЦЮ, ЯКІ ДУЖЕ ДОПОМОГЛИ НАМ У ПРОТИСТОЯННІ РОСІЙСЬКІЙ ЗАГРОЗІ. ЗІ СВОГО БОКУ МИ РАДІ ПОДІЛИТИСЯ НАШИМИ ІНСАЙТАМИ, ЯКІ, Я ВІРЮ, Є ВАЖЛИВИМ РЕСУРСОМ ДЛЯ КІБЕРСПІЛЬНОТ КРАЇН, ЩО ПРАГНУТЬ РОЗБУДОВИ І ПОСИЛЕННЯ СВОЄЇ КІБЕРСТІЙКОСТІ»

Віктор Жора
заступник голови Державної служби
спеціального зв'язку та захисту інформації України

КЛЮЧОВІ ВИСНОВКИ ТА ІНСАЙТИ ПЕРШЕ ПІВРІЧЧЯ 2023 РОКУ

Російське вторгнення призвело до помітних змін в екосистемі кіберкримінал росії, які, ймовірно, матимуть довгострокові наслідки для координації між злочинними угрупованнями і масштабу світової кіберзлочинності.

Перехід від великої кількості деструктивних атак в першому кварталі 2022 року до справжнього агресивного шпигунства / імплантації і вивантаження даних із закріпленням на жертвах та нових операцій інформаційного впливу — встановлює високу планку до вимог практичного захисту критичних об'єктів. Адже люди в командах противника не зазнають «втрат на полі бою», постійно набувають нових навичок завдяки безперервній практиці на нашій інфраструктурі. Тож можемо прогнозувати суттєві ескалації застосування кіберкомпоненту проти нашої країни та всього світу навіть після перемоги України на полі бою.

Ключові інсайти:

ПОДВОЄННЯ КІЛЬКОСТІ ІНЦИДЕНТІВ

Українськими IT-командами впроваджено багато покращень (від використання найсучаснішого захисного стеку до 24x7 моніторингу ДЦКЗ Держспецзв'язку). Проте протягом перших 6 місяців 2023 року кількість інцидентів, зареєстрованих CERT-UA, подвоїлася: від 1,9 інцидентів у середньому за день (57 на місяць) у другому півріччі 2022 р. до 4-5 за день (128 на місяць) у першому півріччі 2023 р.

Контрольовані російською державою ворожі групи готуються до тривалого протистояння із Заходом та залучають дедалі більше людей задля збільшення спроможностей і швидкості операцій.

СЕРЕД ЦІЛЕЙ ШПІОНАЖУ ПЕРЕВАЖАЮТЬ ЦИВІЛЬНИЙ І ПРАВООХОРОННИЙ СЕКТОРИ

У першій половині 2023 р. ми спостерігали постійний інтерес до організацій громадського сектору і правоохоронних органів. За цей період ми зіткнулися з проведенням військовими APT шпигунських операцій, спрямованих на отримання доступу і добування даних від різних силових та державних структур України. Основним їхнім завданням було отримання доступу до матеріалів, зібраних та переданих правоохоронними органами в суди та прокуратуру, запитів на затримання підозрюваних агентів, доказів воєнних злочинів росії.

Крім того, збільшилася кількість кібератак на приватний сектор із метою використання кіберможливостей для відстеження наслідків кінетичних операцій ворога, зокрема ракетних ударів і атак БпЛА. Ба більше, ці атаки були спрямовані на дослідження планів державних підрядників і постачальників в межах проактивної підготовки України до майбутніх заходів.

ЗЛАМАЛИ РАЗ — ЗЛАМАЮТЬ ВДРУГЕ!

Ми виявили показову тенденцію надання переваги спробам повторних атак. Хакери повертаються до попередніх цілей, які володіють і оперують критичними даними, потрібними російським військам. Такий підхід дає зловмисникам можливість стратегічного планування майбутніх операцій і прогнозування нашої реакції. Заздалегідь знаючи про мережеву інфраструктуру, захисні заходи, ключовий персонал і моделі комунікації організації-жертви, нападники мають істотну перевагу, коли йдеться про експлойт організацій, скомпрометованих у минулому.

Другим важливим аспектом є те, що є організації, які мають інформаційну, розвідувальну або іншу цінність для противника, тож він всілякими засобами намагається повернути собі доступ до необхідних йому джерел інформації. Такі організації можуть обробляти запити, звіти, особові справи, бази даних. Часто — це відділи і канцелярії окремих структур.

ФОКУС НА МИТТЄВУ ЕКСФІЛЬТРАЦІЮ ДАНИХ

CERT-UA спільно з партнерами оптимізували збирання розвідувальних даних про загрози (TI) та скоротили середній час на виявлення і реагування (MTTD/MTTR). Тож тепер російські суб'єкти загрози мають менше часу на рух всередині скомпрометованих організацій, що змушує їх робити ще більший акцент на конкретній тактиці: дампінгу документів. У певних випадках траплялося, що більше 20 000 документів разом із обліковими даними браузера витягувалися протягом перших 30 хвилин після успішного проникнення у скомпрометовану систему. Після цього вони починають розповсюджувати шкідливе ПЗ через різні канали — електронну пошту, Signal і Telegram — експлуатуючи довірені зв'язки і контакти з іншими організаціями, важливими для зловмисників як цілі.

Ми спостерігали зміну тактики, яка передбачає зараження систем, визначення пріоритетності жертв і отримання доступу до цінних активів шляхом заміни серверів управління і контролю (C2). Основна приманка для жертв усе ще складається з офісних документів та ШПЗ на базі HTML/JS в Zip/Rar-архівах, які залишаються найпоширенішими і улюбленими форматами доставки. Українські IT-адміністратори недостатньо уваги приділяють блокуванню небезпечних файлів та системних інструментів на рівні Active Directory і пошти.

МЕДІАСЕКТОР — ДАЛІ ПІД ПРИЦІЛОМ

Протягом першого півріччя 2023 року медіасектор продовжував зазнавати постійних атак. Ми ретельно відстежуємо ці атаки, насамперед спрямовані проти журналістів. Метою таких ворожих атак є здобуття контролю над ресурсами й обліковими записами ЗМІ для використання їх у кампаніях із дезінформації і операціях впливу. Слід зазначити, що багато з цих атак пов'язані з угрупованням Sandworm, асоційованим із ГРУ рф, яке є ключовим гравцем у ширшому контексті гібридної війни, яку

веде росія. https://cert.gov.ua/article/4818341

ЗАСТОСУВАННЯ ЛЕГІТИМНОГО ПЗ ДЛЯ ЗЛОВМИСНИХ ДІЙ У ХАКНУТІЙ СИСТЕМІ

Для уникнення детектування та руху всередині мережі й у скомпрометованій системі зловмисники використовують або вбудований функціонал Windows / Linux, або зовнішні інструменти.

Зловмисники часто користуються давно відомим легітимним ПЗ на базі Windows, наприклад WinRar (яке дуже популярне у нашому регіоні), sdelete та іншими різноманітними утилітами Windows. Цей підхід покликаний приховати їхню аномальну діяльність, ускладнюючи її виявлення за допомогою антивірусів та систем виявлення і реагування в кінцевих точках (AV/EDR). Відповідно, вони можуть проводити деструктивні операції, не провокуючи аномалій у моніторингу засобами AV/EDR. https://cert.gov.ua/article/4501891

ЗЛАМ І ЕКСПЛОЙТ ПОШТОВИХ СИСТЕМ ІЗ ВІДКРИТИМ ВИХІДНИМ КОДОМ

Від другої половини 2022 року ми спостерігаємо активне розроблення і застосування експлойтів проти поштових систем із відкритим вихідним кодом, які мають відомі вразливості (CVE). Часті приклади — Zimbra і Roundcube, але і з попереднього півріччя також мусимо відзначити атаки і злам через 0-day експлойт в Microsoft Outlook, який надавав в один клік прямий доступ до пам'яті системи жертви. Якщо ви не оновлюєте свої системи з періодичністю в 2-3 тижні, їх обов'язково хакнуть.

