**Mikrotik с**ъбитие
за професионалисти ентусиасти и
всички който имат желание да
се **забавляват!**

# NetCamp

## 2021

# Mikrotik Scripting работа с файлове.
# Примерен скрипт за откриване на RANSOMWARE

Несебър 08.2021

# Да се запознаем

## инж. Георги Анастасов

*За мен!* *Сертифициран мрежов специалист и консултант за продукти на* ***Mikrotik*** *с опит в проектиране и изграждане на малки и средни компютърни мрежи, сървъри и системи за архивиране.*

**WEB: www.steadypc.com**
**E-mail: office@steadypc.com**
**GSM: +359 878806291**

# Mikrotik Scripting работа с файлове.

## Съдържание



# RANSOMWARE

Видове ransomware
Проблеми и възможни решения

01

# Mikrotik Scripting работа с файлове.
## Видове ransomware

### 1. Криптиране на файлове – cryptolocker.

- ❑ С промяна на файловите разширения;
- ❑ Без промяна на файловите разширения;
- ❑ Без промяна на файловите разширения като междинен слой

- подобно на Bitlocker

- отложено във времето до няколко месеца искане за откуп

- криптирани архиви

# Mikrotik Scripting работа с файлове.
# Защита за ransomware

## 2. Неотложни мерки

- ❑ Архивиране на данните;
- ❑ Подобрена защита на сървъра с архивите;
- ❑ Подобрена защита на софтуера за архивиране;

* Добре организиран достъп с права за различните групи потребители

https://www.veeam.com/blog/first-step-to-protecting-your-backups-from-ransomware.html

- ❑ Антивирусен софтуер - Декриптори – средно след 2 години

https://www.avast.com/ransomware-decryption-tools

### 3. Анализ на риска и оценка на загубите.

- ❑ Анализ на най-важните и най-слабите места;
- ❑ RPO – Recovery Point Objective – количеството загубени данни;
- ❑ RTO – Recovery Time Objective – времето за престой;
- ❑ Цена на престой и цена за необходимия софтуер и хардуер.

*Методология и софтуер за оценка?

