Universitat Oberta de Catalunya

uoc.edu

Amenaces dels dispositius IoT en diferents tipus de xarxes

Miquel Abdón Giménez
Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions
TFM Seguretat en la Internet de les coses 2018-19 Sem. 1

Consultor: **Carlos Hernández Gañán**
PRA: **Victor Garcia Font**

31/12/2018

FITXA DEL TREBALL FINAL

Títol del treball:	*Amenaces dels dispositius IoT en diferents tipus de xarxes*
Nom de l'autor:	*Miquel Abdón Giménez*
Nom del consultor/a:	*Carlos Hernández Gañán*
Nom del PRA:	*Victor Garcia Font*
Data de lliurament (mm/aaaa):	*12/2018*
Titulació o programa:	*Màster Universitari en Seguretat de les Tecnologies de la Informació i de les Comunicacions*
Àrea del Treball Final:	*Seguretat en la Internet de les coses*
Idioma del treball:	*Català,*
Paraules clau	*Seguretat, IoT*

La gran previsió de creixement de dispositius IoT, la seva utilització tant en l'àmbit personal com empresarial i el fet d'estar connectats i disponibles les 24 hores del dia, han provocat que es converteixin en un dels principals objectius dels ciberdelinqüents.

L'objectiu principal d'aquest treball es fer un anàlisi del nombre i tipus d'atacs que reben els dispositius en tres tipus de xarxa: una xarxa domèstica, la xarxa externa d'una universitat i la xarxa interna d'una universitat. També quines són les causes i les motivacions per realitzar aquests atacs.

Per fer-ho, primer s'analitza l'estat de la seguretat dels dispositius IoT, a partir d'un anàlisis de les amenaces de seguretat i de les vulnerabilitats més comuns, i es descriuen accions preventives i recomanacions per la mitigació dels riscos de seguretat. També s'analitza quina és la motivació i les causes per les que aquests dispositius són un objectiu, i els cucs més habituals que hi ha per intentar infectar els dispositius IoT de manera automàtica per fer-los formar part d'una botnet.

Un cop definida la base teòrica, es desenvolupa un sistema per detectar aquests atacs i intentar recuperar payloads de diferents tipus de botnets.

Amb els resultats obtinguts, es procedeix a fer una anàlisi dels atacs de cada xarxa, identificant els espècimens capturats.

The great growth forecast of IoT devices, its uses both in domestic and Enterprise environment and the fact of being powered on and online 24 hours a day have made them one of the main objectives for cibercriminals.

The main objective of this work I to analyse the number and type of attacks that those devices receive in three types of network: a home network, the external network of a university, and the internal network of a university.

To do this, we first analyse the security status of IoT devices, based on an analysis of the security threats and the most common vulnerabilities, and describe preventive actions and recommendations to mitigate the risks of security. It also analyse the motivations and causes for which these devices are a target and the most common worms that exists targeted at infecting IoT devices to make them part of a botnet.

Once the theoretical base is defined, a system to detect those attacks and get payloads is defined and implemented I each network.

With the results obtained, we proceed to analyse the attacks of each network, identifying the captured specimens.

Índex

Llista de figures

1. Introducció

1.1 Context i justificació del Treball

En un món on es preveu, segons Gartner[1], que pel 2020 hi hagi més de 20 milions de dispositius IoT, l'estat de la seva seguretat és un tema cada cop més important.

Els dispositius Internet of Things (IoT) cada vegada més nombrosos, disposen de connectivitat les 24 hores del dia i al tractar-se de dispositius pensats per col·locar i oblidar poden passen desapercebuts o l'usuari pot no ser conscient que disposa de connectivitat (per exemple un fanal, un comptador, un termòstat,...).

S'espera que el seu creixement sigui exponencial en els anys següents permetent afegir sensors i actuadors a diferents àmbits. Les xarxes de gran cobertura i consum baix d'energia (LPWANs) com Narrowband IoT (NB-IoT) permetran augmentar encara més el nombre de dispositius connectats.

L'augment del nombre de dispositius i la necessitat d'implementar lleis i regulacions cada cop més interessades en la seguretat informàtica fan que cada cop més sigui important ser conscient de les vulnerabilitats i riscs de seguretat.

Una mala praxis en el moment de configurar i mantenir aquests dispositius amplia enormement la superfície explotable per un atacant.

Els ciberdelinqüents veuen en aquests dispositius, presses fàcils per poder realitzar molts tipus d'atac, com denegació de servei distribuïda (DDOS) o DNS Rebinding.

Sovint, els administradors de sistemes no poden obtenir informació clara i organitzada sobre la seguretat dels dispositius IoT i com pot afectar les serves xarxes i sistemes.

Aquest treball tracta d'analitzar els tipus d'atacs que es poden esperar en aquests dispositius, les causes i les motivacions. També vol determinar si el tipus d'atacs són diferents en una xarxa universitària (tant externa com interna) i en una xarxa domèstica. També vol analitzar el tipus de cucs que afecten als dispositius IoT i capturar els espècimens. Alhora vol contextualitzar la historia d'aquests cucs i quin és el seu funcionament. En definitiva, vol servir com a font d'informació per poder conèixer l'estat de la seguretat dels dispositius IoT i mostrar exemples pràctics.

