**CEG4430/6430 Homework 3**

(50 Points)

1. Conficker is a piece of sophisticated malware. Many of its designs aim at counteracting the malware analysis, detection, and disruption techniques. Please read the given article (conficker.pdf) and answer the following questions.
   1. A student wants to capture the first packet after 3-way handshake sent from a Conficker binary to the web-based C&C server. Of course, this binary will generate a large number of randomly generated domains. Towards this end, the student leverages the open source DNS relay we used for the lab and configures the conficker-infected host to use this DNS relay as the recursive DNS server. The student instruments the DNS relay to directly answer all DNS requests generated by the infected host.
      1. Scenario-1: The DNS responses (answers) will contain two IP addresses of two web servers that are managed by this student. Will this student be able to capture the first packet after the 3-way handshaking initiated from the Conficker-infected host to his/her server? Justify your answer. (5 Points)

Answer Question 1.a.i: By reading the HW3\_Conficker paper, it is impossible for the student to capture any packets because according to the document specifically with the Domain Generation Algorithm during a check if more than on eIP address is detected then the connection automatically fails.

* + 1. Scenario-2: The DNS responses (answers) will contain one IP address of one web server that is managed by this student. Will this student be able to capture the first packet after the 3-way handshaking initiated from the Conficker-infected host to his/her server? How many such packets can be observed if your answer is not 0? Justify your answer. (5 Points)

Answer Question 1.a.ii: I believe that occording to the document again regarding the Domain Generation Algorithm like for the question before, the student will not be able to capture any packets after the 3-way handshake. This I am justifying with the fact that the IP address returned is one to a web server managed by the student. By reading back through the document is states that an IP addres that is for a local host (127.0.0.1) or other trivial address then the connection will fail. Because this address is a server address, I believe that is falls into the same situation meaning that the TCP connection will fail and no packets will be captured as a result.

* 1. You have installed an antivirus tool called “avenger”. Unfortunately, when Conficker attempts to compromise your host, the avenger is not up to date. Therefore, your host is infected by Conficker successfully. Later, the update is available for this tool to download and install. Will avenger now be able to detect Conficker in your host? (5 Points)

Answer Question 1.b: Once the Conficker infection has taken affect on the system, With this in mind, the infection stops all use of security software and future uses. By that point making any updates to the security useless as the user will not be able to install or even know when they are available. even if there is a new updated version of the security software known as avenger that is used for your system after the infection has already taken place, the user will be unable to install or run the security software at all. This is because of how Conficker C operates by disabling security software and stopping any future updates from being installed and notifications of updates as well.

* 1. Determine if the following statements are true or false and justify your answer.
     1. A Conficker-infected host will result a large number of failed DNS queries (i.e., NXDOMAIN responses) (5 Points)

Answer Question 1.c.i: True, this is based on the Conficker document and specifically when it stats that NXDOMAIN reponses failed when they were unregistered only.

* + 1. A Conficker-infected host will cause a large number of failed TCP connections (5 Points)

Answer Question 1.c.ii: True, this is based on the check system that in place when dealing with TCP 3-way handshake connections when IP address are generated.

* + 1. All IP addresses that are connected by a Conficker are malicious (i.e., either C&C server or other infected peers). (5 Points)

Answer Question 1.c.iii: True, based on reading the Conficker document and the information regarding Conficker connections specifically with C&C server or other infected peers, when you connect to a infected Conficker connection that connection is a malicious connection no matter what.

1. You are provided with the source code for an IRC-based bot (in the .zip file). This is a real bot that can be used for various malicious purposes. It implements all the basic functionalities of a bot. For example, it can update itself and is capable of launching DDoS attacks. It is invaluable resource for you to learn how malware works under the hood although this code is a baby-version. Please answer the following questions and **justify your answers** based on your analysis of the source code (e.g., list the code snippet and explain its function if necessary). The code is available from

<https://www.dropbox.com/s/to2y2kafjhm0gv3/IRCBot.student.zip?dl=0>

* 1. **Question:** For the command in the table**,** please describe what this command is used for, provide **evidence for conclusion based on source code and analysis**, and an example of its usage. (5 Points)

Command: login

Function: Allow the bot to login to the system using the owners login info.

Evidence: Code comments will ask the bot for the login credentials and then the code shows the process of logging in.

Example:

A screenshot of a social media post

Description automatically generated

Command: open

Function: used to open a folder or possibly a file in the system as well as access to other data in the system.

Evidence: There is an example that comments that attempt at opening and seeing information within the system.

Example:

A screenshot of a cell phone

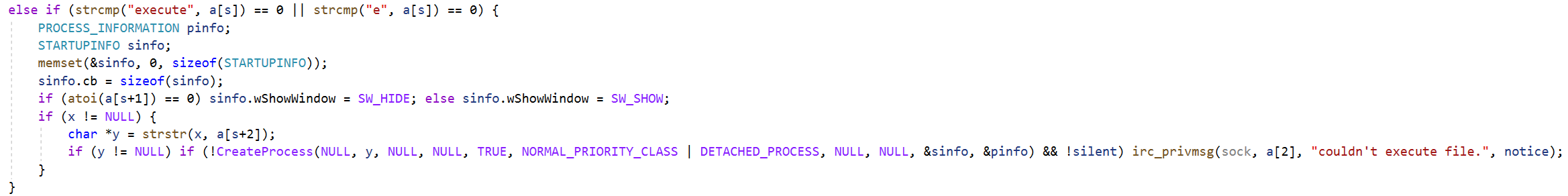
Description automatically generated

Command: execute

Function: this is a command that can be used to startup a program, or piece of software, or even continue to send in information and move onto the next step in what goes on. It can also be used to activate another command as well.

