РОЗРОБКА НАСТУПАЛЬНОЇ ПРОГРАМИ З КІБЕРБЕЗПЕКИ ДЛЯ ЗАВЧАСНОГО ВИЯВЛЕННЯ ТА УСУНЕННЯ ВРАЗЛИВИХ МІСЦЬ У СИСТЕМІ ЗАХИСТУ

Цей документ підготовлений на замовлення USAID. Його самостійно підготував партнер-виконавець «Каталісто» для діяльності USAID «Кібербезпека критичної інфраструктури в Україні». Погляди авторів, висловлені в цьому документі, не обов'язково відображають погляди USAID або уряду Сполучених Штатів.

МОДУЛЬ 3 – ВСТУП

Як міг би засвідчити кожен військовий стратег або професійний спортсмен, найкращим захистом є наступ. Кібербезпека не є виключенням щодо цього вислову. Отже, давайте більш детально розглянемо Наступальну Безпеку і на те, як вона може допомогти організації.

По своїй суті Наступальна Безпека існує для того, щоб ідентифікувати вразливі місця до того, як вони будуть виявлені та використані зовнішніми зловмисниками. Термін «Наступальна Безпека» є парасольковим, він охоплює декілька аспектів кібербезпеки. Давайте розглянемо деякі з них, розпочавши із найбільш базових, далі перейдемо до складніших.

АСПЕКТИ НАСТУПАЛЬНОЇ ПРОГРАМИ З КІБЕРБЕЗПЕКИ

1. Обстеження на предмет виявлення вразливих місць

Обстеження щодо виявлення вразливих місць використовує автоматизовані інструменти, котрі зондують середовище на предмет наявності відомих ризиків. Хоча надійна програма обстеження на предмет виявлення вразливих місць є надзвичайно важливою частиною повної програми кібербезпеки, такі програми занадто сильно покладаються на автоматизовані сканери та різні повторювані або масштабовувані процеси, щоб вони могли самостійно функціонувати в якості Програм Наступальних Операцій.

2. Перевірка на предмет проникнення

Як і перевірка на предмет виявлення вразливих місць, перевірка на предмет проникнення, або ПенТест, намагається перелічити ризики, користуючись комбінацією автоматизованих інструментів та людської винахідливості. При обмеженні його сфери застосування до однієї програми чи середовища, ПенТест може забезпечити значно більш глибоку перевірку і визначити ризики, котрі можуть бути пропущені під час автоматичного сканування.

3. Червона Команда

Термін «Червона Команда» часто використовують як взаємозамінний до терміну «ПенТест». Та не зважаючи на те, що частина їхніх тактик є ідентичними, ці дві програми мають дуже різні стратегії та цілі. ПенТест зазвичай має чіткі часові обмеження, базується на повторюваних процесах із регулярним формуванням звітів, котрі зазвичай надсилаються в зовнішні організації. Залучення Червоної Команди натомість може займати невизначений час, і часто її робота поширюється на все підприємство. Результати досліджень не надсилаються у жодні треті організації. Крім того, тестери Червоної Команди використовують тактики, до яких вдаються реальні зловмисники для досягнення своїх кінцевих цілей. Часто це означає доступ, втручання або маніпулювання найціннішими активами компанії. Вони є «хорошими хлопцями, котрі користуються інструментами поганців» з дозволу власника для того, щоб дослідити рівень ризику, з яким компанія має справу в реальному житті.

Ці зобов'язання можуть бути виконані з дотриманням повної прозорості для команд, що підтримують безпеку, але часто все здійснюється із мінімальним поширенням інформації, щоб дослідити справжню готовність організації до реальної атаки. Усі звіти залишаються всередині компанії і використовуються для визначення ризиків та прийняття рішень щодо дій при виникненні реальних загроз.

4. Полювання на загрозу

Занадто багато організацій чекають на повідомлення про здійснену атаку. Через зростання кількості та масштабності кібератак, а також із постійним виникненням більш складних технологій, до яких вдаються зловмисники для маскування своїх дій, традиційний підхід «будування більших захисних огорож» тепер не працює.

Згідно звіту, нещодавній злом Equifax поставив під серйозну загрозу розголошення, яка виникала останніми роками, особисті дані понад 143 мільйонів американців. Гучні масштабні атаки, такі як у Equifax, служать нагадуванням про те, що захисного підходу боротьби із кіберзагрозами вже недостатньо.

У сьогоднішньому непередбачуваному середовищі, у якому багато швидких і гнучких зловмисників та загрозливих технологій, єдиний метод, до якого може вдатися організація, щоб захистити себе, є використання наступальних кібертехнік для викриття несподіваних ворогів у своїх мережах. Найбільш ефективний підхід – Полювання на Загрозу – є надзвичайно важливим для кожної організації, котра хоче зупинити втручання та запобігти атакам на свої мережі.

