

ЗВІТ З КІБЕРРОЗВІДКИ: APT35 (Charming Kitten)

У цьому звіті досліджується, як Charming Kitten (яку зазвичай відстежують як APT35 і яка в публічних звітах частково перетинається з Magic Hound, Mint Sandstorm, APT42 і TA453) здійснює збір розвідувальної інформації щодо представників політичних, дослідницьких, медійних, дипломатичних кіл і громадянського суспільства. У звіті розглядається питання, чи полягає стійка оперативна перевага цього суб'єкта загроз передусім у технічній складності, чи в його здатності перетворювати професійну довіру на доступ до цифрових ідентичностей. У дослідженні застосовано структурований якісний синтез звітів державних органів, неприбуткових організацій і постачальників рішень, опублікованих у період з 2018 по 2026 рік. Докази було закодовано за шістьма параметрами: цінність цілі, привід, канал комунікації, подія автентифікації, поведінка після компрометації та точка захисного втручання. Для зменшення ризику передчасної атрибуції та упередженості, пов'язаної з таксономіями постачальників, було проведено перевірку ключових припущень і розгляд альтернативних гіпотез.

Докази підтверджують три висновки. **По-перше**, соціальна інженерія, орієнтована на побудову взаємин, є більш стабільною характеристикою в різних звітах, ніж будь-який окремий набір інфраструктури або сімейство шкідливого програмного забезпечення.

По-друге, вибір цілей краще пояснюється їхньою розвідувальною цінністю та доступом до чутливих мереж, ніж лише їхньою належністю до певного сектору.

По-третє, корпоративні та особисті цифрові ідентичності утворюють взаємопов'язану поверхню атаки: коли один канал стає стійким до атаки, операція може переміститися до іншого, зберігаючи ту саму персону та привід. Ці висновки свідчать про те, що блокування індикаторів і загальна обізнаність щодо фішингу є необхідними, але недостатніми заходами. Ефективний захист потребує стійкої до фішингу автентифікації, норм перевірки через різні канали, моніторингу конфігурації цифрових ідентичностей та реагування на інциденти, яке розглядає професійні взаємини як частину ланцюга доказів. Межі атрибуції залишаються невизначеними, однак поведінкову модель оцінено з високим рівнем впевненості.

КЛЮЧОВИЙ ВИСНОВОК: Стійка перевага Charming Kitten полягає не стільки в конкретному шкідливому програмному забезпеченні чи наборі інфраструктури, скільки в її здатності перетворювати професійну довіру на доступ до цифрових ідентичностей.

APT35

(CHARMING KITTEN)

I. ВСТУП

Центральне дослідницьке питання: Яка оперативна логіка найкраще пояснює стійкість кампаній, пов'язаних із Charming Kitten, попри неодноразове публічне викриття інфраструктури, персон та методів цього суб'єкта загроз? Із цього випливають два додаткові питання. Чому політичні спільноти та спільноти, що займаються створенням знань, регулярно стають цілями, і які захисні заходи з найбільшою ймовірністю можуть перервати кампанію до початку збору розвідувальної інформації?

Питання навмисно сформульовано на рівні оперативної логіки, а не технічних сигнатур. Домени, хостинг-провайдери, ланцюги перенаправлень і сімейства шкідливого програмного забезпечення важливі для виявлення, але водночас належать до елементів викритої кампанії, які найлегше замінити. Більш стійким об'єктом дослідження є послідовність, за якою розвідувальна потреба трансформується у вибір цілі, встановлення контакту, довіру, автентифікацію та збір інформації. Ця послідовність може залишатися стабільною навіть тоді, коли інфраструктура та публічні назви суб'єкта загроз змінюються.

Сформований у результаті підхід розглядає довіру як інфраструктуру. Професійні спільноти залежать від слабких соціальних зв'язків, контактів без попередньої домовленості, запрошень на конференції, обміну рукописами, налагодження відносин із джерелами та швидкої співпраці через інституційні межі. Ці практики створюють суспільну цінність, але водночас надають противнику соціально легітимні шляхи для встановлення контакту. Отже, проблема безпеки полягає не у самій відкритості. Вона полягає у відсутності надійної перевірки, коли звичайна професійна взаємодія переходить до дії, пов'язаної з цифровою ідентичністю.

У звіті стверджується, що стійку спроможність цього суб'єкта загроз найкраще розуміти як орієнтоване на цифрові ідентичності шпигунство, організоване навколо доступу через взаємини. Операція обирає людей, чиї комунікації, контакти, судження або неопубліковані роботи мають розвідувальну цінність; створює правдоподібну професійну причину для взаємодії; переносить цю взаємодію між тими каналами, які підтримують довіру; і перетворює накопичену довіру на подію автентифікації. Домени, шкідливі компоненти та хмарні сервіси змінюються. Послідовність вибору цілі, встановлення контакту, налагодження взаємин, автентифікації та збору інформації змінюється значно менше.

Ця відмінність має аналітичне значення. Підхід, зосереджений на шкідливому програмному забезпеченні, розглядає користувача як механізм доставки технічної спроможності. Підхід, зосереджений на цифровій ідентичності, розглядає професійну легітимність людини, мережу її комунікацій і доступ до облікового запису як безпосередню ціль збору інформації. Останній краще пояснює, чому у звітах постійно наголошується на журналістах, дослідниках, дипломатах, активістах, лобістах, політичних працівниках і високопоставлених фахівцях у сфері політики, а також чому операції можуть бути успішними без розгортання спеціально розробленого шкідливого програмного забезпечення [1-4].

У публічних описах іранської кіберактивності різні операції часто об'єднують під невеликою кількістю впізнаваних назв. Charming Kitten і APT35 належать до найбільш широко вживаних. Однак публічні таксономії є аналітичними умовностями, а не природними категоріями. Різні організації групують активність відповідно до власної телеметрії, порогів впевненості та потреб клієнтів. MITRE ATT&CK пов'язує Magic Hound із численними альтернативними назвами, тоді як Microsoft, Mandiant і Proofpoint використовують відповідно Mint Sandstorm, APT42 і TA453 для позначення активності, яка суттєво перетинається, але не обов'язково є повністю тотожною [5]. Розгляд цих назв як точних синонімів створює хибну точність; розгляд їх як не пов'язаних між собою приховує повторювані моделі поведінки.

Тому в цьому звіті «Charming Kitten / APT35» використовується як узагальнювальний термін для публічного використання, а висновки щодо поведінки робляться лише там, де дані з кількох джерел збігаються. У звіті не стверджується, що кожна іранська фішингова операція належить одному підрозділу, спонсору чи оператору. В аналізі розмежовуються три твердження, які надто часто об'єднують: що інцидент схожий на задокументовану операційну модель; що постачальник рішень відніс його до певного названого кластера; і що цей кластер можна атрибутувати конкретній державній організації. Перше твердження може мати вагомі підстави навіть тоді, коли друге й третє залишаються невизначеними.

Це розмежування також відділяє рівень впевненості в атрибуції від рівня впевненості в оцінці поведінки. Публічних доказів може бути недостатньо, щоб визначити, чи були дві кампанії проведені тим самим оператором, але водночас їх може бути достатньо, щоб показати, що обидві використовують однаковий шлях від встановлення взаємин до отримання доступу до цифрової ідентичності. Висновки щодо захисту мають бути найбільш однозначними там, де докази збігаються щодо спостережуваної поведінки, і більш обережними там, де вони залежать від особи спонсора, внутрішньої постановки завдань або організаційних меж, які неможливо безпосередньо встановити за відкритими джерелами.

