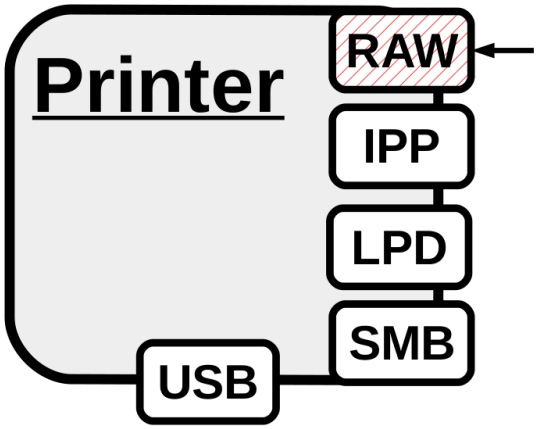
79.02
Рейтинг

GlobalSign

GlobalSign_admin 3 декабря 2018 в 03:01

Взломать 50 000 сетевых принтеров и распечатать произвольный текст? Нет ничего проще!

Блог компании GlobalSign, Информационная безопасность*, Периферия, Интернет вещей

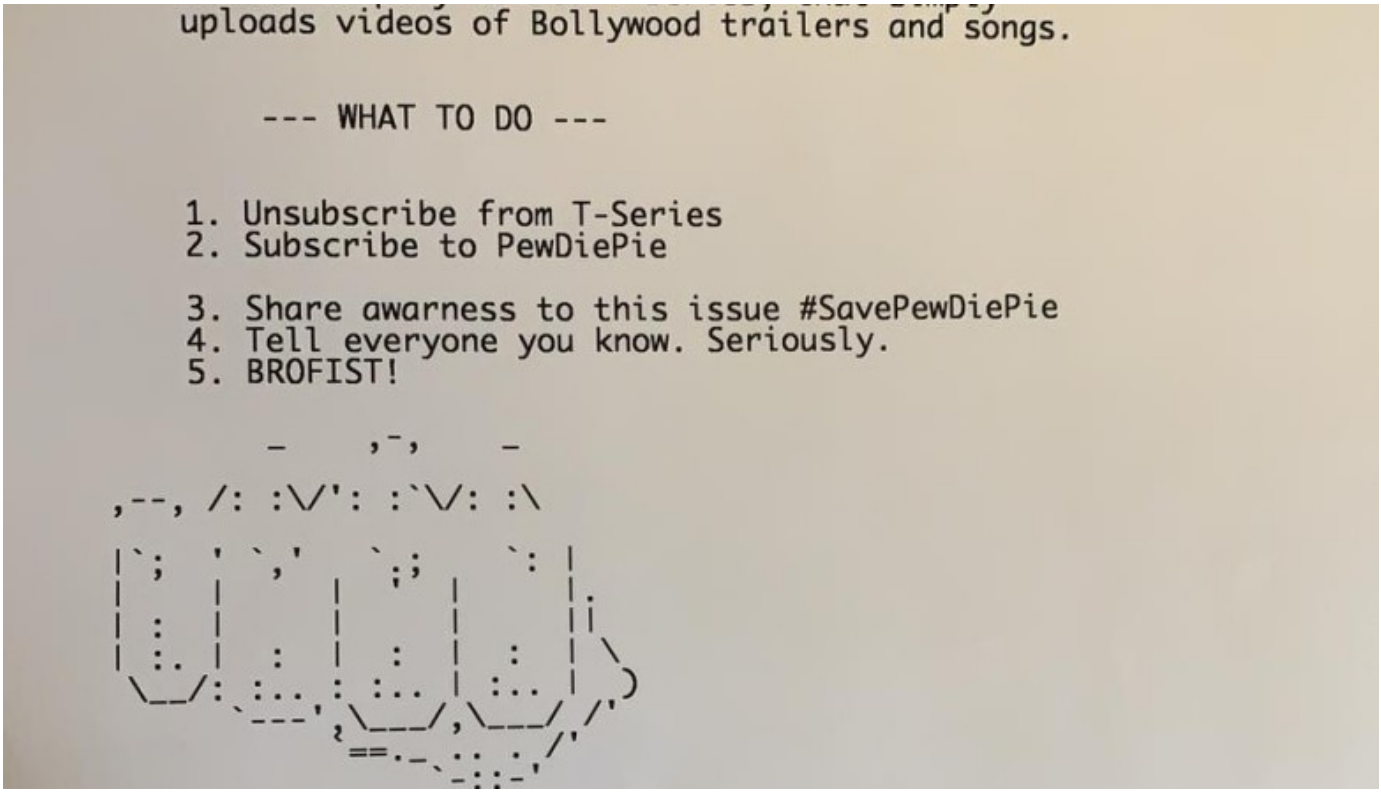


29 ноября 2018 года пользователь твиттера под псевдонимом @TheHackerGiraffe «взломал» более 50 000 сетевых принтеров и распечатал на них листовки с призывом подписываться на YouTube-канал некоего PewDiePie. Он говорит, что таким образом хотел способствовать популярности своего кумира, который сейчас сражается за 1-е место по количеству подписчиков на YouTube.

Здесь интересна простота, с которой хакеру удалось получить доступ к 50 000 принтеров. В сессии вопросов и ответов AMA на Reddit хакер раскрыл подробности этого взлома. Оказывается, в нём нет ничего сложного. Более того, в Сети свободно доступны программные инструменты для эксплуатации многих уязвимостей в старых прошивках принтеров. К сожалению, повторить этот фокус может буквально любой желающий.