Неочікувані вороги існують у шумі мереж і наносять шкоду впорядкованому кіберпросторі шляхом постійного пошуку зловмисних тактик, технік та процедур (ТТП). Ці розробки – такі як поліморфні та оманливі віруси, динамічна інфраструктура, безфайлові віруси, порушення функцій операційної системи – усі вони здатні уникати традиційних засобів захисту.

Під час декількох таких Полювань багато фірм дізнались про те, що період, протягом якого неочікуваний ворог таємно перебуває у мережі, сягає 200-250 днів до моменту, поки його буде викрито. Полювання на Загрозу являє собою активний пошук ознак загрози до того, як спрацює аварійний сигнал. Це ретельне прочісування мереж та баз даних для викриття прихованих небезпек. Шляхом регулярного перевірки їхніх мереж на предмет загрозливих дій, організації можуть «упіймати» атаку в її процесі – доки ще не надто пізно.

Для збору та аналізу величезного обсягу даних цей проактивний підхід спирається на такі складні інструменти, як автоматизація, розвідка загроз, аналітика загроз та штучний інтелект. Ці інструменти можуть швидко визначити та знешкодити загрози, використовуючи індивідуальні моделі.

Але не всі загрози можуть бути виявлені лише з допомогою автоматизованих інструментів. Ці інструменти повинні застосовуватись навченим аналітиком, котрий має глибоке розуміння середовища, у якому вони працюють, а також здатний задавати правильні запитання. Аналітики можуть зрозуміти складні дані, розробити гіпотези, згідно

яких здійснюватиметься Полювання, і протестувати ці гіпотези, щоб з їх допомогою краще ідентифікувати приховані загрози.

Навіть за участі навченого аналітика та з використанням правильних інструментів, вузькоспеціалізованого Полювання недостатньо, воно повинно бути стандартизованим та добре спланованим. Полювання на загрозу вимагає впровадження повторюваних процесів, котрі є невід'ємною частиною загальної стратегії з кібербезпеки організації. Поєднання та свідоме використання таких інструментів, як Інформація щодо Безпеки та Управління Подіями (SIEM), а також Локалізація Кінцевої Точки та Реагування (EDR) може допомогти раціоналізувати цей процес.

Інциденти, такі як атака на Equifax, не повинні бути невідворотними. Організаціям слід вдаватися до дій, спрямованих на покращення їхньої системи безпеки до того, як станеться наступна атака. Три елементи: аналітичні інструменти, талановитий аналітик загроз та стандартизований процес полювання, вбудовані у загальну стратегію безпеки, можуть бути ключем до належного захисту вашої організації.

ВИКОРИСТАННЯ НАСТУПАЛЬНОГО ПІДХОДУ У СФЕРІ КІБЕРБЕЗПЕКИ В ДЕРЖАВНОМУ ТА ПРИВАТНОМУ СЕКТОРАХ

Останніми роками швидко зростає кількість кібератак, котрі завдають шкоди як приватним, так і державним організаціям. Збитки, завдані саботажем та крадіжками об'єктів інтелектуальної власності, щороку налічують кілька мільярдів доларів.

Спільнота, котру турбують питання кібербезпеки, усвідомлює зростання масштабів кіберзагроз, але підхід до захисту, що використовується на даний час, проявляє свою нездатність обмежити небезпеки кіберпростору. Кіберзагрози є динамічними, і атаки у цій сфері є несиметричними та складними для передбачення.

У більшості випадків жертви атак можуть лише підрахувати збитки, завдані рейдами їхніх конкурентів. Правоохоронні органи та приватні компанії публічно обговорюють можливості визначення нових стратегій для захисту своїх активів від атак.

Найбільш правдоподібною гіпотезою, котру було висунуто на засіданні Юридичного комітету сенату США, присвяченому заходам, спрямованим на боротьбу з атаками, у якому брали участь обидва види організацій, є прийняття Наступального підходу у сфері кібербезпеки.

Успішність нещодавніх атак, здійснених кіберзлочинцями, а також хакерами, спонсоровані урядом, дає експертам з кібербезпеки усі підстави вважати, що підхід до захисту, що полягає в очікуванні атаки, є абсолютно непридатним. У багатьох випадках жертви ідентифікують атаки через багато років після того, як атаки власне стаються, і тоді вже занадто пізно вживати пом'якшувальні заходи, а наслідки є драматичними.

З цієї причини правоохоронні органи та приватні організації активно шукають відповідь на запитання щодо можливості впровадження наступальних технік для пом'якшення кіберзагроз, таких як інтрузивні віруси, щоб відстежити втручання або зловмисні програми,

та розгорнути «анти-фішингові» кампанії проти злочинців, котрі підозрюються у здійсненні атак.

