

# Pinkslipbot C&C Proxy Checker

©2017 McAfee LLC

Pinkslipbot C&C Proxy Checker is a command line tool to detect and remove port-forwarding rules maliciously created by W32/Pinkslipbot on home routers. In addition, the tool can detect and disable the malicious service used to repurpose infected machines as command-and-control servers.

## Commands

Command	Description
-h (or) -help (or) /?	Show this help message
-d (or) -del (or) /del	Remove Malicious Port Mappings and Disable Pinkslipbot C&C Service
--thirdparty	Display License Information for third-party libraries used.

## System Requirements

To use this tool, you must have:

- A computer running Windows XP or higher
- An active network connection

## Usage

To use this tool, open a command-prompt window and execute the program without any parameters like so.

```
C:\>AmIPinkC2.exe
```

This runs the tool in “*Detect ONLY*” mode where it finds malicious Pinkslipbot services and port-forwarding rules but does not remove them. The screenshot below shows the output of the tool when it finds a malicious service installed on the local machine and port-forwarding rules created on the router.

```

Administrator: Command Prompt
E:\amipink>AmIPinkC2.exe
-:~
sys+:. -/shdd` oy+- ./sy syy: -yyyys`
syyyyyosdddddd` oyyys/.:syyy /+++` /yyy- syy` .:++:. .:/+/.
syy:.:+shy+:~ddd` oyyssyyyssyy +yys++syy: :yyoyyy. .syyss .syy++oyys. `oyyo+oyys.
syy: .ddd` oyy/ -+:` .yyy +yy/ -yys -yys` /yyy// yyyo+++oyys syyo+++oyyy`
syy: .ddd` oyy/ .yyy +yy: .yyyyyyyyyo yyy yyy+///// syyo/////`
syy/~` /ddd` oyy/ .yyy `oyys++syy:~yyy////oyy+ yyy -syy+/+ss/ .syy+/+ss/
+yyys+::oydddy /oo- .ooo .:~oo+:` +oo- ~oo- +oo -/+o+/- -/+oo+:`
.:+syddhs/-`
-:~
Pinksliptbot Control Server Proxy Detection and Port-Forwarding Removal Tool v1.0 - (C) 2017 McAfee LLC

[MODE] Running in mode: Detect (for disable features pass /del)
[INFO] Looking for Pinksliptbot C2 Proxy Service.
[MLWR] Active Service (hwmon) found at C:\WINDOWS\SysWOW64\rundll32.exe "C:\ProgramData\HardwareMonitor\hardwaremonitor.dll",HwmonServerMainNT
[INFO] Looking for UPnP devices...
List of UPnP devices found on the network :
URL: http://192.168.1.1:5555/rootDesc.xml
Type: urn:schemas-upnp-org:device:InternetGatewayDevice:1

Found a potential Gateway Device at http://192.168.1.1:5555/ctl/IPCConn.
[INFO] Local IP Address: 192.168.1.3
[INFO] External IP Address: 10.120.1.205
[INFO] Retrieving Port Forwarding Rules from gateway device.
Index Proto ExPort InAddr:InPort Description RemoteHost
0 TCP 443 192.168.1.3:443 'NAT-PMP 443 tcp' ''
[MLWR] Potential Pinksliptbot created Port-Forwarding Rule FOUND

E:\amipink>

```

If no infection is found, your system is not vulnerable and you do not need to do anything else.