На иллюстрации: печать по raw-порту 9100

Сообщения на тысячах принтеров вызвали настоящий переполох, поскольку они появились на множестве устройств в разных компаниях: от высококачественных многофункциональных принтеров в крупных корпорациях до небольших портативных принтеров квитанций на заправочных станциях и в ресторанах, пишет издание *ZDNet*.



29 ноября 2018 года такое сообщение распечатали более 50 000 принтеров по всему миру. Фото опубликовал в твиттере пострадавший IT-администратор в Брайтоне (Великобритания). Одна из многих подобных фотографий в твиттере

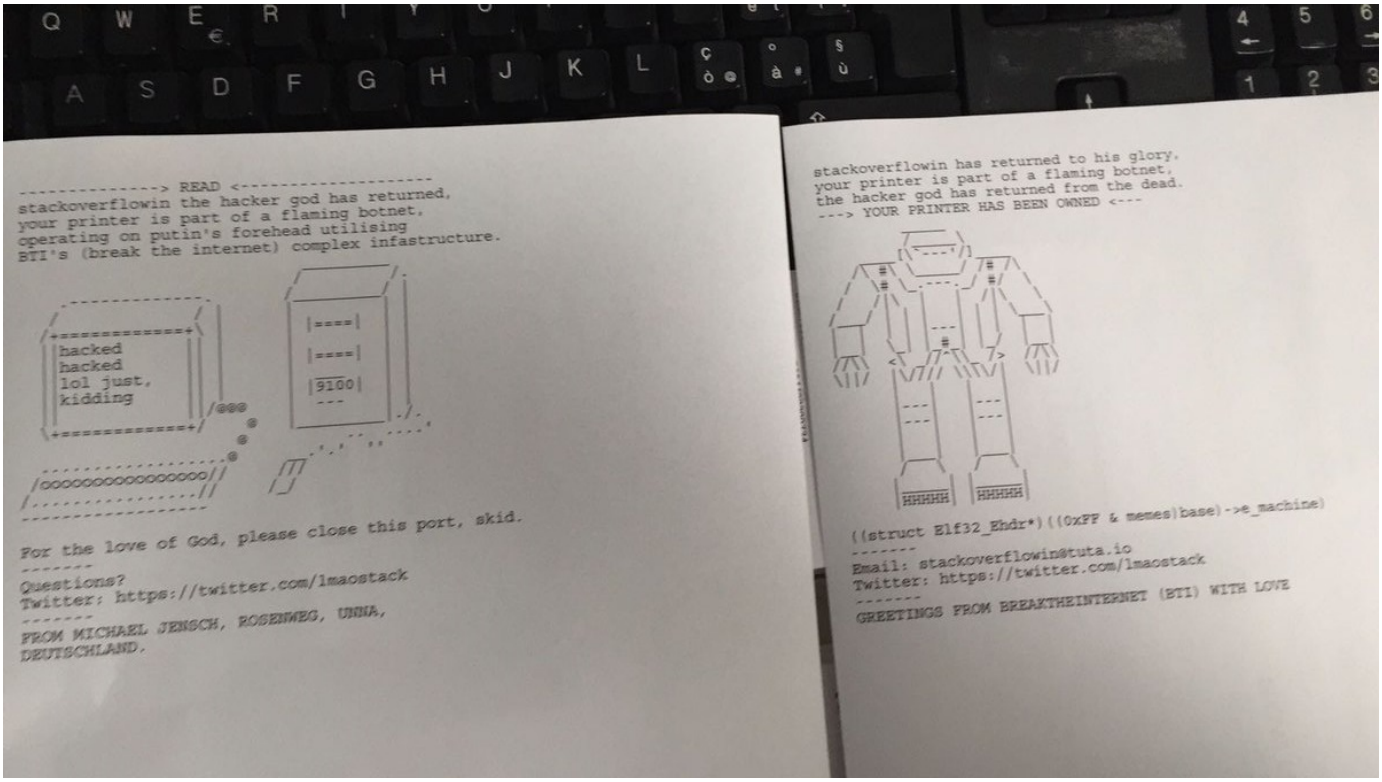
Эта акция — часть большой кампании, которую развернули поклонники PewDiePie. Они сейчас изо всех сил агитируют в социальных сетях, чтобы шведский блогер сохранил лидерство по количеству подписчиков: в данный момент у него 72,6 млн подписчиков, а в спину дышит конкурирующий канал T-Series с 72,5 млн подписчиков.

