УДК [004.92 + 004.32.8]:378

Студ. Д. М. Вольский
Науч. рук. ассист. П. Е. Сулим
(кафедра полиграфического оборудования и систем обработки информации, БГТУ)

ЗАЩИТА УСТРОЙСТВ ПЕЧАТИ ОТ ВЗЛОМА И ПЕРЕХВАТА ДАННЫХ

Введение. Уязвимости сетевых принтеров рассматривались со времен их появления, но за прошедшие годы положение дел нисколько не улучшилось. В принтерах появился *WiFi* и функция автоматического обновления прошивки через Интернет, а в МФУ подороже теперь есть встроенная память, зачастую хранящая копии сканированных и распечатанных документов за длительный период.

Постепенно из баловства атаки на сетевые принтеры превращаются в бизнес. Одни ищут на них конфиденциальные данные, другие используют как точку проникновения в корпоративную сеть, а третьи пытаются извлечь прибыль из массовых рассылок. Какие-то предприимчивые люди уже создали сервис, на котором за определенную сумму рассылают спам, удаленно печатая его на чужих принтерах.

Основная часть. На самом деле атаки на принтеры — не новость, и в какой-то мере даже удивительно, что массово эту идею подхватили только сейчас. Например, во времена активного использования факсов популярностью у всяких сомнительных личностей пользовался факс-спам — рассылка рекламы и не только рекламы по факсу. В 1991 году в США был принят закон, который запрещал такую рассылку, да и факсы в большинстве стран стали встречаться все реже, так что со временем факс-спам пошел на убыль.

Принтерам тоже уже доставалось. В 2008 году исследователь Аарон Уивер (*Aaron Weaver*) опубликовал статью, в которой описал возможность создания веб-сайта, при посещении которого на принтер пользователя будет отправляться запрос на печать определенной страницы.

Были и случаи массовых атак на принтеры — например, в 2016 году хакер взломал сетевые принтеры более чем в десяти колледжах в США и распечатал на них расистские листовки.

Техническая сторона взлома не представляет особой сложности. Для поиска уязвимых устройств традиционно используется поисковая система *Shodan*. Она позволяет указать номер порта и протокол — и получить список сетевых устройств, в которых данный порт свободно

открыт в Интернет, с указанием *IP*-адресов. Последняя атака была нацелена на принтеры с открытыми портами *IPP* (*Internet Printing Protocol*), *LPD* (*Line Printer Daemon*) и портом 9100. Затем пишется скрипт, чтобы рассылать по полученным *IP*-адресам и указанному порту файл *Post Script*, который сразу принимается на печать.

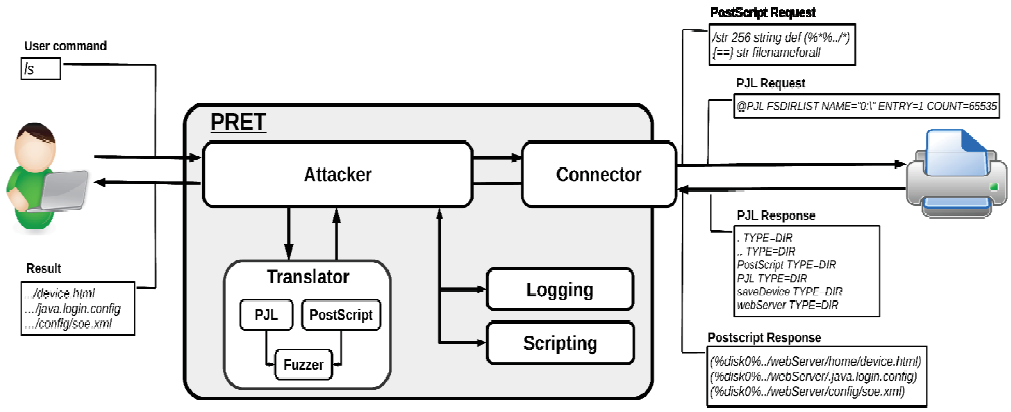

Рисунок – Архитектура *Printer Exploitation Toolkit* (*PRET*)

Выводы. Как избежать взлома принтера? Скорее всего, большинству пользователей совершенно не нужно, чтобы их принтер был доступен из Интернета. Ну а поскольку взломать описанным выше способом можно только сетевые принтеры, то лучше просто отключить свой принтер от Интернета, при этом он останется доступным через локальную сеть.

- Если в настройках принтера есть какие-либо пункты про печать через Интернет, отключите эти возможности.
- У сетевых принтеров часто есть логин и пароль для доступа. Обязательно поменяйте их — ни в коем случае не оставляйте те, что установлены по умолчанию.
- На вашем роутере, скорее всего, есть файрвол. В нем стоит закрыть порты 9100, 515, а также с 721-го по 731-й. О том, как это сделать, читайте в руководстве пользователя к вашему роутеру.
- Старайтесь выключать принтер, когда вы его не используете.