ЕНЕРГЕТИЧНИЙ СЕКТОР ПОСТІЙНО АТАКУЮТЬ

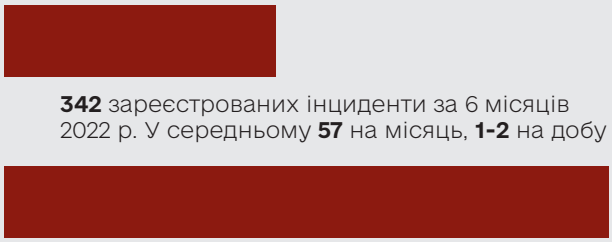
Кількість атак на цю сферу в 2023 році зменшилася після завершення дронових і ракетних ударів по цивільній енергетичній інфраструктурі. Втім, ми спостерігаємо терористичний тиск на міжнародну спільноту через Запорізьку АЕС, а ключові російські APT-угруповання отримали завдання зібрати інформацію про плани України щодо захисту станції та готовності до найгіршого сценарію.

Ключовою проблемою, що призводить до успішного проникнення, є брак надійної ізоляції між операційно-технологічною (OT) і корпоративною мережами, брак тестування на проникнення та моніторингу 24x7.

ТЕНДЕНЦІЇ ТА НОВІ ВИКЛИКИ У ПЕРШОМУ ПІВРІЧЧІ 2023 Р.

Цей набір даних зібрано на основі аналітики інцидентів, наданої підрозділом CERT-UA, без урахування випадків, зареєстрованих SOC Держспецзв'язку та інших кіберцентрів.

ЗРОСТАННЯ КІЛЬКОСТІ ЗАРЕЄСТРОВАНИХ ІНЦИДЕНТІВ



342 зареєстрованих інциденти за 6 місяців 2022 р. У середньому **57** на місяць, **1-2** на добу

+123%

762 зареєстрованих інциденти за 6 місяців 2023 р. У середньому **128** на місяць, **4-5** на добу

ПАДІННЯ ЧАСТКИ КРИТИЧНИХ ІНЦИДЕНТІВ

144 критичні інциденти у другому півріччі 2022 р. (**319** — у першому півріччі 2022 р.)

-81%

27 критичних інцидентів у першому півріччі 2023 р. Це ми вважаємо великим успіхом, досягнутим у результаті покращення співпраці та підвищення довіри підприємств і організацій до CERT-UA, спільної роботи по забезпеченню безпеки ІТ

ЗМЕНШЕННЯ ЧАСТКИ ІНЦИДЕНТІВ КРИТИЧНОГО ТА ВИСОКОГО РІВНІВ

339 інцидентів критичного та високого рівнів трапилося у другому півріччі 2022 р. (**683** — було зареєстровано у першому півріччі 2022 р).

-46%

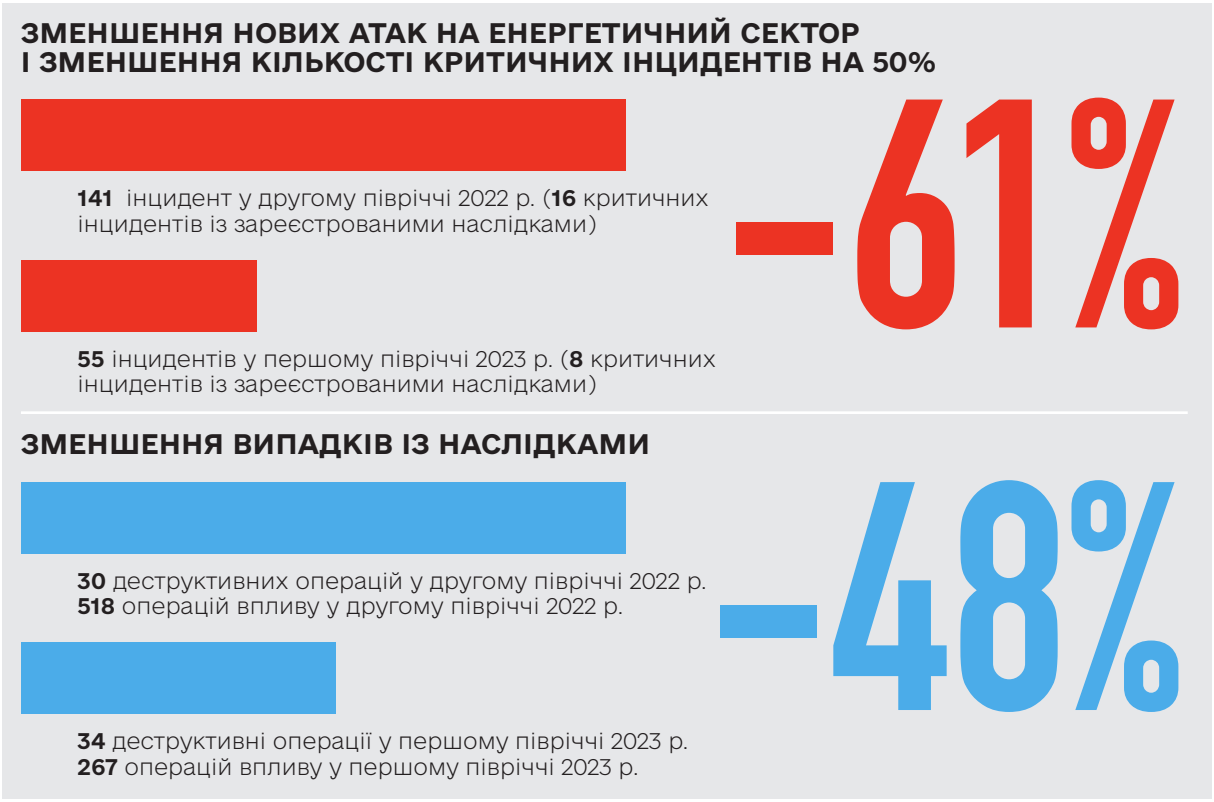
183 інциденти критичного та високого рівнів трапилося у першому півріччі 2023 р.

ЗМЕНШЕННЯ ВИПАДКІВ РОЗПОВСЮДЖЕННЯ ШПЗ ЕЛЕКТРОННОЮ ПОШТОЮ

290 випадків у другому півріччі 2022 р., де переважало ШПЗ

-52,41%

138 випадків у першому півріччі 2023 р., переважно почав домінувати фішинг



З наведених вище даних очевидно, що кількість критичних інцидентів помітно зменшилася. Крім того, покращилося співвідношення між інцидентами високого та критичного рівнів. Для деяких російських груп, які користуються примітивними підходами до розповсюдження ШПЗ (зокрема, для частини кримського ФСБ), застосовувати підхід «раптом пощастить» вже стає тяжче. Адже захищеність української інфраструктури значно покращилася порівняно з ситуацією піврічної давнини за рахунок державно-приватної співпраці, підключення компаній до платформи обміну індикаторами загроз MISP і збільшення довіри до CERT-UA та SOC ДЦКЗ Держспецзв'язку.

До того ж новий сплеск кількості фішингових атак мав більш пріоритетне значення, ніж успішні зараження ШПЗ. Попри те що нападники стають агресивнішими, Україна також нарощує експертизу та стійкість за рахунок мобілізованих IT-фахівців. І хоча зловмисникам стає дедалі складніше завдавати нам значної шкоди, вони все ще багато де досягають успіхів у руйнівних операціях — насамперед там, де є самовпевнені IT-адміністратори, які не вірять у державно-приватне партнерство. А саме логін / пароль адміністраторів IT-систем і мереж є головною ціллю хакера в скомпрометованій системі, тому що адміністратори часто впевнені у своїй недоторканності. У таких випадках якраз реалізовується найгірший сценарій, коли зловмисники можуть залишатися в системах тривалий час, оскільки IT-команда зачистила всі машини, окрім своїх.

ЧАСОВІ МЕЖІ

На рисунку нижче показано активність ключових гравців кібератак проти українських систем та їхню здатність здійснювати конкретну кількість кібероперацій за певний проміжок часу (із розподілом на тижні).

Кожне APT-угруповання за рахунок своїх талантів є унікальним — зі своїми характерними практиками, інструментами, кількістю людей в команді — та покладається на власний кадровий потенціал, а також має свої цільові сегменти. Тож кожна з цих груп здатна проводити обмежений обсяг операцій і зламу внутрішніх мереж. Також зусиль та ресурсів з боку зловмисників вимагає підтримка доступу та повернення на скомпрометовані цілі через закладені імпланти.