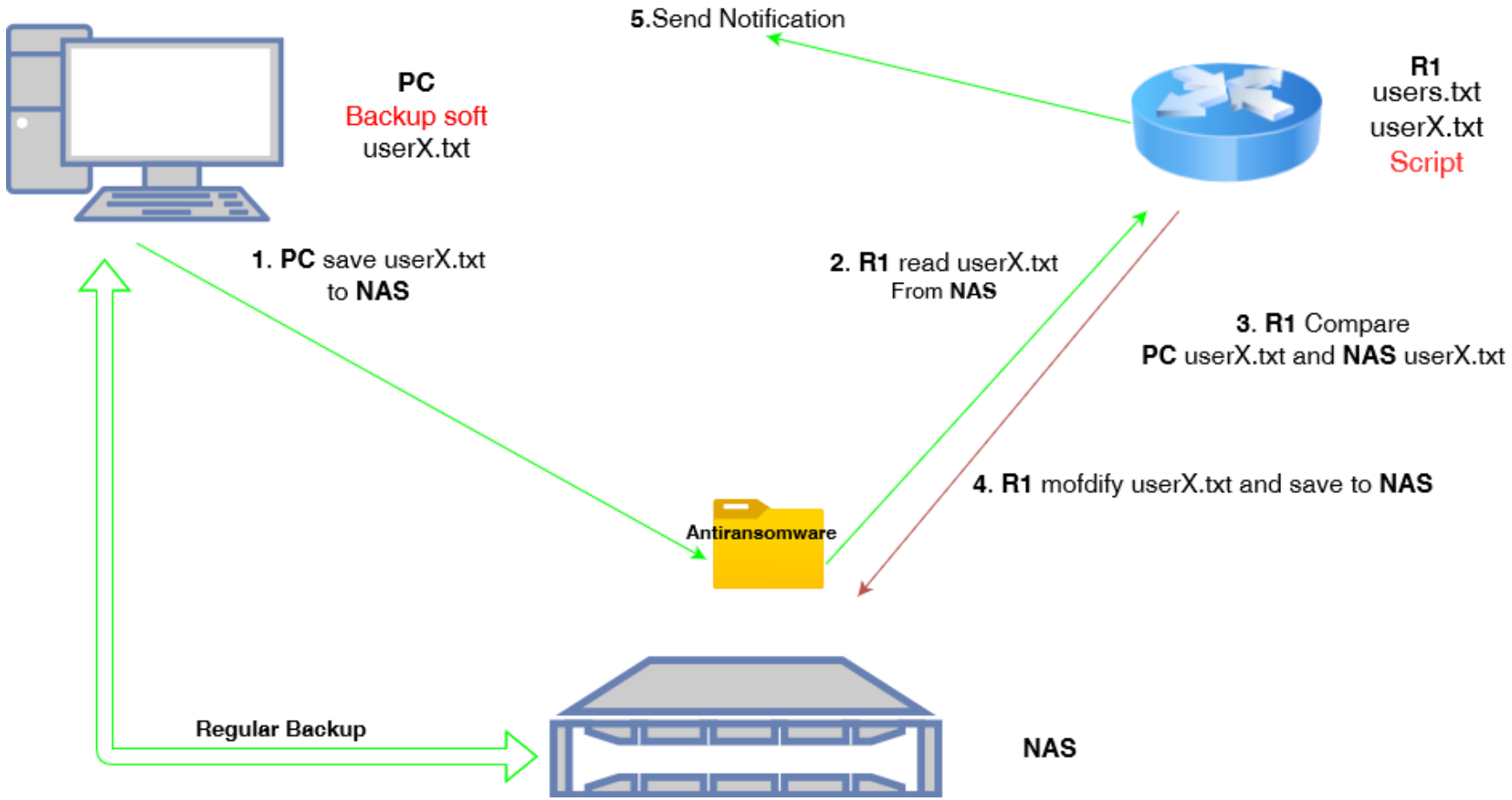
https://www.delltechnologies.com/asset/nl-be/products/storage/industry-market/recovering-business-destructive-cyber-attack.pdf

# Mikrotik Скриптове

02

Дефиниране на задачите
Проблеми
Изисквания и особенности в синтаксиса

# Mikrotik Скриптове
# Дефиниране на задачата



# Mikrotik Скриптове
# Дефиниране на задачата

**Предварително**

-Настройва се SFTP/SMB сървър в **NAS** с достъп до папка ransomware с потребител с достъп само до тази папка;

-В **NAS** архивиращото устройство 192.168.0.200 се създава споделена папка \\192.168.0.200\ransomware която да е отделна от другите задачи за архивиране;

- Създава се txt файл **userN.txt** със съдържание 20 (testword) символа за всяка клиентска **PC** машина.
N-номера на клиентската машина
Копират се файловете на две места - в рутера и на клиентската машина;

- Създава се **users.txt** файл с разделение запетая с имената на файловете и на потребителите, които се архивират в споделената папка ransomware

# Mikrotik Скриптове
# Дефиниране на задачата

1. Настройва се архивиращият софтуер да копира файловете в споделената папка  регулярно.

2. R1 прочита **userN.txt**

3. Стартира се скрипт в **R1** за сравнение на файловете в рутера и в sftp/smb сървъра.

Създава се цикъл за сравнение на съдържанието (testword ) на файла в архивиращото устройство със същия файл от рутера с брой цикли N равен на броя архивирани файлове равен на броя хостове за наблюдение равен на броя имена във файла **users.txt**

# Mikrotik Скриптове
# Дефиниране на задачата

3.1 Отваря се файла **users.txt** в **R1** и съдържанието се прочита и записва в масив usersArray;

3.2 Определя се броя файлове за проверка като се прочита броя елементи N на масива usersArray. Това определя и броя цикли на проверката;

3.3 Организира се **цикъл** за проверка на съдържанието на файловете от NAS
- Прочита се поредното име на файл от usersArray и се записва в променливата userfile;
- отваря се файла с $userfile име на sftp/smb сървъра и се прочита. Стойността се записва в променливата test.

