Безопасность в MikroTik
(по итогам года)

Обо Мне

- ✓ Руководитель ИТ-службы торговой компании
- ✓ MikroTik certified engineer, consultant
- ✓ MikroTik Trainer с 2015года
- ✓ Сертификаты: ccna, mtcna, mtcre, mtcwe, Eltex-коммутация, ФЗ-152, ubuquiti ubwa
- ✓ Работаю с микротик с 2008

telegram: @Nick_The_First

Обо Мне

Провожу учебные курсы в России и Казахстане с компанией «MikroTik-Courses»

1671
Специалистов обучено

2549
Сертификатов выдано

82%
Средний балл

50
Городов посетили

Уязвимости

- Единственная 0-day уязвимость CVE-2018-14847 ликвидирована 24/03/2018 - в течение недели. Слоупоки и конкуренты обсуждают до сих пор.
- Некритичные CVE-2018-1156, CVE-2018-1157, CVE-2018-1158, CVE-2018-1159 ликвидированы в августе в 6.42.7
  (там же сделан отключаемым PMKID – exploit for 802.11)

Варианты эксплуатации

Если ваш MikroTik взломали

«Угон» админки роутера и вымогательство

Блокирование NetInstall с использованием «SecureBoot».

Обычно, установка задержки reformat на 5-8 минут

Майнинг и фишинг

Подмена DNS-серверов, включение SOCKS-Proxy, перехват и перенаправление траффика.

Использование сниффера для нешифрованых протоколов.

Угон роутеров и сброс

- Функция «protected-routerboot».

Параметры удержания «reset»

reformat-hold-button=20s

reformat-hold-button-max=10m

- Если есть доступ «read», сделать

/system routerboard settings export

+ google: MikroTik wiki Netinstall

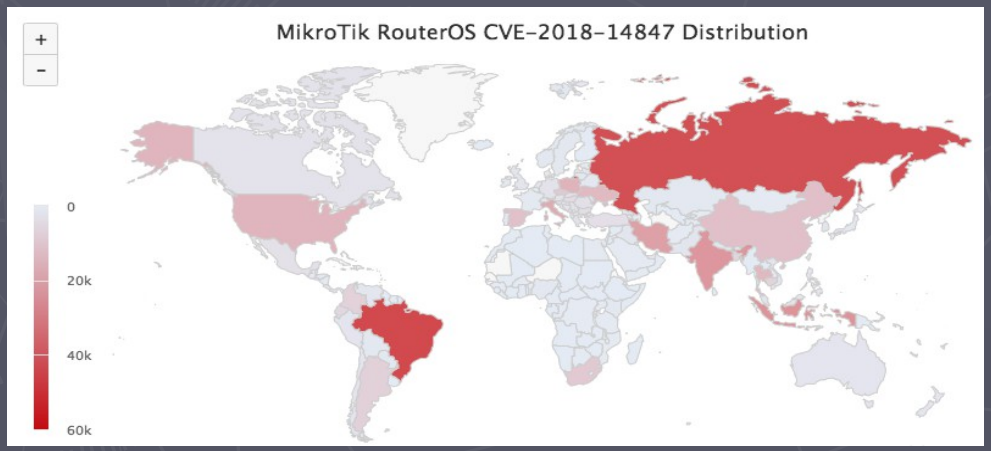
Майнинг на роутерах

- https://www.securitylab.ru/blog/company/kaspersky/344785.php
  «Майнинг на роутерах MikroTik»

  Использует старые уязвимости

  Фишинг более эффективен.