Відповідно, згадки про наміри суб'єкта загроз у цьому звіті є оцінками, а не твердженнями, заснованими на закритій інформації. Висновки з високим рівнем впевненості описують повторювані моделі, про які незалежно повідомляли різні джерела. Висновки із середнім рівнем впевненості пов'язують ці моделі з імовірними потребами у зборі розвідувальної інформації. Припущення з низьким рівнем впевненості розглядаються як орієнтири для майбутнього перегляду, а не включаються до основної тези.

Значення для політики виходить за межі питання атрибуції. Інституції, що займаються створенням знань, є особливо вразливими, оскільки відкритість є частиною їхньої місії. Науковці відповідають на запити щодо звітів, журналісти налагоджують контакти з незнайомими джерелами, аналітики аналітичних центрів приймають запрошення на конференції, а організації громадянського суспільства підтримують транскордонні зв'язки. Ці практики створюють соціальну легітимність, яку технічні засоби захисту не можуть самотійно оцінити. У задокументованих кампаніях, розглянутих у цьому звіті, противник неодноразово використовує цю легітимність, щоб подальший запит на автентифікацію сприймався як звичайна, а не виняткова дія.

II. ПЕРЕДУМОВИ ТА ДОКАЗОВА БАЗА

A. Публічні таксономії суб'єктів загроз

Запис Magic Hound у MITRE ATT&CK містить найширше публічне зіставлення технік і альтернативних назв, пов'язуючи цей кластер із фішингом для викрадення облікових даних, компрометацією облікових записів, збором електронної пошти, виконанням команд та ексфільтрацією через вебсервіси [5]. Звіти постачальників рішень надають детальніший опис. Mandiant описує APT42 як спонсорованого Іраном суб'єкта кібершпигунства, який вибудовує довірливі відносини з окремими особами та використовує кампанії фішингу для викрадення облікових даних, щоб отримати доступ до корпоративних і особистих облікових записів [2]. Microsoft документує операції Mint Sandstorm проти університетів і дослідницьких організацій, зокрема використання цілеспрямованої соціальної інженерії, кількох каналів комунікації, легітимних хмарних сервісів та інструментів, що застосовуються на наступних етапах атаки [3].

Жодна окрема таксономія не розглядається як авторитетна. MITRE систематизує поведінку за техніками та зв'язками між групами; постачальники рішень систематизують активність на основі телеметрії, впливу на клієнтів і кластерів, визначених за власними критеріями; державні звіти можуть об'єднувати випадки для юридичних, політичних або оборонних цілей. Ці матеріали відповідають на різні питання. Тому очевидні розбіжності можуть відображати спостереження за різними рівнями однієї й тієї самої активності, а не фактичну суперечність.

Практичним наслідком є правило декомпозиції тверджень: джерело може підтверджувати твердження щодо приманки, процесу автентифікації або категорії жертв, не обов'язково підтверджуючи ширше твердження про те, що кожна пов'язана подія належить єдиній організації. Це правило не дозволяє впізнаваній назві суб'єкта загроз мати більшу доказову вагу, ніж може забезпечити звітність, що лежить в її основі.

Threat Analysis Group компанії Google аналогічно повідомляла про тривалі пов'язані з Іраном операції з фішингу для викрадення облікових даних, спрямовані проти користувачів із високим рівнем ризику [6]. Звіти Proofpoint про TA453 містять детальну інформацію на рівні окремих кампаній, а в березні 2026 року компанія повідомила про нещодавній випадок, у центрі якого був американський аналітичний центр [4].

B. Звіти державних органів та організацій громадянського суспільства

У спільній рекомендації ФБР та партнерських відомств за 2024 рік описано, як пов'язані з KBIP суб'єкти загроз атакують особисті та робочі облікові записи високопоставлених державних посадовців, співробітників аналітичних центрів, журналістів, активістів, лобістів і співробітників політичних кампаній. У рекомендації особлива увага приділяється видаванню себе за інших осіб, налагодженню довірливих відносин, посиланням на підроблені сторінки входу та запитам на підтвердження багатофакторної автентифікації [1]. У пов'язаній справі Міністерства юстиції стверджується, що протягом кількох років проводилася спонсорована KBIP кампанія зі зламів і витоків інформації, яка спиралася на цільовий фішинг і соціальну інженерію для компрометації особистих облікових записів [7].

Ця рекомендація особливо важлива, оскільки в ній основна увага приділяється особистим обліковим записам. Особиста поштова скринька може перебувати поза межами корпоративних засобів захисту, але водночас містити професійне листування, повідомлення для відновлення доступу, історію контактів і шляхи доступу до організаційних сервісів. Для осіб, які становлять високу цінність, розмежування між особистою та професійною цифровою ідентичністю є радше адміністративним, ніж операційним: одна й та сама людина, її зв'язки, пристрої та канали відновлення доступу охоплюють обидва середовища.

Державні звіти також розширюють часовий горизонт. Кримінальні обвинувачення та рекомендації документують кампанії після проведення розслідувань, тоді як звіти постачальників рішень часто фіксують активність ближче до моменту її здійснення. У сукупності вони демонструють безперервність у двох аспектах: повторюваний вибір цілями осіб, які володіють цінною інформацією, та повторювані спроби перетворити доступ до комунікацій на розвідувальну перевагу. Такий збіг має більшу доказову силу, ніж будь-який окремий спільний домен або інструмент.

Ці державні джерела не об'єднують усю таку активність під назвою АРТ35; однак вони підтверджують, що компрометація цифрових ідентичностей осіб, які становлять високу цінність, є повторюваним інструментом пов'язаних з іранською державою операцій зі збору розвідувальної інформації та здійснення впливу.

На стратегічному рівні Розвідувальне співтовариство США оцінює, що зростання експертних спроможностей Ірану та його готовність проводити агресивні кібероперації роблять його значною загрозою для мереж і даних США [8].

Рекомендації CISA для громадянського суспільства є важливими, оскільки ця категорія цілей часто має обмежені ресурси для забезпечення безпеки, підвищені фізичні та репутаційні ризики й значну вразливість особистих облікових записів [9]. Ці рекомендації підкріплюють ключовий висновок цього звіту: організаційні межі не обмежують загрозу. Особиста електронна пошта цілі, месенджери, фактори відновлення доступу, інформація про подорожі та професійні контакти можуть бути операційно пов'язаними з корпоративним обліковим записом, навіть якщо організація не може безпосередньо ними керувати

Ця модель із високим рівнем впевненості підтверджує гіпотезу доступу через взаємини. Суб'єкт загроз, імовірно, інвестує у ведення розмови, оскільки контекст взаємин можна використовувати повторно. Шлюз безпеки може заблокувати домен, але він не може стерти з пам'яті цілі враження від правдоподібної взаємодії. Після встановлення довіри та впізнаваності та сама персона може перенаправити ціль на інший файловий хостинг, платформу для зустрічей, обліковий запис електронної пошти або застосунок для обміну повідомленнями. Довіра стає переносною інфраструктурою.

В. Вибір цілей як проблема інформаційних мереж

Категорії цілей, що регулярно повторюються (політичні посадовці, дослідники, науковці, журналісти, дипломати, активісти, лобісти та представники діаспори), не належать до однієї галузі та не використовують єдиний набір технологій. Однак усі вони мають доступ до неопублічних оцінок, мереж джерел, планів подорожей, проєктів документів і мап взаємин. Це підтверджує рольову модель вибору цілей: суб'єкт загроз обирає людей, які займають цінні позиції в інформаційній мережі. Рівень посади може мати значення, однак близькість до чутливих обговорень може бути важливішою.

