Здирники з великої дороги

Хакери-вимагачі нахабніють, множаться і вдосконалюються.

Кібератаки з використанням здирницького ПЗ (Ransomware) залишаються однією з найсерйозніших загроз. За даними компанії Sophos, у 2023 році дві третини організацій у світі зазнали здирницьких атак, і 84% уражених приватних організацій повідомили, що атаки коштували їм втрати прибутків. Здирники не лише шифрують дані і вимагають викуп, але й крадуть інформацію або взагалі переходять від шифрування до шантажу витоком даних. Фахівці вказують на такі тренди, як використання злочинцями штучного інтелекту, атаки на хмарні сервіси, експлуатація вразливостей нульового дня.

«МтБ» поцікавився, як зараз працюють кіберздирники і що можна зробити, щоб захиститись від них.

Дослідження Sophos: мати бекапи вигідніше, ніж відкупатися

Компанія ***Sophos*** у травні минулого року оприлюднила результати замовленого нею дослідження кіберздирництва. Всього було опитано 3 тис. керівників з IT та кібербезпеки з організацій, що налічують від 100 до 5000 співробітників і належать до трьох регіонів: Американського, EMEA та Азійсько-Тихоокеанського. Дослідження показало, що частота здирницьких атак залишається на рівні 2022 року: про них повідомили 66% респондентів. У минулі роки цей показник був меншим: 51% у 2020-му і 37% у 2021-му. 84% респондентів повідомили, що їхні організації втратили дохід через кіберздирницькі атаки.

Дослідження виявило чітку кореляцію між річним доходом компанії та ймовірністю зазнати атаки кіберздирників. У 2022 році це сталося з 56% організацій, що мають доходи $10–50 млн, і з 72% тих, доходи яких перевищують $5 млрд. Між імовірністю атаки і кількістю працівників підприємства чіткого взаємозв'язку нема, але найвища вона для компаній з 1–3 тис. персоналу (73%), тоді як для всіх інших становить 62–63%.

Найчастіше здирницьких атак зазнавав сектор освіти (на рівні 79–80%), оскільки навчальним закладам традиційно бракує ресурсів та технологій для адекватного захисту. Найнижчий рівень атак (50%) продемонстрували сектори IT, технологій і телекомунікацій, що свідчить про вищий рівень захисту і готовності до них.

Серед векторів атак найбільш поширеним були використання вразливостей (39%) і скомпрометованих облікових записів (29%). На електронну пошту загалом припало 31% атак: 18% через листи зловмисного змісту і 13% через фішинг. При цьому найвищий відсоток атак з використанням експлойтів (55%) спостерігався в секторах медіа та індустріях дозвілля і розваг, а через компрометацію облікових записів — у державних установах (41%), що є наслідком частих крадіжок даних та малої можливості запобігати використанню цих даних. IT-сектор більш стійкий до обох векторів, але там у 51% випадків атаки запускались через електронну пошту.

Дослідники Sophos фіксують зростання відсотка успішних атак з шифруванням, який у 2023 році був на найвищому історичному рівні (76% випадків). Це, ймовірно, свідчить про зростання майстерності злочинців, які продовжують відточувати свої прийоми. Справді, як можна бачити, відсоток

Рис. 1. Як часто злочинцям вдається зашифрувати дані своїх жертв (джерело: Sophos)

вчасно зупинених атак з шифруванням з року в рік зменшується (**рис. 1**). У 30% атак з шифруванням також було здійснено крадіжку даних задля подальшого шантажу.

