Pinkslipbot C&C Proxy Checker

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:

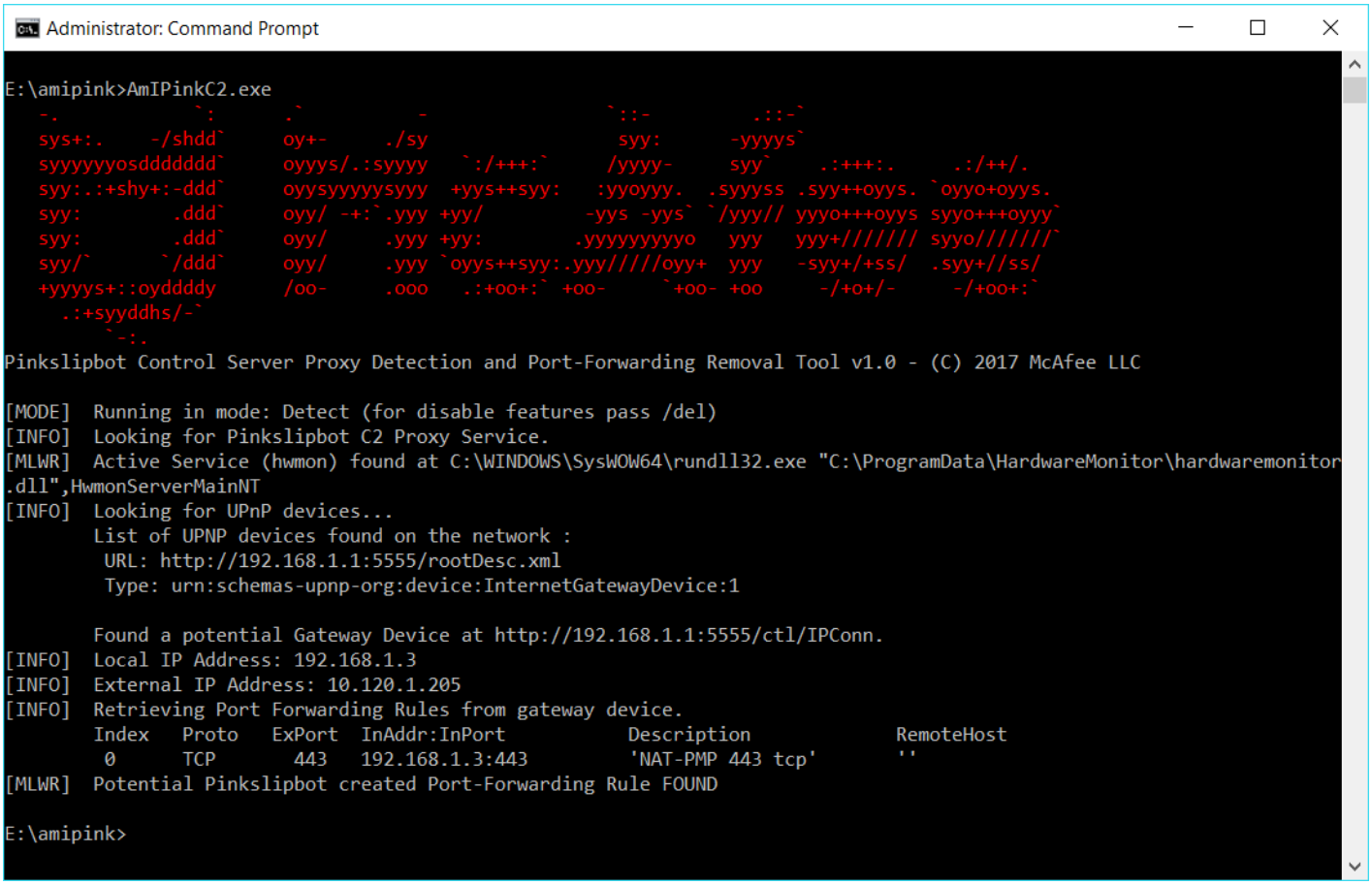
- A computer running Windows XP or higher
- An active network connection