[1] https://www.gartner.com/newsroom/id/3165317

1.2 Objectius del Treball

L'objectiu principal d'aquest treball és analitzar els tipus d'atacs que es poden esperar en els dispositius IoT i quines són les causes i les motivacions de realitzar aquests atacs.

- Entendre a quines amenaces ens enfrontem quan despleguem dispositius IoT i perquè som vulnerables.
- Analitzar l'estructura i els tipus de dispositius IoT presents en el mercat i quins són els problemes de seguretat més comuns.
- Quins atacs reben els dispositius IoT.
- Causes i motivacions dels ciberdelinqüents per atacar dispositius IoT.
- Com s'automatitzen els atacs i creació de botnets.
- Atacs automatitzat dirigits a dispositius IoT famosos.
- Implementació de mesures per augmentar la seguretat d'aquests dispositius i recomanacions de seguretat.
- Quants atacs podem esperar en 24 hores de mitjana en diferents tipus de xarxa?
- Capturar atacs reals en diferents tipus de xarxes i veure quins són els més habituals.

1.3 Enfocament i mètode seguit

L'enfocament i mètode seguit per complir els objectius marcats en aquest treball venen definits per les etapes següents:

Definició del pla de treball
En aquesta primera etapa s'identifica el context i es justifica la importància de realitzar un treball en aquesta àrea. Es defineixen els objectius del treball, la metodologia utilitzada, les tasques necessàries per complir els objectius, s'identifiquen els riscs principals, es realitza una planificació temporal de les tasques i s'enumeren els entregables.

Anàlisi de les vulnerabilitats de seguretat més comuns en dispositius IoT

Es defineix que és una vulnerabilitat de seguretat i es descriuen els diferents tipus de vulnerabilitat més comuns en dispositius IoT.

Com reduir els riscos de vulnerabilitat en dispositius IoT

Es descriu quines són les mesures i recomanacions per desplegar dispositius IoT reduint la superfície explotable per un atacant. També recomanacions als fabricants.

Anàlisi de les motivacions per atacar dispositius IoT

Es defineix que és el que mou a un ciberdelinqüent a atacar dispositius IoT. Es descriuen els usos dels dispositius atacats i com poden formar part d'una botnet. Descripció d'una bonet i les seves parts, i mètodes d'ocultació i transmissió de missatges.

Anàlisi dels mètodes d'atac

S'analitza quins mètodes utilitzen els atacants i es descriu l'automatització i replicació dels atacs. Descripció dels atacs més coneguts a dispositius IoT i la seva història.

Mètode per capturar atacs dirigits

S'analitzen les diferents eines disponibles i es decideix quines s'utilitzaran per capturar, organitzar i identificar els atacs. Es dissenya l'estructura final per capturar atacs dirigits.

Registre d'atacs reals a tres tipus de xarxes

Es col·loquen dispositius per detectar atacs i capturar espècimens de cucs de xarxa destintats als dispositius IoT en tres xarxes diferenciades: xarxa publica d'una universitat, xarxa privada d'una universitat, i una xarxa domèstica.

Anàlisi dels resultats

Es categoritzen els atacs per objectiu, origen, tipus i s'intenta identificar i analitzar els diferents espècimens obtinguts. També es quantifica

Conclusions

Es presenten les conclusions que es deriven de l'execució del treball.

1.4 Riscos preliminars

A continuació s'identifiquen els principals riscos o causes tècniques que poden afectar temporalment la realització d'aquest treball. Per cada risc identificat s'ha valorat la probabilitat i impacte de la materialització del risc i es proposen accions de mitigació:

- **Risc 1: Àmbit sobredimensionat:** La definició inicial del projecte abasta un àmbit massa gran per a la dedicació teòrica i calendari previst
  Probabilitat / Impacte (1-5): 3 / 5
  Accions mitigadores: Simplificar en cas necessari, descartar temes introductoris, o retallar en cas necessari.
- **Risc 2: Cas pràctic massa complex:** El cas pràctic és massa complicat i limita el temps dedicat a la resta de tasques.
  Probabilitat / Impacte (1-5): 3 / 3
  Accions mitigadores: Limitar l'àmbit de l'anàlisi del cas pràctic al necessari
- **Risc 3: Identificació i classificació d'espècimens complicada:** Es poden rebre molts espècimens i en cas de ser nous no poder identificar-los.
  Probabilitat / Impacte (1-5): 3 / 3
  Accions mitigadores: Limitar l'anàlisi a espècimens coneguts i provar d'identificar un nombre menor d'espècimens nous.