На початку 2013 року компанія CrowdStrike презентувала свій Наступальний підхід до кібербезпеки. Фірма оприлюднила деталі щодо злочинного захоплення тисяч точок підключення до мережі сумнозвісних «зомбованих» комп'ютерів Kelihos. Компанія є відомою у спільноті, котру цікавлять питання кібербезпеки, тому що вона вдається до усіх можливих законних методів «*повернення назад украденої інформації від хакерів або повного її знищення для уникнення використання цієї інформації злочинцями*».

Стюарт А. Бейкер, партнер компанії «Steptoe & Johnson LLP», раніше – член Юридичного комітету з питань криміналу та тероризму, у документі «Революція влади: зростання витрат на хакерів та їхніх клієнтів» описав актуальний підхід до кібербезпеки наступними метафорами:

"Не схоже на те, що ми наближаємося до вирішення цієї проблеми"

«Коротко кажучи, ми не можемо знайти шляху вирішення цієї проблеми. Це так само, як неможливо подолати вуличну злочинність, звільнивши поліцію та примусивши пішоходів щороку купувати нові бронежилети для захисту» «Я не закликаю до взяття закону у свої руки та лінчування. Але ми повинні знайти шлях, як дати фірмам, які проводять такі дослідження, можливість вийти за межі їхніх мереж.»

"Якщо ми не зробимо цього, ми ніколи не докопаємося до суті більшості цих атак,"

Слухання в Юридичному комітеті в сенаті США також було присвячене кіберзагрозам з-за кордону, кібератакам, організованим хакерами, послуги яких оплатили уряди інших держав. Цих хакерів були залучено до диверсійних атак та кампаній з кібершпіонажу, що становлять серйозну загрозу урядовій безпеці.

Як відстежити іноземних хакерів? Чи виправданий підхід, що базується на діях у відповідь на атаку?

У цьому документі поглиблено розглядаються дві складові, з яких складається Наступальний підхід:

- Атрибуція, тобто дії, спрямовані на пошук та знаходження ключів для відстежування хакерів

- Відплата, переконання зловмисників обрати іншу політику.

Наступальний підхід у кібербезпеці не є новою концепцією. Його було теоретично обґрунтовано кілька років тому, після чого він довгий час був темою для дебатів. Найпершим запереченням було те, що такий підхід може завдати шкоди громадянській свободі та приватній інформації користувачів.

Фаза атрибуції фактично потребує проведення досліджень широкого діапазону. Щоб відстежити хакерів, потрібно використовувати методи прослуховування телефонних

розмов, а також інструменти кібершпіонажу. Очевидно, що обидва ці методи можуть становити серйозну загрозу для пересічних людей та користувачів Інтернету.

Визнаючи той факт, що кіберпростір не має жодних фізичних кордонів, слід також визнати, що Наступальний підхід може мати вплив на пересічних користувачів Інтернету, котрі перебувають в інших країнах, із серйозними юридичними наслідками. Нещодавно джерела Білого Дому повідомили виданню Нью-Йорк Таймз, що відтепер накладатимуться дуже високі штрафи на будь-який веб сайт або Інтернет сервіс, включно із тими, що базуються за кордоном, якщо вони відмовлятимуться підтримати вимогу ФБР про надання доступу для встановлення засобів для прослуховування телефонних розмов протягом 30 днів після отримання ордеру з суду.

Дебати щодо Наступального підходу у кібербезпеці фокусують увагу на можливості встановити секретні програми на популярні вебсервіси та додатки, щоб шпигувати за широкою аудиторією користувачів Інтернету з дослідницькою метою, що є незаперечним порушенням їх конфіденційності.

Частина світової спільноти з кібербезпеки не підтримує впровадження Наступального підходу. Пан Мікко Гіппонен, головний слідчий у F-Secure, коментував використання спонсорованих державою вірусів із дослідницькою метою наступними словами:

“Чудово зрозуміло, чому правоохоронні органи хочуть використовувати віруси,” “Це збільшення масштабів того, що вони і так робили з точками під’єднання телефонів, Інтернету, з допомогою провайдерів мобільного зв’язку для відстеження вашої локації – усе це тепер згідно рішення суду.” “Хай там як, та немає нічого більш інтрузивного, ніж держслужбовці, котрі стежать за вами через ваш власний комп’ютер або смартфон,” “Вони бачать ваші файли. Вони бачать, що ви шукаєте. Вони можуть отримати ваші паролі. Вони можуть бачити, що ви робите через вашу вебкамеру.”

Не зважаючи на те, що цей підхід не поділяють багато експертів, уряди упродовж останніх десяти років просувають як Наступальний, так і Інвазивний підходи у кібербезпеці. Нещодавні програми з нагляду за підозрюваними, такі як US та UK Tempora є демонстрацією зусиль уряду, спрямованих на національну безпеку.

