УДК 004.778
V. Lakhno [1][0000-0001-9695-4543], **A. Blozva** [2][0000-0002-4377-0916]
D. Kasatkin [3][0000-0002-2642-8908], **Mazin Al Hadidi** [4][0000-0001-9173-4023]
[1] Professor, National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
[2] National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
[3] National University of Life and Environmental Sciences of Ukraine, Department of Computer systems and networks, Kyiv, Ukraine,
[4] Al-Balqa' Applied University | BAU Department of Computer Engineering,

РОМБОВИДНА МОДЕЛЬ ЛАНЦЮЖКУ КІБЕРЗЛОЧИНУ

Анотація У даній публікації розглянуто ланцюжок кіберзлочину, етапи його виконання та ромбовидну модуль реагування на втручання у інфраструктуру компанії. Модель дає можливість швидко і адекватно оцінити загрозу та виконати превентивні дії по захисту комп'ютерної мережі.
Ключові слова: Вбивчий ланцюжок, ромбовидна модель, кібезрбезпека, кіберзлочинці.

Фахівці в області кібербезпеки знають, що хакери безперервно розробляють нові методи. Постійно з'являються нові загрози, які необхідно виявляти і стримувати з тим, щоб ресурси і зв'язок відновлювалися якомога швидше. Для отримання прибутку багато хакерів не гребують такими методами, як вимагання, шахрайство і крадіжка персональних даних. Необхідність постійно захищатися від цих атак привела до створення декількох моделей реагування на інциденти.

Ланцюжок кіберзлочину була розроблена Lockheed Martin для виявлення і запобігання вторгнень кіберзлочинців. Як видно на малюнку, ланцюжок кіберзлочину складається з семи кроків, які допомагають аналітикам зрозуміти методи, інструменти та процедури хакерів. Мета при реагуванні на інциденти полягає в тому, щоб виявити і зупинити атаку на якомога більш ранньому етапі ланцюжка кіберзлочину. Чим раніше буде зупинена атака, тим менший збиток буде завдано і тим менше хакер зможе дізнатися про цільову мережі. Ланцюжок кіберзлочину вказує, які дії повинен виконати хакер для досягнення своєї мети.

Якщо хакер буде зупинений на будь-якому етапі, ланцюжок атаки буде розірвано. Розрив ланцюжка означає, що захиснику вдалося успішно відбити вторгнення хакера. Зловмисники досягають успіху, тільки якщо їм вдається дістатися до сьомого етапу.

Розвідувальна атака: зловмисник виконує дослідження, збирає аналітику і вибирає цілі. За цими даними хакер зможе визначити, чи варто братися за атаку. Будь-яка загальнодоступна інформація може допомогти визначити, що, де і як атакувати. Існує великий обсяг загальнодоступної інформації, особливо якщо мова йде про великих організаціях, включаючи новинні статті, веб-сайти, участь в конференціях і загальнодоступні мережеві пристрої. Постійно зростаючі обсяги інформації про співробітників можна отримати в соціальних мережах.

Зловмисник вибирає цільові об'єкти, які були забуті або не були захищені, оскільки ймовірність проникнення або злому цих об'єктів вище. Всі інформація, отримана зловмисником, аналізується з метою визначити її важливість, а також зрозуміти, розкриває вона можливі додаткові джерела доходу від атаки.

Мета наступного етапу полягає в розробці зброї проти певних цільових систем, наявних в організації, з використанням інформації, отриманої за допомогою розвідувальної атаки. Для розробки цієї зброї конструктор використовує уразливості ресурсів, які були виявлені, і вбудовує їх у засіб, який можна розгорнути. Після застосування цього засобу очікується, що хакер досягне своєї мети щодо отримання доступу до цільової системи або мережу, через що працездатність цієї системи (або всієї

мережі) знижується. Зловмисник продовжить вивчати мережу і захист ресурсів з метою виявлення додаткових слабких місць, отримання контролю над іншими ресурсами або розгортання нових атак.

Вибрати зброю для атаки нескладно. Зловмиснику необхідно подивитися, які атаки можна застосувати для виявлених вразливостей. Існує безліч готових атак, які добре протестовані. Одна з проблем полягає в тому, що, оскільки ці атаки так добре відомі, швидше за все, захисники також з ними знайомі. Часто більш ефективним є використання поки ще невідомої атаки, що дозволяє вислизнути від інструментів виявлення. Зловмисник може прийняти рішення розробити власну зброю, яке буде спеціально призначене для уникнення інструментів виявлення, використовуючи для цього отриману ним інформацію про мережі і системах.

На етапі доставлення, зброю передаються в цільову систему за допомогою вектора доставки. Робитися це може за допомогою веб-сайту, знімних носіїв USB або вкладення в електронне повідомлення. Якщо зброя не буде доставлено, атака закінчиться невдачею. Для підвищення шансів доставки корисних даних зловмисник буде використовувати кілька різних способів, в тому числі шифрування зв'язку, надання коду виду легітимною програми або маскування коду. Датчики безпеки настільки досконалі, що вони неодмінно визнають код шкідливим, якщо не внести в нього зміни, що дозволяють уникнути виявлення. Код може бути змінений так, щоб виглядати невинним, при цьому він продовжить виконувати необхідні дії, навіть не дивлячись на те, що на його виконання може вимагатися більше часу.

