www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Маленькие коробочки

или почему мы любим 7547/TCP

Артемий Цецерский – специалист по тестированию на проникновение, CyberOK

Исследование СайберОК содержит в себе интересные ответы на то, что находится на интересном порту 7547/TCP, о котором многие могут услышать впервые. Пробежимся по тому, какую опасность в себе хранит этот порт и какие интересные физические устройства обитают на нём. Построим поверхность атаки, вспомним, как беспощадно наводили шуму эти маленькие коробочки – разложим это всё тщательно на атомы – на TP-Link-и, Keenetic-и, Mikrotik-и, а также проанализируем насколько это всё уязвимо. Лээтс го!

Введение

В эру развития такого направления как External Attack Surface Management, мы тоже решили стать модными и разработать свою отечественную православную балалайку СКИПА, которая сумеет обезопасить славный Рунет. Эта балалайка перевернула айсберг вверх ногами и показала интересные и необычные результаты...

Кстати, СКИПА и сервисы непрерывного контроля поверхности атак и пентеста доступны для пилотов для корпоративных заказчиков. Безвозмездно. То есть даром. Писать info@cyberok.ru!

Результаты показали, что, оказывается, самый распространенный порт ни 80, ни 443 – те самые Web-порты, а что-то более загадочное – 7547/TCP! И таких устройств с портом почти около 2 млн!

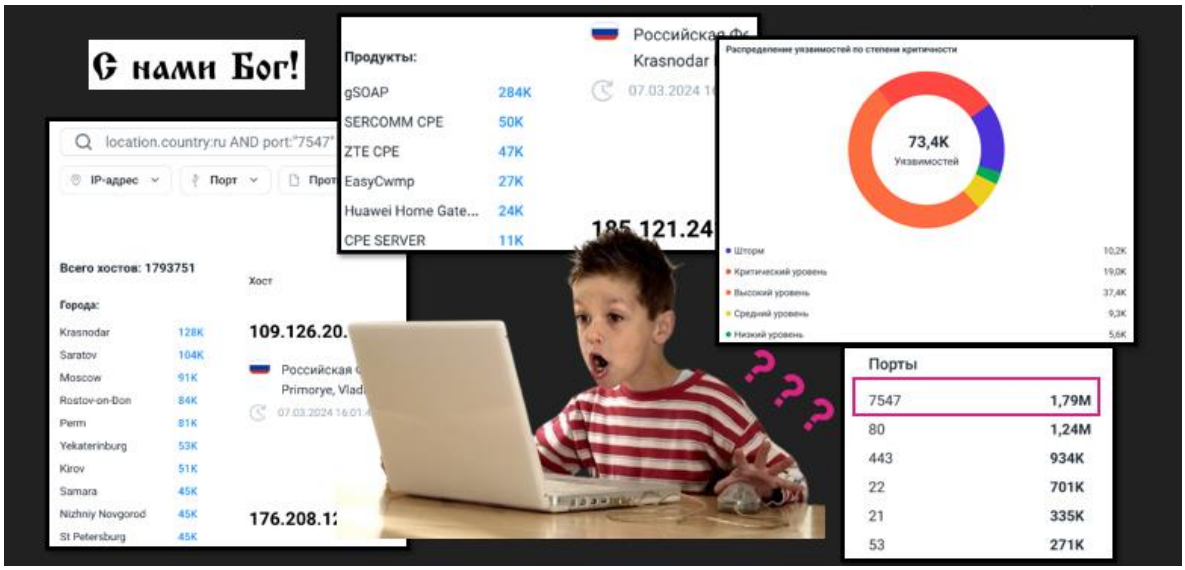

Рис. 1

Немного погуглили, пересерчели, поизучали, что же обитает на этом порту и оказалось, что на нём работает такой интересный протокол как TR-069 или иначе CWMP (CPE WAN Management). Этот протокол помогает провайдером удаленно управлять различными маленькими абонентскими устройствами – конфигурировать, диагностировать и даже обновлять CPE-устройства (маленькие домашние коробочки) при помощи ACS (конфигурационного сервера).