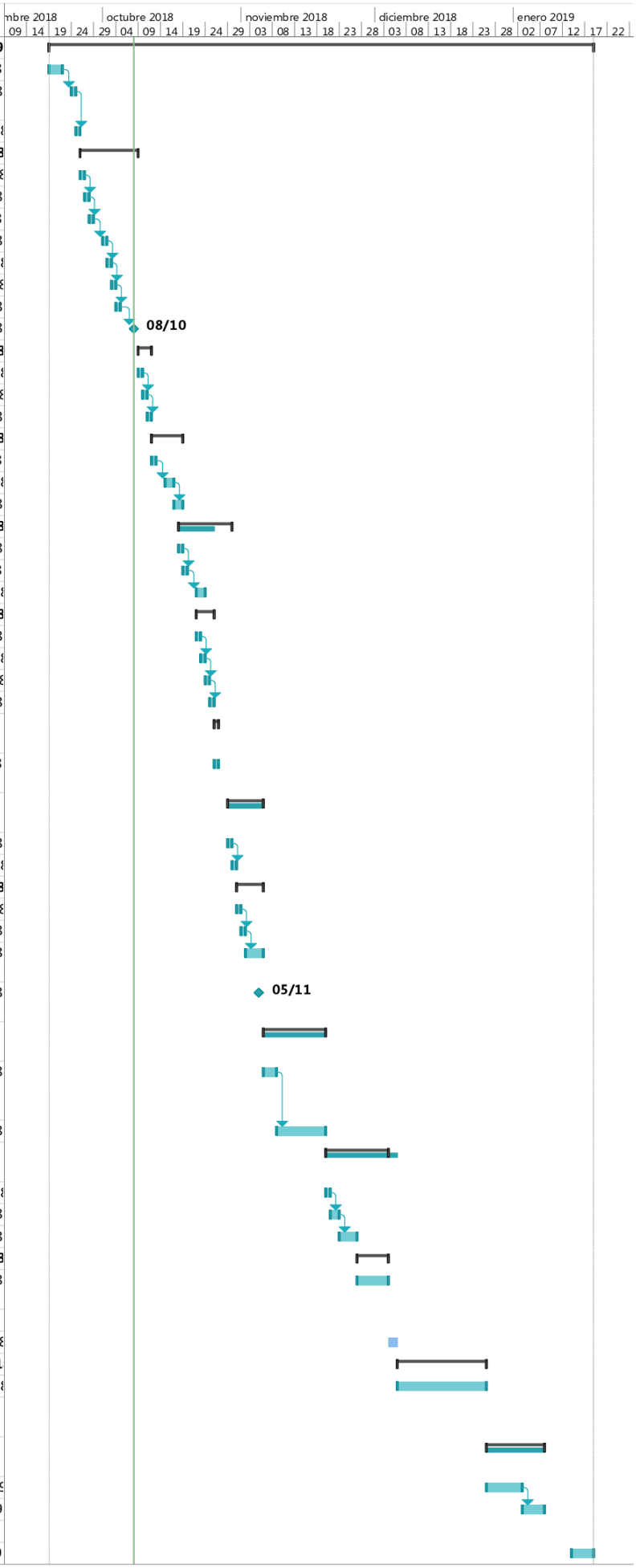
1.5 Planificació del Treball

A continuació es detallen les tasques a realitzar en cadascuna de les fases especificades a l'apartat anterior:

- Documentació prèvia: s'estudia el context i estat de la temàtica del treball.
- Establiment de l'orientació del TFM: es concreten els objectius principals del treball.
- Establiment de l'àmbit del TFM: es detallen els temes dels que tractarà el treball i les tasques que s'hauran de realitzar.
- Pla de treball:
    - Context i justificació: es detalla la importància de desenvolupar un treball que analitzi la seguretat dels dispositius IoT.
    - Objectius: s'explica que es pretén amb el desenvolupament del treball.
    - Metodologia: Es descriuen les fases que es van a seguir per implementar el treball.
    - Llistat de tasques: Es detallen les tasques necessàries a cada fase per cobrir els objectius descrits.
    - Riscos Preliminars: S'expliquen els motius tècnics que poden causar desviacions en l'àmbit o el temps definit per al treball, valorant la seva probabilitat d'aparició, el seu impacte i, enumerant possibles accions mitigadores.
    - Planificació: S'estimen temporalment les dates d'inici i fi de cadascuna de les tasques descrites, mitjançant un diagrama de Gannt, que té en compte les dates d'entrega segons la planificació de l'aula de Treball de Final de Màster.
    - Productes obtinguts: es descriuen els productes (documents) que s'entregaran amb el treball.
    - PAC 1: Pla de treball: Punt de control en que s'entrega a l'aula el pla de treball definit pel TFM.
- IoT
    - Definició : es defineix el concepte d'IoT
    - Tipus: s'especifiquen els tipus de dispositius IoT que podem trobar
    - Serveis habituals: s'especifiquen quins són els serveis habituals d'aquests dispositius.
- Seguretat IoT
    - Actualment: es defineix quina és la seguretat actualment.
    - Millores: es proposen millores en la seguretat.
    - Recomanacions de seguretat: es fan recomanacions en els dispositius actuals.
- Objectius dels ciberdelinqüents
    - Atacs dirigits: es defineix el concepte d'atac dirigit i es posen exemples.
    - Atacs automatitzats: es defineix el concepte d'atac automatitzat.
    - Estructura de botnets: es defineixen els diferents tipus i evolució de les estructures de les botnets.
- Usos IoT Compromesos
    - DDOS: es defineix el concepte de DDOS i la seva implicació amb dispositius IoT.