Отже, ключовою змінною є положення в мережі, а не формальний ранг. Дослідник середньої ланки, який готує матеріали для брифінгу, може забезпечити більш своєчасний доступ до нових напрямів політики, ніж високопоставлений посадовець із добре захищеними системами. Журналіст може поєднувати між собою політичні, дипломатичні мережі та мережі громадянського суспільства, які в іншому разі залишалися б відокремленими. Організатор заходу може надати доступ до списків учасників і закритих програм. Цінність облікового запису полягає у взаєминах і часовому контексті, закладених у ньому.

Такий мережевий підхід також передбачає виявлення наступних цілей. Отримавши доступ до поштової скриньки, противник може визначити постійних кореспондентів, заплановані зустрічі, спільні документи та довірені знайомства. Збір інформації щодо однієї особи може підвищити правдоподібність і точність наступного підходу, створюючи цикл зворотного зв'язку між компрометацією та соціальною розвідкою.

Ця відмінність пояснює, чому університети, аналітичні центри, редакції та організації громадянського суспільства залишаються привабливими цілями, навіть якщо вони не володіють традиційними державними таємницями. Їхні облікові записи містять інформацію, що передує формуванню політики: хто з ким спілкується, які аргументи отримують підтримку, що буде опубліковано та куди подорожуватимуть окремі особи. Твердження Міністерства юстиції щодо іранських кампаній проти академічних і політичних цілей надають ширший контекст, який свідчить про стратегічну цінність досліджень і комунікацій, тоді як корпус звітів постачальників щодо АРТ35 демонструє, як ця цінність використовується шляхом цілеспрямованої компрометації цифрових ідентичностей [7, 11].

Рівень впевненості в рольовій моделі є високим; рівень впевненості в тому, що кожен спостережуваний випадок пов'язаний з одним і тим самим спонсором або тією самою потребою у зборі інформації, є середнім.

С. Аналітичні методи розвідувального аналізу

Аналітичний метод ґрунтується на оприлюдненому ЦРУ посібнику з аналітичних методів, у якому рекомендується проводити перевірку ключових припущень, аналіз конкуруючих гіпотез, використовувати індикатори та ознаки, а також приділяти особливу увагу інформаційним прогалинам як засобам запобігання передчасним висновкам [10]. Ці методи особливо важливі, коли доказова база фрагментована між різними постачальниками. Тому в цьому дослідженні ідентичність суб'єкта загроз розглядається як гіпотеза, рівень впевненості в якій необхідно оцінювати, а не як вихідне припущення, закладене в назві.

III. ДАНІ ТА МЕТОДИ

А. Дизайн дослідження та відбір джерел

Це структурована якісна оцінка, а не статистичне дослідження атрибуції. Одиницею аналізу є задокументована кампанія або повторювана поведінка, а не назва, яку використовує постачальник. Корпус джерел надає пріоритет офіційним рекомендаціям державних органів, судовим документам або офіційним заявам, MITRE ATT&CK і технічним звітам компаній, які безпосередньо спостерігали відповідну телеметрію електронної пошти, цифрових ідентичностей, хмарних середовищ або кінцевих пристроїв. Джерела включалися, якщо вони містили щонайменше один із таких елементів: описану категорію цілей, послідовність взаємодії, механізм автентифікації, поведінку після компрометації або індикатор із визначеними часовими межами. Матеріали, які лише повторювали інформацію з іншого джерела, виключалися з основної доказової бази.

Дизайн дослідження передбачає прозору ієрархію доказів. Найбільшу вагу для тверджень про спостережувану поведінку мають актуальні на момент подій технічні звіти з першоджерел та офіційні рекомендації. Судові документи використовуються для визначення історичного масштабу та ймовірних намірів, однак викладені в них твердження розглядаються як обвинувачення, якщо вони не були підтверджені судовим рішенням. Агреговані бази даних технік використовуються для орієнтування аналізу, а не як заміна доказів із конкретних джерел. Вторинні матеріали виключаються, якщо вони лише повторюють першоджерело.

Одиницею аналізу є операційний епізод: задокументована послідовність, що пов'язує ціль, привід, канал, запитувану дію та спостережуваний наслідок. Це зменшує ризик розглядати кожен електронний лист як окрему подію або кожен кластер, визначений постачальником, як цілісну організацію. Це також дає змогу порівнювати кампанії навіть тоді, коли у звітах розкрито лише частину послідовності.

Доказова база охоплює період з 2018 року до 27 серпня 2026 року. Більш ранні матеріали використовуються там, де вони підтверджують стійку модель; новішим матеріалам надається більша вага для тверджень щодо поточної операційної практики. Випадок Proofpoint за березень 2026 року є найактуальнішим прикладом окремої кампанії в цьому корпусі. Публічні звіти неминуче надмірно представляють виявлені операції, канали, видимі постачальникам, та інциденти, придатні для публічного розкриття. Тому у звіті робляться порівняльні висновки щодо послідовності та значущості для захисту, а не оцінки поширеності кампаній.

В. Схема кодування

Кожне джерело було закодовано за шістьма параметрами: (1) розвідувальна цінність цілі; (2) професійний або особистий привід; (3) канал комунікації або перехід між каналами; (4) запитувана подія автентифікації або виконання; (5) спостережувана або оцінена ціль збору інформації; та (6) найраніша обґрунтована точка захисного втручання. Схема кодування була розроблена для розмежування стійкої операційної логіки та короткочасної інфраструктури.

- Гіпотеза цінності цілі: кампанії організовуються навколо доступу до інформації та мереж, а не лише на основі належності до певного сектору.
- Гіпотеза доступу через взаємини: налагодження довірливих відносин і професійна легітимність є причинно значущими компонентами послідовності вторгнення, а не другорядними елементами, що супроводжують технічний експлойт.
- Гіпотеза достатності цифрової ідентичності: доступу до електронної пошти та хмарних цифрових ідентичностей може бути достатньо для задоволення розвідувальної потреби без використання шкідливого програмного забезпечення на кінцевих пристроях.
- Гіпотеза зниження цінності індикаторів: інфраструктурні індикатори втрачають свою цінність для захисту швидше, ніж поведінкова послідовність кампанії.

Таблиця 1. Матриця збіжності доказів

Аналітичний параметр	Повторювані публічні докази	Оцінка	Рівень впевненості
Доступ через взаємини	Стійкі персони, професійні приводи, переходи між каналами	Налагодження довірливих відносин є частиною механізму отримання доступу	Високий
Вибір цілей	Посади у сферах політики, досліджень, медіа, дипломатії та громадянського суспільства	Положення в мережі краще пояснює цінність цілі, ніж її належність до певного сектору	Високий
Доступ через взаємини	Стійкі персони, професійні приводи, переходи між каналами	Адміністративні межі не обмежують операційний ризик	Високий
Достатність цифрової ідентичності	Доступ до поштових скриньок і хмарних сервісів із використанням або без використання інструментів на кінцевих пристроях	Автентифікованого доступу може бути достатньо для задоволення потреб у зборі інформації	Високий

С. Аналітичні запобіжники та рівень впевненості

Було застосовано три запобіжники. По-перше, перевірка ключових припущень мала встановити, чи не є очевидна безперервність активності наслідком повторного використання постачальниками вже відомих назв. По-друге, під час розгляду альтернативних гіпотез оцінювалося, чи можна належним чином пояснити спостережувану модель звичайним викраденням облікових даних, опортуністичною кіберзлочинністю або діяльністю не пов'язаних між собою іранських суб'єктів загроз, які використовують поширені методи. По-третє, твердження джерел зважувалися залежно від їхньої близькості до доказів: безпосередній аналіз телеметрії та офіційні твердження у матеріалах справ отримували більшу вагу, ніж окремі твердження щодо таксономії. Рівень впевненості є високим, коли незалежні джерела сходяться щодо повторюваної поведінки; середнім, коли висновок залежить від таксономії або неповної видимості; і низьким, коли докази походять з одного джерела або ґрунтуються на аналітичних припущеннях.