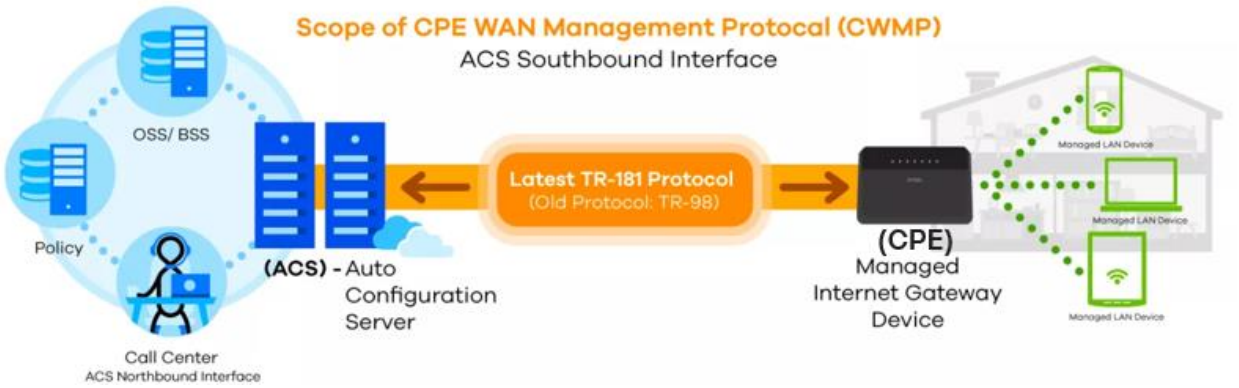

Рис. 2

Почитали мы еще побольше про них новостей и заметили, что от этих домашних коробочек, которые лежат мирно у вас на полках, было немало проблем и вообще они периодически кибер-преступляют – бегают DDoS-ят, атакуют, поджигают Интернет. Часто объединяются в большие банды – ботнеты, примеры тому крупные ботнеты Meris, Mirai. Последний, на минуточку, включал в себя более чем 3 миллиона устройств, многие из которых были проэксплуатированы через протокол TR-069!

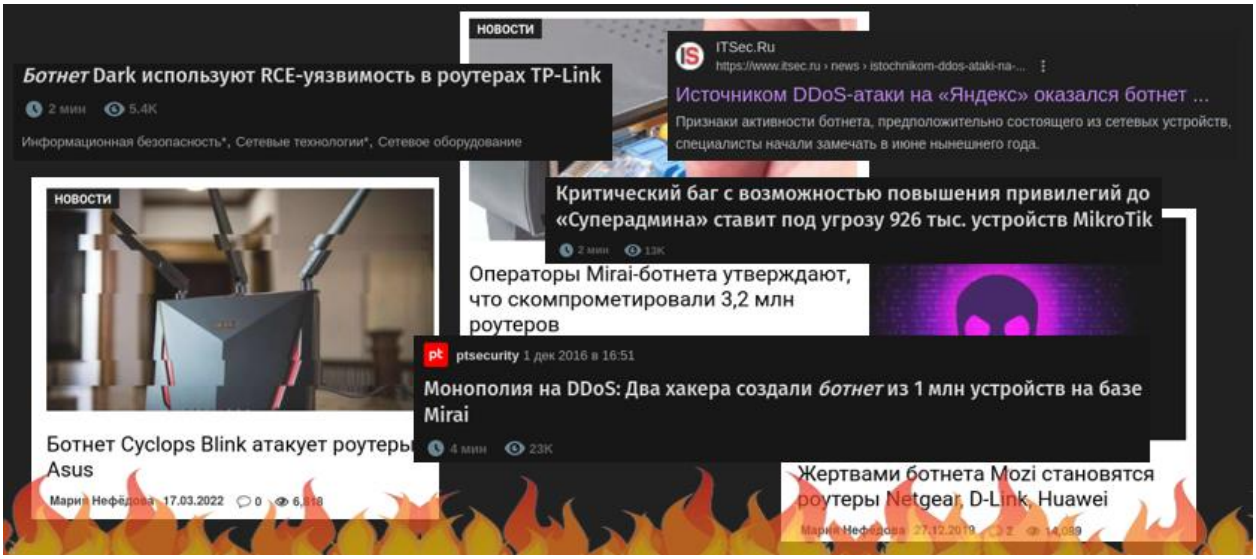

Рис. 3

Это заставило нас задуматься и построить поверхность атаки в Рунете. Запустив нашу СКИПА, способную определять расположенный на порту сервис или ПО, мы получили внушительную статистику распространенности устройств таких вендоров, как TP-Link,

Mikrotik, Keenetic, Sercomm, Huawei, ZTE, и так далее. Ниже представлена наглядная диаграмма этой статистики.