Але Наступальний підхід, як було зазначено, базується не лише на програмах спостереження за підозрюваними. Щодня численні кампанії з кібер шпіонажу проводяться керівниками урядів, котрі визнають стратегічну необхідність проникнення у закордонні мережі для крадіжок інтелектуальної власності та іншого виду секретної інформації.

Провідні фірми, що працюють у галузі кібербезпеки, включно із Mandiant Intelligence Company, звинуватили китайських хакерів у численних кібератаках на США. Служба кібербезпеки Mandiant оприлюднила докладні докази у звіті, у заголовку якого натомість заявлено про залучення ними до роботи хакерів з Peoples Liberation Army.

Сенатор Ліндсей Грахам заявив з приводу загрози з боку Китаю наступне:

“"Наші китайські друзі, схоже, запекло прагнуть вкрасти все, що потрапить їм під руку тут, в Америці,” “Ми збираємося повідомляти на національному рівні про те, що якщо ви продовжуватимете це робити, вам доведеться заплатити високу ціну.”

Конгресмен Майк Роджерс, відомий активною участю у дебатах стосовно акту CISPA, продемонстрував скептицизм щодо можливості здійснювати наступальні дії у приватному секторі.

“Я гарантую, що буде зроблено багато помилок, враховуючи витонченість національних держав, які ховають свої руки у цій діяльності,” “Мене дуже сильно турбує, що станеться, якщо приватному сектору дати можливість вільно захищати себе в будь-який спосіб, тому що багато речей можуть піти не за планом, на мою думку,” – сказав він у лютому.

ФАЗА АТРИБУЦІЇ НА ОСНОВІ ВІРУСУ – КЕЙСУ В ЯПОНІЇ

Японію вважають країною, котру найбільше атакують хакери. Урядові офіси та приватний сектор у минулому постраждали від безлічі кібератак. У зв’язку із цим уряд Японії вирішив почати розробку програмного забезпечення, яке преса помилково визначила як «кібер зброю». Воно здатне відстежувати, ідентифікувати та пом’якшувати атаки в режимі онлайн.

Як зазначило видання The Daily Yomiuri, дослідження цієї програми нового типу розпочалося у 2008 році. Вона являє собою інноваційну технологію, котра намагається автоматично відстежити та знешкодити джерело кіберзагрози.

В реальності ж, згідно заяв уряду, це програмне забезпечення є комп’ютерним вірусом, розробленим компанією Fujitsu для уряду Японії, і воно здатне відстежити джерела кібератак шляхом реверсії шляху, який залишили зловмисники після втручання у кіберпросторі. Фактично агент власноруч інфікує численні точки доступу, що були використані під час атаки, і тоді з високим рівнем точності він може локалізувати джерело наступу, як сталося з атаками Distributed Denial-of-Service (DDoS).

Цей вірус, на думку японського уряду, є унікальним і інноваційним. Він здатний нейтралізувати атаки та зібрати величезну кількість інформації з вражених систем. Це дані, які також можуть бути використані для наповнення профілями картотеки хакерів та запобігання наступним атакам. На думку експертів з кібербезпеки, ця система, за умови майбутнього її розвитку, зможе діяти превентивно, інфікуючи ті системи, котрі найбільш ймовірно будуть використані тими ж самими хакерами у майбутніх наступах.

Коментуючи цей проект, Мотохіро Цучія, професор Університету Кейо та член урядової комісії з питань політики захисту інформації, сказав, що Японії слід посилити «розробку зброї проти кібератак».

Дослідники одностайно відзначають той факт, що Японія є не унікальною державою, що працює над таким проектом. Інші уряди також інвестують кошти у дослідження для розробки наступальних інструментів нового покоління.

Основне питання, яке обговорюється щодо Наступального підходу, полягає в тому, що програми та програмне забезпечення можуть змінити природу зараженої системи, зловживаючи її ресурсами, якщо вони використовувались для розслідування, що є дією, яка не приймається основними експертами з безпеки.

«ВРАЗЛИВОСТІ НУЛЬОВОГО ДНЯ» - ЯК КУЛІ

Не зважаючи на те, що у приватному секторі концепція Наступального підходу у кібербезпеці є відносно новою, ситуація в урядовому та військовому секторах є абсолютно протилежною. Наступальна кібербезпека довший час була предметом дебатів, керівники країн довго обговорювали цей підхід, намагаючись у різний спосіб розробити системи, котрі можуть реагувати, якщо атаку визначено.

Одними з головних частин розробки цих рішень є вразливі місця нульового дня. Уряди США та Китаю, є головними покупцями рішення вразливостей нульового дня згідно з нещодавнім звітом, опублікованим Reuters. Знання про слабке місце, що виникло лише сьогодні, дає хакеру гарантію успіху. Спонсоровані урядами хакери та кіберзлочинці вважають вразливості нульового дня дорогоцінним ресурсом, навколо якого зараз будується ринок. Такі вразливості можуть використовуватися в якості основного компоненту кіберзброї або можуть служити цілям кібершпіонажу.

