Иванова Ирина Александровна
Национальный университет «Одесская юридическая академия»,
студентка 2-го курса факультета кибербезопасности
и информационных технологий

DRIVE-BY ЗАГРУЗКИ

На современном этапе, развития информационных технологий, за персональными данными и возможностью управлять пользовательскими компьютерами, разворачивается настоящая охота. Хакеры создают более сложные и вредоносные вирусы, а специалисты по кибербезопасности строят все более сложную защиту. Несмотря на то, что киберграмотность самих пользователей растет, появляются новые вирусы, заражения которыми сложно избежать. Поскольку некоторые из них хорошо замаскированы, их носителями могут быть, даже официальные сайты и приложения, которыми пользователь постоянно пользуется.

К примеру, группа кибершпионажа под названием Patchwork (или Dropping Elephant) использовала метод drive-by загрузки для создания вредоносного видео-сайта нацеленного на жителей Китая, под названием YoukuTudou. Который загружал и выполнял xRAT троян под видом обновления Adobe Flash Player [1].

Распространение и установка вредоносного кода или программного обеспечения методом Drive-by загрузок, очень привлекает киберпреступников, так как он является более «скрытой» технологией, которая используется операционными системами, приложениями или браузерами для перенаправления пользовательского соединения на сервера с пакетами эксплойтов.

Причин, по которым хакеры при атаках направленных на взлом устройств пользователей используют drive-by загрузку, может быть несколько: кража учетных данных, личной информации, создание ботнетов, заражение других устройств, выведение из строя самого устройства или нане-

сение вреда данным. Всё это легко сделать без наличия необходимого программного обеспечения для защиты операционной системы пользователя, и актуальных версий приложений и браузеров [2].

Существует два основных метода распространения вредоносных программ через загрузку:

1. **Разрешенная загрузка со скрытыми данными.**

Сначала хакер создает носитель для доставки вредоносной программы на устройство пользователя, который может получить замаскированную ссылку, увидеть рекламу или сообщение в ленте социальных сетей, как будто оно было отправлено из источника, которому он доверяет. Это побуждает пользователя перейти по ссылке. И в тот момент, когда веб-страница со встроенным в него эксплойтом открывается, на компьютер или мобильное устройство, устанавливается непреднамеренная загрузка. После установки, хакер успешно проникает в устройство и получает контроль над вашими данными.

Для этого способа хакеры используют метод Bundleverware и Фишинг.

Bundleware – метод объединения разных программ, в том числе и вредоносных, в один загрузочный файл, который на ряду с загрузкой желательной программы, устанавливает вредоносную программу на устройство пользователя.

Фишинг – используется для того, чтобы с помощью сообщений или всплывающих окон, от источников которым пользователь доверяет, заставить пользователя выполнить скачивание. Чаще всего, ссылки на установку вредоносных программ скрыты за ложными уведомлениями о нарушении работы браузера или электронными письмами о взломе аккаунта пользователя.

2. **Неразрешенная загрузка без ведома пользователя.**

Сначала злоумышленник взламывает веб-страницу и помещает туда вредоносный компонент. После этого, пользователи посещают страницу, которая переадресовывает соединение на вредоносный сервер, на котором хранится набор эксплойтов,

которые находят ошибки в пользовательской системе безопасности и выполняют загрузку вредоносного кода.

Этот метод основан на ошибках в программном коде и уязвимостях систем безопасности различных устройств, с которыми для проведения атак, взаимодействуют комплекты эксплойтов.

Комплекты эксплойтов – программное обеспечение, которое предназначено для взлома веб-сервисов или устройств, методом выявления уязвимостей.

Распространенными формами являются эксплойты нулевого уровня (ошибки безопасности, без известных патчей или исправлений). Довольно часто в наборах эксплойтов хранятся небольшие фрагменты кода, которые позволяют незаметно обойти системы безопасности, а затем ввести оставшуюся часть кода для получения необходимого доступа к мобильному устройству или компьютеру [3].

Как и в большинстве аспектов кибербезопасности, лучшей защитой устройств и персональных данных является предосторожность. Для предотвращения drive-by загрузок, важно позаботиться о безопасности устройства. Чтобы сделать это максимально эффективно, пользователь должен следовать следующим советам:

• не использовать учетную запись администратора, для повседневного использования. Так как для установки drive-by загрузок необходимы права администратора.

• устанавливать актуальные обновления для операционной системы и веб-браузер. Потому что в новых версиях исправлены ошибки в системе безопасности. Уязвимостью, которых может воспользоваться пакет эксплойтов.

• не устанавливать ненужные приложения на устройстве. Следует удалять устаревшие приложения, которые больше не получают обновления. Ведь чем больше подключенных модулей установлено, тем устройство более уязвимо для такого вида атак.

• устанавливать программное обеспечение, к которому есть высокий индекс доверия.

• использовать проверенное антивирусное программное обеспечение и поддерживать актуальное обновление антивирусных баз. Важно, чтобы оно отвечало за безопасность устройства, сканировало веб-сайты, а также инспектировало интернет-трафик. Это обеспечит своевременное обнаружение попыток выполнения drive-by загрузок.

• Избегать посещения подозрительных сайтов, которые могут содержать вредоносный код.

• внимательно изучать всплывающие окна, рекламу в приложениях или браузерах, перед тем как выполнять переход на посторонний сайт. Чтобы избежать перехода на вредоносный сайт, обращайте внимание на зернистость фотографии, опечатки или ошибки в грамматике.

• использовать программное обеспечение или расширения в браузерах, которые блокируют рекламу. Это поможет избежать drive-by атак [4].

Список использованных источников:

1. Drive-by Download. [Электронный документ]. URL: https://www.trendmicro.com/vinfo/ru/security/definition/drive-by-download.

2. Drive-by загрузки. Интернет в осаде. [Электронный документ]. URL: https://securelist.ru/drive-by-zagruzki-internet-v-osade/1139/.

3. What Is a Drive by Download. [Электронный документ]. URL: https://www.kaspersky.com/resource-center/definitions/drive-by-download.

4. Drive By Downloads: What They Are and How to Avoid Them. [Электронный документ]. URL: https://www.exabeam.com/information-security/drive-by-download/

Ключові слова: приховане завантаження, експлойт, кібербезпека.
Ключевые слова: скрытая загрузка, эксплойт, кибербезопасность.
Key words: drive-by download, exploit, cybersecurity.

***Научный руководитель**: к.т.н. доцент Задерейко А. В.*