ДЕТАЛЬНА АНАЛІТИКА АКТИВНОСТІ ХАКЕРСЬКИХ УГРУПОВАНЬ ДАЛА МОЖЛИВІСТЬ РОЗПІЗНАТИ, ЩО КОЖНЕ УГРУПУВАННЯ МОЖЕ ПРОВОДИТИ ОБМЕЖЕНУ КІЛЬКІСТЬ ОПЕРАЦІЙ ПРОТЯГОМ МІСЯЦЯ ЧИ КВАРТАЛУ, ДЕТАЛЬНА РЕПРЕЗЕНТАЦІЯ НАЙБІЛЬШ АКТИВНИХ УГРУПУВАНЬ, ТАКИХ ЯК UAC-0010 (ФСБ), UAC-0028(ГРУ), UAC-0102 , UAC-0041, UAC-0082(ГРУ) ПРЕЗЕНТОВАНА НА МАЛЮНКУ НИЖЧЕ

	Січень	Січень	Січень	Січень	Січень	Лютий	Лютий	Лютий	Лютий	Березень	Березень	Березень	Березень	Квітень	Квітень	Квітень	Квітень	Травень	Травень	Травень	Травень	Травень	Червень	Червень	Червень	Червень
UAC-0028					2				2	1	4						1			3		6		2		2
UAC-0102																								2		
UAC-0010	1	4	3	4		4	4	8	7	2	1		1	8	6	2	2	3	7	7	10	7		4	3	4
UAC-0041									1				1	1							1			1		
UAC-0082	1		1	2			2						1	1	1					3	1			1		1
UAC-0156														1	1											
UAC-0024															1				1							
UAC-1045															3	1										
UAC-0120												1			1											
UAC-0107					5						1											1			1	
UAC-0114					1																					
UAC-0100				1	2			2		1	3															
UAC-0056					1	1		18	3	1																
UAC-0150		1			2	1					2	1		1							1	1			5	1
UAC-0050						1	12	10										1								
UAC-0006																		1	11	1		5				1
UAC-0145												1														
UAC-1037												1				1	1									
UAC-0153												1														
UAC-0151												1														
UAC-0109								4				26					1	10								
UAC-0099														1				1			1					
UAC-0166																		1								
UAC-0117																			2							
UAC-0165																	1		1							
UAC-1046																			1							
UAC-0135	1						1																1			
UAC-0096							4																			
UAC-0160																1										
UAC-0064								1																		
UAC-0162								1																		
UAC-0063																	1									
UAC-0035																									3	
UAC-0036																									1	
UAC-0106													1													
UAC-0155													1													
UAC-0143																							1			
UAC-0148	1																									
UAC-0097														1												

ОСЬ КІЛЬКА ІНСАЙТІВ,

які ми винесли, проаналізувавши зміни кожні 6 місяців протягом періоду у 18 місяців з моменту повномасштабного вторгнення:

1. **Частота операцій:** Аналіз інтервалів між успішними проникненнями чи первинними закріпленнями показує, що більшість APT-угруповань, як правило, здатні здійснювати одну операцію на місяць. Проте спроможність проводити більшу кількість операцій варіює в різних угрупованнях, залежно від їхнього розміру та людського потенціалу. Що ми і спостерігаємо в першому півріччі 2023 р., коли група Gamaredon подвоїла свою продуктивність.
2. **Планування цілей:** У разі викриття APT-групи їй зазвичай потрібен певний час, щоб перейти до нової жертви. Ця закономірність також прослідковується на наданому часовому графіку, представленому вище. Планування, підготовка та розроблення кожної цілі займає певний час. Групи, які мають більшу команду, зазвичай витрачають до одного місяця на об'єкт для проникнення і закріплення у ньому. Групи, які мають менше ресурсів, рухаються повільніше і витрачають 2-3 місяці для повної компрометації організації.
3. **Обмежений вибір стратегічних цілей:** Попри численні потенційні цілі, кількість стратегічних і цінних об'єктів для кібератак, дійсно важливих для підтримки воєнних дій росії проти України, досить обмежена. Тому після викриття та ізоляції нападники, як правило, намагаються залягти на дно і скористатися своїми знаннями нутрощів організації, щоб повторно отримати доступ або зайти через альтернативні точки входу. Або експлуатуючи довіру та особливості культури спілкування організації (наприклад, через електронну пошту), чи середовище IT-адміністрування. https://cip.gov.ua/ua/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua Українські організації, які вже були жертвами зламів і співпрацювали з CERT-UA, вживають проактивних заходів для запобігання повторних проникнень в свої мережі та працюють над створенням спроможностей для вчасного виявлення загрози за допомогою 24x7 SOC Держспецзв'язку. Наше завдання — зменшити поверхню атак, а також впевнитися, що OKI та інші організації та їхні IT-команди мають належний рівень захисту.
4. **Опортуністичний підхід та принцип «Жертва один раз — жертва завжди»:** Зловмисники мають достатню кількість потенційних цілей, але кількість важливих цілей завжди обмежена. Тож якщо не виходить «проламатися» в лоб, вони часто вдаються до опортуністичного підходу через пов'язані організації, контракторів, постачальників, щоб продемонструвати своєму керівництву свої можливості, підтримати авторитет. Часто також експлуатуються менеджери паролів та паролі, збережені в браузері IT-адміністраторів. https://cert.gov.ua/article/1751036
5. **Заходи безпеки:** До критичних заходів із підвищення безпеки належать блокування виконуваних файлів на кшталт mshta.exe, wscript.exe, cscript.exe та powershell.exe на всіх пристроях організації, за винятком

конкретних випадків, коли потрібно дозволити роботу з ними окремим структурним підрозділам. Такими простими заходами IT-команда може реально убезпечити організацію від реалізації багатьох загроз неавторизованого ПЗ.

ДЕ І ЧОМУ: СЕКТОРИ, ЩО ЗАЗНАЮТЬ ЦІЛЕСПРЯМОВАНИХ АТАК

На підставі аналізу випадків, де були залучені фахівці Держспецзв'язку, презентуємо розподіл інцидентів за різними галузевими сегментами. Сегмент «Інше» охоплює комерційні та громадські організації, які не потрапили до жодної зі вказаних категорій, і налічує найбільшу кількість випадків (408). З наведених нижче даних очевидно, що основними мішенями для зловмисників є п'ять секторів: численні приватні компанії в секторі медіа та телекомунікацій, місцеві органи влади, організації сектору безпеки та оборони й урядові установи. Варто особливо відзначити цілеспрямовані атаки проти підкатегорії місцевих органів влади у межах державного сектора.

185
Урядові установи

125
Місцеві органи влади

73
Медіа

55
Енергетика

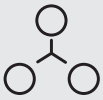
47
Безпека та оборона

42
Телеком / Інтернет-провайдери

19
Логістика / Транспорт

5
Охорона здоров'я / Страхування

4
IT



408
Інше

У першому півріччі 2023 року ФСБ, ГРУ та СВР продовжували нарощувати шпигунські операції з закріпленням через імпланти, спрямовані на збір розвідувальних даних. З іншого боку, певні групи зберігали схильність до деструктивних операцій. APT-угруповання часто поверталися до попередніх жертв, спекулюючи на обізнаності з їхньою інфраструктурою та визнаючи важливість цих цілей як для збору розвідувальних даних, так і з метою завдання шкоди.

Спираючись на спостереження їхньої поведінки, яка містить постійні спроби шпіонажу та імплантації, доцільно припустити, що основним їхнім завданням за вказівкою військового командування було з'ясувати обсяг інформації, зібраної українськими правоохоронними органами. Ця інформація, ймовірно, містить докази, розвідувальні дані та свідчення, які можуть бути використані в кримінальних провадженнях проти шпигунів, конкретних осіб, установ чи організацій у росії, із потенційними наслідками у вигляді санкцій чи інших дій.