Usage

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

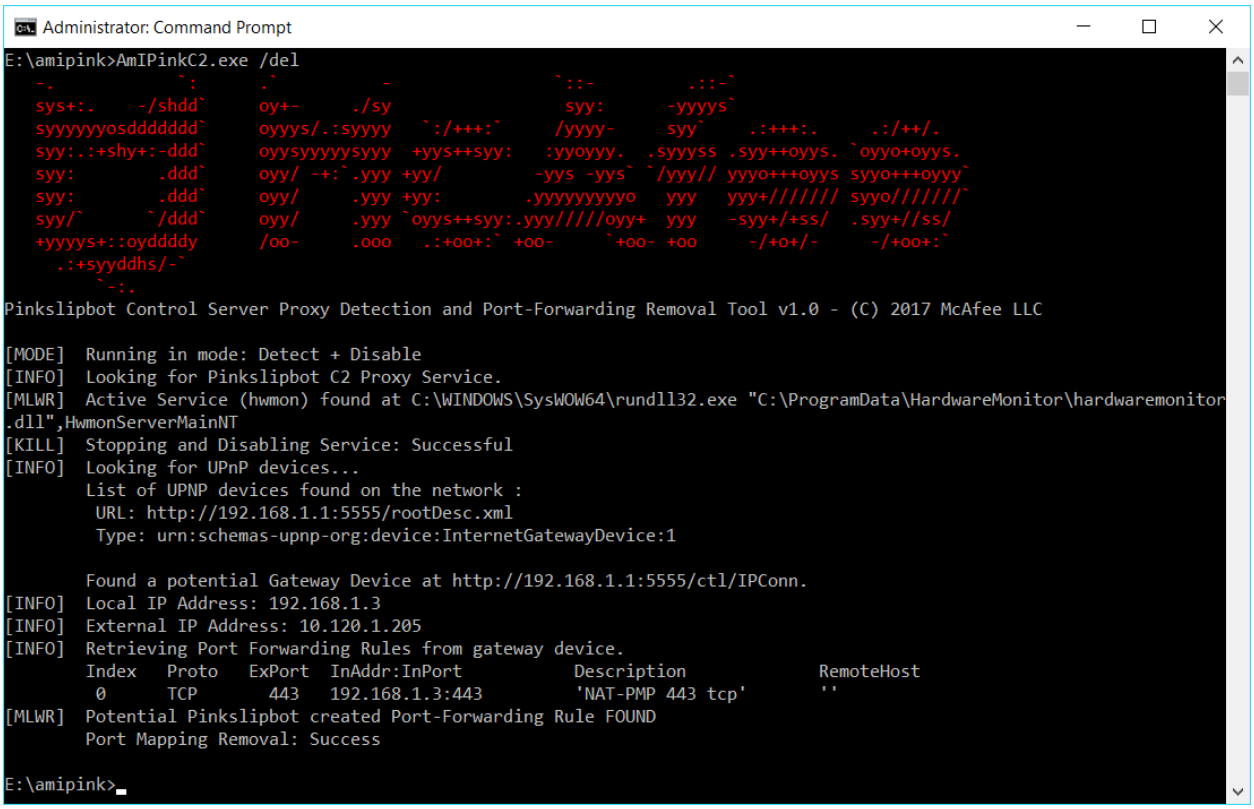
C:\>AmIPinkC2.exe

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.

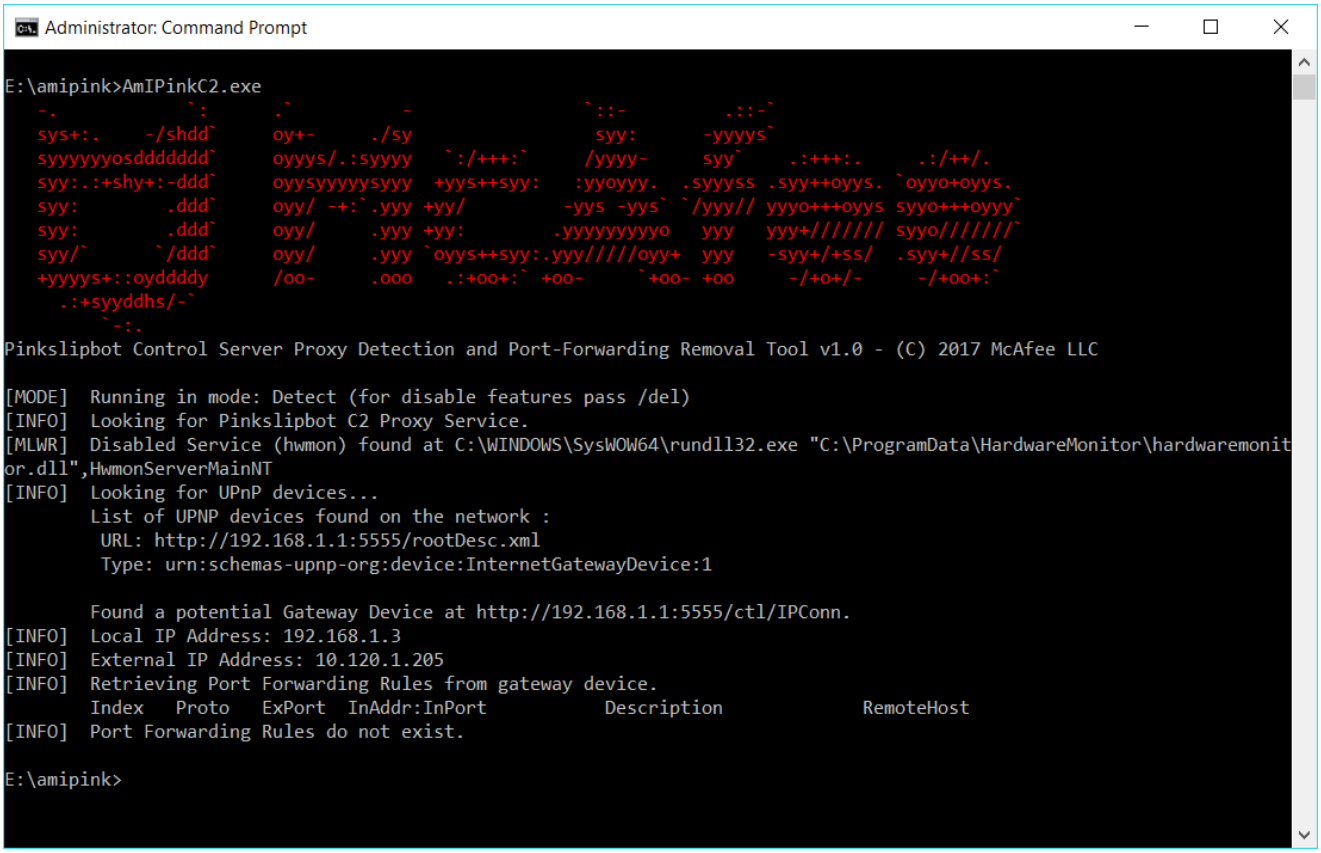


If no infection is found, your system is not vulnerable and you do not need to do anything else.

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.



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.



Notes

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

While great care has been taken to identify port-forwarding rules malicious created by Pinkslipbot, 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.