3.4 Сравнява се test с testword и ако са различни, се уведомява администратора за възможно заразяване.

# Mikrotik Скриптове
# Дефиниране на задачата

4. Ако test и testword са еднакви, се сравнява  test с oldword и ако са различни, се модифицира **userN.txt,** като се записва съдържанието на файла backup-is-old.txt (oldword) в userX.txt файла в NAS.

4.1 Ако test и oldword са еднакви, се изпраща e-mail на администратора за проблем с архивиращата програма на userfile компютъра;

Цикъла се завърта отново

5.След края на цикъла, се изпраща e-mail или fetch телеграм съобщение до администратора, че проверката е завършила без проблем;

6. Създава се задача в  Scheduler, която да се стартира периодично в предварително избран час.

# 03

## Работа с файлове

Масиви. Четене и запис на файлове локално и отдалечено

# Работа с файлове
# Масиви

- Дефиниране на масив

```
:global usersArray array;
```

- Зануляване на масив

```
:set $usersArray ({}) ;
```

- Преобразуване на масив

```
:set usersArray [:toarray $content];
```

- Определяне броя елементи на масив

```
:set n [:len $usersArray];
```

# Работа с файлове
## Четене и запис

1. **Прочитане съдържанието на локални за рутера файлове**

$filenames – име на локалния файл

content – променлива в която се записва съдържанието на файла $filenames

```
:set  content [/file get [/file find name="$filenames"] contents] ;
```

# Работа с файлове
## Четене и запис

**2. Прочитане съдържанието на отдалечени sftp/smb за рутера файлове с fetch.**

set test [/tool fetch url="sftp://192.168.0.200/mnt/Backup1/ransomware/$userfilename" user=ftpuser password=PASSWORD as-value output=user ];

- Съдържанието на файла $userfilename се прочита и записва в променливата test

**3. Изчакване на операция прочитане на файл**

:set test [/tool fetch url="sftp:
:if ($test->"status" = "finished") do={

# Работа с файлове
## Четене и запис

**4. Запис на файл в отдалечени sftp/smb за рутера файлове с fetch.**

/tool fetch upload=yes url="sftp://192.168.0.200/mnt/Backup1/ransomware/$userfilename" user=ftpuser password=PASSWORD src-path=backup-is-old.txt keep-result=no;

- Съдържанието на локалният файл backup-is-old.txt  се записва в NAS във файл $userfilename

https://wiki.mikrotik.com/wiki/Manual:Tools/Fetch

# Работа с файлове
## Особенности при цикли

**5. Цикли**

```
:if ($test->"data" = $oldword) do={
#Comment between do and else are not permited
                                        tool e-mail send……. ;
                                } else={
```

# Работа с файлове

## Скрипт

```
#Antiransomware script v1
#Run script after all backups are done
#Save userfiles names in $userfilename text file in router in the following format "username1.txt"
"username2.txt" "username3.txt" .....
#Save information in each user file - testword

:global date [/system clock get date];
:global filedate;

#admin e-mail
:global adminmail "office@steadypc.com";

#variable filenames is file where is stored all names of user files
:global filenames "users.txt";

#Variable that read content of variable filenames
:global content;
```

# Работа с файлове

## Скрипт

```
# Array that is stored all names of user files from $content
:global usersArray array;

# Array index
:global a integer;

# Array lenght correspond to number of users
:global n ineger;

#Variable in wich user filename is read from userArray
:global userfilename;

#read content of the usefilename stores in NAS
:global test;

#text that is stored in each userfile an have to be compared that is not encrypted
:global testword "Test123@BGSoft.Local";

#Router save to NAS this text in userfilename after chach for $testword
:global oldword "Backup-is-old";
```

# Работа с файлове

## Скрипт

```
#read all filenames of user files and store it to Array
:set $usersArray ({}) ;
:set  content [/file get [/file find name="$filenames"] contents] ;

:set usersArray [:toarray $content];
:set n [:len $usersArray];
```