    - Robatori d'informació: es defineix com s'utilitzen els dispositius IoT per a robar informació.
    - Accés a xarxes internes: es descriu com es poden utilitzar els dispositius IoT per accedir a xarxes internes.
- Atacs dirigits a IoT famosos: S'enumeren alguns atacs dirigits famosos a dispositius IoT.
- Metodologia per registrar els atacs
    - Objectius: es defineix quins objectius ha de complir el registre dels atacs.
    - Definició dels escenaris: es descriuen i s'estableixen els escenaris en que s'ha de desplegar el sistema.
    - Tipus de dispositiu:
        - Honeypot: Definició de Honeypot i avantatges i inconvenients per registrar els atacs.
        - IDS: Definició de IDS i avantatges i inconvenients per registrar els atacs.
    - Definició del mètode de captura: definició del mètode triat per realitzar la captura i la seva justificació.
- Implementació i Registre dels atacs: Es desplega el mètode per registrar els atacs durant una setmana a una xarxa domèstica i a la xarxa interna i externa d'una universitat.
- Anàlisi dels atacs rebuts:
    - Nombre, país i tipus d'atac: es classifiquen els atacs registrats per nombre d'atacs rebuts, país d'origen i tipus d'atac.
    - Honeypot: s'identifica, si es possible, els espècimens capturats a cada xarxa i es fa un anàlisi.
- Conclusions: després de tota la feina feta s'extreuen les conclusions del TFM.
- Redacció de la memòria: es compon i redacta la memòria del TFM.
- Creació del vídeo de presentació: creació del vídeo de presentació explicant la feina feta durant el present treball.
- Defensa del TFM: defensa davant del tribunal del TFM.

Id	Nombre de tarea	Duración	Comienzo	Fin
1	**Treball final de màster**	**88 días**	**mié 19/09/18**	**vie 18/01/19**
2	Documentació prèvia	3 días	mié 19/09/18	vie 21/09/18
3	Establiment de l'orientació del TFM	1 día	lun 24/09/18	lun 24/09/18
4	Establiment de l'àmbit del TFM	1 día	mar 25/09/18	mar 25/09/18
5	**Pla de treball**	**9 días**	**mié 26/09/18**	**lun 08/10/18**
6	Context i justificació	1 día	mié 26/09/18	mié 26/09/18
7	Objectius	1 día	jue 27/09/18	jue 27/09/18
8	Metodologia	1 día	vie 28/09/18	vie 28/09/18
9	Llistat de tasques	1 día	lun 01/10/18	lun 01/10/18
10	Riscos preliminars	1 día	mar 02/10/18	mar 02/10/18
11	Planificació	1 día	mié 03/10/18	mié 03/10/18
12	Productes obtinguts	1 día	jue 04/10/18	jue 04/10/18
13	PAC 1: Pla de treball	0 días	lun 08/10/18	lun 08/10/18
14	**IoT**	**3 días**	**mar 09/10/18**	**jue 11/10/18**
15	Definició	1 día	mar 09/10/18	mar 09/10/18
16	Tipus	1 día	mié 10/10/18	mié 10/10/18
17	Serveis habituals	1 día	jue 11/10/18	jue 11/10/18
18	**Seguretat IoT**	**5 días**	**vie 12/10/18**	**jue 18/10/18**
19	Actualment	1 día	vie 12/10/18	vie 12/10/18
20	Millores	2 días	lun 15/10/18	mar 16/10/18
21	Recomanacions de seguretat	2 días	mié 17/10/18	jue 18/10/18
22	**Objectius ciberdelinqüents**	**8 días**	**jue 18/10/18**	**lun 29/10/18**
23	Atacs dirigits	1 día	jue 18/10/18	jue 18/10/18
24	Atacs automatitzats	1 día	vie 19/10/18	vie 19/10/18
25	Estructures de botnets	2 días	lun 22/10/18	mar 23/10/18
26	**Usos IoT compromesos**	**4 días**	**lun 22/10/18**	**jue 25/10/18**
27	DDOS	1 día	lun 22/10/18	lun 22/10/18
28	Robatori Informació	1 día	mar 23/10/18	mar 23/10/18
29	Accés a xarxes internes	1 día	mié 24/10/18	mié 24/10/18
30	Altres	1 día	jue 25/10/18	jue 25/10/18
31	**Atacs dirigits a IoT famosos**	**1 día**	**vie 26/10/18**	**vie 26/10/18**
32	Atacs dirigits a IoT famosos	1 día	vie 26/10/18	vie 26/10/18
33	**Metodologia per registrar els atacs**	**6 días**	**lun 29/10/18**	**lun 05/11/18**
34	Objectius	1 día	lun 29/10/18	lun 29/10/18
35	Definició dels escenaris	1 día	mar 30/10/18	mar 30/10/18
36	**Tipus de dispositiu**	**4 días**	**mié 31/10/18**	**lun 05/11/18**
37	Honeypot	1 día	mié 31/10/18	mié 31/10/18
38	IDS	1 día	jue 01/11/18	jue 01/11/18
39	Definició del mètode de captura	2 días	vie 02/11/18	lun 05/11/18
40	PAC 2: Resultats de l'anàlisi teòric	0 días	lun 05/11/18	lun 05/11/18
41	**Implementació i Registre dels atacs**	**10 días**	**mar 06/11/18**	**lun 19/11/18**
42	Implementació del sistema per detectar i capturar els atacs	3 días	mar 06/11/18	jue 08/11/18
43	Registre dels atacs	7 días	vie 09/11/18	lun 19/11/18
44	**Anàlisi dels atacs rebuts**	**10 días**	**mar 20/11/18**	**lun 03/12/18**
45	Nombre	1 día	mar 20/11/18	mar 20/11/18
46	Per País	2 días	mié 21/11/18	jue 22/11/18
47	Per tipus d'atac	2 días	vie 23/11/18	lun 26/11/18
48	**Honeypot**	**5 días**	**mar 27/11/18**	**lun 03/12/18**
49	Identificació d'espècimens capturats	5 días	**mar 27/11/18**	lun 03/12/18
50	Entrega PAC 3			
51	Conclusions	2 días	mar 04/12/18	mié 05/12/18
52	**Redacció de la memòria**	**14 días**	**jue 06/12/18**	**mar 25/12/18**
53	Maquetació de la memòria	14 días	**jue 06/12/18**	mar 25/12/18
54	Entrega PAC 4 (Memòria Final)			
55	**Creació del vídeo de presentació**	**9 días**	**mié 26/12/18**	**lun 07/01/19**
56	Preparació del vídeo	6 días	**mié 26/12/18**	mié 02/01/19
57	Gravació del vídeo	3 días	jue 03/01/19	lun 07/01/19
58	Entrega Presentació/vídeo			
59	Defensa del TFM	5 días	lun 14/01/19	vie 18/01/19