Ройтер заявили, що уряд США є «найбільшим покупцем на сірому ринку, де хакери та фірми, котрі працюють у галузі кібербезпеки, продають інструменти для втручання в комп'ютери". Преса повідомила, що уряд США зокрема, а також його розвідувальні агенції та Міністерство оборони «витрачають так багато на купівлю інформації про слабкі місця у комерційних комп'ютерних системах, та про те, як можна цією інформацією скористатися, що вони таким чином перевертають світові дослідження в галузі кібербезпеки з ніг на голову." Це новий метод конкуренції з опонентами у кіберпросторі.

Китайський та американський уряди вклали значні кошти у створення нових кіберодиниць, але згідно інформації розвідувальних агенцій, Наступальний підхід визнано необхідним для збереження безпеки у кіберпросторі, за умови дотримання меж захисного підходу.

Керівник NSA Кейт Александер повідомив на Конгресі, що уряд США витрачає мільярди доларів щороку на «кіберзахист та створення складної та сучасної кіберзброї». Це призвело до появи «понад десятка наступальних кіберодиниць, розроблених для атаки закордонних комп'ютерних систем при необхідності.»

Чарлі Міллер, дослідник, що працює у галузі кібербезпеки, який раніше співпрацював із NSA, підтвердив у Твітері підхід Наступальної програми у кібербезпеці:

"Лише ті люди, котрі за це платять, є на боці наступу,"

Зростаючий ринок вразливостей нульового дня збільшується за рахунок інтенсивних зусиль з боку талановитих хакерів, котрі використовують новий метод монетизації своїх знань щодо вразливих місць певних систем, особливо коли йдеться про продукти широкого вжитку.

Як заявила агенція Ройтер, підрядники міністерства оборони, розвідувальні агенції «витрачають щонайменше десятки мільйонів доларів на рік лише на дослідження», щоб переконатися в тому, що витрати дійсно спрямовано на нові методі роботи в галузі кібербезпеки. Як було заявлено раніше, ринок вразливостей нульового дня є дуже складним через високу «тлінність» товару, враховуючи деякі ключові моменти такого складного бізнесу:

- ***Складності у знаходженні покупців та продавців*** *– Це закритий ринок, на який немає загального доступу. Знайти покупця чи ідентифікувати продавця є критично складно*.

- **Перевірка надійності покупця** *– Невелика кількість надійних посередників, здатних знайти покупця, спонукає шукача розповідати про відкриття багатьом особам, намагаючись знайти покупця з очевидними ризиками.*

- **Цінність неможливо продемонструвати без втрат** *– Однією з найбільш неймовірних проблем, з якими шукач зіштовхується при пошуку можливості продати інформацію про вразливості або експлойт нульового дня, що виник лише сьогодні, це доведення цінності своєї інформації без її розголошення. Єдиним способом, як можна довести цінність інформації, є її розкриття або демонстрація певної її частини. Очевидно, що розкриття інформації до моменту продажу є дуже небажаним, оскільки ставить шукача у становище, коли він може втратити свою інтелектуальну власність без компенсації.*

- **Ексклюзивність прав** *– Остання перепона полягає у ексклюзивності прав на інформацію. З метою отримання якнайбільшої вигоди шукач повинен бути згідний продати усі права на інформацію покупцеві. Однак покупець жодним чином не може захистити себе від того, що шукач може продати цю ж інформацію багатьом зацікавленим сторонам, чи навіть оприлюднити її після продажу.*

Чинний на даний момент підхід до роботи із вразливостями нульового дня полягає у купівлі експлойтів. Для зменшення ймовірності того, що вони можуть бути також куплені опонентами уряду, такими як диктатори чи злочинці, численні фірми, що працюють у галузі кібербезпеки, продають так звані підписки на експлойти, котрі гарантують певну їх кількість на рік.

У звіті Ройтер також ідеться про участь представників уряду у кампаніях з прихованого незаконного стеження та шпіонажу для уряду з очевидною метою закупівлі нових технологій для здійснення розвідувальних дій у кіберпросторі, в тому числі і з використанням вірусних атак, що вражають мережеві системи.

У багатьох випадках ефективність цих експлойтів нульового дня є досить тривалою, оскільки через відсутність оновлень цільових систем, типові атаки нульового дня мають середню тривалість 312 днів. Після публічного оприлюднення спостерігається зростання обсягу таких атак у 5 разів.