Принтеры просто выводили текстовое сообщение с призывом подписаться на канал.

Аналогичные взломы

Нынешний взлом 50 000 принтеров не уникален. Такое происходило неоднократно. Например, нечто похожее провернул 24 марта 2016 года хакер weev (настоящее имя Эндрю Ауерхаймер), который вывел на тысячах сетевых принтеров расистские и антисемитские сообщения. Интересно, что Ауерхаймер присоединился к «белому движению» в тюрьме, где отбывал 41-месячный срок за предыдущее преступление, связанное с компьютерным взломом.

В феврале 2017 года этот трюк повторил другой хакер Stackoverflowin, который напечатал глупые рисунки на более чем 150 000 принтеров.



Сообщение Stackoverflowin

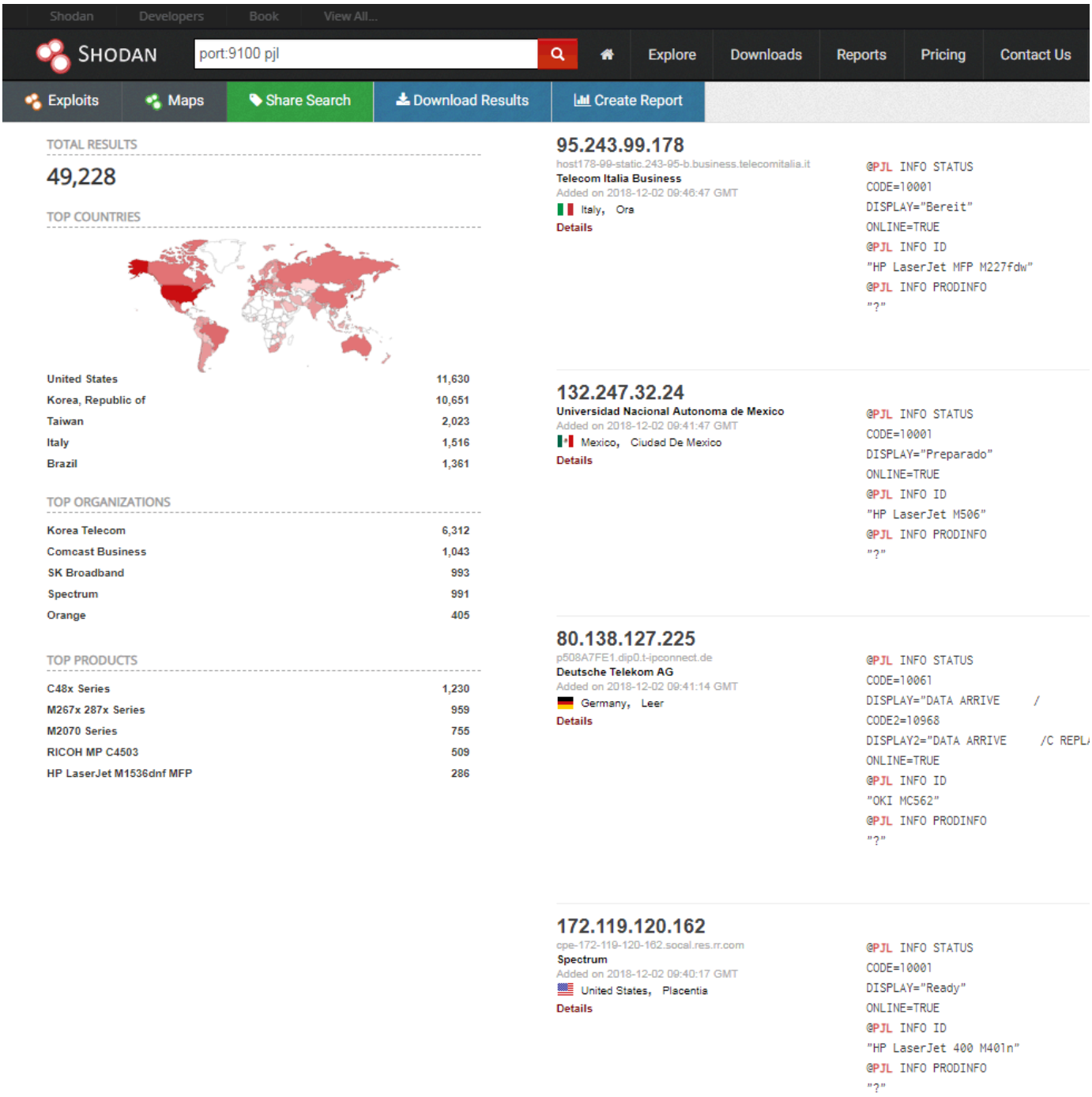
Технические детали

Как мы уже говорили, техническая сторона взлома не представляет особой сложности. @TheHackerGiraffe говорит, что сделал это из скуки: «Мне стало скучно после четырёх часов игры в Destiny 2 и я решил, что хочу кого-нибудь взломать».

> Here is how the entire #pewdiepie printer hack went down:
>
> 1. I was bored after playing Destiny 2 for a continous 4 hours, and decided I wanted to hack something. So I thought of any vulnerable protocols I could find on shodan
>
> (1/)
> — TheHackerGiraffe (@HackerGiraffe) December 1, 2018

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 PostScript, который сразу принимается на печать.