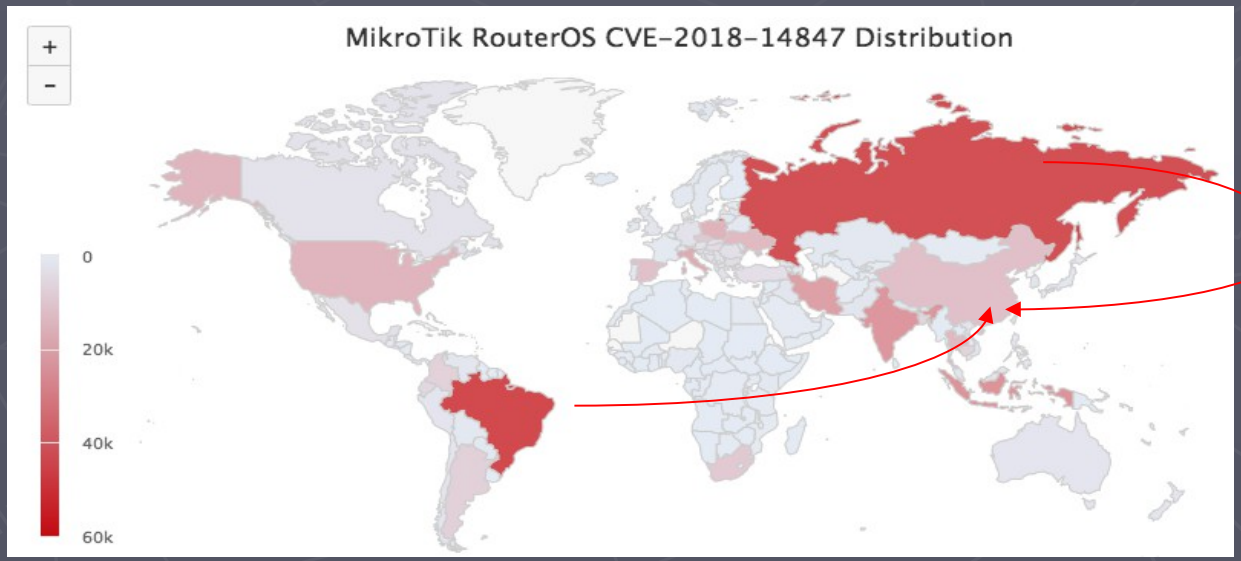
  Сниффинг более опасен.



Кража паролей на транзите

«Ваш sniffer настроен против вас»

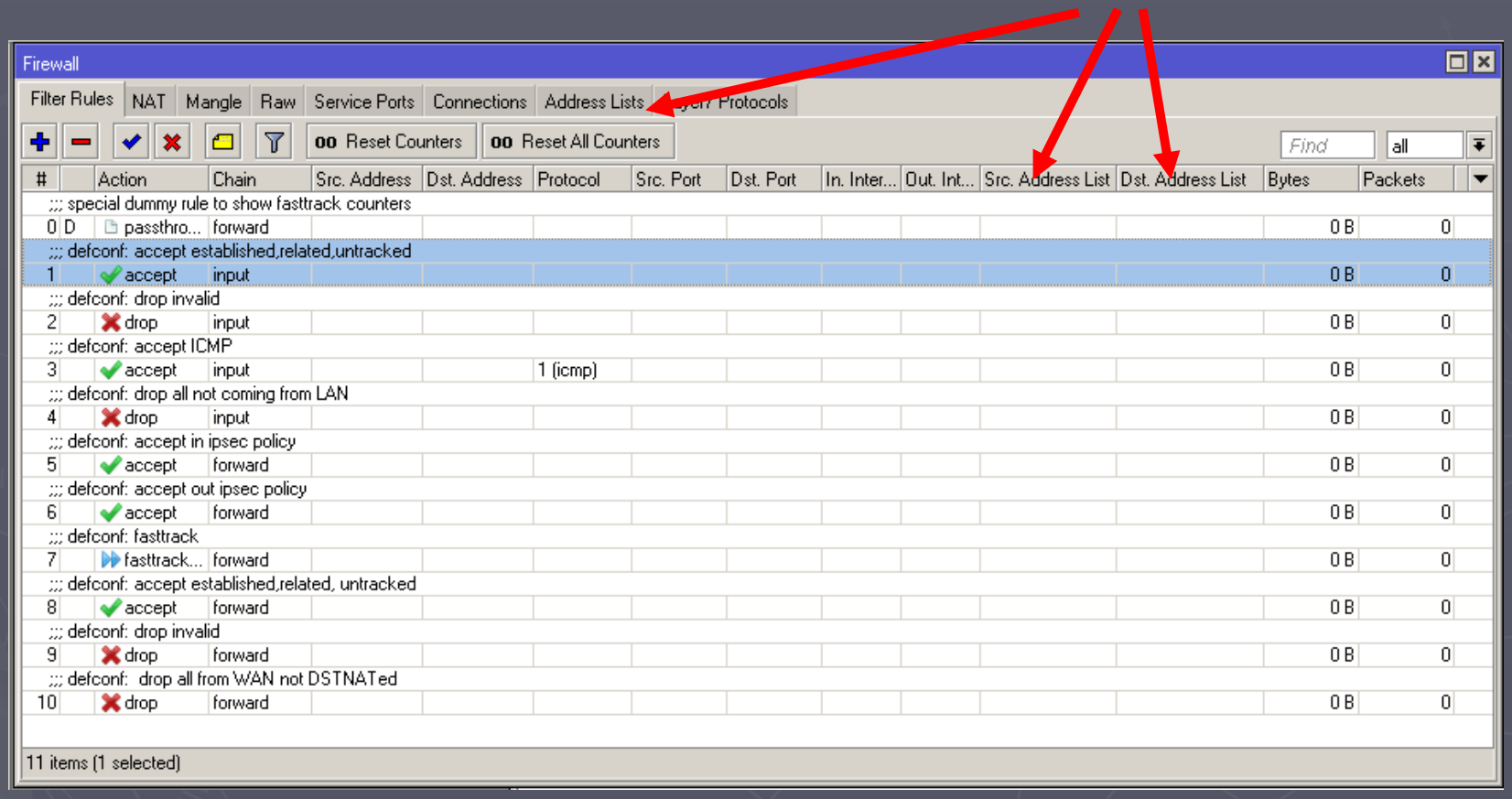
Пароли telnet, smtp, pop3, ftp, http перехватываются хакерами