Evidence: There is an example of the command in use to display information to the bot.

Example:



Command: die

Function: The function of this command could be used to destroy the bot when needed.

Evidence: An example of the command in use.

Example:

A screenshot of a cell phone

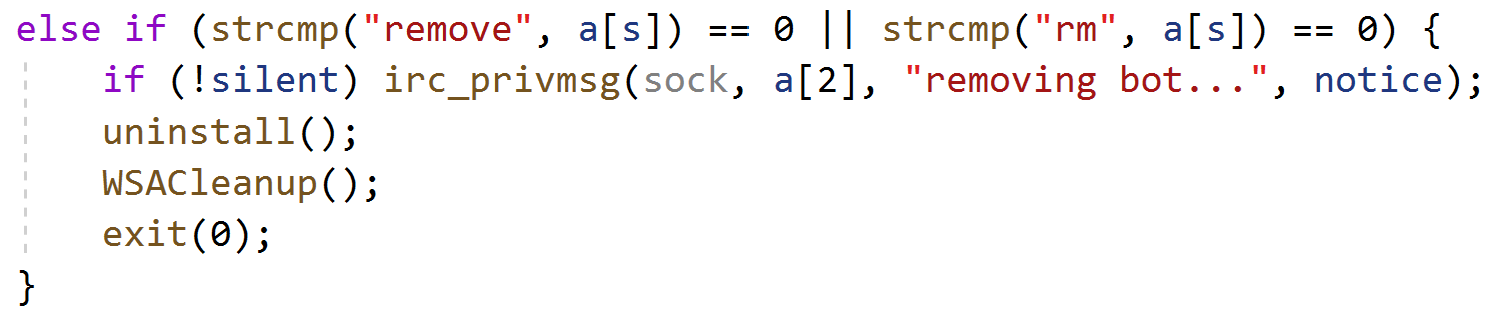
Description automatically generated

Command: remove

Function: This command is used to delete or erase something from the system. This can include files, folders, as well as applications on the system.

Evidence: The command is used to remove a bot from the system.

Example:



Command: download

Function: This command is used for gathering software packets and data from an outside source and adding then onto your own system. Such as when you download a new video game to play or a new software for school.

Evidence: Within the code is an example of a download happening from a web URL variable.

Example:

A screenshot of a social media post

Description automatically generated

Command: update

Function: Update is a command that takes the current version of an app or software and replaces it with a new version that has new changes and uses that the older version did not. It has similar functions as download where it gathers software data from a web source and installs the software or data. But specifically talered to new versions of the software or application.

Evidence: in the code there is an example of the download command being used.

Example:

A screenshot of a cell phone

Description automatically generated

Command: systeminfo

Function: The purpose of this command is to gather data and information about the system itself that is being used.

Evidence: There is a function in the code that gathers system infoand then sends it out to be displayed.

Example:

A screenshot of a social media post

Description automatically generated

Command: netinfo

Function: This is used for retrieving and showing the information regarding the network that the system is currently using I believe.

Evidence: There is a function in the code and is used to get and display the netinfo data.

Example:

A screenshot of a social media post

Description automatically generated

* 1. **Question:** Compare pairs of commands and present your analysis based on the source code. (5 Points)

**Command Comparison:**

**die vs remove**

Both commands can be used for similar uses but die is more tailored specifically for a smaller range of elements to interact with while the remove command can be used for a more wider range of elements to use with.

**download vs update**

Both commands deal with gathering software information regarding a program or software application, but update specifically deals with removing and replacing the data with a newer version that was created.

**open vs execute**

Both commands can be used to do the same thing for very specific moments but only execute can use open when this execute command is ran. The open command cannot run the execute command the same way.

* 1. **Question:** Analyze the source code and list three commands that can be used for issuing DDoS attacks against network services. Explain how they can be used for such attacks. (10 Points)

With analyzing the code, I believe that three commands that could be used for issuing a DDoS attack against network services could be as follows:

* + 1. Download

The reason for Download is because downloads can be used as a starting point for an attack if someone happens to click on a download link they think is harmless and then it gives the attacker an opening to do what they need to. Setting up download link traps like this is one way that could work.

* + 1. Repeat

I think repeat is another one, because it can be used in the form of a flood attack where the attacker is constantly repeating and spamming the users with data to slow down connection and give attackers the opening to do what they wanted to do. An example is during an SYN Flood attack.

* + 1. Ping

As for Ping, I am not to sure exactly how it can be used for a DDoS attack off the top of my head, my possible guess from when an attacker tries to ping a server and pretend to be one of the other users, then allowing the attacker access to the server information. All done with there IP address and contacting the server trying to beat the normal user and get connected to the server and into the system.