However, if the output from your execution looks like the screenshot above, you should run the tool again from an elevated command-prompt and pass the “/del” parameter. This instructs the tool to disable the malicious service and remove maliciously created port forwarding rules on your router. The screenshot below shows the output of the tool when run with the “/del” parameter.

```
Administrator: Command Prompt
E:\amipink>AmIPinkC2.exe /del
-.-.-
sys+:. -/shdd` oy+- ./sy` syy: -yyys`
syyyyyyosdddddd` oyyys/.:syyy` :/++:` /yyy- syy` .:++:. .:/+/.
syy:.:+shy+: -ddd` oyyssyyyyssyy` +yys++syy: :yyoyyy. .syyss .syy++oyys. `oyyo+oyys.
syy: .ddd` oyy/ -+:`.yyy +yy/` -yys -yys` /yyy// yyyo+++oyys syyo+++oyyy`
syy: .ddd` oyy/ .yyy +yy: .yyyyyyyyyo` yyy yyy+///// syyo/////`
syy/` /ddd` oyy/ .yyy` oyyss++syy: .yyy/////oyy+` yyy -syy+/+ss/` .syy+//ss/`
+yyys+::oydddd` /oo- .ooo .:+oo+:` +oo-` +oo- +oo -/+o+/-` -/+oo+:`
.:+syddhs/-`
-.-.-
Pinksliptbot Control Server Proxy Detection and Port-Forwarding Removal Tool v1.0 - (C) 2017 McAfee LLC

[MODE] Running in mode: Detect + Disable
[INFO] Looking for Pinksliptbot C2 Proxy Service.
[MLWR] Active Service (hwmon) found at C:\WINDOWS\SysWOW64\rundll32.exe "C:\ProgramData\HardwareMonitor\hardwaremonitor.dll",HwmonServerMainNT
[KILL] Stopping and Disabling Service: Successful
[INFO] Looking for UPnP devices...
List of UPnP devices found on the network :
URL: http://192.168.1.1:5555/rootDesc.xml
Type: urn:schemas-upnp-org:device:InternetGatewayDevice:1

Found a potential Gateway Device at http://192.168.1.1:5555/ctl/IPConn.
[INFO] Local IP Address: 192.168.1.3
[INFO] External IP Address: 10.120.1.205
[INFO] Retrieving Port Forwarding Rules from gateway device.
Index Proto ExPort InAddr:InPort Description RemoteHost
0 TCP 443 192.168.1.3:443 'NAT-PMP 443 tcp' ''
[MLWR] Potential Pinksliptbot created Port-Forwarding Rule FOUND
Port Mapping Removal: Success

E:\amipink>
```

You should run the tool again to confirm that the repair functionality worked as intended. If everything worked as expected, your output should look similar to the screenshot below.

```

Administrator: Command Prompt
E:\amipink>AmIPinkC2.exe
-.-
sys+:.  -/shdd`  oy+-  ./sy  syy:  -yyys`
syyyyyosdddddd`  oyyys/.:syyy  `:/++:`  /yyy-  syy`  .:++:.  .:/+/.
syy:~+shy+:~ddd`  oyyssyyyyssyy  +yys+syy:  :yyoyy.  .syyss  .syy++oyys.  `oyyooyys.
syy:  .ddd`  oyy/ -+:`.yyy  +yy/  -yys  -yys`  /yyy//  yyyo++oyys  syyo++oyyy`
syy:  .ddd`  oyy/  .yyy  +yy:  .yyyyyyyyyo  yyy  yyy+/////  syyo/////`
syy/  `/ddd`  oyy/  .yyy  `oyys+syy:.yyy////oyy+  yyy  -syy+/ss/  .syy+//ss/
+yyys+::oyddd  /oo-  .ooo  .:~oo+:`  +oo-  `+oo-  +oo  -/+o+/-  -/+oo+:`
.:+syydhs/-`
-.-

Pinksliptbot Control Server Proxy Detection and Port-Forwarding Removal Tool v1.0 - (C) 2017 McAfee LLC

[MODE] Running in mode: Detect (for disable features pass /del)
[INFO] Looking for Pinksliptbot C2 Proxy Service.
[MLWR] Disabled Service (hwmon) found at C:\WINDOWS\SysWOW64\rundll32.exe "C:\ProgramData\HardwareMonitor\hardwaremonit
or.dll",HwmonServerMainNT
[INFO] Looking for UPnP devices...
List of UPnP devices found on the network :
URL: http://192.168.1.1:5555/rootDesc.xml
Type: urn:schemas-upnp-org:device:InternetGatewayDevice:1

Found a potential Gateway Device at http://192.168.1.1:5555/ctl/IPConn.
[INFO] Local IP Address: 192.168.1.3
[INFO] External IP Address: 10.120.1.205
[INFO] Retrieving Port Forwarding Rules from gateway device.
Index Proto ExPort InAddr:InPort Description RemoteHost
[INFO] Port Forwarding Rules do not exist.

E:\amipink>

```

## Notes

This tool is not a replacement for anti-malware software. It will just disable (and not remove) the malicious Pinksliptbot service if found.

While great care has been taken to identify port-forwarding rules malicious created by Pinksliptbot, they are often used for legitimate purposes, such as hosting a web server on your computer. Please run the tool in *detect only* mode and confirm that the port-forwarding rules were not created by you before removing them using the “/del” parameter.

## Third-Party Licenses

This tool uses “MiniUPnPc”, an excellent open-source library for adding UPnP IGD control point support. Its license is listed as follows.

```

MiniUPnPc
Copyright (c) 2005-2016, Thomas BERNARD
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions are met:

```

- \* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- \* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- \* The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.