Схоже, їхнім завданням є збирання даних із метою отримання уявлення про:

- Поточну ситуацію та справи, що готуються до передачі до суду
- Інформацію, яку вдалося зібрати Службі безпеки України та іншим правоохоронним органам як доказову базу для майбутніх арештів
- Плани й докази, зібрані українськими правоохоронними органами для міжнародних судів

- Перелік важливих свідків і зацікавлених сторін для майбутніх судів над воєнними злочинцями
- Осіб, яких було заарештовано, та про те, як допомогти цим особам уникнути відповідальності та потрапити до росії

Ці дані вони використовують для контррозвідувальних операцій та атрибуції даних

- Персональні ідентифікаційні дані (PII) та інформацію про осіб, встановлених українськими правоохоронними органами, щодо яких правоохоронці звертаються до суду чи прокуратури за дозволами на арешт чи допит особи

- Елітних солдатів і офіцерів, яких було взято в полон під час бойових дій і які підлягають / не підлягають обміну

Концепція «Жертва один раз — жертва завжди» підкреслює закономірність, яку демонструють суб'єкти загрози: повторно нападати на цілі, які ці суб'єкти скомпрометували в минулому, що зумовлено їхніми можливостями користуватися уже здобутою інформацією та знаннями про осіб і облікові записи, які були їхніми цілями.

Здійснюючи повторні атаки на раніше скомпрометовані цілі, суб'єкти загрози мають намір скористатися отриманими знаннями про внутрішні процеси, персонал, канали комунікації та вразливості цих організацій. Вони усвідомлюють, що отримані розвідувальні дані можуть їм дати значну перевагу

при організації майбутніх кібератак. Отже, вони продовжують цілеспрямовано атакувати тих самих осіб, облікові засоби електронної пошти чи навіть конкретні підрозділи всередині організації з метою збереження доступу, добування цінних даних і просування своїх зловмисних намірів.

Ця стратегія «Жертва один раз — жертва завжди» підкреслює поточну й щораз більшу загрозу для організацій від діяльності кіберзлочинців, які експлуатують отримані відомості для максимізації наслідків своїх атак. Це вказує на потребу в надійних і адаптивних заходах кібербезпеки, щоб протидіяти таким постійним загрозам.

Показові випадки, відомі широкому загалу, про які ми писали:

Цілеспрямовані атаки проти українських медійних агенцій	17 січня 2023 року в телеграм-каналі «CyberArmyofRussia_Reborn» було опублікувало дані, нібито викрадені з Українського національного інформаційного агентства «Укрінформ» в результаті нібито проведеної операції зламу і витоку. Хактивісти стверджували, що вони «спалили всю мережеву інфраструктуру» організації, намагаючись запобігти публікації новин на вебсайті. Згодом CERT-UA оприлюднила звіт про кібератаку на вказану організацію, підтвердивши ціль та час, проте дійшла висновку, що під час цієї атаки було зафіксовано використання п'яти різновидів програм-вайперів: CaddyWiper, ZeroWipe, SDelete, AwfulShred та idSwipe. Ми припускаємо, що цю атаку було здійснено угрупованням UAC-0082 (Sandworm), асоційованим із Головним центром спеціальних технологій ГРУ рф. **Основне завдання**: компрометація українського державного інформаційного агентства і створення передумов для підвищення ефективності російської пропаганди. https://cert.gov.ua/article/4818341 https://cip.gov.ua/ua/news/ukrinform-mogli-atakuvati-khakeri-z-ugrupuvannya-sandworm-pov-yazanogo-z-rosiiskim-gru-poperedni-dani-doslidzhennya-cert-ua
Злами і витоки даних у страхових і медичних організаціях	Російським хакерам-добровольцям вдалося зламати бази даних низки ключових страхових компаній і медичних організацій та викрасти масив персональних ідентифікаційних даних із номерами телефонів, висновками лабораторних аналізів, результатами тестів на COVID. **Основне завдання**: збір даних про громадян України з метою подальшого проведення кібер- або інформаційних операцій. https://cip.gov.ua/ua/news/vorozhi-khakeri-aktivizuvali-polyuvannya-na-personalni-dani-gromadyan

Атаки на енергетичний сектор	Український енергетичний сектор залишається пріоритетною ціллю для зловмисників, яким вдавалося приховувати свою присутність у мережах деяких організацій впродовж 18 місяців. Мав місце один випадок операції з порушення роботи. Судячи із зареєстрованої діяльності та віктимології впродовж квітня-травня, СВР (яка фокусується переважно на західні країни) та багато інших внутрішніх гравців отримали завдання провести кампанію зі збору даних про готовність та плани українців щодо Запорізької атомної електростанції (ЗАЕС). **Ймовірне основне завдання:** підтримка терористичних операцій, пов'язаних із загрозою ядерного вибуху на ЗАЕС.

ХТО І ЯК:

Ми зафіксували постійну діяльність щонайменше 23 російських кібертерористичних хакерських груп. Усі вони переслідують різні цілі, зокрема і воєнні, та атакують державний і приватний сектори. Тут ми надаємо аналіз діяльності найбільш небезпечних і дієздатних груп: Gamaredon (контрольована ФСБ), Sandworm (контрольована ГРУ) та «незалежні хактивісти», які виявилися «парасолькою» для контрольованих державою злочинців.

У 2023 році найбільш активними угрупованнями були UAC-0010 (Gamaredon / ФСБ), UAC-0056 (ГРУ), UAC-0028 (APT28 / ГРУ), UAC-0082 (Sandworm / ГРУ), UAC-0144 / UAC-0024 / UAC-0003 (Турла / ГРУ), UAC-0029 (APT29 / СВР), UAC-0109 (Заря), UAC-0100, UAC-0106 (XakNet), UAC-0107 (CyberArmyofRussia). Зареєстровані кібератаки було асоційовано з цими APT-угрупованнями.

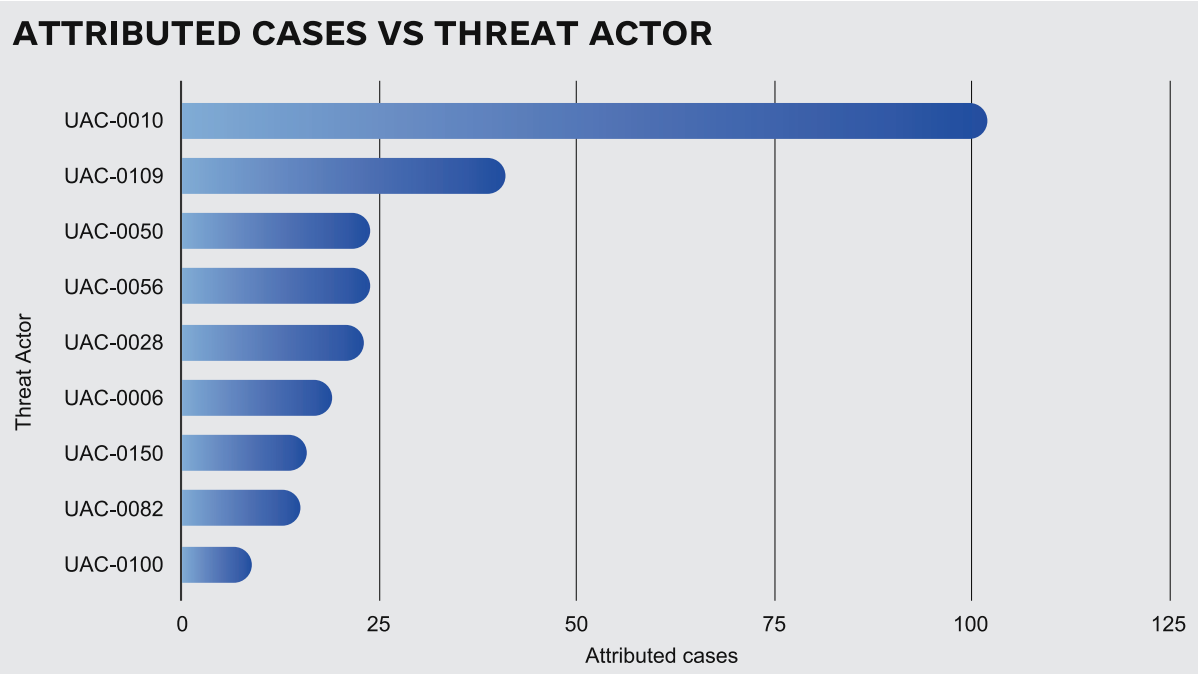


Рис. 1. Найактивніші суб'єкти загрози, які генерували найбільшу кількість випадків упродовж першого півріччя 2023 р.