# Работа с файлове

## Скрипт

```
#Global Loop to check content of each user file
#read testword and userid of each userfile. If testword is different then is snding notification to
administrator
:for a from=0 to=($n-1) do={
        :set userfilename [($usersArray->$a)];
        :set test [/tool fetch url="sftp://192.168.0.200/mnt/Backup1/ransomware/$userfilename"
user=ftpuser password=BG192837465r! as-value output=user ];
:delay 1;
```

# Работа с файлове

## Скрипт

```
:if ($test->"status" = "finished") do={
                        :if ($test->"data" != $testword) do={
                                :if ($test->"data" = $oldword) do={
#if content of the usefilename is equal to oldword send email to admin with possible backup problem with user “userfilename“
#If content of usefilename is different from olword or testword - send email to admin with possible ransomware problem with userfilename
#Comment between do and else is not permited
                                                tool e-mail send to=$adminmail subject="$userfilename Possible backup problem" body="$date Possible antiransomware backup problem with user $userfilename";
                                        }  else={tool e-mail send to=$adminmail subject="$userfilename Ransomware infection" body="$date Possible ransomware infection with user $userfilename"};
                        };
        };
```

# Работа с файлове

## Скрипт

```
#Save content of file backup-is-old.txt "Backup-is-old" in $userfile to NAS
/tool fetch upload=yes url="sftp://192.168.0.200/mnt/Backup1/ransomware/$userfilename" user=ftpuser
password=BG192837465r! src-path=backup-is-old.txt keep-result=no;
};
#Send e-mail to admin that router has check NAS files
tool e-mail send to=$adminmail subject="Ransomware infection check done" body="$date Ransomware
infection check for $n users has done";
#END OF SCRIPT
```

04

# Софтуер за архивиране

Дефиниране на изискванията към софтуера за архивиране

SMB SFTP (SSH File Transfer Protocol)

# Софтуер за архивиране

- **Идея и изисквания;**
- **Примерни програми;**
- **Проблеми** за системните администратори

# Софтуер за архивиране
## Изисквания към софтуера

**1. Файловете за архивиране, да могат да се избират с Browse  и chackbox.**

- до  3 файла с избираемо разширение;

- Поле: Име на файла – име на потребителя;

- Избираемо поле - разширение – xlsx, docx, pdf, dwg, jpg, txt;

- съдържание на файла – до 20 символа – същото трябва да съвпада с фразата за проверка в рутера;

- Системата генерира файл с избраното разширение и съдържание, указано от потребителя или го избира.

# Софтуер за архивиране

## Изисквания към софтуера

**2 Местоназначение на файловете за архивиране**

- Да се въведе пътя на NAS  устройството и папката за архивиране в мрежата;

- Да се въведат данните на SFTP акаунта (username, password) за достъп до архивиращото NAS устройство;

- Данните за акаунта в SFTP сървъра да се съхраняват в криптиран вид;

- Да се архивира без компресия и криптиране;

- Приложението да се стартира автоматично като service в Windows.

2.1 Метод за трансфер на данните към архивиращото NAS устройството SFTP/SMB.

# Софтуер за архивиране
## Изисквания към софтуера

**3. Периодичност на архивирането**
- 1 на ден;
- на всеки X часа (X=1..24)

* Системата архивира файла в архивиращото устройство като изтрива предишния.

При влизане в SMB с Microsoft акаунт, за потребителско име трябва да се ползва MicrosoftAccount\me@email.com