Изучаем взломанный микротик

- ✓ Поиск троянов в sheduler и не только
- ✓ Пароли наверняка «ушли».
- ✓ Логины и пароли PPP – прежде всего
- ✓ Проверяем настройку DNS
- ✓ Проверяем функционал socks-proxy
- ✓ Проверяем фаервол!

Дефолтный фаервол



Взломанный фаервол

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

oo Reset Counters | oo Reset All Counters | Find | all

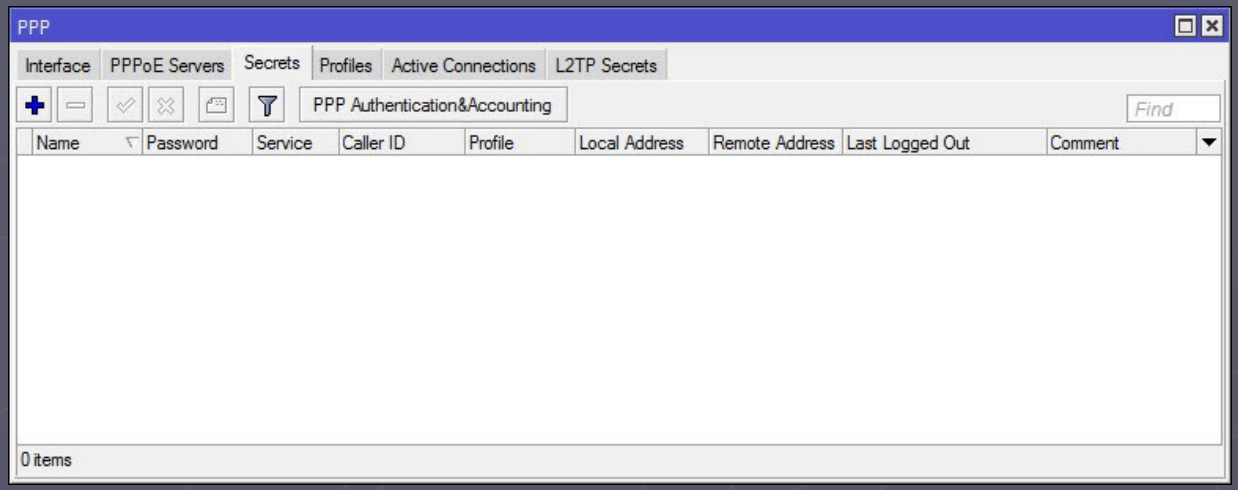
#		Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Src. Address List	Dst. Address List	Bytes	Pa
;;; special dummy rule to show fasttrack counters														
0	D	passthro...	forward										0 B	
;;; defconf: accept established,related,untracked														
1		accept	input										0 B	
;;; defconf: drop invalid														
2		drop	input										0 B	0
;;; defconf: accept ICMP														
3		accept	input			1 (icmp)							0 B	0
;;; defconf: drop all not coming from LAN														
4		drop	input										0 B	0
;;; defconf: accept in ipsec policy														
5		accept	forward										0 B	0
;;; defconf: accept out ipsec policy														
6		accept	forward										0 B	0
;;; defconf: fasttrack														
7		fasttrack...	forward										0 B	0
;;; defconf: accept established,related, untracked														
8		accept	forward										0 B	0
;;; defconf: drop invalid														
9		drop	forward										0 B	0
;;; defconf: drop all from WAN not DSTNATed														
10		drop	forward										0 B	0