Ми проаналізували контекст (часові межі, завдання, наслідки), віктимологію (атаковані сектори, країни), основні тактики, методики і протоколи (TTP), а також атрибуції на підставі нашого власного досвіду, маркерів і спостережень.

Якщо розглянути розподіл інцидентів і суб'єктів загрози (представлених вище) та зосередитися на найбільш болючих і загрозливих (зображених на рисунку нижче), стає очевидним, що провідну роль відіграють команди військової розвідки ГРУ — ідентифіковані як UAC-0056 (Ember Bear), UAC-0028 (APT28) і UAC-0082 (Sandworm). На них припадає 50 серйозних інцидентів.

На противагу цьому, команда ФСБ — UAC-0010 (Gamaredon) — долучилася лише до 11 інцидентів критичного або високого рівня тяжкості (як показано нижче) із загальної кількості у 103 інциденти, асоційовані з їхніми TTP, які ми спостерігали за період моніторингу серед усього спектру організацій, що зверталися до нас або перебувають під нашим захистом.

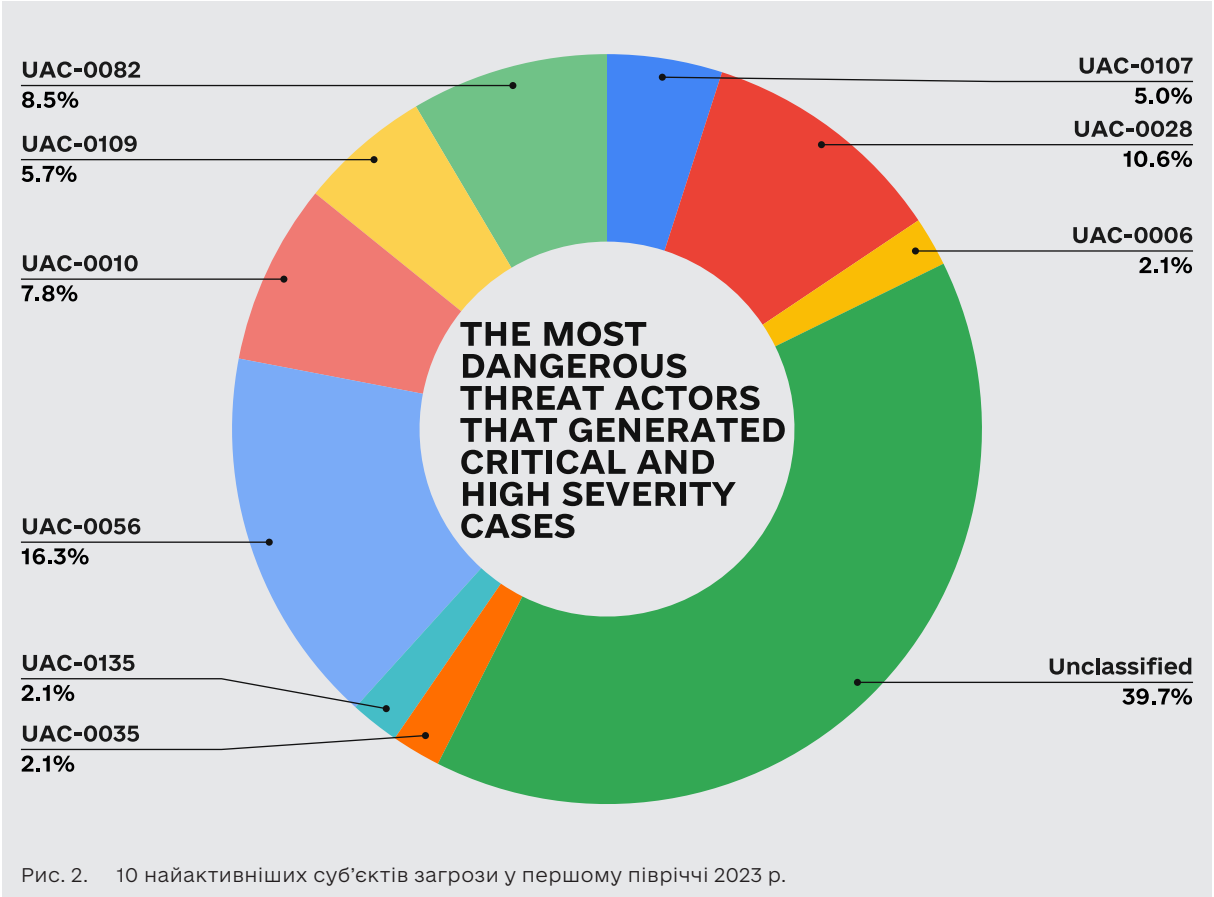


Рис. 2. 10 найактивніших суб'єктів загрози у першому півріччі 2023 р.

Результати нашого аналізу свідчать, що кіберпідрозділу ФСБ Gamaredon вдалося значно збільшити загальну кількість операцій. Якщо за увесь 2022 рік CERT-UA зареєструвала 128 випадків, то лише за перше півріччя 2023 року — вже 103. Проте не всі з них були настільки успішними, як раніше.

За даними CERT-UA, фішинг був найпомітнішою тактикою, яку зловмисники застосовували в першому півріччі 2023 р. (рис. 3). Це суттєва відмінність, адже в першому та другому півріччі 2022 року домінувало розповсюдження ШПЗ. Однак зараження шкідливим ПЗ і робота через Remote Access Trojan та C2, поряд із проникненнями через відомі експлуатовані вразливості чи скомпрометовані облікові записи, виділяються серед усього спектру як улюблені та досі дуже дієві стратегії.

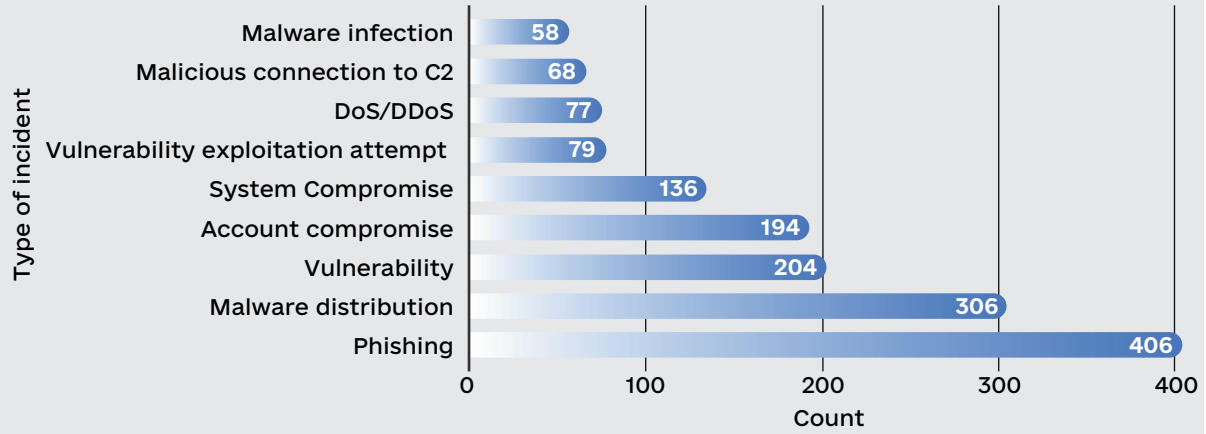


Рис. 3. Розподіл типів інцидентів, зареєстрованих упродовж першого півріччя 2023 р.