Також підраховано, що 97% організацій, чиї дані було зашифровано, змогли їх повернути. У 70% випадків для цього використано бекапи, 46% сплатили викуп, 2% вжили якихось інших заходів. Важливість бекапів демонструє приклад Італії та Сінгапуру, де відсоток їх використання найнижчий (відповідно 55% і 57%), при цьому в них і найнижчі рівні відновлення даних (93% та 90%), а в Італії на додачу найвищий показник сплати викупу (56%). Існує певна кореляція між заможністю компанії і ймовірністю сплати викупу. Зокрема 55% організацій з річним доходом понад $5 млрд відкупалися від здирників, 63% відновлювали дані з резервних копій, тоді як фірми з доходом меншим за $10 млн у 36% випадків платили викуп, і 80% скористались бекапами. Пояснення таке, що менші організації не мають коштів, щоб відкупитись, і змушені будувати стратегію захисту на бекапуванні, тоді як у великих зазвичай надто складна IT-інфраструктура, щоб можна було вчасно відновити дані з копій, до того ж вони справді мають змогу віддати грошима.

Що стосується середнього розміру викупу, то за рік він майже подвоївся: з $812 тис. у 2022-му виріс до $1,5 млн у 2023-му. Зросла і кількість організацій, які платять великі викупи: у 2023-му році 40% повідомили про сплату $1 млн і більше порівняно з 11% у 2022-му. Середня вартість відновлення, без урахування викупу, виросла до $1,82 млн, а максимальна становила майже $4,5 млн. При цьому бекапування є майже удвічі вигіднішим за відкуп: у першому разі медіанні витрати становлять $375 тис, у другому — $750 тис. (середні відповідно $1,62 млн і $2,6 млн). У майже 40% відновлення відбувалось в межах тижня, 30% — впродовж місяця, і тут переваги резервного копіювання теж проявилися: серед тих, хто відновився за тиждень, 40% використовували резервні копії, і 33% платили викуп (за місяць — відповідно 32% і 29%).

Від шифрування до шантажу

Є звіти з кібербезпеки, які вендори формують на основі даних, отриманих з власних сервісів керованого захисту. Зокрема у січні аналітику щодо кіберздирництва у 2023 році оприлюднила компанія ***Check Point*** на базі служби ThreatCloud AI, яка обробляє дані від 150 тис. підключених мереж. За даними дослідників, у 2023 спроб здирницьких атак зазнали 10% усіх організацій світу порівняно з 7% у 2022-му (тобто кількісно більше на третину), що є взагалі історично найвищим показником (**рис. 2**). Різниця в оцінках з Sophos, вочевидь, пояснюється іншою методологією.

В Азійсько-Тихоокеанському регіоні відсоток атак навіть ще трошки вищий (11%), а в Америках він зріс майже удвічі з 5% до 9%. Найбільше постраждали освітні та наукові організації (22%), державні та військові установи (16%) та заклади охорони здоров'я (12%).

Як зауважує компанія, у 2023 році ландшафт кіберздирництва зазнав суттєвих змін, що позначилося сплеском активності як традиційних здирників, так

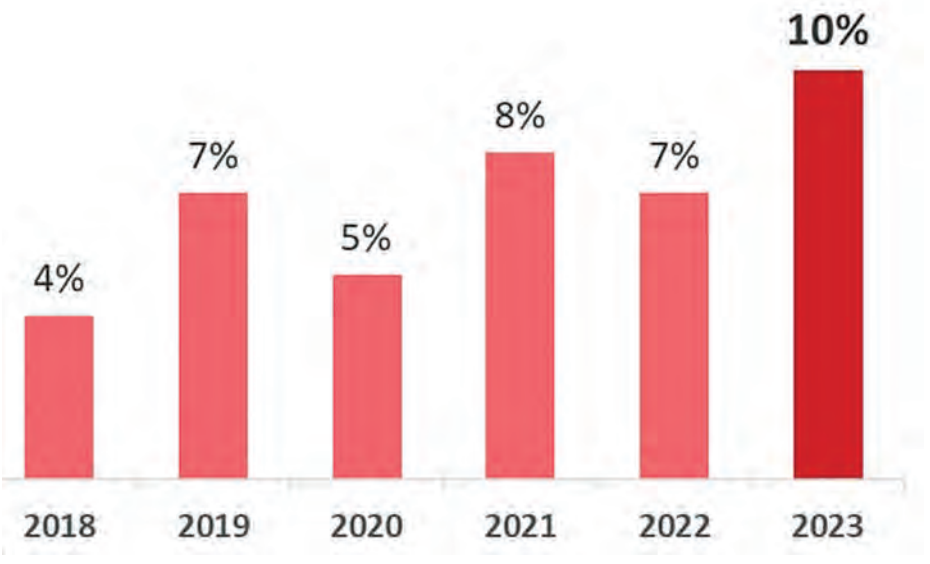

Рис. 2. Відсоток організацій, які зазнали спроб здирницьких атак, 2018–2023 рр. (джерело: Check Point)