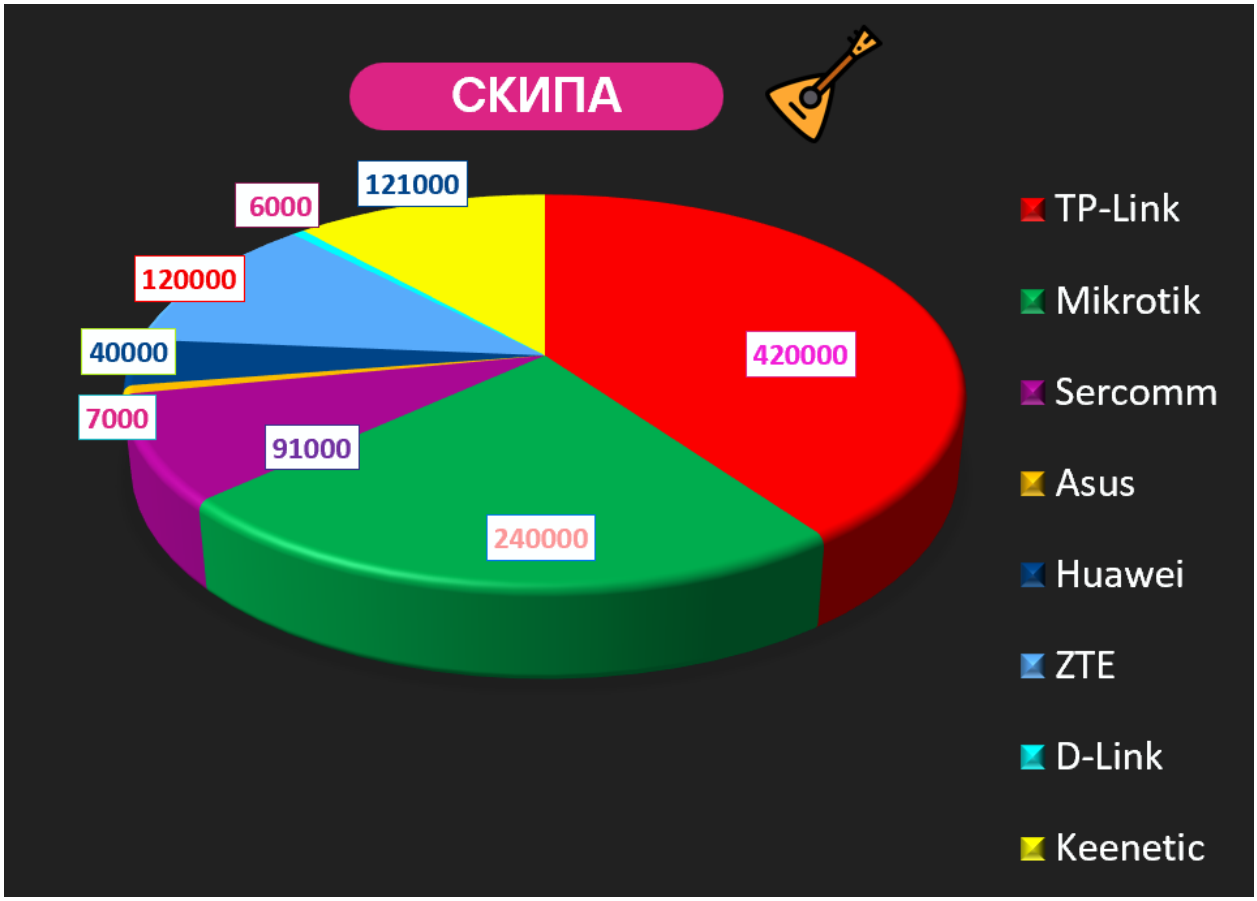

Рис. 4

Цифры огромные и правда, но так чем же подкрепляется опасность такого большого количества устройств в комбинации с TR-069? На самом деле аргументов несколько:

- 90% сервисов TR-069 работает по HTTP без SSL шифрования.
- Basic/Digest аутентификация защищающая устройство (простой перебор паролей на таких объемах?).
- Использование паролей вида: admin:admin, root:root, support:support, ...
- Устаревшее ПО 10+ летней давности.

Мы решили пойти дальше и стали изучать взаимодействие на примере ACS и CPE и заметили, что элементарно незрелое ИБ со стороны некоторых провайдеров подчеркивается размещением на ACS устаревшего релиза Nginx версии 1.6, релиз которой был более чем 10 лет назад!

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Рис. 5

В некоторых случаях у некоторых провайдеров данные об устройстве вашей локальной сети уходят куда-то в Интернет. Да, так бывает и да, не всегда. Так, на примере ниже, кому-то можно узнать о всяких штукенциях обитающих в моей сети. История умалчивает, где и как могут использоваться, храниться такие данные, но факт есть факт.