Аналітика щодо діяльності груп ФСБ. UAC-0010 / Gamaredon

Як наведено в аналітиці вище, ретельніше дослідження зареєстрованих інцидентів показує, що угруповання UAC-0010 демонструвало помітне зростання продуктивності. Кількість зареєстрованих випадків, пов'язаних із цією групою, зросла з 76 у другому півріччі 2022 року до 103 у першому півріччі 2023 року. Таке значне зростання кількості кібероперацій разом зі зміною фокусу і тактики порівняно з попередніми періодами можна пов'язати з декількома факторами. Зокрема, ми спостерігаємо серйозне розповсюдження інструментів, інструкцій, західних книжок — всього, що дозволяє збільшити залучення талановитої молоді до хакінгу. Ми вважаємо, що Gamaredon зумів збільшити чисельність і потенціал команди завдяки вливанню нових талантів із величезного пулу кваліфікованих працівників росії та мобілізації IT-фахівців із приватного сектора для служби в армії рф.

Як зазначалося в нашому матеріалі https://cert.gov.ua/article/5160737, кількість одночасно інфікованих UAC-0010 / FSB / Gamaderon комп'ютерів, які функціонують переважно в межах інформаційно-комунікаційних систем державних органів України, може сягати кількох тисяч. Як вектор первинної компрометації зловмисники здебільшого використовують електронні листи та повідомлення в месенджерах (Telegram, WhatsApp, Signal), які переважно розповсюджують за допомогою заздалегідь скомпрометованих облікових записів.

У першому півріччі 2023 р. UAC-0010 демонструвало явну зацікавленість щодо усіх напрямів правоохоронної діяльності (54,1% їхніх випадків), а також проявляло стійкий інтерес до всіх організацій, пов'язаних із силами оборони України. Маючи потужні людські ресурси, ця група застосовує примітивні, проте досить результативні методи.

Ми припускаємо, що старі оператори повертаються до відомих мішеней, тоді як новачки працюють над проникненням до нових жертв (брокери доступу). Через суттєве покращення приватно-державної співпраці та взаємодії між ключовими суб'єктами кіберзахисту в країні вони стикаються з труднощами у збереженні і підтриманні доступу. Тож змушені прискорювати проникнення і відхід та не «спалювати» жертв, до яких вони успішно підтримують доступ.

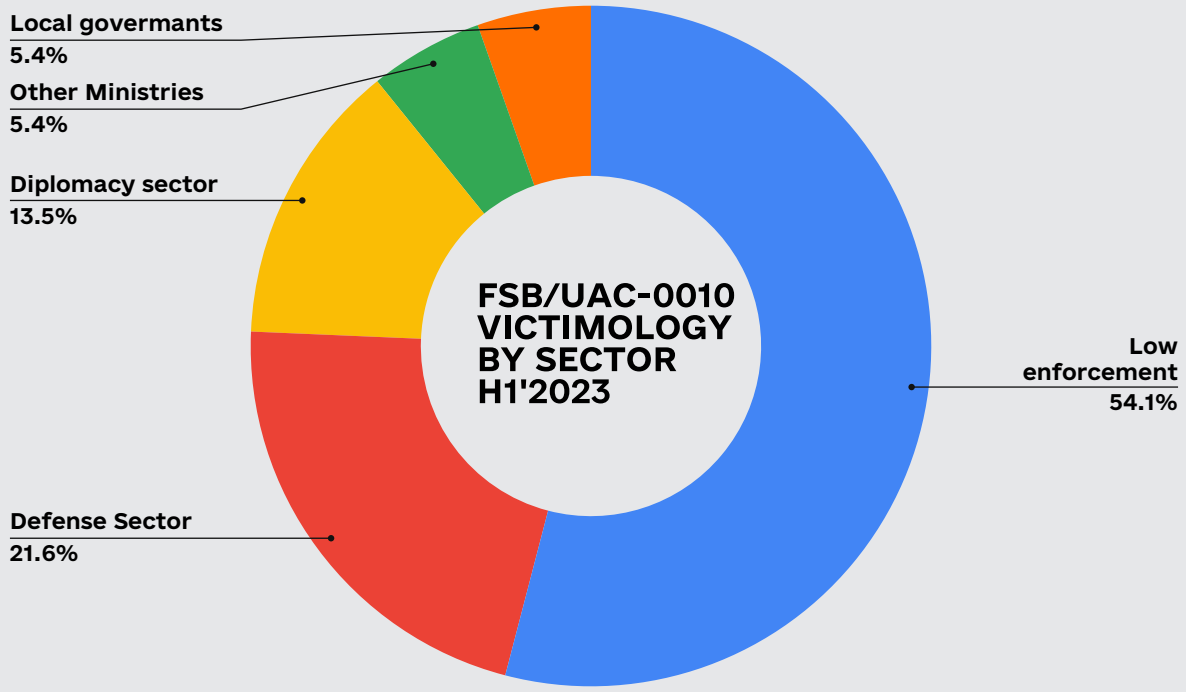


Рис. 4. Віктимологія UAC-0010 у першому півріччі 2023 р. за секторами.

На рисунку нижче показано аналіз методів, використовуваних у кампаніях UAC-0010, серед зареєстрованих випадків SOC і CERT. Найпоширенішою тактикою цієї групи є розповсюдження ШПЗ, тоді як інші групи здебільшого орієнтовані на фішингові кампанії.

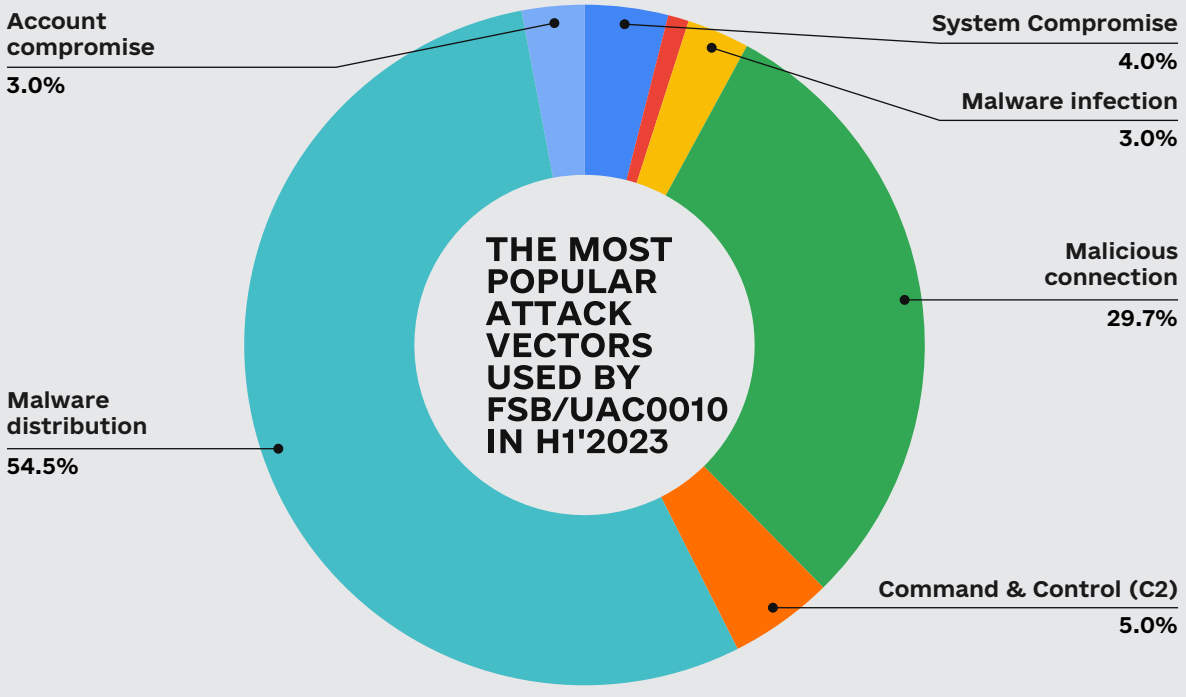


Рис. 5. Методи / вектори UAC-0010 / ФСБ, застосовані впродовж першого півріччя 2023 р.