D. Збіжність джерел, відсутність даних і контрфактичне тестування

Четвертим запобіжником було явне врахування відсутності даних. У публічних звітах непропорційно широко представлені кампанії, які були виявлені, розслідувані або визнані придатними для публікації. Тому відсутність згадок про певну техніку не можна інтерпретувати як доказ її відсутності. В аналізі розмежовуються етап, який не спостерігався, етап, наявність якого була прямо виключена на основі телеметрії, та етап, який не був необхідним для досягнення очевидної цілі збору інформації.

П'ятим запобіжником було контрфактичне тестування. Для кожного основного висновку в аналізі ставиться питання, якими мали б бути докази, якби альтернативне пояснення було правильним. Якби звичайного масового викрадення облікових даних було достатньо, можна було б очікувати менш ретельного відбору цілей, менш тривалого налагодження довірливих відносин і меншої уваги до професійного контексту. Якби розгортання шкідливого програмного забезпечення завжди було кінцевою метою, кампанії, що завершуються отриманням доступу до поштової скриньки або хмарних сервісів, були б аномальними, а не повторюваними. Ці порівняння не доводять наміру, але вони чіткіше визначають умови, за яких пріоритетне пояснення залишається переконливим.

IV. РЕЗУЛЬТАТИ

A. Доступ через взаємини як операційна спроможність

У межах усієї доказової бази соціальний контакт є не просто оболонкою навколо шкідливого посилання. Це поетапна спроможність, що використовується для зниження порогу перевірки з боку цілі. Mandiant повідомляє про персони, які протягом певного часу налагоджують взаємини з цілями; Microsoft описує цілеспрямовану взаємодію з дослідниками; у рекомендації під керівництвом ФБР наголошується на видаванні себе за професійні контакти; а випадок Proofpoint 2026 року розпочався з безпечного запрошення, перш ніж взаємодія набула шкідливого характеру [1-4]. Привід часто відповідає реальній роботі цілі: конференція, інтерв'ю, проєкт звіту, запит від медіа, обговорення політики або спільний інтерес до певного регіону.

Доступ через взаємини має як безпосередню, так і залишкову цінність. Безпосередньо він підвищує ймовірність того, що ціль відкриє документ, продовжить розмову або пройде автентифікацію в запропонованому сервісі. У довгостроковій перспективі він створює сценарій, який можна повторно використати після невдалої спроби, перенести до іншого каналу або використати іншою персоною. Сама розмова стає формою підготовки доступу.

Це допомагає пояснити терплячість суб'єкта загроз. Ретельно підготовлений і заснований на попередньому дослідженні підхід може здаватися неефективним, якщо оцінювати його як фішингову кампанію за кількістю повідомлень. Він є більш раціональним, якщо розглядати його як операцію зі збору інформації, у якій одна поштова скринька може відкрити доступ до багаторічного листування, чутливих вкладень, потенційних контактів і соціальної мапи, необхідної для визначення наступної цілі.

С. Суміжність цифрових ідентичностей між особистими та організаційними обліковими записами

У кількох джерелах описується активність, яка переміщується між корпоративною електронною поштою, особистою електронною поштою, хмарними сховищами, соціальними мережами та сервісами обміну повідомленнями. Це не випадкове використання різних каналів. Воно дає змогу операції обходити найсильніший засіб захисту в середовищі цілі. Захищена корпоративна поштова скринька може використовуватися для встановлення довіри, перш ніж спілкування перейде до особистого облікового запису; або ж особисті взаємини можуть бути використані для того, щоб спонукати ціль пройти автентифікацію в організаційному середовищі.

Суміжність цифрових ідентичностей ускладнює визначення відповідальності за ризик. Роботодавець може контролювати корпоративний обліковий запис, але не особисту поштову скриньку, що використовується для професійної комунікації; університет може захищати електронну пошту викладачів, але не обліковий запис для відновлення доступу або застосунок для обміну повідомленнями, який використовується під час подорожей. Противник отримує перевагу від таких прогалин у сферах відповідальності, оскільки жодна окрема сторона, відповідальна за захист, не бачить повної історії взаємин, пристроїв та автентифікації.

D. Легітимні сервіси та доставка з низьким рівнем аномальності

У кампаніях часто використовуються легітимні документи, розміщені у хмарних сервісах, сервіси обміну файлами або платформи для проведення зустрічей. У випадку Proofpoint за березень 2026 року безпечний PDF-файл, розміщений у OneDrive, використовувався на етапі налагодження довірливих відносин, перш ніж подальше посилання перенаправило ціль на сторінку для викрадення облікових даних, оформлену під OneDrive. Microsoft також повідомляє про використання легітимних платформ і багатоетапної доставки в межах активності Mint Sandstorm [3, 4]. Висновок для захисту полягає не в тому, що хмарні сервіси самі по собі є підозрілими, а в тому, що репутація сервісу не може замінити контекст взаємодії.

Легітимні сервіси виконують дві функції. Вони успадковують репутацію широко використовуваних платформ і дають змогу початковим етапам кампанії залишатися технічно безпечними. Розміщена у хмарному сервісі програма заходу, сторінка для планування зустрічі або спільний документ можуть підтримувати привід, не містячи кінцевого механізму викрадення облікових даних. Тому системи виявлення, які оцінюють лише перший артефакт, можуть визначити низький рівень ризику для взаємодії, значущість якої стає очевидною лише з часом і при аналізі різних каналів.

Одиниця аналізу для захисту має відповідати послідовності дій противника. Сигнали, які окремо є слабкими — новий співрозмовник, безпечний документ, зміна каналу та подальший запит на автентифікацію, — можуть стати переконливими, якщо їх поєднати у хронологічній послідовності. Це проблема кореляції так само, як і проблема фільтрації.

.

Цей висновок також пояснює, чому спрощені рекомендації для користувачів є малоефективними. Комунікація може бути грамотною, релевантною та частково легітимною. Вирішальне питання полягає в тому, чи було запитувану дію незалежно перевірено: Чи справді ця особа є тією, за кого себе видає? Чи очікувався цей документ? Чи відбувається автентифікація у правильному тенанті та контексті браузера? Чи було змінено канал взаємодії або чи почала вона швидко переходити до більшої конфіденційності? Засоби захисту мають забезпечувати можливість легко відповісти на ці питання до того, як відбудеться дія, пов'язана з цифровою ідентичністю

Е. Доступ до цифрової ідентичності як ціль збору інформації

Модель, зосереджена на шкідливому програмному забезпеченні, недооцінює розвідувальну цінність поштової скриньки або хмарного облікового запису. Електронна пошта містить вміст, контакти, хронологію, вкладення, повідомлення про автентифікацію та соціальний контекст. Хмарні цифрові ідентичності можуть надавати доступ до спільних дисків, календарів, делегованого доступу, дозволів застосунків і механізмів відновлення доступу. MITRE пов'язує ширший кластер зі збором електронної пошти та маніпуляціями з обліковими записами, тоді як звіти державних органів і постачальників рішень неодноразово зосереджуються на викраденні облікових даних і доступі до сесій [1, 5].

Доступ до поштової скриньки може забезпечувати безпосередній збір інформації, підготовку до видавання себе за жертву та збереження доступу шляхом внесення змін до налаштувань відновлення або пересилання. Він також може розкрити мовні особливості, характер комунікації та контекст, необхідні для переконливого видавання себе за жертву. Отже, обліковий запис є одночасно сховищем інформації та платформою для майбутніх операцій.