# Софтуер за архивиране

## Примерни програми

- MiniTool® ShadowMaker
  https://www.minitool.com/backup/system-backup.html

- Iperius Backup
  https://www.iperiusbackup.com/download-software-backup.aspx

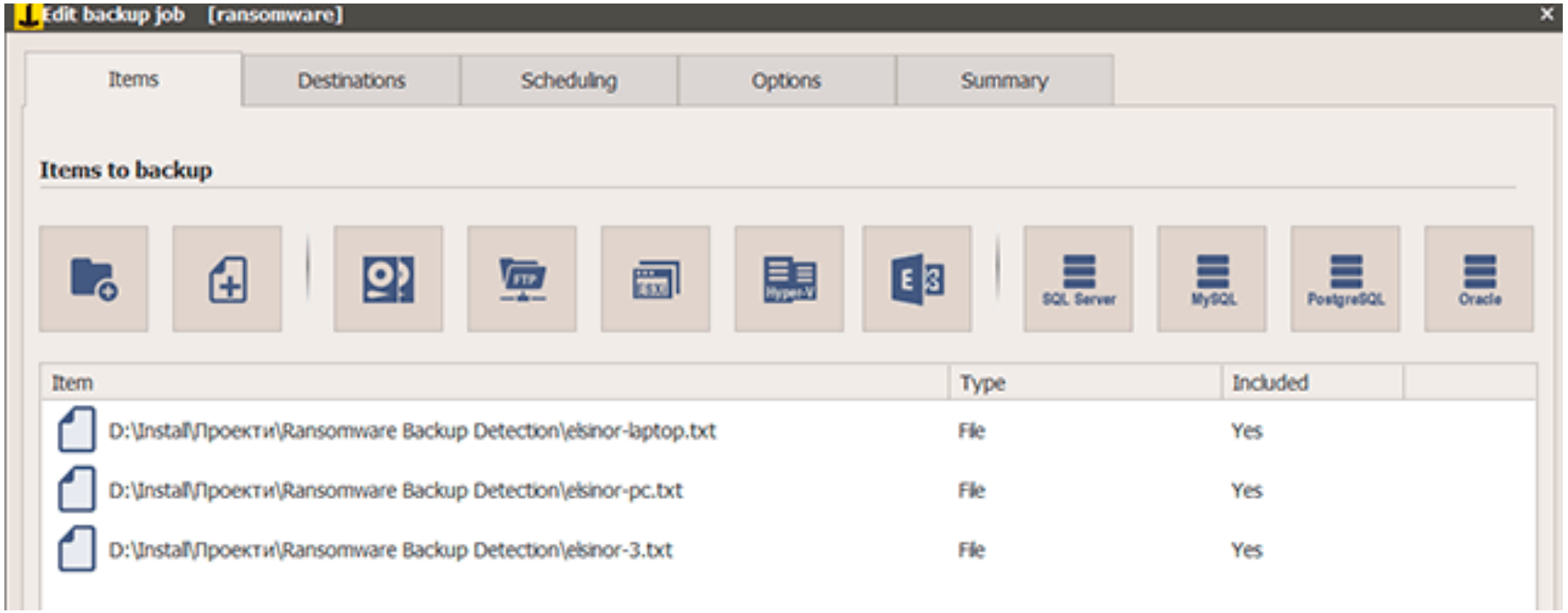
- EaseUS Todo Backup
  https://www.easeus.com/backup-software/tb-free.html

