Рудзей В.М., магістрант,
Грабар О.І., к.т.н., доц.,
Житомирський державний технологічний університет

APT-АТАКИ

Проблема кібератак носить глобальний характер і досить гостро постає у сучасному інформаційному суспільстві. Кібератаки за досить короткий проміжок часу перетворилися з поодиноких випадків на один з головних бізнес-ризиків для організацій у всьому світі. У глобальному контексті провідні держави світу все більшої уваги приділяють захисту критичних інформаційних ресурсів та можливості впливу на інформаційні ресурси інших держав. Кібератака у вузькому сенсі - замах на інформаційну безпеку комп'ютерної системи.

Що таке APT-атака? APT - скорочення від Advanced Persistent Threat (складна постійна загроза або цільова кібератака), з одного боку, складна постійна загроза (APT) є високоточної кібератакою. З іншого боку, APT можна назвати хакерську угруповання, спонсоровану державою, організацією або людиною, що оплачують цільову атаку. Кінцева мета атаки - отримання доступу до машини зберігає секретну, конфіденційну або будь-яку цінну інформацію, але при цьому «вхідний точкою» може бути комп'ютер не зберігає будь-якої цінної інформації, що знаходиться в одній мережі/підмережі з цільової машиною. Таким комп'ютером може виявитися система автоматизації електронапруги, комп'ютер рядового співробітника, або навіть мобільний телефон прибиральниці.

Будь-який користувач, що підключився до Інтернету, є потенційною мішенню.

Почнемо з того, що apt-атака має наступні етапи:

- Збір інформації - атакуюча угруповання шукає і аналізує сайти, домени, інформацію про співробітників, акаунти співробітників, інформацію про партнерах, технічну документацію та іншу загальнодоступну інформацію.
- Дослідження мережі - етап включає в себе складання карти мережі, запис IP- адрес серверів, маршрутизаторів, комутаторів, DNS-серверів, пошук VPN тунелей, ханіпотов, проксі і т.д.
- Пошук вразливостей - етап включає в себе пошук вразливостей на серверах, маршрутизаторах і т.д.
- Експлуатація вразливостей - зловмисники зламують сервер, маршрутизатор або інше комп'ютерне обладнання, що знаходиться в мережі або підмережі цільової машини.
- Злом акаунтів співробітників - проводиться в основному для фішингу, актуально для збору інформації, логінів і паролів, особливо актуально, коли необхідно уникнути виявлення системами вторгнення, а також коли не знайдений вразливостей в мережевій інфраструктурі.
- Фізичне проникнення - використовується досить рідко, в тому випадку, якщо шукана інформація не має електронного варіанту або комп'ютер зберігає секретну інформацію ізольований від мережі, а так само з метою фізичного доступу до комп'ютера.
- Закріплення в системі - зловмисник закріплюється в системі для довгострокового доступу до інформації.

Потрібно враховувати і розуміти той факт, що повної захищеності не може бути, особливо у великій інфраструктурі. Можна сказати що мережа - це поле бою, на якому перемагає той, хто краще знає систему.

Активне застосування хакерських APT-атак, викликає занепокоєння у фахівців із захисту інформації. 16 фахівців із захисту інформації, які працюють у великих американських компаніях, підготували доповідь «Час переважання APT», в якому описуються проблеми і завдання, з якими стикаються великі компанії і організації. Хакери використовують APT для злому інформаційних систем різних компаній і розкрадання особистих даних. Жертвами APT ставали компанії Google, RSA Security, Epsilon, Citigroup, The Washington Post і національні лабораторії Міненерго США - Oak Ridge і Pacific Northwest. Директор з інформаційних систем і безпеки eBay Дейв Каллінейн (Dave Cullinane) заявив: «Немає жодних сумнівів, що атака APT, метою якої часто є розкрадання грошей, займає перше місце в списку всіх кібератак».

Фахівці радять захисникам даних охороняти активи, які є найбільш цінними для компанії або організації. Автори доповіді також рекомендують забезпечити високорівнева збір і аналіз інформації, використовувати засоби інтелектуального моніторингу, проводити ефективну політику навчання персоналу. Останнє не менш важливо, так як, кінцеві користувачі найчастіше піддаються атакам шкідливого ПЗ і стають жертвами цільового фішингу. «Саме тому, зараз виникла необхідність в розробці нового антивірусного ПО для більш швидкого виявлення фішинг-атак», - зазначає Каллінейн.

Отже, у всіх випадках застосовується експлойт, який отримує контроль над ПК жертви і встановлює вихідну мережеву комунікацію до C&C-серверу, який далі передає шкідливе ПЗ, яке виконує найрізноманітніші дії.