Ройтер повідомляє, що переглянутий каталог продукції одного з підрядників містив різні програми для кібершпигунства. У статті йдеться про продукт як "перетворити будь-який

айфон на підслуховуючий пристрій", а інший "являв собою систему для встановлення шпигунського програмного забезпечення на принтер або інший пристрій і переміщення цього шкідливого програмного забезпечення на найближчий комп'ютер за допомогою радіохвиль, навіть коли прилади ні до чого не підключені.

У Наступальному підході до кібербезпеки вразливості нульового дня вважаються кулями, що б'ють на ураження. Їхня вартість залежить від багатьох факторів, таких як ціль продукту, рівень його розсіювання, і звісно масштаби використання. «Сьогоднішній» експлойт може бути продано урядовій організації за ціною, що у 100 разів перевищує ціну для приватного покупця.

ХАКЕРСЬКИЙ БАНК У ПРИВАТНОМУ СЕКТОРІ

Приватний сектор щодня страждає від атак з боку конкурентів, хактивістів та кіберзлочинців. Теперішній підхід передбачає підтримання «захисної позиції» в очікуванні, коли уряд та правоохоронні органи звернуть увагу на проблему, з надією, що злочинців буде відстежено та упіймано.

На жаль, така політика довела свою неспроможність кинути виклик динамічним загрозам, інтенсивність та складність яких зросла. Після другого відхилення акту CISPA, приватний сектор почав думати про більш агресивний підхід до кібербезпеки.

"Це правильно – жалітися на крадіжки (інтелектуальної власності) через дипломатичні канали, але у якийсь момент ви повинні перестати жалітися і висунути офіційне звинувачення," наполягав голова комітету Сенатор Шелдон Уайтхауз, посилаючись на твердження генерального директора NSA пана Александера, котрий відзначив, що кіберзлочинність призвела до найбільшого перерозподілу статків та знань."

«Не схоже на те, що ми наближаємося до вирішення цієї проблеми" – заявив Стюарт Бейкер, партнер юридичної компанії Steptoe & Johnson, порівнявши теперішній підхід із стримуванням вуличної злочинності «через прохання пішоходів купувати собі щороку нові бронежилети». «Я не закликаю до взяття закону у свої руки та лінчування. Але ми повинні знайти шлях, як дати фірмам, які проводять такі дослідження, можливість вийти за межі їхніх мереж.» «Якщо ми цього не зробимо, ми ніколи не дістанемося до суті більшості з цих атак» - сказав він.

Основні контрзаходи, до яких можуть вдатися приватні організації, полягають у використанні шпигунського програмного забезпечення для стеження за системою, що підозрюється у хакерстві. Саме так діють правоохоронні органи згідно рішень суду. Використання шкідливих програм не обмежується відстежуванням подій в Інтернеті, подібні засоби використовуються також для інфікування мобільних пристроїв для шпигування за їхніми власниками. Мобільний шпіонаж є останньою межею у стеженні. При втручанні у пристрій стає можливим відстежування потрібного профілю, аналіз пошукових активностей, доступ до контактів та повідомлень, слухання середовища та спілкування через вмонтований мікрофон або доступ до зображень, зроблених камерою.

Іншою варіантом для приватних компаній є спроба створити інфраструктуру "honeypot" (пастка для хакера), щоб ловити зловмисників у поєднанні з іншими наступальними

методами, такими як “фіш-фішинг”. Таким чином приватні фірми можуть спробувати скомпрометувати інфраструктуру зловмисника за допомогою шкідливого коду, щоб відновити вкрадені дані або зробити їх непридатними для використання.

Однією з приватних індустрій, котра продемонструвала найвищий рівень схильності до Наступального підходу у кібербезпеці є індустрія розваг. Вона є жертвою незаконного розсилання файлів, яке порушує авторські права на цифрові матеріали. У вічній боротьбі проти піратства кіберзлочинці були на крок попереду. Тому компанії цього сектору зараз переглядають можливості атакування піратів спеціально розробленими для цього інструментами.

У нещодавному звіті Комітету з питань крадіжок американської інтелектуальної власності використання вірусних програм було визнано дозволеним заходом безпеки для боротьби з піратством. У документі пропонується багато методів боротьби з піратством цифрового вмісту, захищеного авторським правом, включаючи зараження комп'ютерів шкідливим програмним забезпеченням, яке може його знищити. Іншою можливістю є встановлення вірусної програми для відстежування мереж піратів, шпигування за їхніми діями та записування уражених IP адрес. У багатьох випадках використані для піратства машини не є власністю хакерів, а у інших випадках злочинці вкрали IP адреси, щоб використати їх у своїй незаконній діяльності. Моніторинг цієї інформації дозволяє індустрії відстежувати злочини та географічне розташування піратів.