- FileFort Backup Software
  https://www.nchsoftware.com/backup/index.html

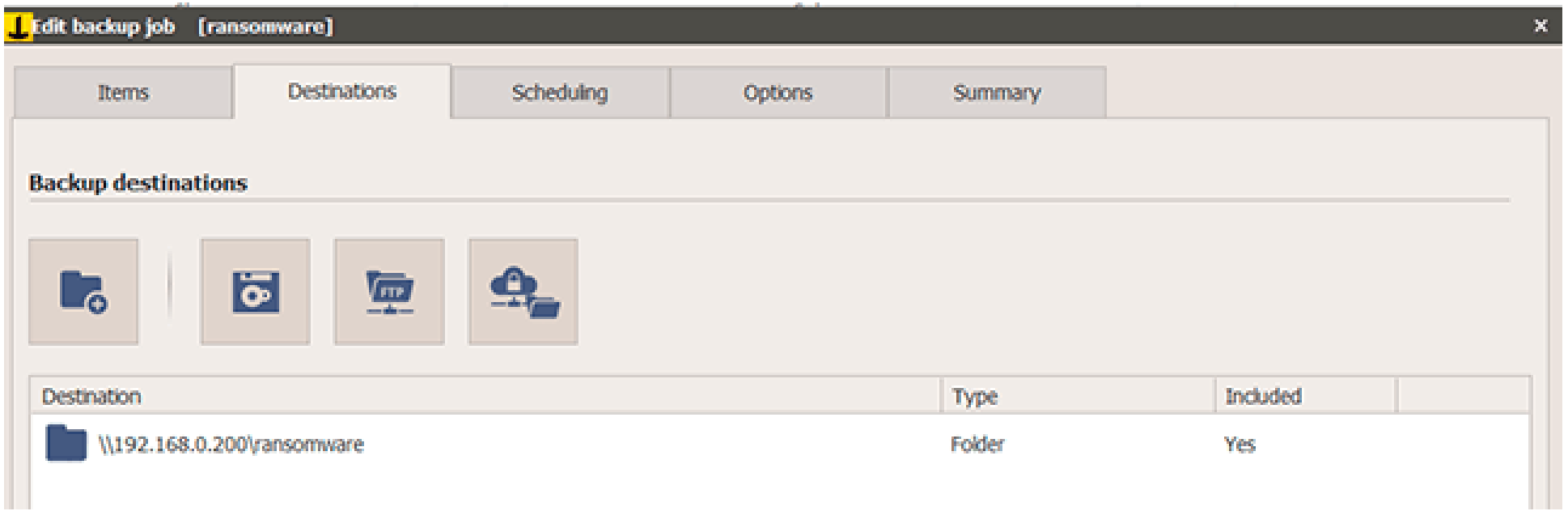
- Comodo BackUp
  https://www.comodo.com/home/backup-online-storage/backup-first-time-setup.php