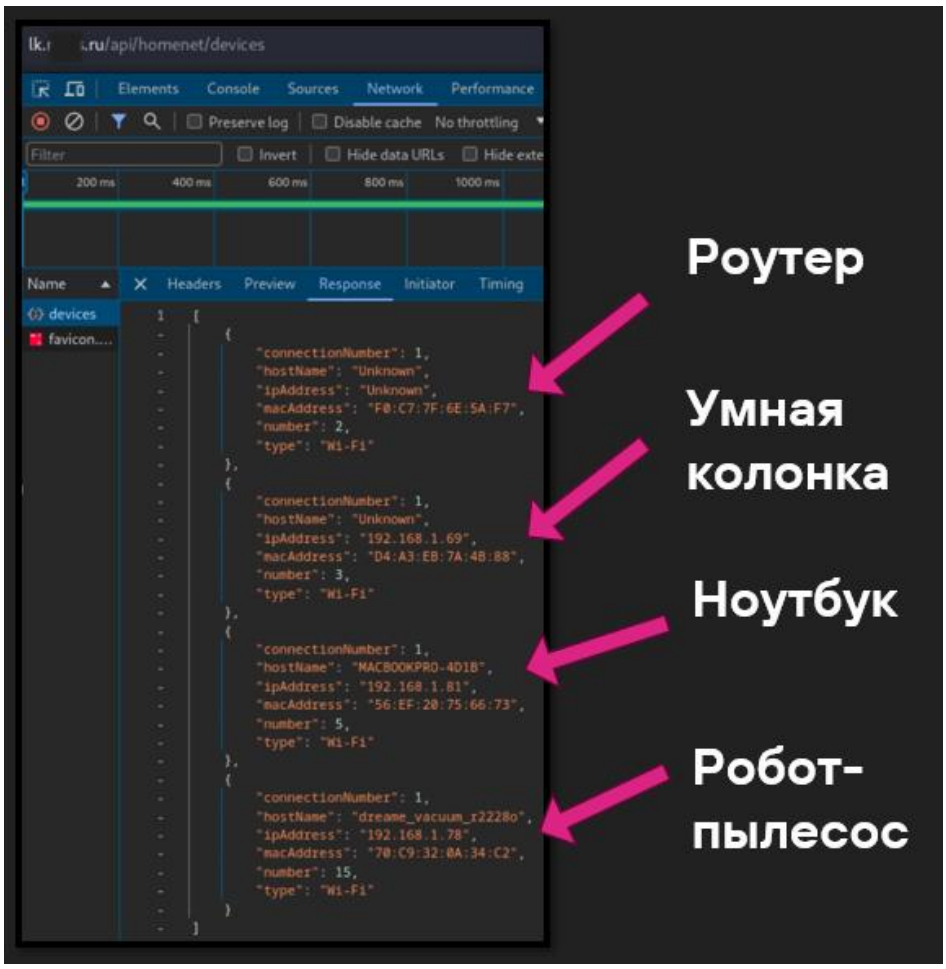

Рис. 6

Мы решили исследовать глубже и пошли в лес за прошивками. Найти прошивку под домашний роутер оказалось проще простого, да и вообще можно найти версии на любой вкус – оригинальное, кастомные, всех видов и провайдеров.

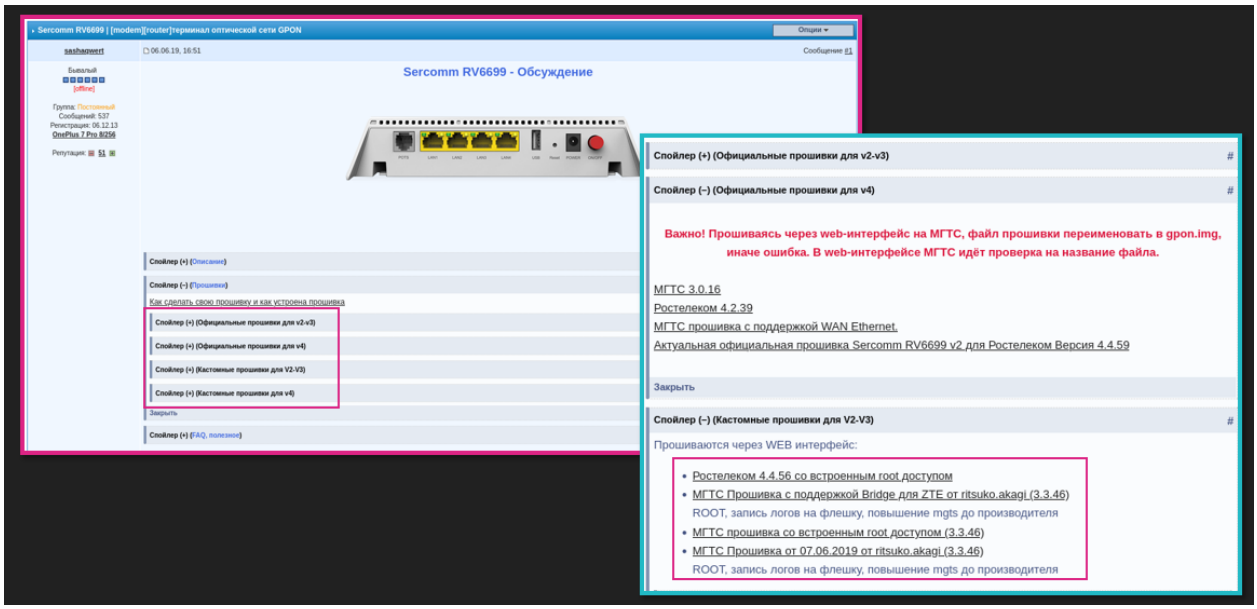

Рис. 7

Порыскав немного в прошивках, можно найти различных зашитых пользователей, в том числе и операторских, найти URL-адреса куда ходят за обновлениями или ещё чем-либо, а также узнать о встроенном супер-админе, к которому на самом деле уже давно имеются пароли в чистом виде, что в свою очередь помогает подключиться к своей коробочке и познакомиться с ней еще ближе.