і «мегаздирників» (mega-ransomware), цей тренд супроводжується «тривожним переважанням» вразливостей нульового дня, що збільшує розмір завданої шкоди і кількість жертв. На додачу через тиск нових регуляторних правил багато компаній були змушені публічно повідомляти про інциденти кібервимагання, через що домінуючим наративом у 2023 році були безупинні атаки «мегаздирників».

Окрім того, відбулась зміна стратегії атак. У 2023-му році дедалі більше хакерських угруповань зосереджувались на крадіжці даних і погрожували жертвам викласти їх у публічний доступ, нерідко навіть не вдаючись до шифрування.

Компанія ***Zscaler***, спираючись на дані від власного хмарного сервісу кіберзахисту, який обробляє понад 300 трлн сигналів на день, станом на середину 2023 року також зафіксувала збільшення числа здирницьких атак на 37,75%. Приголомшливе тризначне зростання демонструють атаки з подвійним здирництвом, тобто ті, коли хакери не лише зривають нормальну діяльність жертв, але й викрадають дані і шантажують їх зливом. Зокрема на 550% зросла кількість атак проти виробників товарів для дому і особистої гігієни, на 433% — проти індустрії мистецтва, розваг і відпочинку, на 267% — проти енергетики. Zscaler зазначає, що зростання відбувається порівняно з відносно низькою базою попередніх років, проте ці цифри демонструють еволюцію та всеосяжний характер здирницьких атак, цілями яких є широкий спектр різних галузей. Навіть ті сектори, де традиційно рівень атак був низьким, можуть зазнавати сплесків, а експоненційне зростання відображає вдосконалення інструментів і ненаситну гонитву здирників за наживою.

На відміну від Check Point, Zscaler бачить головними жертвами цих випадків виробничу сферу (14,8% всіх випадків), на другому місці сфера послуг (11,66%), і лише на третьому – освіта (7,64%). Ці дані складено на основі числа повідомлень на сайтах, де викладаються вкрадені дані, що дає уявлення про співвідношення, хоча не обов'язково про увесь масштаб інцидентів, тому що про багато з них не повідомляється або вони вирішуються у приватному порядку шляхом сплати викупу. Географічно найбільше атак з подвійним здирництвом припадає на США (40,34%), далі Канада (6,75%) і Велика Британія (6,44%). Цікаво, що на Україну припадає менше атак, ніж на Росію (відповідно 0,09% і 0,13%).

Окрім цифр, Zscaler виділяє кілька трендів у розвитку кіберздирництва. По-перше, як вже йшлося, дедалі більше кіберзлочинців переходять до атак без шифрування, натомість вимагаючи викуп за нерозголошення даних, що ускладнює роботу захисників. Атаки без шифрування за задумом менше порушують діяльність компаній, які таким чином зазнають менших збитків і в змозі сплатити більший викуп. Окрім того, такі компанії з меншою ймовірністю розголошуватимуть факт зламу, захищаючи свою ділову репутацію. Адже збитки через втрати продажів, судові процеси і підірвану довіру можуть значно перевищувати суму викупу. Також атаки, які не надто впливають на діяльність компанії, з більшою ймовірністю залишаться непоміченими правоохоронними органами і кібердослідниками. Нарешті, атаки без шифрування складніше вчасно виявити і зупинити, особливо якщо злочинці використовують легітимні інструменти і служби Windows (стратегія «living-off-the-land).

Другим трендом є використання зловмисниками штучного інтелекту (чатботи, написання коду, машинне навчання, автоматизація процесів тощо), це дозволяє створювати більш складні і ефективні техніки, проти яких важче захищатися, а також спрощує діяльність менш «просунутим» гравцям.