1.6 Breu sumari de productes obtinguts

El Treball de Final de Màster es divideix en els següents entregables parcials, que formaran part del resultat final del projecte:

- PAC1: Pla de treball, que emmarca i defineix la realització del projecte, el seu àmbit i la previsió temporal de la seva execució.
- PAC2: Els resultats de l'anàlisi teòric. Inclou un anàlisi de les amenaces de seguretat, tipus de botnets, tipus d'atacs, motivacions i definició i tipus de dispositius IoT. També es concreta quin tipus de mecanismes s'utilitzen per tal de capturar els atacs. Recomanacions per millorar la seguretat d'aquests dispositius.
- PAC3: Els resultats de l'anàlisi pràctic en tres xarxes diferents. Inclou el nombre d'atacs, país d'origen, espècimens obtinguts, tipus de botnet atacant.
- PAC4: Es recopila tots els productes anteriors per generar la memòria final del projecte, i es completa amb les conclusions, glossari, bibliografia i annexos.
- Presentació/ Vídeo: Una presentació de resum amb la veu en off de l'autor, descrivint la feina realitzada.

2. IoT

2.1 Definició

L'Internet de les coses, IoT per les seves sigles en anglès es refereix al concepte de tots aquella sèrie de dispositius connectats a internet. Aquests, s'identifiquen més amb coses que en equips informàtics. Per exemple, termòstats, neveres, fanals o endolls poden esdevenir dispositius IoT en el moment que disposen d'una connexió a la xarxa per enviar o rebre informació o comandes.
Una de les característiques principals, per la seva naturalesa de cosa més que dispositiu de xarxa i per disminuir el cost, és la baixa capacitat de processament de càlcul i, sovint, el baix ample de banda.

2.2 Tipus

En el mercat hi ha diferents tipus de dispositius IoT. Si els classifiquem segons el propòsit, tenim les següents categories:

- Sensors: Permeten adquirir dades.
- Actuadors: Permeten realitzar accions.
- Sensors/Actuadors: Permeten adquirir dades i actuar en funció d'aquestes o d'ordres externes.

Dins d'aquests podem trobar els dispositius de domòtica, eHealth, SmartCitty, Transport, Controladors-Sensors industrials, el vehicle connectat, per posar uns exemples.

2.3 Serveis habituals

Cada dispositiu IoT té unes característiques concretes, però es pot observar que la major part dels dispositius connectats a internet, disposa d'un servei web (habitualment pel port 80) per tal de configurar i administrar el dispositiu. A més, se sol habilitar el port 23 (Telnet) per a poder administrar els dispositius.

Alguns dispositius IoT disposen de sistemes més avançats i segurs com SSH i ús de comunicacions xifrades a la interfície web (443, SSL), però no es gaire habitual, degut a la poca capacitat de procés d'aquests dispositius.

3. Seguretat IoT

3.1 Actualment

Actualment no hi ha gaire seguretat en els dispositius IoT. Els processadors dels dispositius solen tenir poca capacitat del procés pel que no es sol disposar d'eines criptogràfiques per assegurar les comunicacions i les dades. Tampoc es pot definir filtratge de ports en el mateix dispositiu o sistemes de validació avançats.