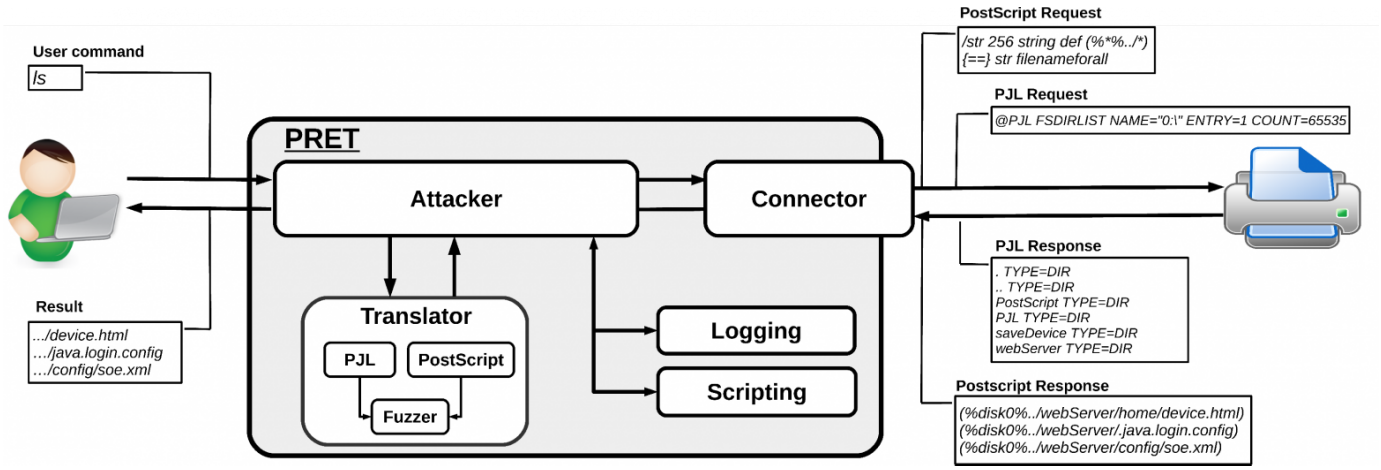


Количество принтеров с открытым портом 9100. Скриншот из поисковой системы Shodan (2 декабря 2018 года)

В Reddit AMA хакер @TheHackerGiraffe сказал, что он отправил сообщения только только 50 000 принтеров, хотя мог задействовать и большее количество: поисковик выдал более

800 000 непропатченных принтеров с выставленными в интернет портами по протоколам IPP, LPD и JetDirect. Но хакер выбрал только 50 000 принтеров с открытыми портами 9100.

Список уязвимых принтеров можно скачать с Shodan. Затем хакер взял инструмент Printer Exploitation Toolkit (PRET), исходный код которого свободно опубликован в интернете и использовал его для подключения к принтерам. Кстати, PRET позволяет не только вывести на печать сообщение, но и получить доступ к внутренней сети, к файлам, а также просто повредить принтер, среди прочего.