Кіберзлочинці дедалі більше зосереджують увагу на організаціях, які мають страхування від кіберризиків, оскільки знають, що ті з більшою імовірністю сплатять викуп, адже його компенсує страхова компанія. Також об'єктами атак стають муніципалітети, державні установи, правоохоронні органи, школи та інші громадські заклади, які зазвичай не мають адекватного захисту і водночас мають цінну інформацію, яку легко продати.

Окрім того, що більшість здирницьких груп включені в модель Ransomware-as-a-Service, Zscaler звертає увагу на зростання кількості брокерів початкового доступу, тобто угруповань, які здійснюють злам організації і продають доступ здирникам або їхнім партнерам. Завдяки цьому хакери, які володіють навиками проникнення, можуть отримувати прибуток, не маючи компетенції для проведення повномасштабних здирницьких атак.

Оскільки дедалі більше компаній користуються хмарними ресурсами для обчислень і зберігання даних, імовірно, здирники розроблятимуть інструменти, оптимізовані для атак проти цих ресурсів і робочих процесів. Компрометація хмарного середовища може зачепити одразу багатьох користувачів. Окрім того, очікується, що злочинці намагатимуться атакувати бізнес-критичні сервери і бази даних, для чого розроблятимуть здирницьке ПЗ для інших операційних систем, окрім Windows, а саме Linux і ESXI. Можливо, й для macOS. Зокрема для цього вони вже використовують замість традиційних мов C та C++ більш сучасні, зокрема Rust, яка забезпечує швидше шифрування і глибокий контроль за системними ресурсами, є відносно стійкою до зворотної розробки (reverse engineering) і водночас має більш інтуїтивно зрозумілий синтаксис.

Нове як незабуте старе

Компанія ***WithSecure*** торік випустила звіт на тему «професіоналізації кіберзлочинності», у якому пише, що велетенські прибутки кіберздирників спричинили еволюцію злочинної індустрії загалом і стрімке постання підпільних торгівельних майданчиків, де продають продукти і послуги. Багато в чому ця екосистема кіберзлочинності все більше скидається на сервіс-орієнтовану технологічну індустрію, де окремі сегменти бізнесу передаються на аутсорсинг за моделлю «as-a-Service».

Багато великих угруповань кіберздирників виступають у ролі провайдерів послуг RaaS, надаючи партнерам інструменти і професійні знання, за що отримують частину прибутків. Ці прибутки, своєю чергою, призвели до швидкого утворення сервісної індустрії, яка забезпечує новостворені угруповання хакерів усіма засобами, яких вони потребують. А завдяки криптовалютним розрахункам

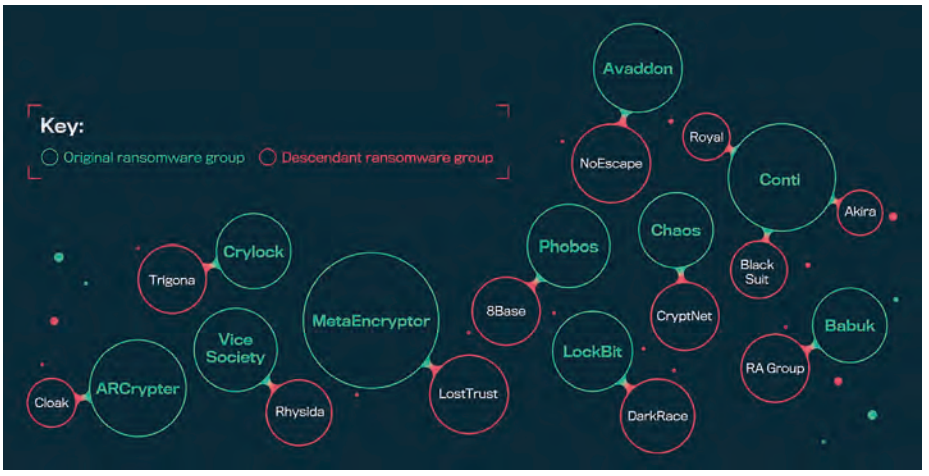

Рис. 3. «Брунькування» кіберздирників. Зеленим позначено оригінальні угруповання, червоним — їхніх нащадків (джерело: WithSecure)

і dark web'у всі ці угруповання можуть анонімно купувати і продавати послуги і отримувати прибутки.