Els fabricants dels dispositius deixen usuaris i paraules de pas per defecte i confien en que els usuaris les canviïn. A vegades, els dispositius IoT tenen serveis vulnerables o backdoors posats pels propis fabricants.

Alguns d'aquests backdoors o forats de seguretat, poden ser hardware: uns pins de control exposats que permeten accedir a les dades, o habilitar l'accés com a root en un port determinat,...

Sovint no hi ha actualitzacions dels dispositius que puguin solucionar vulnerabilitats en els dispositius i el mètode per actualitzar-los no es pot automatitzar (excepte si es pot accedir per Telnet/SSH) i ha de ser d'un a un via interfície web o físicament.

Els administradors i els usuaris a vegades no perceben el risc que poden suposar aquest tipus de dispositius per la seguretat de la xarxa. En veure dispositius simples desconeixen que poden ser vulnerables, i al configurar-los en xarxes internes i confiables no es dubte de la seva seguretat.

3.2 Millores i recomanacions de seguretat

Per tal de millorar la seguretat s'hauria de començar pels fabricants de dispositius IoT. Des del moment del dissenys del dispositiu s'ha de tenir en compte la seguretat. Algunes de les millores és la de forçar a canviar la paraula de pas de l'usuari administrador després del primer accés, bloquejar el compte un cert temps cada X intents (per evitar atacs de força bruta), actualitzacions de seguretat durant el temps de vida del dispositiu, dissenyar eines per veure l'estat de les actualitzacions dels dispositius i actualitzar múltiples dispositius alhora. Implementar sistemes de validació i autenticació més robustos i millorar el hardware per a que es pugui utilitzar criptografia.

En el cas dels administradors, tenir en compte que són dispositius susceptibles de ser atacs i compromesos i que, per tant, s'han de defensar i securitzar, amb firewalls perimetrals, amb definicions de polítiques de monitorització i seguretat. S'han de deshabilitar els serveis no necessaris del dispositiu per reduir la superfície d'atac. S'ha de vigilar també la seguretat física dels dispositius.

4. Objectius dels ciberdelinqüents

Els dispositius IoT són un objectiu molt interessant pels ciberdelinqüents ja que normalment, estan encesos les 24 hores del dia, tenen poca seguretat i no estan monitoritzats. L'objectiu dels ciberdelinqüents és aconseguir unir els dispositius IoT a una xarxa botnet.

4.1 Atacs dirigits

Un atac dirigit és un tipus d'atac en que les accions per aconseguir el control o el fi de l'atac es realitzen per un dispositiu o organització en concret. L'atacant busca dades a internet que facilitin l'atac com per exemple provar d'identificar la xarxa de l'organització enumerant els dominis del DNS de l'organització. Una de

les primeres accions de l'atacant és escanejar els ports oberts del possibles objectius. Quan un atacant detecta un equip IoT primer prova a identificar-lo i, si ho aconsegueix, primer prova a accedir amb usuaris i paraules de pas per defecte i si no funciona, prova a prendre el control mitjançant vulnerabilitats conegudes.
Aquest tipus d'atac permeten utilitzar els dispositius IoT de trampolí per accedir a altres sistemes o bé capturar dades i informació de la xarxa interna.

4.2 Atacs automatitzats

Els atacs més nombrosos, tant a dispositius IoT com a altres tipus de dispositius són els automatitzats. Les fases d'un atac automatitzat en dispositius IoT sol ser la següent:

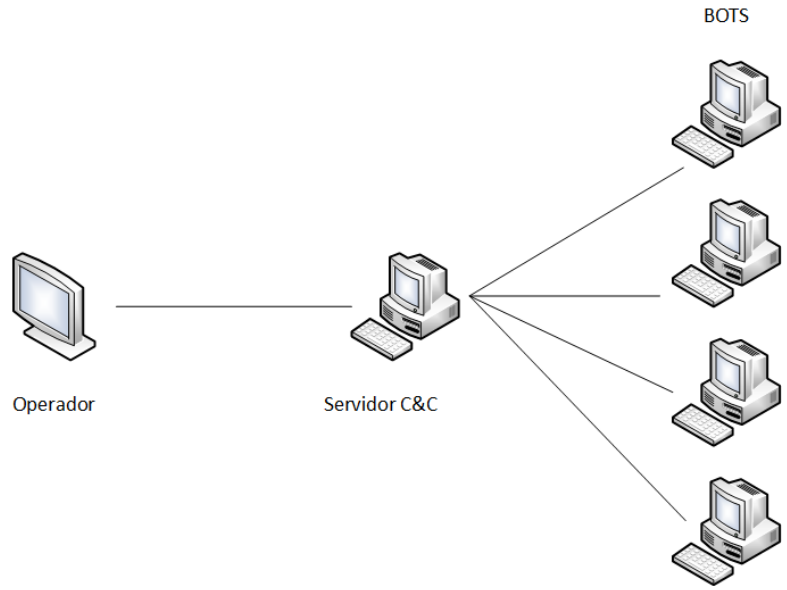
- Un dispositiu IoT compromès (IoTc)realitza un escanejat de ports a una IP aleatòria.
- IoTc detecta un port obert en una ip susceptible de ser un dispositiu IoT (Telnet, per exemple).
- IoTc utilitza un llistat d'usuaris i paraules de pas per defecte i prova d'accedir al sistema.
- Si pot accedir, executa una sèrie d'ordres automatitzades per infectar el dispositiu IoT víctima (IoTv).
- En aquesta fase IoTv queda compromès, s'uneix a una botnet i espera ordres o passa a realitzar totes les passes anteriors.