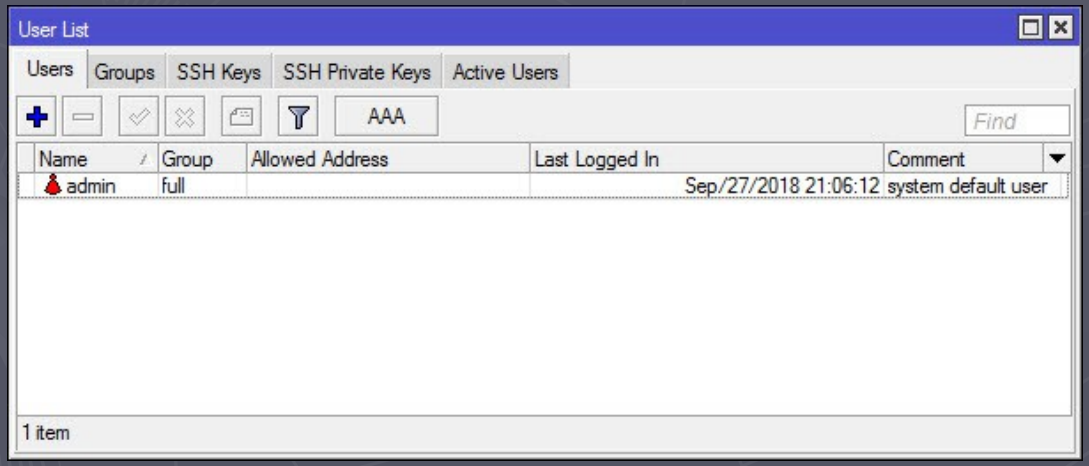
all
dynamic
forward
input
input
output
static

11 items (1 selected)

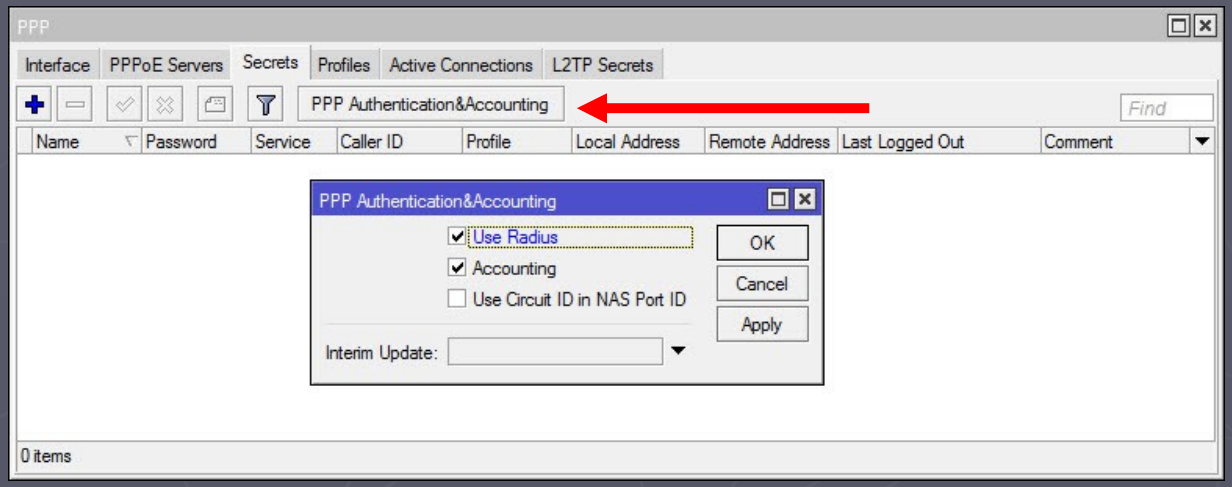
```
/command        use command at th
jan/02/1970 00:00:24 system,error
down
[admin@MikroTik] > /ip firewall filter set [find chain="input"] chain="input "
[admin@MikroTik] >
```

