KhNUIAIR(Institutional Repository of KhNUIA)

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 004.056.53

Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ ПОШИРЕННЯ КІБЕРЗАГРОЗ

Інтернет-речі (IoT)

Актуальність проблеми незахищених IoT-мереж невпинно зростає протягом останніх кількох років. Тенденція стосується безлічі пристроїв, задіяних в споживчих і промислових цілях, що підключаються до мережі без дотримання належних заходів безпеки.

В останні роки хакери почали використовувати більшу кількість вразливостей пристроїв для створення масштабних ботнетів з тисяч і мільйонів заражених пристроїв: маршрутизаторів, Smart-TV тощо. Різноманітні Інтернет-речі вже давно перетворилися в улюблену ціль атак хакерів. Їм достатньо

придбати будь-якої пристрій і самостійно вивчити, як він захищений. Якщо його зламати, то система захисту не може бути оновлена оперативно. Використовуючи один пристрій, хакеру дуже легко потрапити всередину мережі, яка може містити цікаву для них інформацію: банківські реквізити, медичні записи, корпоративні дані.

Більшу частину пристроїв для Інтернет-речей виробляють співробітники стартапів, які використовують апаратне і програмне забезпечення зі сторони, придбане у постачальника і недостатньо захищене від зломів. На створення більшості IoT-девайсів було витрачено мінімум грошей, тому не дивно, що їх легко зламати.

З ростом кількості пристроїв і датчиків, підключених до мережі, зростає і кількість кіберзагроз. Наприклад, розумний холодильник став частиною бот-мережі і почав розсилати спам; розумна кавоварка виявилася причиною атаки на індустріальні мережі з подальшим зараженням комп'ютерів для моніторингу технологічного процесу вірусом-здирником.

При проектуванні нових технологій слід брати за основу безпеку. Однак, часом розробники, навмисно або ненавмисно, залишають недокументований канал, який не просто збирає інформацію про застосування пристрою, але і дозволяє проникати в особистий простір кінцевого користувача.

Немає сумнівів в тому, що мережі пристроїв Інтернет-речей (IoT), заражених шкідливими програмами, стануть однією з найпоширеніших у майбутньому проблем забезпечення кібербезпеки.

Кіберзагрози для розумних міст

Термін «розумне місто» зазвичай застосовується по відношенню до міст, які активно використовують Internet-технології безліччю різноманітних способів, щоб більш ефективно функціонувати і відповідати потребам своїх жителів.

Серед мотивів зловмисників, які спонукають їх атакувати розумні міста: бажання перевірити свої хакерські здібності, крадіжка грошей і особистих даних користувачів, а також корпоративної інформації.

Серед цілей хакерів при атаках на критичну інфраструктуру розумних міст: навмисна організація ДТП, організація перебоїв в подачі електроенергії; крадіжка особистої інформації користувачів, крадіжка електроенергії; перехоплення управління пристроями і системами; порушення транспортної системи та інші.

KhNUIAIR(Institutional Repository of KhNUIA)

Атака на розумні міста проходить в чотири етапи: статистичний аналіз (аналіз механізмів і систем, чиї уразливості можуть бути використані), сканування (виявлення цілей і точок входу), збір інформації (отримання даних для доступу шляхом фішингу тощо здійснення самої кібератаки.

Вразливим місцем розумних міст є в тому числі некоректне використання розумних технологій на його території.

Перехоплення рахунку (Account takeover)

У разі вчинення крадіжки персональних даних (identity theft), метою шахраїв зазвичай є особисті дані, такі як імена, поштові адреси і адреси електронної пошти, а також дані кредитних карт або інформація про акаунт (рахунку). Це дозволяє шахраям, наприклад, здійснювати замовлення товарів в Інтернеті під чужим ім'ям і оплачувати їх, використовуючи чужу кредитну картку або списання коштів з чужого рахунку. З тією ж метою може використовуватися фішинг (phishing), котрий включає в себе використання фіктивних веб-сайтів, електронної пошти або текстових повідомлень для доступу до персональних даних.

Восени 2017 року організація US-CERT - один з підрозділів Міністерства внутрішньої безпеки США, яке реагує на інциденти, пов'язані з комп'ютерною безпекою, повідомила про потенційну загрозу Wi-Fi мережам. За словами експертів, протокол шифрування WPA2 (Wi-Fi Protected Access II), який забезпечує захищену передачу даних між бездротовою точкою доступу і пристроями, був зламаний. Знайдена вразливість дозволяє хакерам, які перебувають в зоні дії домашньої або офісної мережі, отримати пароль від Wi-Fi, прослуховувати інтернет-трафік і перехоплювати будь-яку інформацію, що передається по незашифрованих каналах зв'язку.

DDoS-атаки

Основне знаряддя хакерів - це ботнет, мережа з пристроїв, заражених шкідливим ПЗ, яке змушує їх виконувати певні дії без відома користувача. Якщо говорити саме про ботнети, що генерують DDoS, то, наприклад, один з найвідоміших ботнетів Mirai налічує 400-500 тисяч заражених IoT-пристроїв, які атакували DNS-сервіс компанії Dyn, паралізував роботу цілого ряду компаній, включаючи Twitter, the Guardian, Netflix, Reddit, CNN та багато інших.

Слід розуміти, що в разі DDoS-атак важлива не кількість ботів, а обсяг і патерни трафіку, які вони генерують. І якщо ботнети, що поширюють трояни і спам - це в основному пер-

сональні комп'ютери, рідше - сервери, то DDoS-ботом може стати абсолютно будь-який пристрій, що має IP-адресу і інтерфейс для підключення до Інтернету.

При цьому, ботнети з IoT-пристроїв кидають справжній виклик фахівцям з кібербезпеки, тому що генерують трафік по TCP- протоколу, який практично не відрізняється від легітимного.

У 2017 році все виразніше стає помітна тенденція вимагання грошей під загрозою DDoS-атак. Такий підхід отримав назву Ransom DDoS або RDoS. Зловмисники посилають компанії жертві повідомлення з вимогою викупу, який може становити від 5 до 200 біткоінів. У разі несплати вони обіцяють організувати DDoS-атаку на критично важливий онлайн-ресурс жертви.

Атаки типу знищення сервісу (DeOS)

Отримання прибутку є основним спонукальним мотивом зловмисників. Тим не менш, деякі з них зосереджені на блокуванні або навіть знищенні атакованих систем і процесів.

Зловмисники шукають шляхи усунення мережі «безпеки», яку організації використовують для відновлення систем і даних після поразки шкідливим або здирницьким ПО, а також інших інцидентів. Як показали результати атаки шифрувальника Nyetya (Petya) влітку 2017 року і Bad Rabbit у жовтні 2017 року, дані атаки не були здирницьким ПО, а справжньою DeOS-атакою, яка просто знищувала дані заражених систем по всьому світу. Кількість подібних атак в майбутньому буде зростати.

Одержано 25.10.2017