# Софтуер за архивиране

## Примерни програми

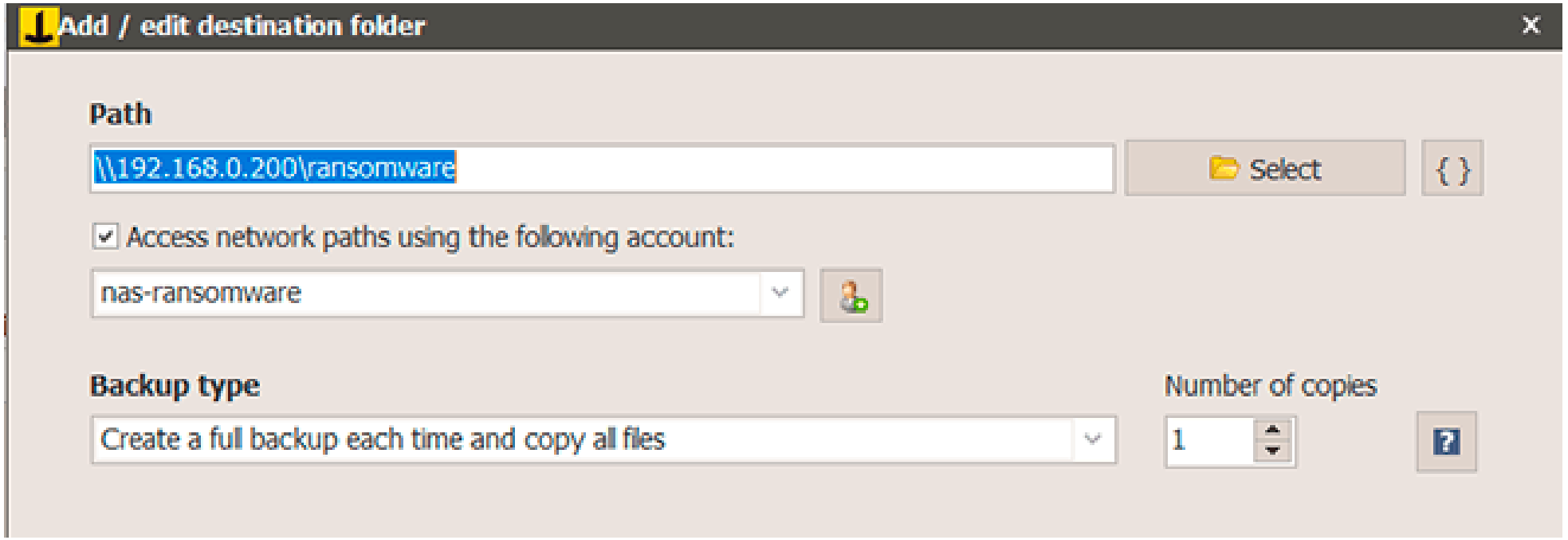


# Софтуер за архивиране
## Примерни програми



# Софтуер за архивиране

## Примерни програми



# Проблеми

**4. Конфликт с други архивиращи програми**

- При използване на метод с SMB архивиране е възможно да се получи конфликт с кеширани мрежови автентикации към архивиращото устройство от други архивиращи програми от същия компютър

Може да се провери наличието на подобни  connections с кеширани мрежови автентикации с командата net use.

Ако има подобен проблем, преди стартиране на копирането на файлове към архивиращото устройство трябва да се стартира следната команда:
net use * /delete /yes
net use \\servername /user:\\servername\username password

# Софтуер за архивиране 2

Собствено решение

05

# Софтуер за архивиране 2
## Собствено решение

В ПРОЦЕС НА  РАЗРАБОТКА

# SMB

В ПРОЦЕС НА  РАЗРАБОТКА

# SFTP

В ПРОЦЕС НА  РАЗРАБОТКА

# Архивиране на конфигурация

06

**NAS SMB**

Периодично архивиране на NAS

# Архивиране на конфигурацията
## NAS SMB

- **Четене на датата**

:global newdate [/system clock get date];  **Aug/28/2021;**

- **Извличане на части от стринг с команда pick**

:pick <var> <start>[<end>]

:put [:pick "abcde" 1 3]  - извлича елемент от <start> включително до преди <end>
01234  Броенето започва от 0.
bc

# Архивиране на конфигурацията
## NAS SMB

❑ **Търсене на елемент от стринг или масив с find**

:find <arg> <arg> <start> - връща позицията на търсения елемент в стринга или масива

:put [:find "mikrotik" k 1];
2
:put [:find "mikrotik" k 2];
7

:local text “abcde”
:put [:pick $text 1 [:find $text “d”] ]
bc

:put [:find "abc" "a" -1];

# Архивиране на конфигурацията
## NAS SMB

- Слепване на стрингове **concatenation** - с точка

**28-aug-2021**

:global filename ("$id"."-"."$dd"."-"."$mmm"."-"."$yyyy");

- Слепване на масиви – със запетая.

# Архивиране на конфигурацията

## NAS SMB

```
#Backup to NAS smb script
:global adminmail "office@steadypc.com";

#get date and system identity of the router
:global newdate [/system clock get date];
:global id [/system identity get name];

#convert mmm/dd/yyyy to dd-mmm-yyyy
:global mmm [:pick $newdate 0 3 ];
:global dd [:pick $newdate 4 6 ];
:global yyyy [:pick $newdate 7 11 ];

#concatenate id and date in filename
:global filename ("$id"."-"."$dd"."-"."$mmm"."-"."$yyyy");
```

# Архивиране на конфигурацията
## NAS SMB

```
#Export configuration
:export file=ros-backup.rsc;

#Save backup file with new name to NAS
/tool fetch upload=yes url="sftp://192.168.0.200/mnt/Backup1/mikrotik-backup/$filename"
user=ftpuser password=PASSWORD src-path=ros-backup.rsc keep-result=no;

#Send e-mail to admin that router has save backup file to NAS
tool e-mail send to=$adminmail subject="$id Sucsesful save backup file"
body="$[/system clock get date] Router $id Sucsesful save Backup configuration file to
NAS";
#END OF SCRIPT
```

# ВЪПРОСИ

# Благодаря за вниманието!