У своєму звіті за підсумками трьох кварталів минулого року WithSecure зазначає, що, попри багаторічні зусилля урядів та бізнесу, здирництво ніде не поділося і навіть процвітає. Як з'ясували дослідники, підживлює цю злочинну «індустрію» постійний притік нових здирницьких угруповань. Зокрема до їхнього числа належить майже половина угруповань, які займаються багатобічним здирництвом — multi-point ransomware (більш відомим як подвійне і потрійне здирництво). Загалом WithSecure нарахувала за три квартали 2023 року на 50% більше багатобічних здирницьких атак, ніж за цей же період попереднього року, а витоків — більше, ніж за увесь 2022-й. Чверть витоків даних також є «заслугою» нових гравців.

При цьому, зауважує WithSecure, нові угруповання часто пов'язані з більш старшими або принаймні використовують вихідний код зловмисного ПЗ, який потрапив у публічний доступ. Наприклад, одна з найбільш активних організацій, Conti, у 2022 році проголосила свою підтримку вторгнення Росії в Україну, але невдовзі припинила існування після того, як проукраїнський учасник злив у мережу її власні дані, зокрема вихідний код. Це, своєю чергою, призвело до постання нових груп, таких як Royal, Akira і Black Suit. Вихідні коди інших угруповань, Lockbit і Babuk, також були злиті незадоволеними учасниками і знайшли застосування в інших бандах (**рис. 3**).

Цими витоками «перехресне запилення» кіберздирників не обмежується. Їхні угруповання, як і IT-компанії, мають свій персонал, і так само, як в IT, люди часом змінюють роботу, забираючи з собою свої навички і знання. Проте, на відміну від законного IT-бізнесу, ніщо не заважає злочинцеві прихопити ресурси банди (наприклад, код або інструменти) і використовувати їх на новому місці.

Ложкою меду тут є те, що здирницький бізнес є настільки успішним, що зловмисники не бачать потреби в якихось значних інноваціях. «Якщо еволюція здирництва полягає у Дарвінових варіаціях на ту саму тему, організації фактично можуть передбачити, що їх очікує, і підготуватися до того неминучого дня, коли банда кіберздирників постукає у їхні цифрові двері», — роблять висновок дослідники.

Поліція проти здирників

Правоохоронні органи різних країн у взаємодії з Інтерполом, Європолом і компаніями-виробниками зі сфери кіберзахисту періодично вживають заходів проти кіберздирників і намагаються зупинити їхню діяльність. Іноді це вдається, іноді ні.