Архитектура Printer Exploitation Toolkit (PRET)

В январе 2017 года программу выложила группа исследователей вместе с научной работой о бедственной безопасности сетевых принтеров. В своей работе они подробно описали шесть уязвимостей в более чем 20 моделях сетевых принтеров со старыми прошивками. Инструмент предназначен для тестирования сетей и поиска уязвимостей.

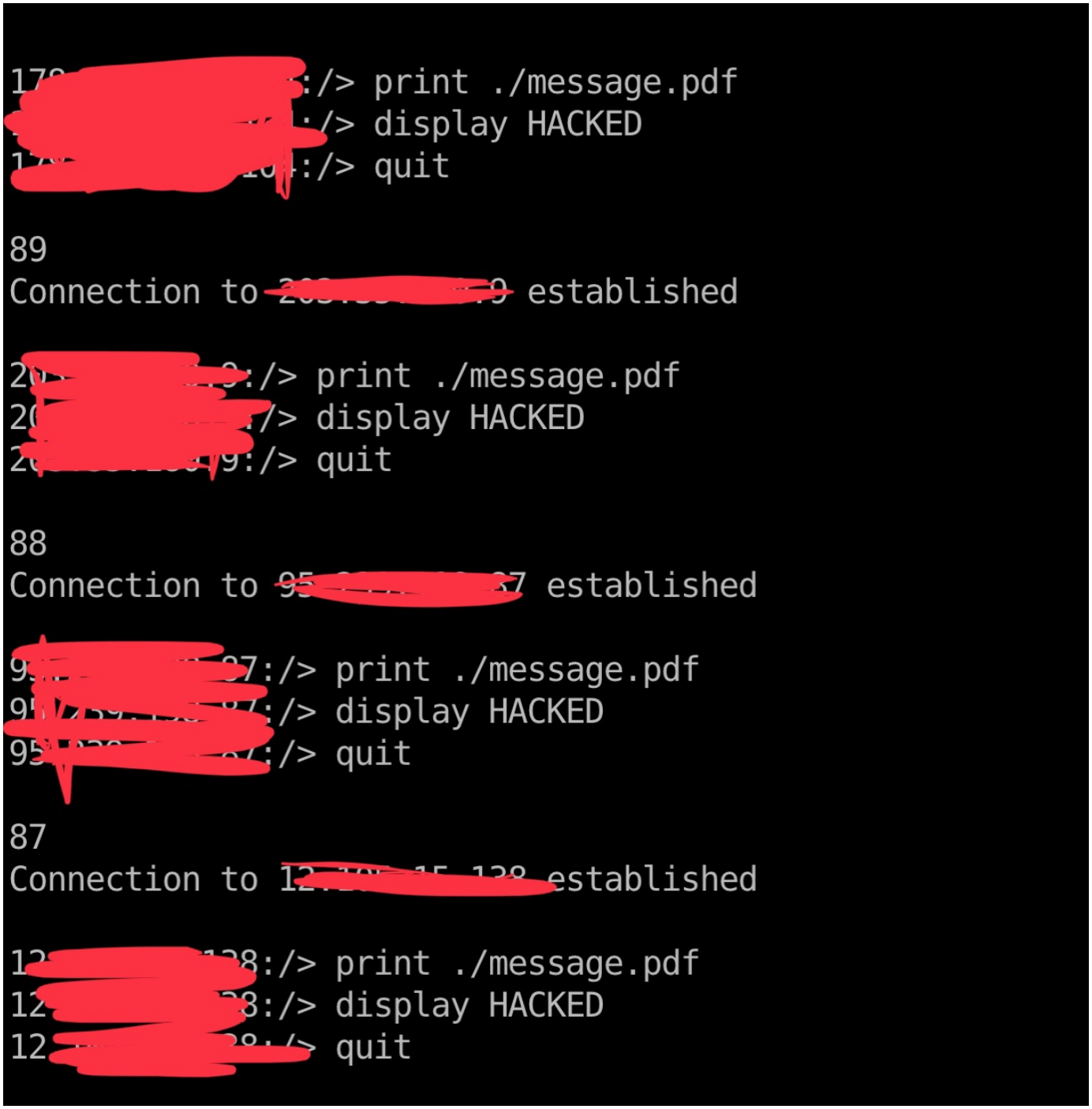
@TheHackerGiraffe запустил такой bash-скрипт. Скрипт берёт список принтеров с Shodan (`potential_bros.txt`) и циклом прогоняет по каждому IP-адресу PRET с командами, указанными в `commands.txt` :

```
#!/bin/bash
while read -r line; do
ip="$line"
torify ./PRET/pret.py $ip pjl -q -i ./commands.txt
done < "./potential_bros.txt"
```