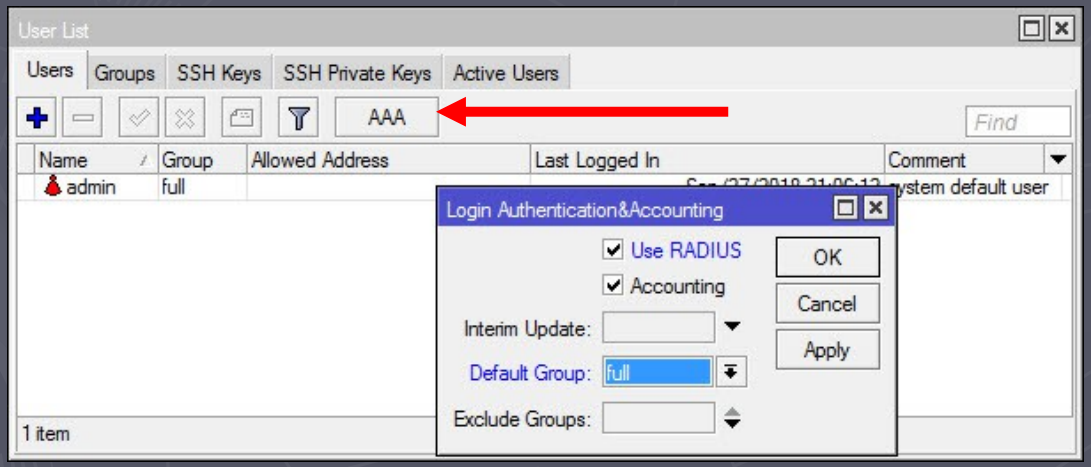
Список пользователей





Список пользователей





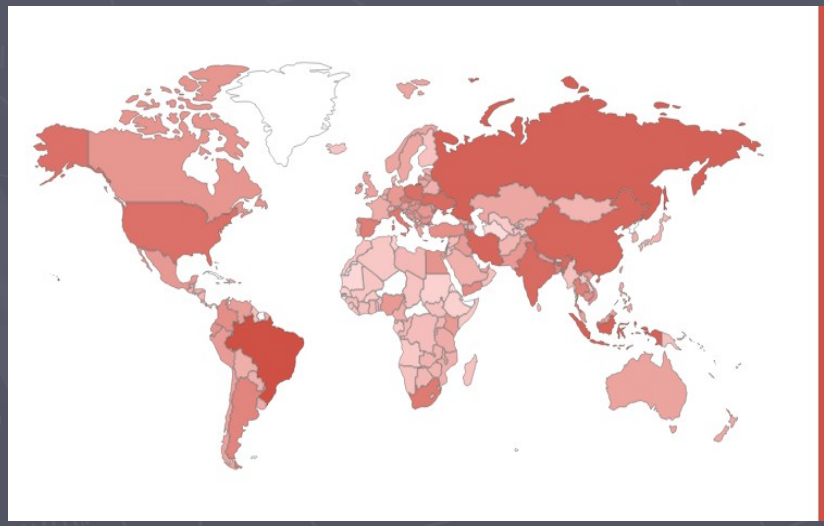
Ломаем микротик правильно

- Старый «новый» способ взлома
- Полноценный вирус на языке RouterOS
  полного кода здесь НЕ БУДЕТ
  Будут фрагменты
- Где спрятать секретный код?

Интересный отчёт

- https://www.shodan.io/report/DfYzmDYi

Открытые FTP-серверы MikroTik



Top Countries

1. Brazil	42,963
2. Russian Federation	23,476
3. Indonesia	22,354
4. Iran, Islamic Republic of	20,396
5. China	19,469
6. India	16,661
7. Ukraine	15,886
8. Poland	13,388
9. United States	13,033
10. Italy	9,486

Вирус-бутфорсер FTP

FTP – инструмент администратора !
Автоисполнение файлов script.auto.rsc

- ✓ RouterOS имеет средства работы с FTP
- ✓ В языке есть обработчик ошибок
- ✓ Много мест, где спрятать вируса в роутере
- ✓ Не нужен компьютер
- ✓ Не существует программы-антивируса

