Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

«ТАК»

Телекомунікації, автоматизація,
комп'ютерно-інтегровані та інформаційні технології

З нагоди 60-річчя кафедри автоматики та телекомунікацій

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Покровськ, 25-26 листопада 2020 р.)

Покровськ
ДВНЗ «ДонНТУ»
2020

НЕБЕЗПЕЧНІ ЗАГРОЗИ БЕЗПЕЦІ WEB-ДОДАТКІВ У 2020 РОЦІ

Демидов З.Г., старший науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій zakhar.demidov82@gmail.com;
Колмик О.О., науковий співробітник науково-дослідної лабораторії з проблем інформаційних технологій dev.univd@gmail.com
Харківський національний університет внутрішніх справ, Харків, Україна

Згідно даних досліджень, які провели експерти компаній, що займаються кібербезпекою, у 2020 році знизилась доля веб-додатків, які містять у собі вразливості високого рівня ризику. Кількість вразливостей, яке у середньому доводиться на один додаток, знизилось у порівнянні з минулим роком майже у півтора рази. Не дивлячись на це, загальний рівень захищеності веб-додатків оцінюється, як низький. Спеціалісти з'ясували, що до 20% додатків містять у собі вразливості, які надають змогу зловмисникам отримати повний контроль над системою. А отримавши доступ до всієї системи, у тому числі і до серверу, зловмисники мають можливість розміщувати на атакованому сервері власний контент, атакувати його відвідувачів, заражаючи їх комп'ютери, а також використовувати його, як майданчик для кібератак на інші системи.

Серед найпоширеніших загроз веб-безпеці у 2020 році можна виділити – межсайтовий скриптінг (XSS), SQL- ін'єкції, розподілену відмову в обслуговувані (DDoS) та інше. Але ці атаки описуються всюди, тому трохи розповім про інші, не менш небезпечні, але більш рідкісні.

Brute-force login attack - є найбільш поширеною атакою, використовуваною проти веб-додатків. Мета даної атаки - отримати доступ до акаунтів користувачів шляхом багаторазових спроб вгадати пароль користувача або групи користувачів. Brute force відкриває доступ до баз даних клієнтів, електронним адресам, до використання зламаного майданчика з метою поширення шкідливих програм, розсилки спаму і т. п. Отримавши точку входу в веб-додаток за допомогою перебору паролів, зловмисник може виконувати різні протиправні дії від імені користувача, скористатися його особистими даними з метою шантажу, вимагання, здійснити крадіжку конфіденційної інформації та грошових коштів. Незважаючи на те, що даний метод є найбільш грубим і найменш витонченим він залишається одним з найпопулярніших методів злому. Так компанія ESET - один з лідерів в області інформаційної безпеки повідомляє про зростання кількості спроб атак методом brute-force протягом пандемії COVID-19 [1].

Malware - скорочено від англійського «malicious software» - шкідливе програмне забезпечення, призначене для нанесення шкоди системам, мережам та пристроям, або крадіжки даних [2]. Шкода, яку може нанести шкідлива програма, залежить від того, до якого типу вона відноситься. Різні типи

шкідливих програм по різному проникають в систему, поширюються та заражають її.

Вірус - це найпоширеніший тип шкідливих програм. Ця програма або частина програмного коду, без відома користувача упроваджується в комп'ютери і виробляє там різні несанкціоновані дії. Вірус може поширюватися між комп'ютерами і навіть мережами шляхом самовідтворення - подібно до того, як біологічний вірус переходить від одного носія на іншого. Збиток, який вірус здатний завдати системі або пристрою, може бути найрізноманітнішим: від створення набридливих спливаючих вікон до знищення жорсткого диска або крадіжки даних користувача.

Троян - шкідливе програмне забезпечення, яке приховує справжню мету своєї діяльності за допомогою маскування. Основна відмінність трояна від класичного вірусу полягає в методі поширення: зазвичай він проникає в систему під виглядом звичайної, легітимної програми, за що і отримав свою назву. Використовується для крадіжки особистої інформації, поширення інших вірусів або просто порушення продуктивності комп'ютера. Крім того, може використовуватися для отримання несанкціонованого віддаленого доступу до заражених комп'ютерів, зараження файлів та пошкодження системи.

Хробак - вид шкідливого програмного забезпечення, здатний самостійно поширюватися шляхом створення власних копій. На відміну від вірусів, які призначені для неконтрольованого розповсюдження, хробаки, як правило, націлені на виконання конкретних дій. Це може бути, наприклад, подолання захисту системи від несанкціонованого доступу для подальшого проникнення інших шкідливих програм.

Вірус-вимагач - це шкідливе програмне забезпечення, яке блокує комп'ютери або особисті файли користувачів, вимагаючи викуп за відновлення доступу. Зазвичай вимагач потрапляє в систему через фішингові повідомлення електронної пошти. Коли жертва відкриває його і натискає на посилання, програма автоматично встановлюється на пристрій.

Шпигунська програма - це шкідливе програмне забезпечення, як випливає з назви використовується для шпигунства. Так само як і інше шкідливе ПЗ, несанкціоновано проникає на комп'ютер або мобільний пристрій та збирає інформацію. Шпигунська програма відстежує історію переглядів, імена користувачів, паролі, а також інформацію про банківські картки, яка згодом відправляється зловмисникові.

Adware або рекламне програмне забезпечення - вид небажаного програмного забезпечення, яке відображає рекламні оголошення на пристрої, до якого воно впроваджено. Adware дуже дратує, але не завжди небезпечна. Вона може бути використана для збору даних про користувача та продажу їх тому, хто більше заплатить. Але головне її призначення - показувати користувачам рекламу, якої може бути дуже багато. Крім того, adware може

без дозволу змінювати домашню сторінку в браузері, перенаправляти на випадкові сайти, показувати спливаючі вікна, встановлювати плагіни на панелі інструментів.

На будь-яку помилку є людський фактор, і якщо люди будуть дотримуватися правил безпеки, то жоден вірус не зможе вразити їх девайс або ресурс.

Список використаних джерел:

1.https://eset.ua/ru/news/view/816/kolichestvo-atak-metodom-podbora-parolya-vozroslo-iz-za-perekhoda-na-udalennyj-rezhim-raboty

2. https://www.skydns.ru/guides/chto-takoe-malware/

Анотація

Представлен перелік небезпечних вразливостей для девайсів і ресурсів з невеликим описом не самих поширених з них.

Ключові слова: вразливість, вірус.

Аннотация

Представлен перечень опасных уязвимостей для девайсов и ресурсов с небольшим описанием не самых распространённых из них.

Ключевые слова: уязвимость, вирус.

Abstract

A list of dangerous vulnerabilities for devices and resources is presented with a small description of not the most common ones.

Keywords: vulnerability, virus.