Цей висновок змінює поріг оцінки серйозності інциденту. Введення облікових даних або підозрілу сесію не слід класифікувати як невелике вторгнення лише через те, що жодне шкідливе навантаження не було виконано. Якщо очевидна розвідувальна потреба може бути задоволена через електронну пошту, хмарне сховище, контакти або делегований доступ, подія, пов'язана з цифровою ідентичністю, і є вторгненням і має розслідуватися відповідним чином.

Ф. Інтегрована оцінка

У сукупності ці п'ять висновків описують цілісну операційну систему. Дослідження цілей дає змогу визначити особу, з якою можна встановити соціальний контакт і яка володіє цінною інформацією або має цінні взаємини. Доступ через взаємини забезпечує правдоподібну причину для контакту. Перехід між каналами та використання легітимних сервісів знижують рівень аномальності. Подія, пов'язана з цифровою ідентичністю, перетворює цю довіру на автентифікований доступ, а скомпрометований обліковий запис забезпечує як збір інформації, так і матеріал для подальшого вибору цілей.

Система є стійкою, оскільки її компоненти взаємозамінні. Заблокований домен можна замінити; персона може перейти на іншу платформу; сторінку для викрадення облікових даних можна створити заново; а від шкідливого програмного забезпечення можна відмовитися, якщо доступу до хмарних сервісів достатньо. Незамінною вимогою залишається правдоподібний шлях від професійного контексту цілі до дії, яка розкриває цифрову ідентичність. Саме ця вимога є найбільш стабільним напрямом для захисту.

Отже, гіпотеза достатності цифрової ідентичності оцінюється з високим рівнем впевненості. Інструменти на кінцевих пристроях залишаються релевантними; Microsoft і MITRE документують подальше виконання команд у деяких операціях, однак їх відсутність не повинна знижувати оцінку серйозності інциденту, якщо його розвідувальна ціль може бути досягнута через доступ до облікового запису. Сторони, відповідальні за захист, повинні розглядати аномальну сесію, за якою слідують пошук у поштовій скриньці, налаштування пересилання, зміни делегованого доступу, надання дозволів застосункам або доступ до файлів, як повний шлях кібершпигунства, а не лише як підготовчий етап до використання шкідливого програмного забезпечення.

V. КЕЙС-СТАДІ: КАМПАНІЯ ПРОТИ АНАЛІТИЧНОГО ЦЕНТРУ В БЕРЕЗНІ 2026 РОКУ

A. Реконструкція послідовності

Proofpoint повідомила, що TA453 атакувала американський аналітичний центр у період загострення регіонального конфлікту на початку 2026 року. Перший контакт містив запрошення цілі взяти участь у круглому столі з питань протиповітряної оборони. Потім у межах операції комунікація відбувалася через особисті та корпоративні облікові записи, а також було надіслано безпечний PDF-файл, розміщений у Microsoft OneDrive. Лише після налагодження довірливих відносин у межах взаємодії було надіслано шкідливе посилання на підроблений PDF-файл. Ланцюжок перенаправлень вів через `transfergocompany[.]com` до оформленої під Microsoft OneDrive сторінки для викрадення облікових даних, розміщеної на `fileportalshare[.]netlify[.]app`. На сторінці була заздалегідь заповнена адреса електронної пошти цілі, що підвищувало її правдоподібність і спрощувало взаємодію [4].

У вигляді послідовності кампанія складалася з п'яти аналітично відмінних етапів: вибір цілі, встановлення професійного контакту, налагодження довірливих відносин і перехід між каналами, представлення ресурсу, що відповідав контексту, та спонукання до дії, пов'язаної з цифровою ідентичністю. Кожен етап зменшував невизначеність для оператора, водночас підвищуючи залученість цілі. Подальший запит набував довіри завдяки попередній безпечній взаємодії.

Ця послідовність ілюструє залежність від попередніх етапів. Шкідливий етап не можна оцінювати так, ніби він надійшов від невідомого відправника без будь-якого контексту, оскільки в межах кампанії було докладено зусиль, щоб зробити відправника знайомим для цілі. Тому засоби захисту та навчання, які розглядають кінцеве посилання окремо від попередньо сформованих взаємин, відкидають саме ту інформацію, яка необхідна для розуміння того, чому запит виявився успішним.

Цей випадок є цінним для аналізу, оскільки він дає змогу чітко простежити послідовність дій. Запрошення на першому етапі не було технічно шкідливим. Легітимний документ сам по собі не був кінцевим засобом атаки. Шкідливі домени були необхідними компонентами, але їх було введено лише після створення правдоподібного професійного контексту. Підхід, орієнтований на індикатори, починає аналіз ближче до завершення операції; підхід, орієнтований на цифрову ідентичність, починає його з вибору цілі та створення підстав для довіри.

Цей випадок також демонструє, чому оцінювання ефективності захисту має зміщуватися на більш ранні етапи. Підрахунок заблокованих фішингових URL-адрес оцінює засіб захисту, що спрацьовує безпосередньо перед подією автентифікації. Він не показує, чи розпізнали користувачі з високим рівнем ризику незвичний розвиток взаємин і повідомили про нього, чи могла організація перевірити зовнішню персону або чи було встановлено зв'язок між контактом через особистий обліковий запис і подальшим входом до корпоративного облікового запису. Такі сигнали на ранніх етапах складніше автоматизувати, але вони можуть забезпечити більші можливості для захисного втручання.

В. Захисні контрфактичні сценарії

Таблиця 2. Операційна послідовність і найраніші можливості для захисного

Етап	Спостережувана поведінка	Найраніша корисна точка втручання
Вибір цілі	Біографія, публікації, професійні зв'язки та заходи відображені у приманці	Визначати рівні ризику для ролей із високою публічною видимістю та скорочувати обсяг зайвої публічної інформації
Встановлення контакту	Небажаний, але контекстуально правдоподібний професійний контакт	Забезпечити можливість швидкої незалежної перевірки професійного контакту
Налагодження довірливих відносин	Безпечна взаємодія, перехід між каналами, планування зустрічей або обмін документами	Зберігати контекст розмови та позначати незвичні переходи між каналами
Автентифікація	Запит на вхід, надання дозволу, відновлення доступу або дію багатофакторної автентифікації	Застосовувати стійку до фішингу автентифікацію та затверджені способи входу
Збір інформації	Пошук у поштовій скриньці, пересилання, використання токенів, доступ до документів або видавання себе за іншу особу	Корелювати телеметрію цифрових ідентичностей і хмарних сервісів; відкликати сесії та механізми збереження доступу

Таблиця демонструє, чому засоби захисту, найближчі до етапу автентифікації, є необхідними, але недостатніми. Найранішим втручанням часто є перевірка професійного контакту, тоді як найнадійнішим технічним бар'єром є стійкий до фішингу протокол. Якщо обидва заходи не спрацюють, телеметрія цифрових ідентичностей і хмарних сервісів, що враховує послідовність дій, надає останню можливість обмежити збір інформації та успадкований ризик видавання себе за іншу особу.

VI. АЛЬТЕРНАТИВНІ ПОЯСНЕННЯ ТА СТІЙКІСТЬ ВИСНОВКІВ

А. Звичайне викрадення облікових даних

Фішинг для викрадення облікових даних є широко поширеним, і жоден окремий тип приманки не є унікальним для АРТ35. Альтернативне пояснення стає менш переконливим, коли докази включають ретельний вибір цілей, тривале налагодження професійних довірливих відносин, безперервність взаємодії між різними каналами та профіль жертв, релевантний для розвідувальних цілей. Ці елементи потребують витрат, яких опортуністичні суб'єкти загроз зазвичай уникають. Самі по собі вони не доводять атрибуцію, але в сукупності підвищують імовірність того, що кампанія спрямована на задоволення потреби у зборі інформації, а не на невибірковий перепродаж облікових записів. Це альтернативне пояснення залишається правдоподібним для окремих інцидентів і має бути перевірене до їх ескалації.