Відомо, що китайські хакери є найбільш агресивними та наполегливими. Група, що працювала над згаданим вище звітом про роль Китаю у викраденні торгівельних секретів американських компаній пропонує в якості сумнівного методу захисту… хакерську атаку у відповідь

“Без нанесення пошкоджень власній мережі порушника, компанії, що піддаються кібератакам повинні бути здатними забрати свої електронні файли назад або запобігти використанню украденої в них інформації,”

“Ці атаки, здійснювані приватними компаніями, підвищуватимуть для крадіїв вартість їхніх дій, потенційно відлякуючи їх і примушуючи не ставити такі дії на перше місце,” “ Лише тоді, коли небезпека проникнення в мережу компанії та вилучення комерційної таємниці перевищує винагороду, така крадіжка зменшиться від загрози до неприємності». Зазначається у звіті.

Потреба відмовитися від неефективних традиційних контрзаходів у кібербезпеці, таких як брандмауери та антивірусні програми, штовхає спільноту, котру турбує кібербезпека, спонукає спільноту з кібербезпеки оцінити концепцію «активної оборони», за якою приватні особи проникають у комп’ютер хакера та вилучають їхні ж викрадені файли.

Стюарт Бейкер, колишній секретар Департаменту державної безпеки, відзначив важливість впровадження агресивного підходу до боротьби з закордонними хакерами. У своєму блозі Бейкер запропонував певні методи переслідування крадіїв, наприклад «зараження» інструментів дистанційного доступу (RAT), котрі хакери використовують для зловживань у комп’ютерних мережах.

“Це лише питання часу, коли контр- хакерська атака стане можливою,” написав Бейкер. “Справжнє питання полягає в тому, коли вони стануть законними.”

Під час останньої конференції RSA головні посадовці у галузі інформаційної безпеки (CISOs) та провідні фахівці з безпеки брендових компаній та урядових служб обговорювали можливості впровадження Наступального підходу у кібербезпеці. Джеф Бардін, головний стратег компанії Treadstone 71 заявив:

“Хакерство та руйнування бізнесу досягло найбільших масштабів за усі часи і більше не може бути ігнороване,” “Ми хочемо дати зрозуміти своєму ворогові, що якщо він атакує компанію, за це буде розплата.”

Дослідження, проведене компанією Wisegate показало, що 40% опитаних керівників з галузі кібербезпеки зазначили, що «слід хоча б обговорити здійснення контратак», 30% були неготові через те, що «надто багато юридичних та етичних моментів» є невирішеними. І 58% навіть ніколи не починали обговорювати політику «ударів у відповідь».

“Ми повинні почати думати, як наші вороги, шукати різні підходи та техніки, щоб збити хакерів з пантелику,” “Ми користуємося послугами етичних, тобто «білих» хакерів для перевірки надійності наших захистів, і ми наближаємося до того, щоб наші програми працювали так, наче ми намагаємося проникнути у систему. Нам потрібно прийняти такий спосіб мислення та зосередитися на ризиках.”- сказав Тім МакКрейт, учасник Wisegate, CISO уряду Альберти, Канада.

Наступальні тактики у кібербезпеці мають етичні та юридичні невирішені питання. Також слід врахувати те, що економічна складова впровадження агресивного підходу є несумісним з економічним станом більшості компаній.

Цей підхід має незаперечний побічний ефект, коли потерпілі, є вони винними у піратстві чи ні, отримають вірус на свій комп’ютер, і це матиме серйозні наслідки. Давайте візьмемо до уваги користувача, котрий має деякий піратський контент на своєму ПК, і тому може бути звинувачений у піратстві. В такому випадку його комп’ютер може бути пошкоджено під час законної контратаки.

В тому ж документі обговорюються можливі ситуації, коли хакерська атака у відповідь може завдати шкоди комп’ютерним системам невинних користувачів Інтернету. Також потрібно врахувати, що хакери для проведення своїх атак використовують комп’ютери третіх осіб, котрі про це не знають. Тим не менше, Джеймс Льюіс, старший науковий співробітник Центру стратегічних та міжнародних досліджень, не погоджується з таким підходом, оскільки ініціативи приватних компаній по всьому світі щодо зламу хакерів можуть порушувати міжнародне законодавство та втручатися у відносини між державами.

“Можемо створити ризик того, що якийсь ідіот у компанії вчинить помилку і спровокує побічне пошкодження, яке втягне нас у війну з Китаєм.” – сказав Льюіс.

У звіті написано, що комісія «неготова підтримати» проведення хакерських атак у відповідь через потенційну можливість побічних пошкоджень або зловживань, а також, що «перед продовженням руху вперед потрібне проведення подальших робіт та досліджень».

У звіті зазначається, що комісія «не готова підтримати» хакерство, через потенційну можливість заподіяння шкоди або зловживання, додаючи, що «перш ніж рухатися вперед, необхідно провести подальші роботи та дослідження.

