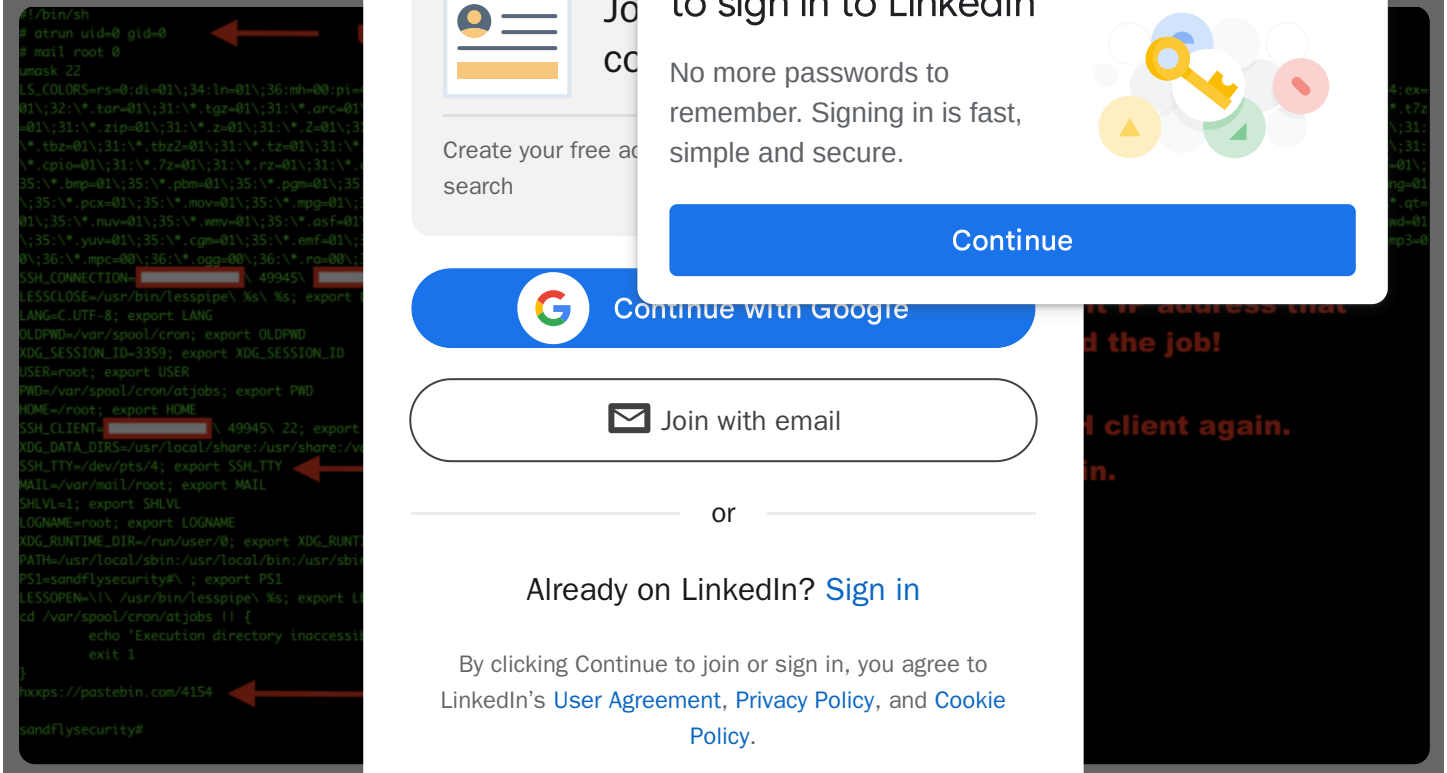
Top Content



Investigating Malicious Linux At Jobs - Sandfly Security, Ltd.

Getting an Attacker IP Address from a Malicious Linux At Job

Craig Rowland

Published Jul 25, 2019

+ Follow

repeatedly like *cron*. But consider if a

from the date of intrusion. You may th

at a future date whe me mat again for them.

This is why it's alwa *t* commands you don't recognize with st. But also, it's not a bad idea to m ot running things they shouldn't. For i jobs is mandatory. This is b mand you are in luck because by def f the system into the entry.

Checking for Malic

There are two ways y command to dump all at jobs and then

```
root@ubuntu-18-1
2       Sat Jul
3       Sat Jul 25 21:56:00 2020 a root
4       Sat Jul 25 21:56:00 2020 a root
1       Sat Jul 25 21:32:00 2020 a root
root@ubuntu-18-1:~#
```

The above we see four jobs for the root user. The first column is the *at* job number which we can list individually with the *at -c <jobnum>* command:

```
LANG=C.UTF-8; export LANG
OLDPWD=/var/spoo
XDG_SESSION_ID=3
USER=root; expor
PWD=/var/spool/c
HOME=/root; expo
SSH_CLIENT=192.1
XDG_DATA_DIRS=/u                                              ktop; export XDG_DAT
SSH_TTY=/dev/pts
MAIL=/var/mail/r
SHLVL=1; export
LOGNAME=root; ex
XDG_RUNTIME_DIR=
PATH=/usr/local/                                              t/bin:/usr/games:/us
PS1=sandflysecur
LESSOPEN=\|\ /us
cd /var/spool/cr
        echo 'E
        exit 1
}
hxxps://pastebi
```


This dumps each job number and you can see some interesting things. The most import part is the SSH_CONNECTION and SSH_CLIENT variables. These contain the IP addresses of the machine that created the jobs!

If you want to see all the *at* jobs at once quickly, you can simply use the cat command to dump them like this:

Always Check At J

In general, *at* jobs a ux hosts. If you see an *at* job and you di no did and why. If you're investigating od idea and can give you valuable clu ir connection information from oth

Have Sandfly Che

Even better than wa bs, you can have our agentless secur e persistence attacks on Linux 24 we'll show you what it is in plain details.

James King 6y

Love these blog posts, keep up the good work!

Like · Reply | 1 Reaction