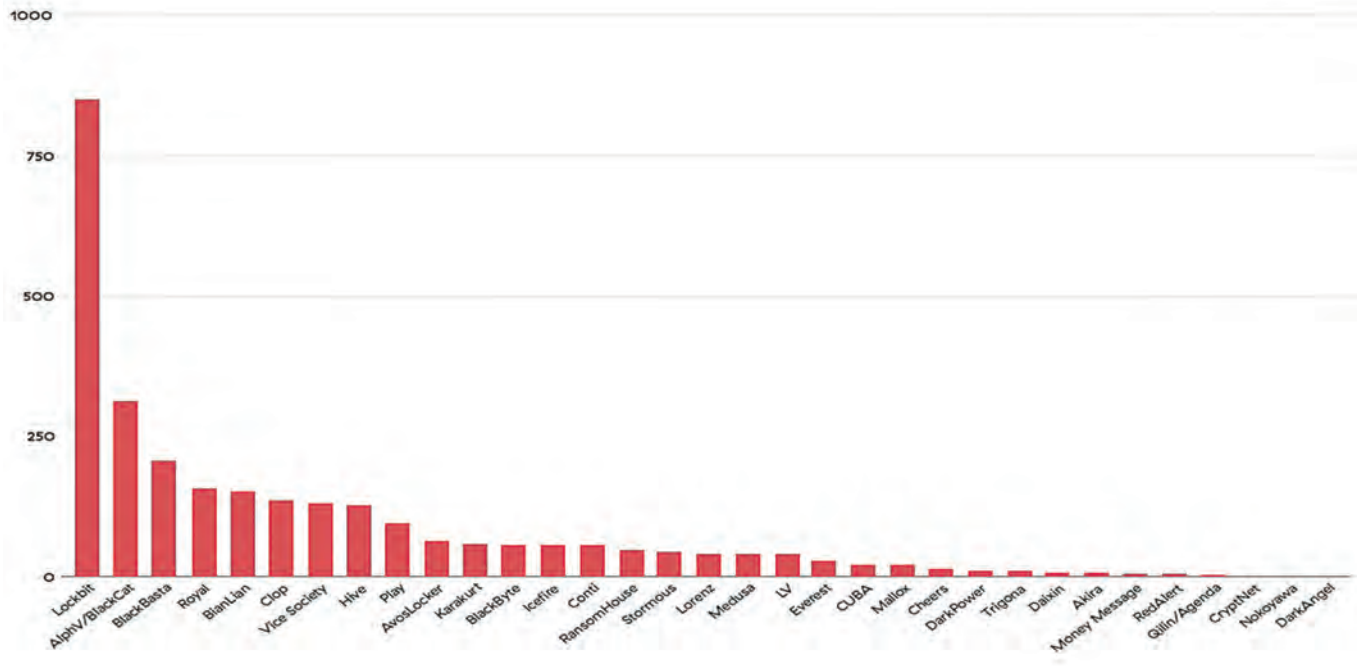

Рис. 4. Кількість жертв крадіжки даних за групами кіберздирників, квітень 2022 – квітень 2023 (джерело: Zscaler)

Найактивнішим кіберздирницьким угрупованням торік був Lockbit. За даними Zscaler станом на квітень минулого року, ним було здійснено утричі більше атак, ніж AlphV, який зайняв друге місце (**рис. 4**). Це угруповання з'явилось у 2019 році, є надавачем послуг RaaS і має зв'язки з російськими кіберзлочинцями. За оцінками FBR станом на червень минулого року, це угруповання здійснило тільки в США 1700 атак і заробило $91 млн. У листопаді хакери Lockbit атакували мережі Boeing і погрожували оприлюднити «велетенські обсяги» секретних даних.

У лютому 2024 року міжнародна коаліція на чолі з Національною агенцією з боротьби зі злочинністю Великої Британії (NCA) взяла під контроль сайт Lockbit для публікації вкрадених даних і розмістила відповідне повідомлення (**рис. 5**). Партнери Lockbit, які намагалися зайти у панель управління, отримували інше повідомлення, в якому йшлося, що правоохоронцям відомо про них усе. Агенції отримали доступ до вихідного коду і «великого обсягу даних» про діяльність злочинців та їхніх спільників. В рамках операції «Кронос», у якій брали участь NCA, FBR, Європол та правоохоронні органи інших країн, було заарештовано двох учасників угруповання в Польщі та Україні, які мали бути екстраговані в США, і висунуто обвинувачення двом громадянам Росії. Було заморожено 200 криптовалютних рахунків і закрито 34 сервери, що належали Lockbit або їхнім партнерам. Також отримано ключі дешифрування.

Як повідомляється на сайті вітчизняного МЗС, від України брали участь Нацполіція, СБУ і Офіс генерального прокурора. В Україні злочинців представляли батько і син, від дій яких постраждали фізичні особи, підприємства, державні установи та заклади охорони здоров'я у Франції.