Содержимое `commands.txt` :

```
print ./message.pdf
display HACKED
quit
```

В связи с большим количеством IP-адресов скрипт лучше запустить где-нибудь на сервере.



Атака в действии, скриншот с сервера. Фото: @TheHackerGiraffe

@TheHackerGiraffe не считает свои действия незаконными, потому что принтеры свободно открыты для управления через интернет: «Представьте большую кнопку „Печать” в интернете», — говорит он.

Независимо от целей взлома и глупого использования, нынешний инцидент многое говорит о защите сетевых устройств (точнее, об отсутствии этой защиты). Как видим, огромное количество пользователей не думает об обновлении прошивок и не следит за выпуском патчей. Впрочем, это давно известно, сейчас произошла лишь наглядная демонстрация, к чему такое может привести.

«Люди недооценивают, насколько легко хакер-злоумышленник может использовать такую уязвимость, чтобы вызвать серьезный хаос, — написал @TheHackerGiraffe — Они могут украсть файлы, установить вредоносное ПО, нанести физический ущерб принтерам и даже использовать принтер в качестве плацдарма для дальнейшей атаки на внутреннюю сеть».

Впрочем, принтеры — ещё не самая интересная мишень. Например, Shodan находит около 190 000 открытых FTP-серверов…

Теги: Shodan, IPP, Internet Printing Protocol, LPD, Line Printer Daemon, Printer Exploitation Toolkit, PRET, порт 9100

Хабы: Блог компании GlobalSign, Информационная безопасность, Периферия, Интернет вещей

Комментарии 27

hokum13
03.12.2018 в 04:41

Принтер имеет белый IP, на принтере открыт 9100-й порт… Теперь это тоже называют взломом? Хулиганство — да, взлом — нет.

Примерно такой уровень:

+7 Ответить

Valeratal
03.12.2018 в 04:50

а вот «сесть» можно как за настоящий взлом :)

+2 Ответить

Naerus
03.12.2018 в 11:28

Только вот насыпать яду в солонки попадает под предумышленное нанесение тяжкого вреда здоровья и во все вытекающие вплоть до убийства, потому что не докажешь что ты не знал, для чего применяется солонка) Но с принтерами тоже считаю что под взлом это не попадает.