Звичайне викрадення облікових даних залишається правдоподібним поясненням деяких інцидентів, особливо коли спостерігається лише одне повідомлення або один домен. Однак воно є менш задовільним поясненням для всього корпусу даних, оскільки не враховує повторювану відповідність між біографією цілі, професійним приводом, багатоетапним контактом і розвідувальною цінністю отриманого доступу до поштової скриньки. Пріоритетна модель пояснює як поширену техніку, так і вибіркові зусилля, що супроводжують її застосування.

В. Безперервність, зумовлена таксономією

Оскільки постачальники спостерігають різні фрагменти активності, агрегування може помилково об'єднувати різних операторів. Це є найсерйознішим викликом для висновків на рівні суб'єкта загроз. У звіті ця проблема вирішується шляхом визначення безперервності на рівні поведінки та прямої відмови від однозначного зіставлення альтернативних назв. Отже, висновок є вужчим, ніж твердження «усе це здійснив один підрозділ». Він полягає в тому, що численні джерела, які використовують різні таксономії та телеметрію, описують повторювану модель пов'язаного з іранською державою кібершпигунства, побудовану навколо цілеспрямованої соціальної інженерії та доступу до цифрових ідентичностей. Рівень впевненості в цій моделі є високим; рівень впевненості щодо точних організаційних меж — від середнього до низького.

Проблема таксономії не зникає; вона змінює рівень, на якому слід формулювати висновки. Твердження про єдину командну структуру або зв'язок зі спонсором залишаються попередніми. Твердження про повторювану операційну модель є більш стійкими, оскільки їх можна безпосередньо оцінювати на основі описаної послідовності дій. Тому у звіті безперервність поведінки не використовується як доказ організаційної ідентичності.

С. Ефекти відбору в публічних звітах

Кейс-стаді постачальників відбираються з огляду на їхню видимість та пояснювальну цінність. У них можуть бути непропорційно широко представлені незвичні інструменти, успішно виявлені атаки або кампанії проти клієнтів із розвиненою телеметрією. Рекомендації державних органів можуть об'єднувати результати кількох розслідувань для формування широких рекомендацій щодо захисту. Ці упередження обмежують можливість оцінювання поширеності. Однак вони не спростовують повторювану послідовність дій, задокументовану незалежними джерелами. Тому у звіті не стверджується, що кожна спроба встановлення контакту відповідає цій моделі або що модель має відомий рівень успішності.

Упередження відбору також може призводити до недооцінювання непомітної компрометації цифрових ідентичностей. Кампанії, які завершуються успішною автентифікацією без використання шкідливого програмного забезпечення, можуть залишати менше помітних артефактів, ніж вторгнення на кінцеві пристрої, особливо коли доступ здійснюється через легітимні хмарні сервіси. Унаслідок цього в публічних звітах можуть бути непропорційно широко представлені технічно нові невдалі атаки та недостатньо представлені успішні атаки із застосуванням ефективної соціальної інженерії. Така можливість додатково підкреслює необхідність обережно формулювати твердження щодо частоти.

VII. ІНВЕРСІЯ МЕЖ ДОВІРИ

Отримані висновки підтверджують концептуальну модель, яку в цьому звіті названо інверсією меж довіри. Традиційна архітектура безпеки передбачає, що довіра має встановлюватися всередині контрольованої технічної межі та не поширюватися на зовнішні суб'єкти. Кампанія змінює цей порядок на протилежний. Вона встановлює соціальну довіру за межами цієї межі через професійну релевантність, спільні інтереси або знайому персону, а потім переносить цю довіру на рішення щодо автентифікації. Таким чином, шкідлива подія сприймається користувачем як така, що вже має довіру, навіть якщо система їй не довіряє.

Інверсія не означає, що людська довіра є ірраціональною. Довіра є адаптивною реакцією на повторювані соціальні сигнали та необхідною умовою для наукової діяльності, журналістики, дипломатії та громадянського суспільства. Перевага противника полягає у відтворенні достатньої кількості таких сигналів, щоб запит, пов'язаний із цифровою ідентичністю, здавався природним продовженням легітимної роботи. Тому ефективний захист має додавати перевірку в точці переходу, не вимагаючи від користувачів ставитися до кожних нових взаємин як до ворожих.

Ця модель також доповнює архітектуру нульової довіри. Технічна модель нульової довіри передбачає, що системи мають постійно перевіряти цифрові ідентичності та контекст, а не покладатися на розташування в мережі. Інверсія меж довіри додає спостереження щодо більш раннього етапу: легітимна спроба автентифікації може бути спричинена за допомогою соціальної інженерії. Надійна автентифікація, перевірка взаємин і моніторинг після автентифікації охоплюють різні частини одного й того самого шляху та мають бути побудовані як скоординована система.

Інверсія меж довіри пояснює три повторювані особливості. По-перше, розвідка зосереджується на біографії, публікаціях, заходах і взаєминах, оскільки ці деталі створюють правдоподібний шлях до встановлення контакту. По-друге, операція може передбачати тривалу безпечну взаємодію, оскільки час, витрачений на підвищення соціальної легітимності, зменшує перешкоди під час подальшої події, пов'язаної з цифровою ідентичністю. По-третє, операція отримує перевагу від переходів між каналами, оскільки довіра прив'язується до персони та сценарію, а не до конкретної платформи.

Модель також виявляє асиметрію в захисті. Організації зазвичай мають високу видимість у момент автентифікації, але низьку видимість щодо взаємин, через які автентифікація здавалася обґрунтованою. Суб'єкт загроз має протилежну картину: він може мало знати про внутрішні засоби захисту, але здатний спостерігати за публічним професійним контекстом цілі. Ефективний захист має поєднати ці два інформаційні середовища, не перетворюючи легітимну професійну діяльність на всеохопне спостереження.

VIII. НАСЛІДКИ ДЛЯ ЗАХИСТУ

A. Захист події, пов'язаної з цифровою ідентичністю

Стійка до фішингу автентифікація є найбільш прямим технічним заходом, оскільки вона знижує цінність викрадених паролів та одноразових кодів. Користувачі з високим рівнем ризику повинні використовувати ключі доступу (passkeys) або апаратні ключі безпеки, використання слабких резервних методів має бути мінімізоване, а відновлення доступу до облікового запису слід розглядати як частину тієї самої системи довіри. Посилення захисту автентифікації є необхідним, але недостатнім: викрадення сесій, надання дозволів шкідливим застосункам і маніпуляції з відновленням доступу можуть створювати альтернативні шляхи отримання доступу.

NIST визначає стійкість до фішингу як здатність протоколу автентифікації запобігати розкриттю секретів або дійсних результатів роботи автентифікатора підставному верифікатору без необхідності покладатися на пильність користувача [12]. Ця властивість має вирішальне значення для кібершпигунства з високим рівнем контексту, оскільки засіб захисту залишається ефективним навіть тоді, коли соціальний привід є надзвичайно переконливим. Це переносить частину навантаження з людського судження на дизайн протоколу.

