[10 - Router Forensics] GFOSS - Panoptis

Το mikrotik router έχει την έκδοση RouterOS 6.40.5 που ήταν ευάλωτη στο CVE 2018-14847. Με αυτό το CVE ο κακόβουλος χρήστης πήρε τα στοιχεία του admin. Επειδή δεν είχε μπει access list ώστε η διαχείριση να γίνεται μόνο από το εσωτερικό δίκτυο, χρησιμοποιήθηκε το WinBox για την εγκατάσταση ενός web proxy και μετά με την βοήθεια του filezilla (sftp) διέγραψε τα html αρχεία του proxy και έβαλε ένα νέο αρχείο (error.html) το οποίο περιείχε σε javascript έναν miner. Αυτό είχε ως αποτέλεσμα οι χρήστες του δικτύου όταν προσπαθούσαν να συνδεθούν σε μία σελίδα, να γίνονται όλοι miners.

Για την εκμετάλλευση του CVE 2018-14847, χρησιμοποιήθηκε κάποιο αυτά exploit scripts ή κάποιο δικό του.

https://github.com/BasuCert/WinboxPoC Exploit Mitigation Third Party Advisory
https://github.com/BigNerd95/WinboxExploit Exploit Mitigation Third Party Advisory
https://github.com/tenable/routeros/blob/master/bug_hunting_in_routeros_derbycon_2018.pdf Exploit Third Party Advisory https://github.com/tenable/routeros/tree/master/poc/bytheway Exploit Third Party Advisory
https://github.com/tenable/routeros/tree/master/poc/cve_2018_14847 Exploit Third Party Advisory https://n0p.me/winbox-bug-dissection/ Exploit Third Party Advisory
https://www.exploit-db.com/exploits/45578/

Δοκιμάσαμε το 2ο και είδαμε ότι δούλεψε με επιτυχία

panoptis@panoptis_2019:/tmp/WinboxExploit$ python3 WinboxExploit.py 192.168.192.60 192.168.192.60
User: admin
Pass:

User: admin
Pass:

User: admin
Pass: 123456

Πρόσθεσε έναν κανόνα στο firewall ώστε να κάνει redirect την 8080 στην 80 και απενεργοποίησε το web service, έτσι ώστε να μην εμφανίζεται το πραγματικό login page του mikrotik, αλλά το error.html που χρησιμοποιεί ο proxy.

Επίσης δημιούργησε τα παρακάτω scripts

name="test" owner="admin"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
last-started=jun/13/2019 01:55:13 run-count=213 source=dns_lookup

name="mydns" owner="admin"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
last-started=jun/13/2019 01:54:52 run-count=217 source=dns

name="dns2" owner="admin"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
last-started=jun/13/2019 01:54:48 run-count=233 source=./dns

Τα οποία τα εκτελεί με κάποιους schedulers αντίστοιχα.

name="dns_lookup" start-date=jun/04/2019 start-time=08:09:13 interval=1m
on-event=test owner="admin"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon run-count=217
next-run=02:00:13

name="dns_controler" start-date=jun/04/2019 start-time=08:15:52 interval=1m
on-event=mydns owner="admin"
policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon run-count=217
next-run=02:00:52

name="mydns2" start-date=jun/04/2019 start-time=08:21:48 interval=1m on-event=dns2
owner="admin" policy=ftp,reboot,read,write,policy,test,password,sniff,sensitive,romon
run-count=217 next-run=02:00:48

Το error.html που πρόσθεσε ο χρήστης, περιέχει επίσης ένα κομμάτι javascript κώδικα το οποίο ανοίγει ένα socket και συνδέεται σαν client στον server 192.168.22.62:4444. Ο client, παίρνει σαν input ότι shell του στείλει ο server και επιστρέφει το stdout και stderr στον server. Έγινε κάποια προσπάθεια προσομοίωσης αλλα δυστυχώς δεν τα καταφέραμε.

Εξερευνώντας το δίσκο του Router, παρατηρήσαμε ότι έχει 2 partitions.
Στο πρώτο partition(boot partition), ο κακόβουλος χρήστης τοποθέτησε ένα backdoor με όνομα “test”, 4 Ιουνίου και ώρα 09:02, το οποίο εκτελείται κάθε φορά που κάνει reboot η συσκευή.
Όταν εκτελείται, προσπαθεί να συνδεθεί στον ίδιο server (192.168.22.62) με mysql protocol.
Ο js κώδικας στο αρχείο error.html και το backdoor test συνδέονται σε κάποιο host, private δικτύου (192.168.22.0).

Έγινε χρήση του wireshark κατά την εκτέλεση του test και δεν φαίνεται να κάνει κάποιο tunneling.

Συνδέονται κάπου τοπικά(σε pc - vm που βρίσκεται στο ίδιο δίκτυο ή σε δίκτυο που δρομολογείται από κάποιον άλλον κεντρικό router).