0 Ответить

hokum13
04.12.2018 в 04:16

Так meG@Duc| свою деятельность тоже как работу с уязвимостью позиционировал. А по факту один серийный отравитель, а другой просто хулиган, но ни как не хакеры. И оба очень любят играть на публику.

0 Ответить

iig
03.12.2018 в 05:14

С одной стороны это унылое скрипт-кидди.
С другой стороны, производители железок ценой в килобаксы могли бы хоть какую-то авторизацию придумать.

+1 Ответить

jevius
03.12.2018 в 05:45

Сейчас киддисы побегут в своих универах принтеры ломать

Скажите им что такие поиски в шодане платные уже.

0 Ответить

Polaris99
03.12.2018 в 05:53

Да вроде не такие уж и килобаксы, брал год назад цветной лазерный Lexmark с поддержкой сети — обошелся в 90 евро. А в диапазоне до 200 вообще куча моделей есть.

0 Ответить

firedragon
03.12.2018 в 06:37

Не будем показывать на одного производителя сетевого оборудования где пустой пароль по умолчанию.
Описанное в статье действительно хулиганство, а вылечить можно простым файрволом.
Причем во многих железках я видел простейшие картинки что нужно сделать для защиты, но всем бехразлично.

0 Ответить

Diordna
03.12.2018 в 16:49

Почему не используют нат?

0 Ответить

CherryPah
03.12.2018 в 21:36

1) Нат придуман вообще не для этого
2) Ну вот такая вот прихоть у моего ISP — раздавать всем белую статику
3) В будущем всем грозят ipv6 где статика будет вообще у любой кофеварки
4) А как тогда печатать на принтере из соседнего офиса? (я знаю, подавляющее число комментаторов тут тоже думаю знает, а вот владелец магазина навряд ли)

0 Ответить

Diordna
04.12.2018 в 20:49

2 и у моего тоже но принтер стоит за роутером обычно в локалке, хотя можно арендовать кучу ip
3 грядет эра невиданных доселе ботнетов…
4 администиирование

+1 Ответить

402d
03.12.2018 в 06:49

это лень сисадминов, а не проблема производителя принтера.
Ну не нужна тут авторизация, и так хватает проблем с сетевой печатью,
а теперь еще головная боль добавиться и с авторизацией.

0 Ответить

maledog
03.12.2018 в 09:38

По моему наблюдению, в подавляющем большинстве организаций, где rdp и порты принтера

торчат наружу вобще нет сисадмина, а настраивает проброс порта племянник главного бухгалтера, который в 11 классе учится. А если где и есть сисадмин, то воспринимается он начальством исключительно как начальник над эникеями и никак иначе. Потому вместо администрирования ему приходится заниматься типичной менеджерской работой.

+1 Ответить

maledog
03.12.2018 в 09:29

Есть у них авторизация. Смотрите IPP. Просто по-умолчанию включены все протоколы в том числе и те, которые были разработаны в эпоху до массового распространения сетей. Это как ругать modbus-tcp за небезопасность.
Бонус скрипт-киддям — в нашей стране открытым портом наружу могут торчать еще и кассовые аппараты. Можно доставить немало неприятных минут обладателям ввиду того, что они еще и в ОФД данные отправляют.

0 Ответить

Polaris99
03.12.2018 в 05:24

Странно, что печатали исключительно ASCII, подавляющее большинство таких принтеров поддерживает PCL со всеми отсюда вытекающими последствиями. Хоть бы фантазию какую проявили.

0 Ответить

402d
03.12.2018 в 06:02

Печатался не ASCII а pdf документ.
порт 9100 принимает print-ready data, т.е. нужно было просто собрать задание на печать несколько строк преамбулы PJL и @PJL ENTER LANGUAGE=PDF
потом текст pdf'ки и конец задания. А 50 тысяч получилась выборка из открытых, тех моделей, которые понимают PDF. В основном это средний и дорогой сегмент рынка принтеров. Дешевые принтеры ждут готовую картинку от компьютера. Например в QPDL.
PDF -> PCL6 или PostScript этот уже не смог осилить.

0 Ответить

Polaris99
03.12.2018 в 06:21

Ну так тем более бред, зачем печатать из PDF банальный ASCII курьером? Какая-то тотальная деградация. JetDirect поддерживает на порядок больше принтеров, чем PDF. А про готовую картинку я прекрасно осведомлен, спасибо. Приходилось реализовывать поддержку

печати на микроконтроллерах, так что уже по цене принтера я примерно могу сказать, GDI он или PCL.