Вирус-бутфорсер FTP

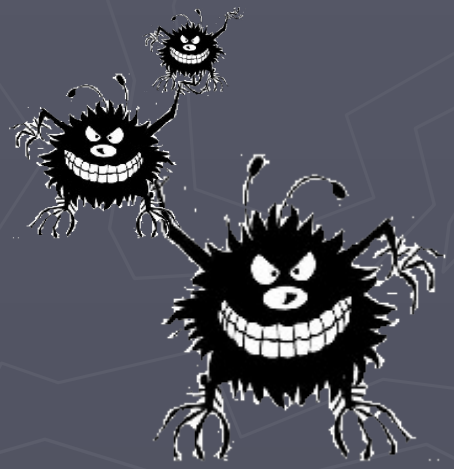
Простой отладочный вариант кода:

```
:local v [:toa "12345, password, 123, qwerty, admin"]
:local i 0
:local j [:len $v]
:while ((!ok)&&(i<j)) do={
:set $p [:pic $v $i] ;
:set $ok true;
:do {/too fe mode=ftp user=admin password=$p src-path=/vir.txt address=$addr
    port=21 dst-path=/vir.auto.rsc upload=yes} on-er={:pu ("Failed with
    password:".$p);set $ok false};
:if $ok do={:put ($p." is VALID password")};
set i ($i+1);
}
```

Процесс внедрения

С версии 6.42 права скриптов из NetWatch урезаны… но есть много иных интересных точек внедрения.

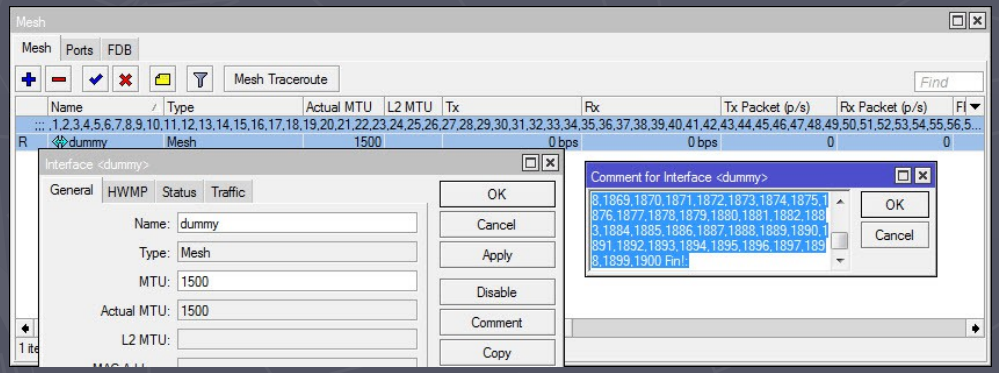
Scheduler – хорошее место. Но ненадежное. Туда можно «поселить» копию-«смертника». Админ найдет, порадуется и удалит не всё.



Тёмные уголки в MikroTik

Вирус для RouterOS, это скрипт. Скрипт, это переменная типа «string».

Возможно изменять вирус «на лету», сохранять в любых хранилищах скриптов: dhcp-lease, dhcp-client, dhcp-server-alert, ppp-profile, и много других точек.



Export против троянов

«/Export» показывает всю настроенную конфигурацию маршрутизатора.

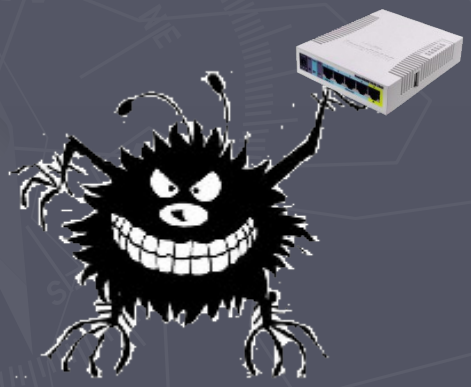
НО…

Существует возможность скрыть код от экспорта.

Демо?

Поиск жертв

1. Сканирование подсети
2. Просмотр neighbors list
3. Внешние списки с FTP другого микротика
4. Иные варианты



Как и зачем?

1. Мощные DDoS атаки трафик-генератором или ping.
2. Всё тот же фишинг и сниффинг
3. Распределенная сеть VPN
4. Выполнять произвольный код скачав его с C&C-сервера (fetch + import). Позволяет обойти ограничение на длину файлов 4k.
5. Для архитектуры MIPSBE (RB951, RB2011) возможно установить Bitcoin/Litecoin -майнеры

Зачем на самом деле?

- Изучить возможности встроенного скриптового языка RouterOS в части создания самоизменяемого самовоспроизводящегося кода;
- Привлечь внимание к уязвимым конфигурациям роутеров и простым паролям администраторов;

Спасибо за внимание!

Приходите к нам изучать MikroTik ☺