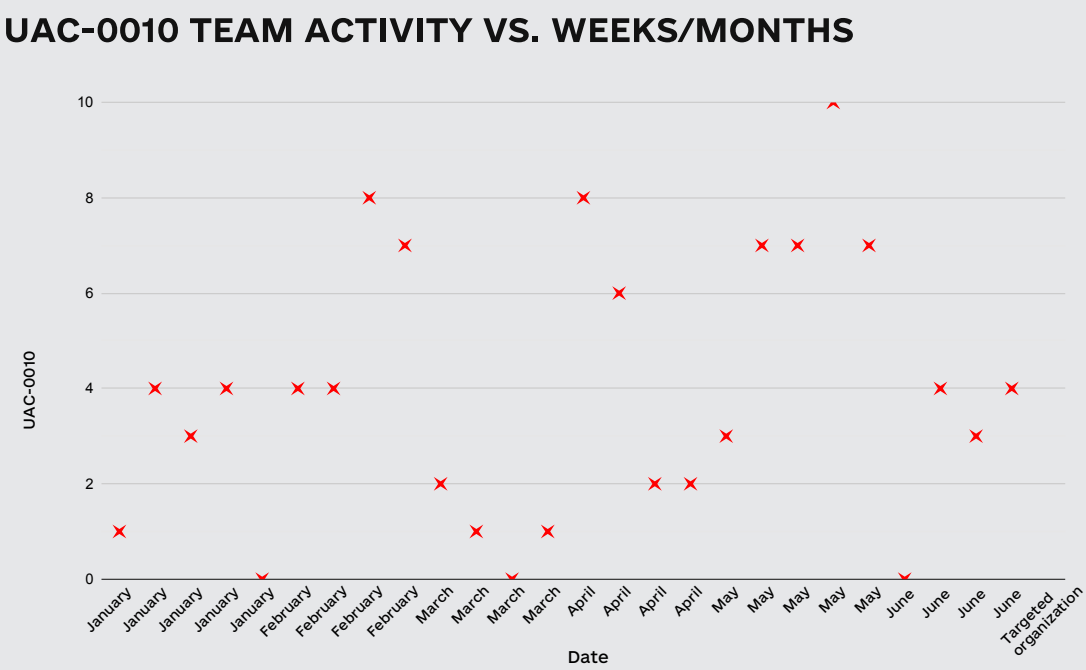


Рис. 6. Зображено кампанії та діяльність UAC-0010 / Gamaredon за перше півріччя 2023 р., що дає уявлення про часові проміжки у тижнях між виявленнями цього суб'єкта на різних жертвах. Ця візуалізація ефективно демонструє швидкість і оперативність, з якою ця команда проникає в нові та раніше атаковані організації.

Втім, щоб отримати точнішу картину виявлення дійсно небезпечних втручань, ми розробили описану нижче аналітику. Вона підтверджує наші здогади щодо того, що для серйозніших операцій суб'єктам загрози потрібно більше часу на проведення кампаній і облаштування плацдарму. Як ми бачимо, на одну операцію первинного доступу чи повторну спробу необхідно від 20 до 30 днів.

Для ще більшого посилення ефекту від хакерських кампаній від квітня 2023 року хакери застосовують тактику компрометації новинних агенцій і сторінок у Facebook, де вони розміщують провокаційну і контроверсійну інформацію.

Під час війни відбувається очевидне «злиття» злочинних хакерських груп із державою-агресором. Є численні випадки використання інструментарію хакерських груп Trickbot / Conti для здійснення атак на об'єкти критичної інфраструктури, зокрема енергетичної. Іншим прикладом є діяльність групи Tropical Scorpius, яка застосовує у своїх атаках бекдор RomCom.

Найчастіше члени UAC-0010 реалізують інтерактивний доступ до віддаленого робочого столу за допомогою PowerShell на EOM або може бути встановлено Anydesk. Їхня команда адміністраторів активно вживає окремих заходів для забезпечення відмовостійкості їхньої мережевої інфраструктури та уникнення детектування на мережевому рівні. Наприклад, з метою обходу необхідності використання підсистеми DNS, для визначення IP-адрес серверів управління використовуються сторонні сервіси і/або ресурси Telegram (Telegraph). Протягом доби IP-адреси проміжних управляючих вузлів можуть змінюватися від 3 до 6 і більше разів, що, зокрема, свідчить про відповідну автоматизацію процесу.

Аналітика щодо діяльності груп ГРУ. Sandworm UAC-0082 / UAC-0165

Медіа є цікавою та актуальною мішенню для військових хакерів із Головного розвідувального управління Міністерства оборони російської федерації. Незважаючи на те, що це суто цивільна ціль, з погляду російського командування ЗМІ є важливими для воєнних та інформаційних операцій. Тож вони і надалі перебуватимуть під прицілом російських хакерів у формі. Адже характерною рисою цієї гібридної війни є використання хакерських інструментів в операціях впливу: це стало візитівкою російської федерації.

Це свідчить про збереження російського підходу, спрямованого на завдання шкоди цивільній інфраструктурі поза традиційним театром бойових дій.

Цей підхід передбачає використання агресивної пропаганди, а також ракетних і дронових ударів по критичних об'єктах енергетики і шляхах експорту аграрної продукції. Це стратегічне бачення знаходить своє відображення у завданнях, поставлених перед військовими хакерами, оскільки значна частка їхніх кібератак спрямована проти важливих цивільних служб, як-от ЗМІ, комунікаційних мереж та громадського сектора.

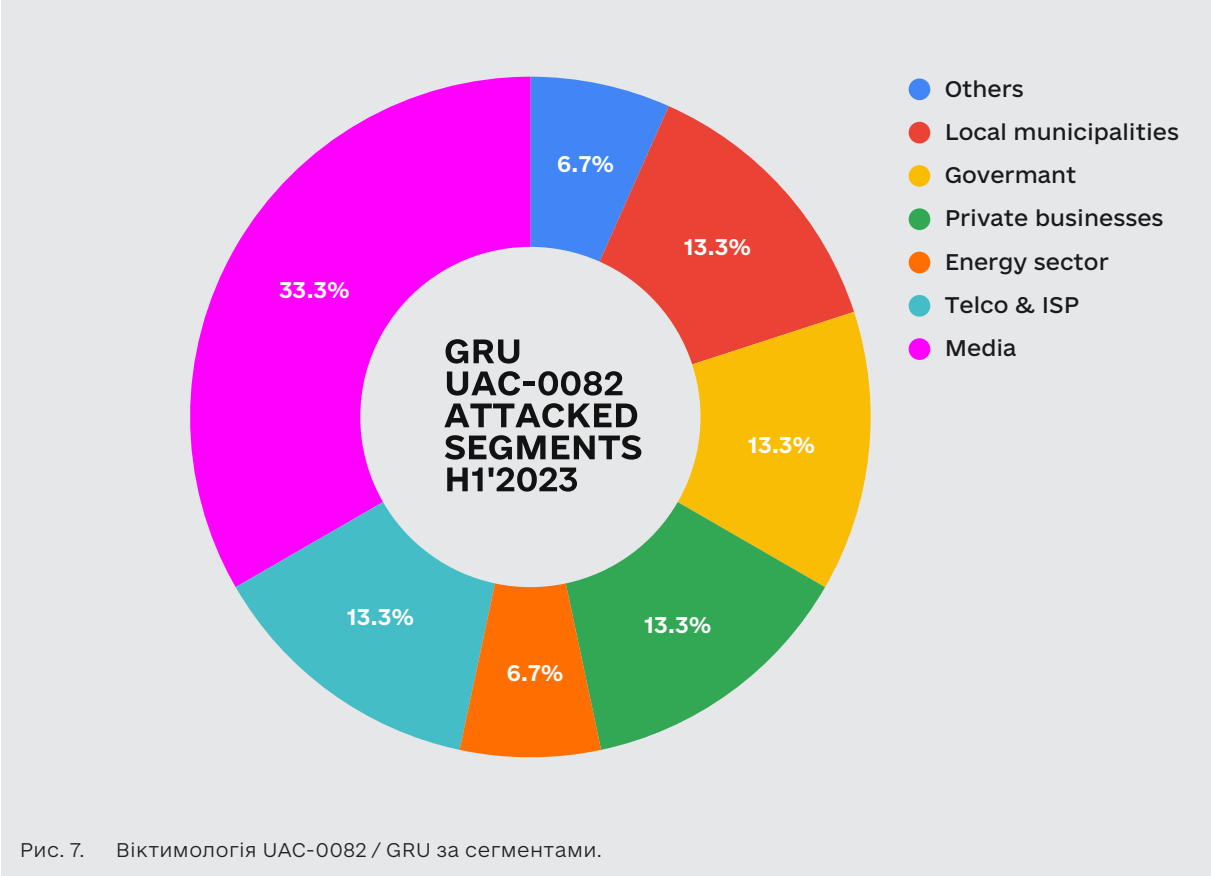


Рис. 7. Віктимологія UAC-0082 / GRU за сегментами.