Впровадження має здійснюватися відповідно до рівня ризику, але не імпровізовано. Адміністратори, керівники вищої ланки, дослідники з доступом до чутливої інформації та особи, які постійно стають цілями пов'язаних із державами суб'єктів загроз, повинні першими отримати найнадійніші доступні засоби автентифікації разом із перевіреними процедурами відновлення доступу. Спільні рекомендації CISA за 2025 рік також передбачають пріоритетне впровадження стійкої до фішингу багатофакторної автентифікації для привілейованих облікових записів і облікових записів із широким доступом, а також поєднання централізованого входу із подіями цифрової ідентичності, доступними для аудиту [13].

В. Моніторинг поведінки після автентифікації

Телеметрію цифрових ідентичностей слід поєднувати з даними аудиту поштових скриньок і хмарних сервісів. До важливих для виявлення подій належать створення нових правил для вхідних повідомлень, налаштування пересилання, надання делегованих дозволів, зміни параметрів відновлення доступу, незнайомі пристрої, підозріле надання дозволів застосункам, аномальне використання токенів, швидкий пошук у поштової скриньці та незвичний доступ до файлів. Мета полягає не в тому, щоб класифікувати кожну аномалію як APT35, а в тому, щоб виявити послідовність збору інформації достатньо рано для відкликання доступу та збереження доказів.

Розробка механізмів виявлення має зосереджуватися на послідовностях подій, а не на окремих аномаліях. Новий пристрій, після появи якого створюються правила поштової скриньки, спостерігається незвична пошукова активність, надається делегований доступ або здійснюється завантаження великого обсягу документів, є більш значущим сигналом, ніж будь-яка з цих подій окремо. Базові моделі поведінки мають враховувати характерні для користувача подорожі, дослідницьку діяльність і моделі співпраці, щоб звичайна мобільність не створювала для аналітиків надмірного інформаційного шуму.

Зберігання даних є не менш важливим. Налагодження довірливих відносин може тривати тижнями, тоді як автентифікація та збір інформації відбуваються швидко. Організаціям необхідно зберігати достатню історію подій цифрових ідентичностей, поштових скриньок, надання дозволів застосункам і аудиту хмарних сервісів, щоб реконструювати перехід від встановлення контакту до отримання доступу. Без такої хронології слідчі можуть виявити компрометацію, але не побачити механізм, який зробив її можливою.

С. Інституціоналізація перевірки професійних взаємин

Загальне навчання з протидії фішингу зосереджується на орфографічних помилках, терміновості та підозрілих вкладеннях. Кампанії, розглянуті в цьому дослідженні, можуть не мати жодної з цих ознак. Спільнотам із високим рівнем ризику потрібна інша норма: незалежно перевіряти особу та запитувану дію перед переходом до іншого каналу, переглядом неочікуваних матеріалів, приєднанням до закритих зустрічей або проходженням автентифікації. Організації повинні забезпечити простий спосіб перевірки запрошень на конференції, запитів від медіа, запрошених науковців і незнайомих партнерів, не створюючи негативного ставлення до легітимної професійної взаємодії.

Сервіс перевірки професійних взаємин має бути швидким, конфіденційним і простим у використанні. Користувачам із високим рівнем ризику потрібен канал, за допомогою якого можна перевірити запрошення, відправника, запит на зустріч або процедуру входу, не змушуючи їх відмовлятися від легітимної взаємодії. Сервіс має зберігати оригінальне повідомлення та його контекст, перевіряти заявлені взаємини через незалежний канал і надавати чітку рекомендацію замість загального попередження.

Важливе значення має інституційна норма: звернення по перевірку має сприйматися як прояв професіоналізму, а не як привід для ніяковості. Пов'язані з державами оператори отримують перевагу, коли користувачі бояться здатися невічливими або недостатньо технічно обізнаними. Керівництво може змінити цей стимул, зробивши перевірку запитів, пов'язаних із цифровою ідентичністю, звичайною практикою дослідницької та комунікаційної гігієни.

D. Визначення масштабу інцидентів у суміжних цифрових ідентичностях

Коли компрометація цифрової ідентичності є ймовірною, під час реагування слід паралельно зберігати докази та відкликати доступ. Доказова база включає оригінальне повідомлення та його заголовки, перенаправлення, події цифрової ідентичності, записи сесій і токенів, правила поштової скриньки, делегований доступ, надані дозволи, зміни параметрів відновлення доступу, активність із файлами та, де це доречно, телеметрію кінцевих пристроїв. Під час визначення масштабу інциденту слід з'ясувати, чи контактувала та сама персона з особистою електронною поштою або обліковими записами в застосунках для обміну повідомленнями, однак збір даних із таких облікових записів потребує згоди та відповідних правових повноважень. Інциденти з високим рівнем ризику також можуть мати наслідки для фізичної безпеки, захисту джерел, подорожей або контррозвідки.

Визначення масштабу інциденту має також охоплювати соціальну мережу, пов'язану зі скомпрометованим обліковим записом. Слідчі повинні визначити кореспондентів, які отримували повідомлення, документи або запрошення на зустрічі від жертви протягом імовірного періоду несанкціонованого доступу, та попередити їх через перевірений канал. Це не просто сповіщення; це стримування ризику, що виникає через успадковану довіру до облікового запису.

Плани реагування також мають розрізняти зміну пароля та анулювання сесій. Зміна пароля може не завершити активні сесії, не відкликати токени застосунків, не видалити правила пересилання та не відновити змінені методи відновлення доступу. Повне реагування на компрометацію цифрової ідентичності має охоплювати кожен механізм збереження доступу, після чого необхідно здійснювати моніторинг спроб повторного проникнення.

Е. Оцінювання стійкості замість проходження навчання

Проходження навчання є слабким показником спроможності до захисту. Кращими показниками є частка користувачів із високим рівнем ризику, які використовують стійку до фішингу автентифікацію; час, необхідний для відкриття сесій і усунення механізмів збереження доступу; охоплення сповіщеннями про правила поштової скриньки, делегований доступ і надання дозволів застосункам; частка підозрілих спроб встановлення контакту, які були незалежно перевірені; а також здатність організації підтримувати надійний канал для повідомлення про інциденти у разі втрати доступу до облікового запису. Ці показники дають змогу оцінити, чи здатна організація перервати операційну послідовність, а не те, чи переглянули користувачі загальні навчальні матеріали.

Зріла програма оцінює як ефективність захисту, так і складність його використання. Корисні показники включають час, необхідний для перевірки підозрілих взаємин, навантаження від хибнопозитивних спрацювань на користувачів із високим рівнем ризику, частку успішних перевірок процедур відновлення доступу та частку інцидентів, реконструйованих між особистими й корпоративними середовищами за згодою користувача. Ці показники демонструють, наскільки засоби захисту придатні до використання в умовах реального професійного навантаження.

Управління має передбачати розподіл відповідальності між функціями безпеки, юридичного супроводу, захисту приватності, комунікацій і захисту керівництва. Орієнтоване на цифрові ідентичності кібершпигунство охоплює всі ці сфери. Технічно надійний засіб захисту, недоступний для користувачів особистих облікових записів, або канал повідомлення про інциденти, непридатний для роботи з конфіденційними взаєминами з джерелами, залишатиме передбачувані прогалини.