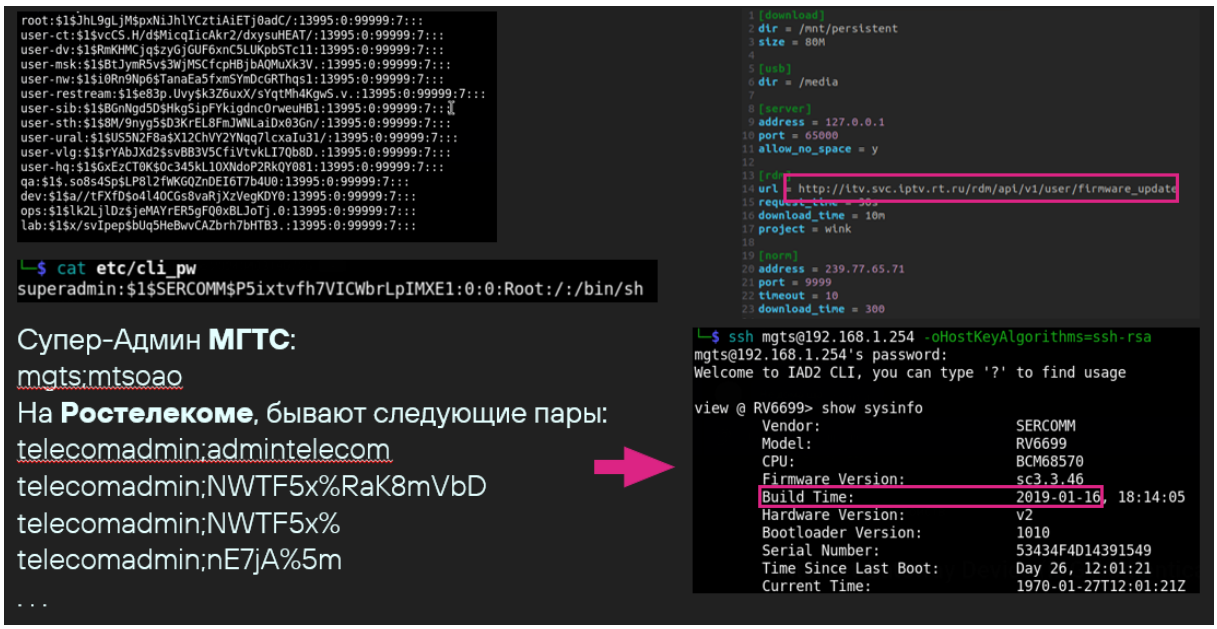

Рис. 8

Нас подбодрили найденные пароли, но мы решили пойти еще проще и посмотреть в сторону простых комбинаций. Оказывается, все сделано за нас и мы можем только подтвердить, что с 2017 года ситуация не изменилась. И на каждом 10-м устройстве можно пройти аутентификацию с помощью ТОП-10 паролей.

Рис. 9

Определение программного обеспечения на порту 7547/TCP показало, что львиную долю занимает gSOAP, в особенности большая часть из них – это версии 2.7. Это ПО релиза 2006 года. Получается, что скоро всех ждёт на своем 20-летии.

