Relazione prova Botnet Binotto-Team

La botnet è stata implementata in modo da reperire informazioni relative alle cartelle, ai file presenti nelle cartelle e in modo tale da poter scaricare e leggere i file considerati interessanti. In più la botnet può prendere informazioni di base sulla macchina e sulla rete usata dalla macchina. In particolare durante la prova ci si è connessi a due macchine, reperendo alcune informazioni.

La botnet è stata implementata in modo tale da creare una cartella specifica per ogni client che si connette, in modo tale da conservare il lavoro effettuato su una macchina in una cartella ad-hoc.In più viene generato un fileLog che tiene traccia di tutti i movimenti fatti sul client. In particolare di seguito viene riportata una parte del fileLog:

### FILELOG RESULT ###

[CONNECTED] Established a connection with the Victim using socket: ('192.168.1.188', 44300)

Information on the victim's Operating System ('192.168.1.188', 44300):

Operating System: Linux

Machine: x86\_64

Host: Ubuntu-20-04-LTS

Processor: x86\_64

Platform: Linux-5.15.0-52-generic-x86\_64-with-glibc2.35

Release: 5.15.0-52-generic

Path: /home/alessio/Documents/final test/Binotto Team - Erasmo

[DONE] Info received.

[REMOTE CONTROL] Procedure activated; you are now on the victim's pc in the path below...

/home/alessio/Documents/final test/Binotto Team - Erasmo$ network

### Dati configurazione di rete ###

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255

inet6 fe80::9406:ff6d:57df:81b6 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:63:f0:81 txqueuelen 1000 (Ethernet)

RX packets 29 bytes 5962 (5.9 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 119 bytes 14476 (14.4 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.188 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fdac:c077:5c58:0:a815:7e34:a9bd:fd74 prefixlen 64 scopeid 0x0<global>

inet6 fdac:c077:5c58:0:48f0:3733:26f6:1457 prefixlen 64 scopeid 0x0<global>

inet6 fe80::9d7:8073:fa98:3b11 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:b5:01:f3 txqueuelen 1000 (Ethernet)

RX packets 669 bytes 91153 (91.1 KB)

RX errors 0 dropped 4 overruns 0 frame 0

TX packets 468 bytes 61885 (61.8 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Loopback locale)

RX packets 290 bytes 32621 (32.6 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 290 bytes 32621 (32.6 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Oltre a queste informazioni, sono state trovate anche altre informazioni su altri file, in particolare con l’ausilio della funzione “filespath”\* sono risultati interessanti i seguenti file trovati e scaricati:



\*La funzione filespath scorre tutto il file system e trascrive su un file tutti i nomi dei file e il relativo path che hanno l’estensione da noi richiesta.



Sulla seconda macchina provata sono stati trovate le seguenti informazioni interessanti:

### FILELOG RESULT ###

[CONNECTED] Established a connection with the Victim using socket: ('192.168.1.224', 47146)

Information on the victim's Operating System ('192.168.1.224', 47146):

Operating System: Linux

Machine: x86\_64

Host: Ubuntu-20-04-LTS

Processor: x86\_64

Platform: Linux-5.15.0-52-generic-x86\_64-with-glibc2.35

Release: 5.15.0-52-generic

Path: /home/alessio/Documents/final test/Binotto Team - Erasmo

[DONE] Info received.

[REMOTE CONTROL] Procedure activated; you are now on the victim's pc in the path below...

/home/alessio/Documents/final test/Binotto Team - Erasmo$ info

Operating System: Linux

Machine: x86\_64

Host: Ubuntu-20-04-LTS

Processor: x86\_64

Platform: Linux-5.15.0-52-generic-x86\_64-with-glibc2.35

Release: 5.15.0-52-generic

Path: /home/alessio/Documents/final test/Binotto Team - Erasmo

/home/alessio/Documents/final test/Binotto Team - Erasmo$ network

### Dati configurazione di rete ###

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255

inet6 fe80::9406:ff6d:57df:81b6 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:63:f0:81 txqueuelen 1000 (Ethernet)

RX packets 123 bytes 22162 (22.1 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 1263 bytes 89673 (89.6 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.224 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::e19:8dfb:3aca:f9d2 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:a3:93:73 txqueuelen 1000 (Ethernet)

RX packets 11453 bytes 821800 (821.8 KB)

RX errors 0 dropped 8 overruns 0 frame 0

TX packets 75390 bytes 106007373 (106.0 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Loopback locale)

RX packets 3079 bytes 292620 (292.6 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 3079 bytes 292620 (292.6 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

/home/alessio/Documents/final test/Binotto Team - Erasmo$ exit

[REMOTE CONTROL CLOSED] Remote Control procedure successfully closed!

[CLOSED] Client Connection ('192.168.1.224', 47146) closed succesfully!

NOTE:

La cartella caricata contiene tutto il materiale trovato sulle due macchine e in particolare per ogni macchina è stato caricato il fileLog e un file contenente tutti i dati catturati da wireshark