Крім того, вони полюють за обліковими записами окремих військовослужбовців, які мають доступ до певних важливих військових платформ.

Після повномасштабного вторгнення росії в Україну в більшості випадків, до яких причетна група Sandworm, кінцевою метою цієї APT є здійснення руйнівних кібератак, пов'язаних зі стиранням серверів, виведенням із ладу систем віртуалізації, відключенням активного мережевого обладнання, видаленням даних із систем

Новий тренд операційної безпеки

Переважну більшість руйнівних атак здійснено групою Sandworm під керівництвом ГРУ.

Новим трендом став підхід сповіщення про ці події широкому загалу, коли після таких атак влаштовують витоки документів, схем і технічної документації у телеграм-каналах, які імітують «незалежних добровольців», але де-факто контрольовані цією групою.

Раніше група Sandworm використовувала для оприлюднення результатів своєї діяльності телеграм-канал @CyberArmyofRussia_Reborn.

Однак від 25 квітня 2023 року вони користуються каналом @solntsepekZ для кращої операційної безпеки. Найбільш показовий випадок — https://cert.gov.ua/article/3718487

зберігання і шифруванням кінцевих точок. Протягом перших 6 місяців 2023 року вони розробили нові варіанти шкідливого ПЗ (понад 10 нових зразків), користуючись легітимними утилітами (як-от SDelete, WinRaR) або вбудованими системними функціями (наприклад, сховищами NAS).

Енергетичний сектор — один з їхніх улюблених. У певних випадках своєчасно виявлені спроби хакерів здійснити атаки на енергетичні об'єкти підтверджують факт застосування конкретної тактики багатоетапного впливу: знеструмлення, знищення контролю підстанції, знищення проміжної телекомунікаційної підстанції (модему), руйнування робочої станції працівника і затирання серверного обладнання.

Складність атак на енергетичний сектор істотно підвищилася, оскільки хакерам відомо, що ці мережі та компанії (з 2014 року) мають схожу будову і спільні слабкі місця чи передові практики захисту. Це дало їм змогу краще готувати операції. На жаль, IT-команди на об'єктах не завжди мають компетенцію та засоби для виявлення та протидії.

Історія

Під час нещодавнього розслідування на одному енергетичному об'єкті нам вдалося зібрати докази первинного проникнення до мережі ще в середині 2021 року, що було частиною ширшої кампанії підготовки до війни. Це свідчить про планування вторгнення і проактивних кібероперацій, у тому числі про залучення хакерських груп до конвенційних воєнних операцій із метою посилення ефекту і негативного впливу на промислові системи управління тощо.

План цієї операції використовував залежність телекомунікацій, транспорту, банківських установ та інших організацій із переліку критичної інфраструктури від електропостачання. Зловмисники користувалися отриманим доступом у конвенційних операціях, залежно від розвитку ситуації.

«Хактивісти»
Killnet, HackNet, Zarya, NoName057, Anonymous Russia

Більшість атак було зафіксовано з боку Killnet, NoName057(16), XakNet, Anonymous Russia і Cyber Army of Russia.

- Ці хакерські групи насправді співпрацюють між собою. Вони атакували ті самі або схожі цілі та перепощували повідомлення одна одної в соцмережах.
- Втім, їхні заяви рідко описують характер ймовірних кібератак.

Протягом першої половини 2023 р. ми помітили зростання кількості інформаційних операцій із кіберскладовою. Ця категорія охоплює широкий спектр дій — від скоординованої нетипової поведінки в соціальних мережах із просуванням наративів, пов'язаних із війною росії проти України, до витоків начебто здобутих хактивістами даних, спрямованих на завдання репутаційної шкоди.

Суб'єкти загрози публікували нібито ексфільтровані дані (в тому числі шляхом зламу й витоку) з різних причин:

→ щоб довести факт заявленого втручання;

→ щоб завдати шкоди репутації жертви;

→ щоб вплинути на громадську думку або як зразок більшого масиву даних для продажу.

Новий тренд

Крім того, нині вони поєднують злами і витоки з публікацією фейків через скомпрометовані медіаресурси, щоб охопити більшу аудиторію.

Показові випадки:

https://cip.gov.ua/ua/news/kiberataka-na-derzhstat-ukrayini-vorog-ukotre-prozvituvav-pro-peremogu-yakoyi-ne-bulo

https://cip.gov.ua/ua/news/rosiiski-khakeri-namagayutsya-diskredituvati-uryadovu-komandu-reaguvannya-na-komp-yuterni-nadzvichaini-podiyi-cert-ua

Посилання

Рекомендуємо переглянути такі матеріали:

1. https://cert.gov.ua/article/5213167
2. https://cert.gov.ua/article/5160737
3. https://cert.gov.ua/article/4905829
4. https://cert.gov.ua/article/4905718
5. https://cip.gov.ua/ua/news/cert-ua-zavdyaki-spivpraci-z-recorded-future-viyaviv-shpigunsku-kampaniyu-grupi-apt28-bluedelta-proti-ukrayinskikh-organizacii
6. https://cert.gov.ua/article/3947787

Наші сподівання та прогнози з огляду на наявний контекст, спостереження та набутий досвід.

ЗРОСТАННЯ СКЛАДНИХ АТАК НА ЛАНЦЮЖКИ ПОСТАЧАННЯ

Ми передбачаємо, що компанії, які розробляють ПЗ для критичної інфраструктури та військових, зазнаватимуть активних цілеспрямованих атак у довгостроковій перспективі. IT-менеджмент повинен пильно стежити за кожним комітом і захищати інтелектуальну власність ПЗ шляхом обфускації даних чи додаткової аутентифікації.

ЩЕ БІЛЬШИЙ ЗСУВ У БІК ШПІОНАЖУ

Ми передбачаємо сповільнення руху всередині мережі та перехід до активнішої імперсонації користувачів. Зловмисники стають вкрай обережними, щоб уникнути викриття, що змушує їх відмовлятися від запуску саморобного ШПЗ, яке може підняти тривогу. Натомість вони схиляються до використання легітимних інструментів і процесів, ефективніше змішуючись із оточенням, щоб не привертати уваги до своєї діяльності.

БІЛЬШ КОМПЛЕКСНІ АТАКИ ТА ІНСТРУМЕНТИ

Наш прогноз показує, що суб'єкти загрози посилюють складність ланцюжків атак. Вони користуються передовими методиками для створення заплутаніших сценаріїв атак. Включно з розробкою і розгортанням дуже складного шкідливого ПЗ, яке має ширше розповсюдження, здатне атакувати різні операційні системи і навіть демонструє кросплатформні можливості. Підвищення складності атак підкреслює потребу в постійному вдосконаленні засобів безпеки організацій з метою випередження загроз, що зростають.

БІЛЬШЕ ЛЮДЕЙ У РОСІЙСЬКІЙ КІБЕРЗЛОЧИННОСТІ ТА У ВІЙСЬКУ

Ми вже спостерігаємо зростання кількості успішних операцій і кампаній розповсюдження. росія залучає молодь і використовує для її навчання та освіти західні матеріали, готуючи нове покоління патріотично мотивованих хакерів, які в майбутньому легко можуть стати суб'єктами кіберзлочинної загрози чи операторами програм-вимагачів.

Підготовлено за підтримки Європейського Союзу та Проєкту USAID «Кібербезпека критично важливої інфраструктури України»

Створення цієї публікації стало можливим завдяки підтримці американського народу, наданій через Агентство США з міжнародного розвитку (USAID), та підтримці Європейського Союзу.

Щоб дізнатися більше,
підпишіться за цим посиланням:
https://share-eu1.hsforms.com/1SNVq2857Q82uZWUfbxCyhw2b2xj0

Контакт-центр для ЗМІ
press@cip.gov.ua

**Державна служба спеціального зв'язку
та захисту інформації України**