4.3 Estructura de botnets

Un cop un dispositiu IoT es compromès i passa a formar part d'una botnet, aquest desplega una sèrie de mecanismes de comunicació C&C[2]. Aquests canals permetran a l'operador de la botnet controlar i coordinar els seus robots.

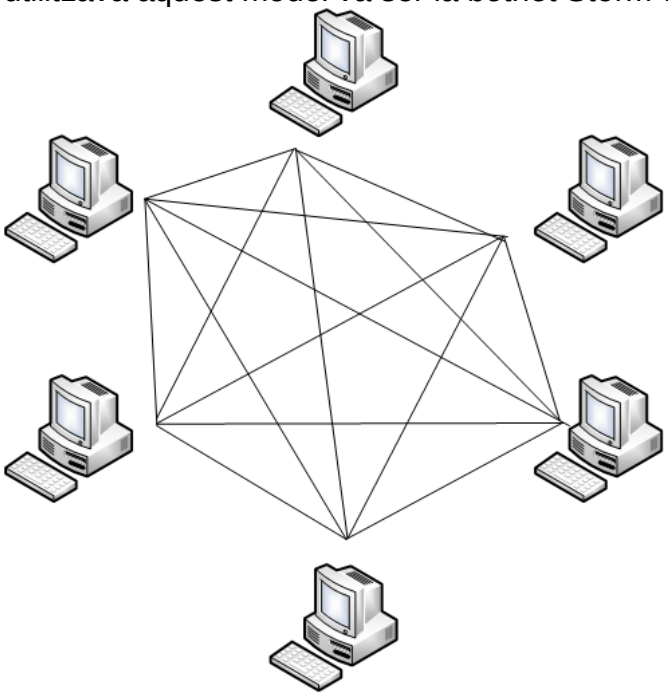
L'estructura més simple d'una botnet consisteix en un servidor C&C que es comunica directament amb els seus bots. Aquesta xarxa és fàcil de desmantellar i detectar al ciberdelinqüent, bloquejant l'accés al servidor i comprovant l'accés a aquest o qui el va registrar.

[2] De Command and Control



Il·lustració 1 Estructura d'una botnet bàsica

Per tal d'evitar la detecció i dificultar el desmantellament, hi ha diverses tècniques que utilitzen els ciberdelinqüents. Una d'elles és utilitzar una xarxa amb model p2p, on tots els nodes tenen la mateixa responsabilitat de fer passar peticions i respostes cap als operadors de xarxes zombis. Una de les xarxes zombies que utilitzava aquest model va ser la botnet Storm[3].

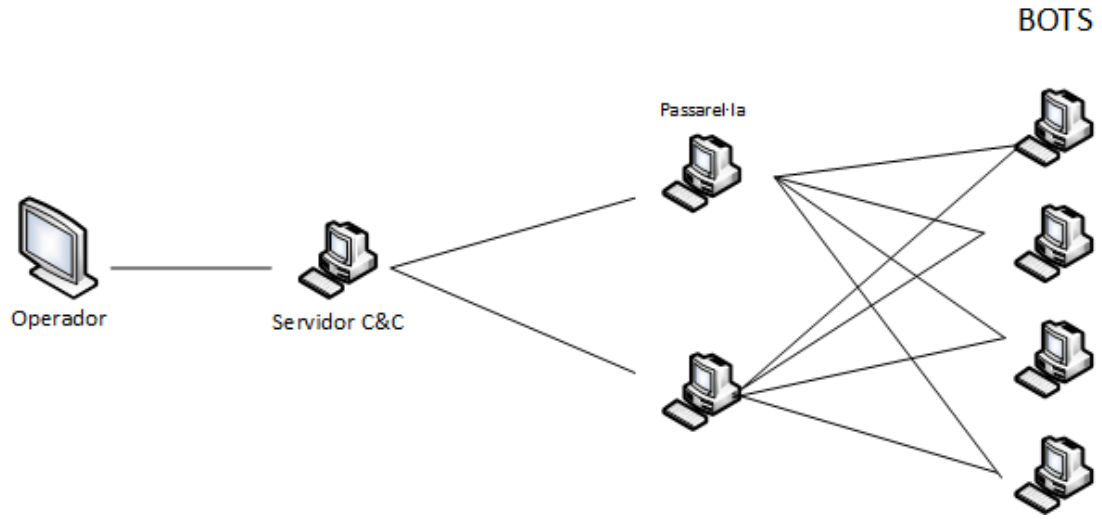


Il·lustració 2 Estructura d'una botnet p2p

Una altra estructura és utilitzar múltiples servidors intermediaris entre el servidor C&C i els bots de la xarxa. Aquesta estructura es pot paral·lelitzar per tenir múltiples servidors C&C, amb moltes passarel·les que controlin els bots, per

[3] https://en.wikipedia.org/wiki/Storm_botnet

maximitzar l'anonimat de l'operador i minimitzar la pressa de control per agents externs.