Після того як зброя була доставлена, зловмисник з його допомогою зламує систему в уразливому місці і отримує контроль над цільовою системою. Найбільш поширеними цілями експлойтів є додатки, уразливості операційних систем і користувачі. Організатору атаки необхідно використовувати експлойт, який дозволяє домогтися потрібного йому ефекту. Це дуже важливо, оскільки, якщо задіяти неправильний експлойт, очевидно, що атака не спрацює, а небажані побічні ефекти, серед яких відмова в обслуговуванні або численні перезавантаження системи, привернуть непотрібну увагу, в результаті чого аналітики з кібербезпеки зможуть легко отримати інформацію про атаку і наміри хакера.

Саме під час ін’єкції хакер створює лазівку в систему, щоб забезпечити постійний доступ до мети. Для того щоб зберегти цю лазівку, важливо, щоб віддалений доступ ніяк не виявляв себе для аналітиків з кібербезпеки або користувачів. Спосіб доступу повинен залишитися непоміченим після сканування, виконуваного засобами антивірусів і перезавантаження комп'ютера, необхідної, щоб лазівка заробила. Цей постійний доступ також може забезпечувати автоматичну зв'язок, що особливо ефективно, коли для управління ботнетом необхідно кілька каналів зв'язку.

Ціль наступного етапу полягає у встановленні управління та контролю (CnC або C2) над цільовою системою. Зламані хости зазвичай виводяться з мережі і підключаються до контролера в Інтернеті. Це пов'язано з тим, що здебільшого шкідливого ПО потрібне ручне взаємодія для ексфільтрації даних з мережі. Останній етап ланцюжка кіберзлочину описує досягнення зловмисником поставленої спочатку мети. Це може бути крадіжка даних, проведення DDoS-атаки або використання зламаної мережі для створення і розсилки спаму. На цьому етапі зловмисник вже глибоко укорінився в системі організації, приховуючи свої дії і замітаючи сліди. Видалити хакера з мережі надзвичайно складно.

Зловмисники не діють в рамках тільки однієї події. Навпаки, події об'єднуються в пов'язану ланцюг, в якій кожна з них має бути успішно завершено, і тільки після цього можна переходити до наступного події. Цей потік подій можна зіставити з ланцюжком кіберубійства, яка розглядалася раніше в цій главі.

Наведений нижче приклад (Рис.1) ілюструє весь процес дії зловмисника у міру того, як він проходить по ланцюжку кіберзлочину в вертикальному напрямку, використовує зламаний хост, щоб переміститися по горизонталі до іншій жертві, а потім почати інший потік дій.

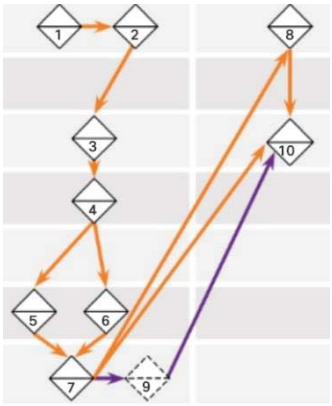

Рис 1. Ромбовидна модель ланцюжку кіберзлочину

Зловмисник виконує в Інтернеті пошук компанії-жертви Gadgets, Inc., отримуючи більшу частину результатів домен цієї компанії gadgets.com. Зловмисник використовує знову виявлений домен gadets.com для виконання нового пошуку, знаходить публікації на форумі від користувачів, які стверджують, що вони є мережевими адміністраторами gadget.com. У профілях цих користувачів є їх адреси електронної пошти. Зловмисник відправляє мережевим адміністраторам gadget.com фішингові повідомлення електронної пошти з вкладеним трояном. Один адміністратор (NA1) gadget.com відкриває шкідливе вкладення. Воно виконує прикладений експлойт, забезпечуючи виконання програмного коду. Зламаний хост користувача NA1 відправляє повідомлення HTTP Post на IP-адресу, реєструючи його в контролері CnC. Зламаний хост користувача NA1 отримує відповідь HTTP. Відтворення програмного коду дозволяє дізнатися, що під шкідливі програми задані і інші IP-адреси, які є резервними на випадок, якщо перший контролер не відповість. Через відповідь HTTP-повідомлення CnC, відправлене на хост NA1, шкідлива програма починає діяти як проксі для нових підключень TCP. Через проксі, встановлений на хості NA1, зловмисник виконує веб-пошук "most important research ever" (найважливіше дослідження, яке коли небудь проводилось) і знаходить другу жертву, Interesting Research Inc. Зловмисник шукає в списку контактів електронної пошти NA1 будь-які контакти з Interesting Research Inc. і виявляє контакт директора з наукових досліджень Interesting Research Inc. Директор з наукових досліджень Interesting Research Inc. отримує адресний фішингових електронного листа з електронної пошти NA1 в Gadget Inc., відправлене з хоста NA1, з тим же вмістом, яке спостерігалося в подію 3. Наразі зловмисник скомпрометував вже дві жертви, від яких можна запускати додаткові атаки. Наприклад, зловмисник міг би знаходити потрібні адреси електронної пошти старшого наукового співробітника, який став би додаткової потенційною жертвою. Крім того, зловмисник також може налаштувати інший проксі-сервер для ексфільрації всіх файлів старшого наукового співробітника.