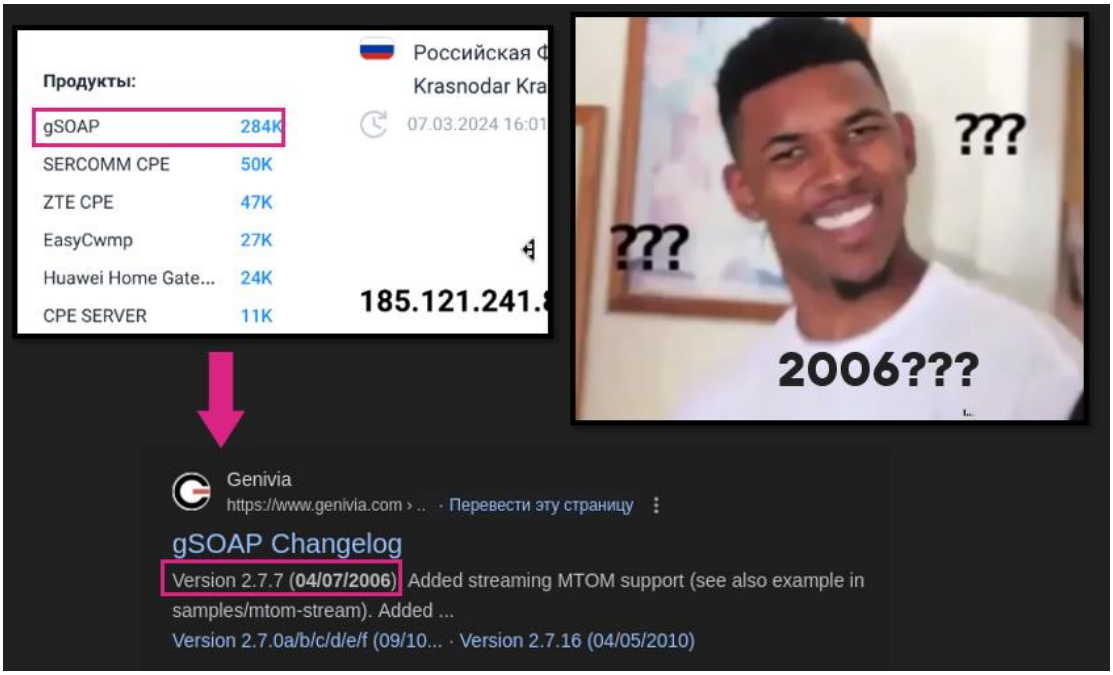

Рис. 10

На него имеются и уязвимости, однако громких инцидентов с ними не возникало. Это подчеркивает одну положительную сторону, что если уязвимо – то не всегда взламываемо!

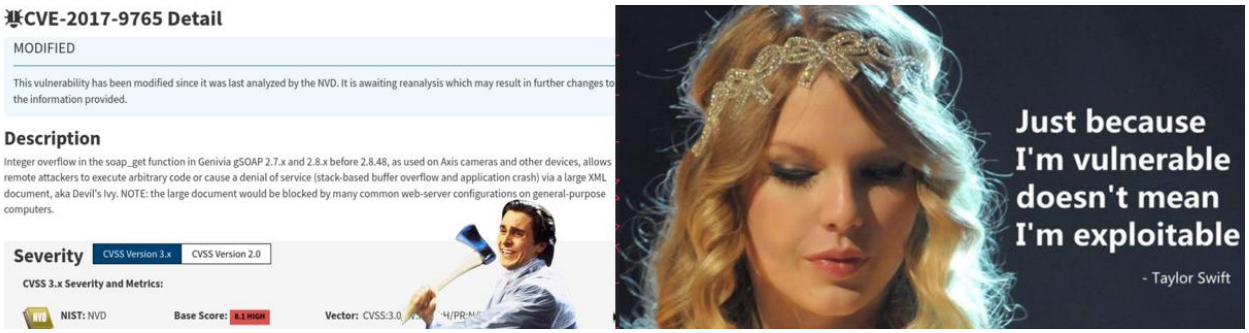

Рис. 11

Еще большую часть порта 7547 занимает ПО EasyCWMP – это опен-сорсная реализация протокола CWMP. Наша СКИПА сумела определить 76 тысяч устройств в РФ, а Shodan в свою очередь нашел 600 тысяч в мире. Мы стали искать известные уязвимости, однако результат был нулевым, что очень странно, ведь ПО уже более 5 лет не обновлялось, да и написано на C – языке, на котором не все умеют разрабатывать безопасно. Кстати, Mirai Botnet построен был на уязвимости в RomPager, которая стрельнула неожиданно и массово, разрушая интернет, так что стоит быть начеку!