0 Ответить

402d
03.12.2018 в 06:38

может размер пакета минимизировал? Тут же проще было у себя на компьютере назначить печать в файл и немного подредактировать при желании prn файл.

+1 Ответить

402d
03.12.2018 в 05:34

до небольших портативных принтеров квитанций на заправочных станциях и в ресторанах
вот в это не верю от слова совсем.
pos принтеры с 9100 есть, но вот способных распечатать, то что он рассылал среди них нет.

0 Ответить

Polaris99
03.12.2018 в 06:22

Если там действительно PDF слался, то да, сомнительное заявление.

0 Ответить

402d
03.12.2018 в 06:54

Был неправ. Pos принтер выведет кучу мусора и правильно plain текст из pdf файла.

0 Ответить

amarao
03.12.2018 в 10:48

'S' in 'network printer' stands for security.

+5 Ответить

DmitrySpb79
03.12.2018 в 16:16

А зачем вообще принтеру белый IP и проброс портов? Из дома на рабочем принтере печатать?

И да, многим действительно в голову не придет что кто-то чужой будет печатать на их принтере,

профит-то с этого нулевой…

0 Ответить

Xenos_rus
03.12.2018 в 17:24

В мире немало древних локалок с белыми адресами, сам когда-то в такой конторе работал. Поэтому даже проброса портов не нужно, достаточно банально не закрыть фаерволом.

0 Ответить

iig
04.12.2018 в 03:42

Если большой группенпринтер за выходные уничтожит несколько пачек бумаги — для кого-то это небесплатно.

0 Ответить

Diordna
03.12.2018 в 16:53

IoT меня пугает как грядущая стихия паролить которую юзерам будет влом.

+1 Ответить

dimonoid
03.12.2018 в 21:47

Через неделю MrBeast «взламывает» все те же 50000 принтеров и тратит всю заправленную бумагу из лотков, делая реванш невозможным, на печать текста:
1) Unsubscribe from PewDiePie.
2) Subscribe to MrBeast

0 Ответить

Только полноправные пользователи могут оставлять комментарии. Войдите, пожалуйста.

ПОХОЖИЕ ПУБЛИКАЦИИ

15 сентября 2020 в 17:44

Безопасность через неясность недооценивается

+33 14K 44 101 +101

26 ноября 2019 в 06:51

Доменную зону .ORG продают частной компании. Общественность призывает ICANN расторгнуть контракт

+19 12K 15 14 +14

16 августа 2019 в 03:25

Фотографии в заложниках. Первый взлом цифровых камер по WiFi (протокол PTP/IP)

+15 9.1K 49 9 +9

ЛУЧШИЕ ПУБЛИКАЦИИ ЗА СУТКИ

вчера в 06:00

Как и почему в Калифорнии появилась Кремниевая долина?

+28 6.2K 39 28 +28

вчера в 08:20

Продление жизни временных значений в C++: рецепты и подводные камни

+25 2.7K 41 3 +3

вчера в 11:06

Пишем свой Credential Provider на C# для авторизации в Windows

+21 3K 41 4 +4

вчера в 19:50

Разработка антенн для тестирования клеток Фарадея в МРТ

+17 963 13 5 +5

вчера в 06:31

Шьём HDMI-USB Video capture

+17 3.9K 22 8 +8

ИНФОРМАЦИЯ

Дата основания	1996
Местоположение	Япония
Сайт	www.globalsign.com
Численность	Неизвестно
Дата регистрации	30 января 2018

БЛОГ НА ХАБРЕ

24 мая в 14:23

Автоматическая установка сертификатов S/MIME для корпоративных пользователей

1.7K 2 +2

16 мая в 16:37

Chrome на Android сломал чужие MitM-сертификаты, но это можно исправить

3.9K 7 +7

4 мая в 13:22

Что такое «цифровая трансформация» на деловом жаргоне

2.4K 2 +2

22 апреля в 11:04

Reticulum — радиопротокол для mesh-сети. Зашифрованная пиринговая связь без интернета

15K 12 +12