Правоохоронцям допомагала компанія ***Trend Micro***, яка повідомила, що їй вдалось запобігти випуску нової версії зловмисного ПЗ Lockbit і надати захист для своїх партнерів. Втім, у своєму досить довгому і детальному пості Trend Micro розповіла, що, попри всі успіхи, в останній рік Lockbit втрачав позиції серед колег по злочинному ремеслу. У квітні минулого року організація почала додавати на свій сайт витоків повідомлення про вигадані успіхи. У січні 2024-го її звинуватили у несплаті брокерові доступу, а невдовзі Lockbit забанили на двох злочинних форумах зі статусом «кидайла». Також Trend Micro має дані, що хоча впродовж останніх двох років Lockbit займав перше місце за кількістю атак, доля його прибутків невпинно зменшувалась. «Сподіваємось, що Lockbit стане наступною великою групою, яка спростує твердження, що є організації надто великі, щоб впасти», — так закінчили свій висновок спеціалісти.

Як повідомляв відомий журналіст і експерт з кібербезпеки Браян Кребс, Lockbit намагався відродитись, створивши новий сайт у dark net'і, проте на той час організація вже поховала рештки своєї репутації. 13 лютого, ще до міжнародної акції, Lockbit атакував ресурси округу Фултон, що у штаті Джорджія, порушивши роботу телефонного зв'язку, Інтернету і навіть судів, і виклав маленьку порцію файлів, погрожуючи злити все, якщо влада округу не сплатить викуп.

Вже на новому сайті Фултон числився серед жертв, які мали розплатитись до 1 березня, згодом дату пересунули на 29 лютого. Того дня Фултон зник зі списку. Представник Lockbit заявив Кребсові, що Фултон сплатив викуп, доказом чого є сам факт, що дані не було оприлюднено. Проте голова округу на прес-конференції повідомив, що

Рис. 5. Повідомлення учасників від міжнародної робочої групи «Операція "Кронос"» про захоплення ресурсів Lockbit

ніхто нічого не платив. Бретт Каллоу, експерт з компанії Emisoft, припустив, що хакери насправді втратили всі поцуплені дані і відчайдушно намагалися переконати партнерів, ніби все гаразд. «Я сильно підозрюю, що це кінець бренду Lockbit», — сказав він.

Не такими результативними були дії проти торішніх здирників №2 — AlphV/BlackCat. У грудні FBR оголосило про те, що, використовуючи соціальну інженерію, змогло захопити сайт AlphV і отримати 946 ключів шифрування. Проте за лічені години після заяви ФБР на сайті AlphV зникло повідомлення про закриття, змінившись іншим — про те, що сайт «роззахоплено». Злочинці визнали, що близько 400 жертв отримали дешифрувальник, але заявили, що через дії FBR інші 3000 «ніколи не отримають свої ключі».

Протягом дня ФБР і хакери змагались за контроль над сайтом, і на ньому по черзі з'являлись плашки протилежного змісту. Як пояснювало видання Ars Technica, в мережі Tor, якою користуються злочинці, контролювати сайт можна лише маючи приватний ключ, і в даному разі ним володіли обидві сторони. А оскільки змінити приватний ключ, прив'язаний до адреси, неможливо, встановилася патова ситуація. Як відповідь AlphV/BlackCat збільшила виплату партнерам до 90% від суми викупу і зняла заборону на атаки проти закладів сфери охорони здоров'я.

У лютому цього року хакери AlphV/BlackCat зламали великого канадського оператора нафто– і газопроводів Trans-Nothern Pipelines і, за власною заявою, вилучили 190 ГБ даних. Тоді ж було атаковано нафтовидобувні та комунальні підприємства в США, Канаді та Іспанії. Наприкінці лютого BlackCat атакував Change Healthcare — технічний підрозділ найбільшої американської компанії галузі медичного страхування UnitedHealth Group, на кілька тижнів порушивши роботу аптек по всій країні.