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

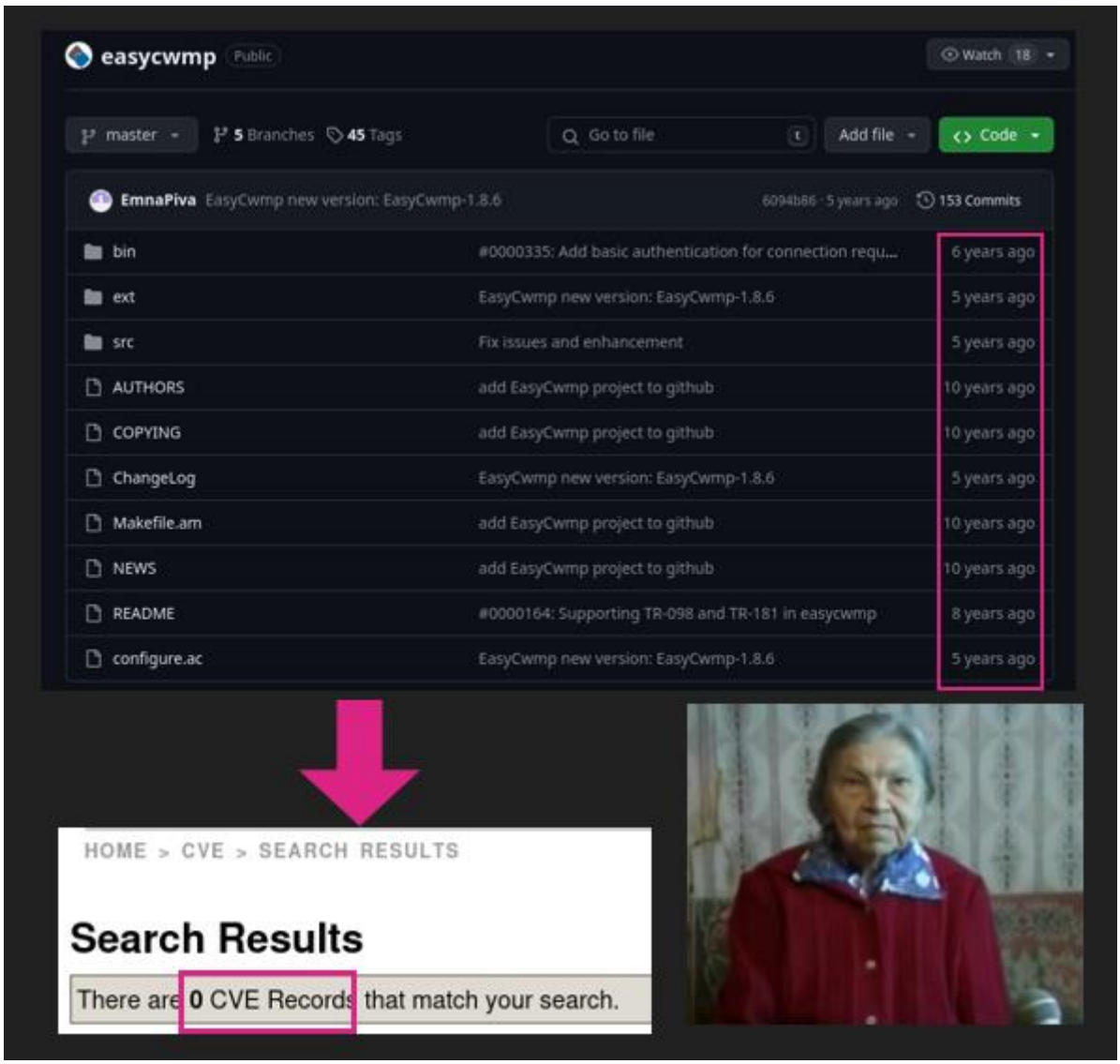

Рис. 12

Повышая «градус» коробочек, рассмотрим такую большую маленькую коробочку, уже не совсем домашнюю – Mikrotik!

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Рис. 13

Это устройство относительно бюджетное и его любят ставить небольшие организации, но и часто его не совсем корректно настраивают.
В Рунете таких коробочек расположилось более чем 200 тысяч. Любой сетевой безопасник советует не выставлять неиспользуемые сервисы в Интернет и ставить сервисы на нестандартные порты, однако, согласно табличке ниже, не все администраторы применяют такую практику.

Сервис	Порт	Количество устройств
Winbox	8291/TCP	125,000
SSH	22/TCP	35,000
API	8728/TCP, 8729/TCP	27,000
WebFig	80/TCP, 443/TCP	29,000
Telnet	23/TCP	20,000
SNMP	161/UDP	7,000

Рис. 14 В таблице указаны открытые и торчащие порты

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Злоумышленников всегда при массовом взломе устройств интересует определение версии ПО. Mikrotik более чем на 120 тысячах устройств легко позволяет определить версию RouterOS при отправке специфичного запроса на сервис Winbox (8291/TCP).