БЕЗКОШТОВНІ ЗАСОБИ АКТИВНОГО ЗАХИСТУ

В той час як уряди та приватні компанії ведуть дебати щодо Наступального підходу до кібербезпеки, перехід до практики є дуже швидким. Набір інструментів із відкритими джерелами інформації стає доступним на публічному домені для приватних компаній, котрі вирішили переслідувати порушників.

Модель «активного захисту» набирає численну підтримку у приватному секторі, і це підштовхує спеціалізовані компанії, такі як CrowdStrike, HBGary та Mykonos до складання комерційної пропозиції.

Основами методів активного захисту є все від інструментів, схожих на «пастки», щоб спіймати потенційних зловмисників та простежити за ними. Здатність привернути увагу хакерів, вивчаючи їхні тактики, є надзвичайно важливою. З боку захисту існують різні опції, наприклад, компанія може безпосередньо атакувати підозрюваних у злочині, який їм загрожує, або може вибрати інший шлях: обмежити свій активний захист, заважаючи хакерам, наприклад, підриваючи їхню розвідувальну діяльність і навіть точно визначаючи їхнє фізичне розташування.

Дмітрій Альперович, співзасновник та технічний директор компанії CrowdStrike відзначає, що активний захист передбачає дії, спрямовані на визначення загроз у реальному часі та ідентифікацію особи зловмисника, поширення неправдивої інформації та руйнування систем нападника як крайній захід.

“Захисні техніки у чистому вигляді… не будуть працювати ефективно, якщо ворог має високий рівень професіоналізму і рішуче налаштований проникнути у систему, він знайде варіант як це зробити. Тож вам потрібно знайти інші способи їх стримувати. Це передумова активного захисту ", - зазначає Альперович.

Іншою можливістю є проведення розвідувальної діяльності серед потенційних зловмисників, намагаючись ідентифікувати шляхи їхніх дій та цілі/інформацію, яку вони використовують. Фірма CrowdStrike, що працює у галузі кібербезпеки, планує випустити різноманітні засоби для активного захисту. Компанія анонсувала розповсюдження поліморфної програми для аналізу та декодування, а також безкоштовних інструментів для стеження за атакувальниками через Tor.

Цей ринок є дуже плідним. Експерти з кібербезпеки Джон Странд, Пол Азадурян, Етан Робіш та Бенджамін Донеллі пропонують набір інструментів Linux distro для захисту через напад.

ADHD є класифікацією засобів активного захисту із попередньо розробленими інструментами для контратак, що можуть бути використані для втручання в систему з допомогою відбитків пальців атакувальника.

Дистрибутив включає наступні інструменти захисту:

- *Артилерія (Artillery)*

- *Капкан для ведмедя (BearTrap)—відкриває тригерні порти власника системи для привернення уваги хакерів, автоматично помічає їх та заносить до чорного списку.*

- *Зняття маски (Decloak) – для ідентифікації реальної IP адреси користувача, навіть через проксі.*

- *Медоїд (Honey Badger) – для визначення фізичного розташування користувача.*

- *Нова (Nova) (Заплутування мережі та віртуалізована система анти-зондування) – визначає проведення розвідувальних робіт в мережі та надає хакеру неправдиву інформацію щодо кількостей та типів систем у цільовій мережі, використовує мережу віртуалізованих пасток. Нова не використовує визначення вірусів на основі підпису, натомість вона створює системи пасток для атакувальника, щоб він з ними взаємодіяв, та попереджає системного адміністратора про підозрілу активність.*

- *Павукова пастка (The Spidertrap) – є набором вебсторінок, котрі можуть умисно або неумисно бути використані, щоб примусити пошукову програму або бота здійснити нескінченну кількість запитів, або призвести до руйнування пошукової програми, якщо вона не якісно сконструйована.*

- *Жучок (Web Bug Server) – вставляє системного «жучка» всередину документу, який може бути використаний для приховування HTML коду, що неодмінно викриє IP адреси та іншу інформацію про хакера.*

“Ми хочемо змінити рахунок на нашу користь, не вдаючись до атак у відповідь,” – відмічає Странд. Експерт заперечує легітимність таких інструментів, вважаючи, що пропозицію адресовано експертам з кібербезпеки, котрі підтримують ідею законного включення їх у використання. «Люди запитують: «Чи це законно?» Ми можемо відповісти: «Майже. Дуже близько.»

“Ми не можемо проникати у їхні комп’ютери та копирсатися у їхніх файлах, навіть якщо вони є поганими хлопцями або злочинцями. Вони мають право на захист своєї інформації, і ми намагаємося не перетинати цю межу” – зазначив Странд.

МАТЕРІАЛИ

1. Модуль_3_Whitepaper1-7_Secrets_of_Offensive_Security
2. Модуль_3_Whitepaper2-An-introduction-to-ODS-Strategy-whitepape