

Cyber Attack Workout Instructions

Introduction

Welcome to your team's *Cyber Attack* workout, in which you will experience malware from both the adversary and the victim. This workout introduces you to a type of malware known as a botnet. A botnet is a type of malware run on a client computer which establishes a connection back to a botnet controller. The botnet controller can then do almost anything on the victim computer. To learn more about botnets, read this article: <https://usa.kaspersky.com/resource-center/threats/botnet-attacks>.

For this workout, you will log into a victim computer built just for you and run the botnet. Then an online service known as Shinobot provides you the experience of controlling your botnet remotely.

Your Mission

- Once you are logged in, double click shinobot on the desktop.
- A command prompt opens and immediately starts executing. Look for the **host ID** and **password**. You will want to write these down or take a picture of them with your phone. If the botnet scrolls through, you'll need to scroll back up and take a picture.
- Go back to your browser on your school computer and browse to <http://shinobotps1.com/>. Then click on the C&C tab.
- Find your **host ID** that you wrote down from above and login with the credentials you were provided.

Task 1: Verify you have successfully started your botnet victim by recording information requested (the host ID and password)

Task 2: Log into the botnet Command and Control (C&C) Server at <http://shinobotps1.com/>. To verify you have successfully logged in, you will be asked to provide the local IP address. Hint: it will be in the form of 10.x.x.x (where x is some number). (Enter this on the assessment page)

Task 3: Run a command on the victim using the C&C server. In the assessment, you will indicate which movie you see come up on the victim computer. (You will have to refer back to the “desktop” to see the movie.)

```
cmd /K start telnet towel.blinkenlights.nl
```

Task 4: Explore various command templates until you find the password stored on the target machine. Report the password you find in the assessment.

Task 5 (Challenge): Come up with your own script or action to perform on the botnet victim. (There are some examples found on the C&C server)