ІХ. ОРІЄНТИРИ ТА УМОВИ ДЛЯ ПЕРЕГЛЯДУ

Оцінку слід переглянути, якщо нові докази змінюють характер взаємозв'язку між соціальним доступом і технічною експлуатацією. Наведені нижче орієнтири є більш стійкими з аналітичної точки зору, ніж будь-який окремий домен:

- **Скомпрометовані довірені облікові записи:** Якщо їх регулярне використання зростатиме, репутація відправника втратить свою цінність, а незалежна перевірка взаємин набуде більшого значення.
- **Викрадення сесій:** Якщо доступ за схемою «противник посередині» стане домінуючим, прив'язані до пристрою облікові дані та безперервний контроль ризиків сесій стануть важливішими, ніж лише стійкість паролів.
- **Мобільне стеження:** Якщо компрометація мобільних пристроїв стане регулярною, реагування має розширитися від доказів, пов'язаних із цифровими ідентичностями та хмарними сервісами, до даних про місцезнаходження, контактів і особистої безпеки.
- **Ширший вибір жертв:** Якщо ретельний відбір цілей поступиться невивірковому масштабному таргетуванню, заходи захисту, орієнтовані на окремі ролі, необхідно буде розширити до моніторингу на рівні всієї організації.
- **Деструктивна активність:** Якщо порушення роботи витіснить збір інформації, пріоритети безперервності діяльності, відновлення та безпеки стануть важливішими за модель кібершпигунства, розроблену в цьому звіті.

Х. ОБМЕЖЕННЯ

Цей звіт повністю ґрунтується на публічно доступних доказах. Автори не мають доступу до засекречених звітів, інтерв'ю з жертвами, необробленої телеметрії або повних матеріалів інцидентів. Звіти постачальників рішень залежать від видимості активності в середовищах їхніх клієнтів і власних методів кластеризації. Твердження державних органів не є рівнозначними висновкам, встановленим у судовому порядку, а державні рекомендації можуть навмисно не містити чутливих доказів. Дані про короткочасну інфраструктуру швидко втрачають актуальність. Активність в особистих облікових записах недостатньо представлена у звітах, оскільки вона часто перебуває поза межами корпоративного журналювання, а доступ до неї може бути неможливим з етичних або правових причин.

Відсутність необробленої телеметрії обмежує можливості встановлення причинно-наслідкових зв'язків. Публічні звіти можуть точно описувати послідовність дій, водночас не висвітлюючи невдалі напрями операції, паралельні цілі або результати збору інформації. Тому в цьому звіті не оцінюються показники успішності кампаній, кількість жертв або відносна поширеність використання шкідливого програмного забезпечення та викрадення облікових даних. Ці показники неможливо достовірно визначити на основі доступного корпусу джерел.

Аналіз також успадковує мовне упередження джерел. Англomовні публічні звіти є більш доступними та часто зосереджуються на західних цілях, що може спотворювати видимий географічний та інституційний розподіл активності. Майбутні дослідження могли б отримати користь від багатомовних звітів, досліджень, орієнтованих на жертв, та анонімізованої телеметрії від різних постачальників, яка дала б змогу перевірити, чи узагальнюється запропонована послідовність за межами найбільш помітних випадків.

Отже, внесок цього звіту є концептуальним і орієнтованим на захист, а не на остаточне визначення організаційної структури. У ньому визначено повторювану операційну модель та сформульовано точки втручання, які можна перевірити. Звіт не встановлює командну структуру активності, пов'язаної з APT35, не визначає частоту або рівень успішності кампаній і не доводить, що конкретний інцидент належить певному названому суб'єкту загрози. Будь-яке операційне використання має зберігати це розмежування.

ВИСНОВКИ

Кібершпигунство, пов'язане з Charming Kitten, найдоцільніше розглядати як розвідувальну операцію, що здійснюється через цифрові ідентичності, а не просто як повторюване використання набору фішингових інструментів. Публічні звіти державних органів і представників приватного сектору сходяться щодо стійкої моделі: обрати особу, яка має доступ до цінної інформації або взаємин; створити професійно правдоподібний привід для контакту; налагодити довірливі відносини через доступні канали; спонукати до події автентифікації; та здійснювати збір інформації через отриманий доступ до цифрової ідентичності. Ця модель зберігається, оскільки професійна довіра є водночас цінною та переносною.

Основний внесок цього звіту полягає у зміні масштабу аналізу. Він переходить від каталогізації артефактів до пояснення того, як потреба у зборі інформації перетворюється на соціально правдоподібну подію, пов'язану з цифровою ідентичністю. Такий масштаб зберігає технічну деталізацію, водночас демонструючи, чому заміна інфраструктури не усуває саму спроможність. Стійким механізмом є перетворення професійного контексту на автентифікований доступ.

Для сторін, відповідальних за захист, висновок є конкретним: необхідно захищати перехід від взаємин до автентифікації, а не лише кінцеву URL-адресу. Організації мають поєднувати стійку до фішингу автентифікацію, телеметрію, що враховує послідовність дій, швидку перевірку взаємин, підтримку суміжних цифрових ідентичностей із дотриманням приватності та реагування на інциденти, яке розглядає доступ до поштової скриньки як подію збору інформації. Кожен засіб захисту охоплює окремий етап; найбільшу цінність вони мають при спільному застосуванні.

Цей висновок змінює ключове питання захисту. Основна проблема полягає не лише в тому, як розпізнати шкідливе посилання. Вона полягає в тому, як організація може захистити легітимну відкритість від її перетворення на неперевірену цифрову довіру. Відповідь поєднує технічні та соціальні засоби захисту: стійку до фішингу автентифікацію, моніторинг після автентифікації, норми незалежної перевірки, підтримку користувачів із високим рівнем ризику та реагування на інциденти, яке поєднує докази, пов'язані з цифровою ідентичністю, з контекстом взаємин, що її оточують.

Точні межі між APT35, APT42, Magic Hound, Mint Sandstorm і TA453, імовірно, продовжуватимуть змінюватися в міру того, як постачальники отримуватимуть нові можливості для спостереження, а суб'єкти загроз реорганізовуватимуться. Ця невизначеність має стримувати категоричність тверджень щодо атрибуції, але не затримувати заходи захисту. Поведінкова послідовність є достатньо стійкою, а наслідки компрометації цифрової ідентичності — достатньо серйозними, щоб виправдати дії ще до досягнення повної впевненості щодо суб'єкта загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] Federal Bureau of Investigation et al., "Iranian Cyber Actors Targeting Personal Accounts to Support Operations," Joint Cybersecurity Advisory (2024).
- [2] Mandiant, "APT42: Crooked Charms, Cons, and Compromises," Google Cloud Threat Intelligence (2022).
- [3] Microsoft Threat Intelligence, "New TTPs Observed in Mint Sandstorm Campaign Targeting High-Profile Individuals at Universities and Research Organizations," Microsoft Security Blog (2024).
- [4] Proofpoint, "Iran Conflict Drives Heightened Espionage Activity Against Middle East Targets," Proofpoint Threat Insight (2026).
- [5] MITRE ATT&CK, "Magic Hound (G0059)," Enterprise ATT&CK (accessed 2026).
- [6] Google Threat Analysis Group, "Countering Threats from Iran," Google (2021).
- [7] U.S. Department of Justice, "Three IRGC Cyber Actors Indicted for Hack-and-Leak Operation Designed to Influence the 2024 U.S. Presidential Election," Office of Public Affairs (2024).
- [8] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," ODNI (2025).
- [9] Cybersecurity and Infrastructure Security Agency et al., "Mitigating Cyber Threats with Limited Resources: Guidance for Civil Society," CISA (2024).
- [10] Central Intelligence Agency, "A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis," U.S. Government (2009).
- [11] U.S. Department of Justice, "Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," Southern District of New York (2018).
- [12] National Institute of Standards and Technology, "Digital Identity Guidelines: Authentication and Authenticator Management," NIST Special Publication 800-63B-4 (2025).
- [13] Cybersecurity and Infrastructure Security Agency et al., "Phishing Guidance: Stopping the Attack Cycle at Phase One," TLP:CLEAR Joint Guidance (2025).