1 березня на крипторахунок, який дослідники вже асоціювали з BlackCat, надійшов платіж на суму $22 млн. Як повідомляв Браян Кребс, за два дні партнер BlackCat, який і здійснив атаку, написав на російськомовному хакерському форумі, що Change Healthcare сплатила викуп у розмірі $22 млн, але він своїх кревних досі не отримав. «На жаль для Change Helthcare, їхні дані досі в нас», — написав хакер. У відповідь на це представник BlackCat оголосив, що вони... припиняють свою діяльність і вже знайшли покупця на вихідний код свого ПЗ. На сайті угруповання знову з'явилася плашка від FBR.

Проте, на відміну від випадку з Lockbit, експертне середовище не повірило у смерть AlphV. Було помічено, що плашка, власне, та сама, яку «федерали» повісили у грудні. Це більше було схоже на «кидок» партнерів, фіктивний вихід, щоб нікому не платити. Як розповів Reuters дослідник Віл Томас, це може бути спробою присвоїти гроші партнерів і почати все з чистого аркуша. Вважається, що BlackCat — це ребрендинг іншого угруповання під назвою Dark Side. «Не здивуюсь, якщо вони повернуться знову в недалекому майбутньому», — підсумував Томас.

27 березня Держдеп оголосив винагороду у розмірі до $10 млн за інформацію про BlackCat.

То як захищатись?

Як бачимо, навіть якщо здирників прижучити, вони можуть виринути знову під іншим іменем. Понад те, сплата викупу сама по собі не гарантує, що здирники знищать вкрадені дані. Тож треба давати собі ради самостійно.

Фахівці компаній, які продають рішення та послуги з кібербезпеки, пропонують практичні поради, як протистояти здирницьким атакам. Як і скрізь, тут є дві стратегії, які доповнюють одна одну: запобігання і подолання. Важливо бути готовими до того, що успішна здирницька атака врешті станеться. Як уже йшлося, дієвим методом є створення та підтримка резервних копій даних. Хоча здирники дедалі частіше нехтують шифруванням, надаючи перевагу шантажу зливом даних — можливо, саме з цієї причини, — бекап все ж дозволить впоратись з більш традиційною атакою і не платити викуп. Тому варто регулярно здійснювати резервне копіювання, тренувати відновлення з бекапів і мати актуальний план реагування на інциденти.

Що стосується запобігання атакам, то тут є підходи організаційні й технічні. Оскільки чи не найпопулярнішим каналом ініціювання здирницьких атак є фішингові листи, важливе місце займає навчання персоналу кібергігієні і вмінням розпізнавати ознаки фішингу. Гігієна полягає і в тому, щоб вчасно встановлювати оновлення, особливо ті, які є критичними, і регулярно переглядати конфігурації інструментів безпеки.

З технічних засобів радять використовувати інструменти безпеки, які захищають від поширених векторів атак, зокрема засоби захисту кінцевих точок з потужними можливостями протидії експлуатації вразливостей, а також архітектуру доступу з нульовою довірою (ZTNA) для запобігання зловживанню вкраденими обліковими даними. Доцільно запровадити політики доступу з найменшими привілеями, аби користувач мав доступ лише до тих ресурсів, які потрібні йому для роботи, завдяки цьому хакери не потраплять до чутливих даних чи систем навіть у разі компрометації облікового запису. Додатковий рівень захисту створить багатофакторна автентифікація. Ізоляція браузера за допомогою вбудованої пісочниці втримає здирницьке ПЗ від просочування у пристрій користувача і далі в корпоративну мережу. Врешті можна взагалі від'єднати критичні програми та ресурси від Інтернету, тоді зловмисники не зможуть скористатися вразливостями в них.

Не зайвими будуть добре знані рішення безпеки типу DLP для захисту від крадіжки даних, окремі пісочниці та системи пасток. Також можна впровадити рішення типу SIEM чи XDR, які забезпечують автоматичне реагування на атаки, їх цілодобове виявлення, знешкодження та розслідування — чи то локально, чи то в партнерстві з провайдером послуг MDR (Managed Detection and Response).

Кіберзлочинці, і здирники зокрема, щодалі відточують свою майстерність і вдосконалюють інструменти. Щоб не потрапити на гачок, потрібно не відставати.

Василь ТКАЧЕНКО, МтБ