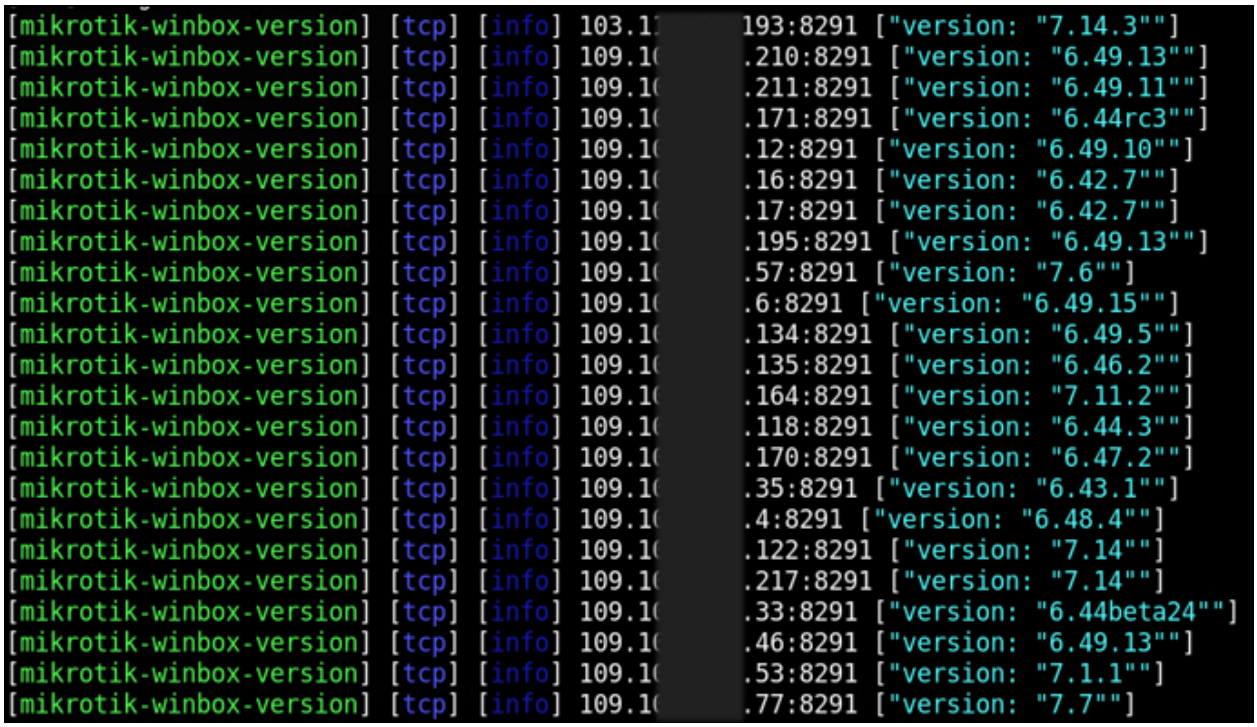

Рис. 15

Определив версии RouterOS на Mikrotik, мы построили диаграмму устаревших, уязвимых устройств. В расчёт брались версии ранее 2022 года включительно. По этой диаграмме можно сделать выводы, что существует достаточно много устаревших устройств и администраторы не совсем любят обновляться, а более чем 12 тысяч устройств функционируют на версии ПО старее 2018 года.

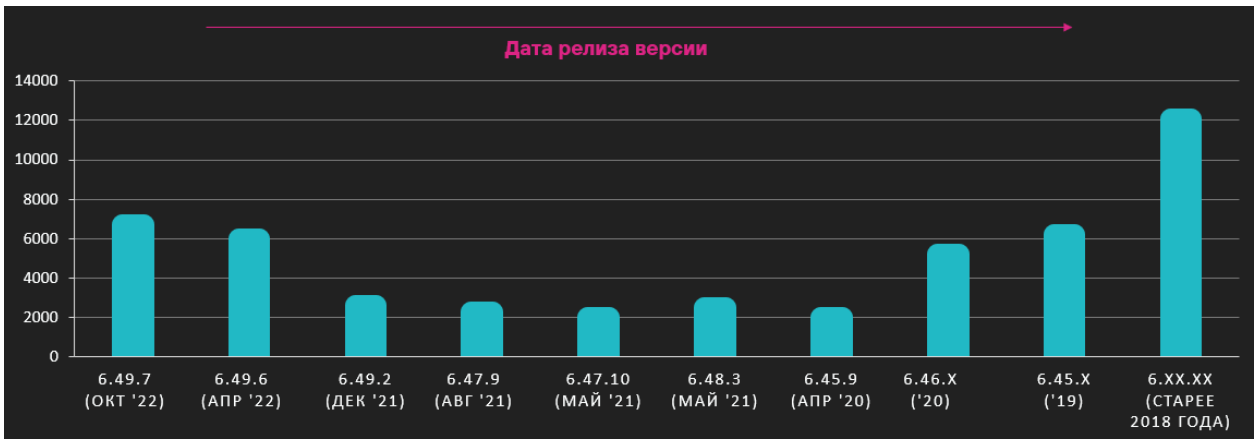

Рис. 16

www.cyberok.ru
info@cyberok.ru
+7 (495) 137-7337

Дополнительно мы провели safe-check проверку на некоторые «хайповые» уязвимости.

Оказалось, что в Рунете можно встретить более чем 30 тысяч роутеров, подверженных **CVE-2023-30799 (CVSS: 7.1),** которая позволяет повыситься аутентифицированному пользователю от админа – к супер-админу. Более чем 1400 устройств имеют уязвимый SNMP сервис, позволяющий выполнить удаленный код (**CVE-2022-45315 (CVSS: 9.8)).** Ну и замыкает тройку самая известная критическая уязвимость CVE-2018-14847 в службе Winbox, позволяющая выполнить код на роутере.

Заключение

А на этом мы заканчиваем это увлекательное изучение маленьких коробочек, обитаемых в ваших и наших Интернетах. И хочется сделать следующие выводы:

- не забывать обновляться, хотя бы при критических уязвимостях;

- внедрять строгую парольную политику, чтобы принудительно пользователи не могли устанавливать слабые пароли;

- не выставлять в интернет лишние сервисы – фильтровать порты от злоумышленников.