Il·lustració 3 Estructura d'una botnet avançada

En tots els casos, s'utilitzen comunicacions xifrades per tal de mantenir la xarxa segura.

5. Usos IoT Compromesos

Un sol dispositiu IoT no permet realitzar gaires accions, degut a les seves característiques, però quan s'uneixen múltiples dispositius en una botnet, es poden transformar en una eina molt poderosa. Els ciberdelinqüents utilitzen els dispositius IoT compromesos per a obtenir un rendiment, normalment econòmic.

5.2 DDOS

Un atac de denegació de servei distribuït (DDOS per les sigles en anglès), consisteix en un atac on múltiples nodes de manera coordinada fan peticions de servei a un servidor amb l'objectiu d'acaparar tots els recursos d'aquest i aconseguir que els usuaris legítims no puguin accedir als recursos del servidor.

Aquest és l'ús més habitual d'una botnet. El ciberdelinqüent amenaça a una entitat amb denegar els servidors del seu negoci si no abona una quantitat. En cas que no es faci aquest ingrés, el ciberdelinqüent denegarà el servei durant les hores de màxim negoci.

5.3 Robatori d'informació

Els ciberdelinqüents utilitzen els equips compromesos per a robar informació de les víctimes. El dispositiu IoT compromès pot capturar les dades que circulen per la seva xarxa (sniffing) per tal d'adquirir credencials vàlides o informació.

En aquest cas també es poden manipular les dades que circulen per la xarxa. En un atac conegut[4] [5] , el ciberdelinqüent pren el control d'un dispositiu IoT i l'utilitza per a realitzar atacs de DNS Rebinding i capturar les credencials (bancaries especialment) dels usuaris de la xarxa interna.

5.4 Accés a xarxes internes

Els ciberdelinqüents utilitzen els dispositius IoT compromesos per a penetrar dins d'una organització. Per exemple un ciberdelinqüent pot prendre el control d'una impressora amb una interfície web i des d'aquesta, realitzar accions sobre la xarxa interna, la qual no és accessible directament per l'atacant.

En aquest cas, també es pot utilitzar les interfícies sense fils per accedir a xarxes internes cablejades (si el dispositiu IoT disposa de les dues interfícies).

5.5 Criptominat

La baixa potencia d'aquests dispositius, no els fa gaire viable el minat tot i que l'augment de la popularitat en les criptomonedes associat al valor d'aquestes, ha fet que el minat sigui un negoci lucratiu mentre els dispositius IoT no estan fent altres tasques.
La criptomoneda més utilitzada pels ciberdelinqüents és Monero, ja que el seu algoritme CyptoNight, està més indicat per CPUs que per GPUs.

5.6 Spam / Phishing

Els dispositius IoT poden ser utilitzats per enviar spam i campanyes de phising. D'aquesta manera el ciberdelinqüent pot dificultar la seva localització.

6 Atacs dirigits a IoT famosos

Els dispositius IoT han estat un objectiu d'atacs automatitzats des de com a mínim l'any 2008, en que va aparèixer el programa hydra.

6.1 Hydra

Hydra utilitza un atac de diccionari en la seva fase d'explotació. Un cop el dispositiu es infectat, es connecta a una xarxa IRC per rebre ordres. Cerca dispositius basats en l'arquitectura MIPS i permet fer atacs SYN Flood.

6.2 Psyb0t

Va aparèixer l'any 2009 i és molt similar a hydra. També esta orientat a l'arquitectura MIPS i permet fer a més, atacs UDP i ICMP Flood.

---

[4] https://www.bleepingcomputer.com/news/security/half-a-billion-iot-devices-vulnerable-to-dns-rebinding-attacks/
[5] https://armis.com/dns-rebinding-exposes-half-a-billion-iot-devices-in-the-enterprise/

6.3 Tsunami/Kaiten

Tsunami (2010) és la unió entre el malware derivat d'Hydra Chuck Norris i el troià DDoS Kaiten. Tsunami permet als membres de la botnet realitzar atacs SYN Flood, UDP Flood, ACK i PUSH, però a més, atacs més sofisticats com HTTP Layer 7 Flood i TCP XMAS. El 2016 es va infiltrar a propòsit dins la ISO oficial de Linux Mint.

6.4 Gafgyt/BASHLITE

Gafgyt (2014) utilitza llistats d'usuaris i paraules de pas per defecte per accedir als dispositius Iot. Explota la vulnerabilitat Shellshock[6] per infectar dispositius funcionant amb BusyBox. Ha permès fer atacs de més de 620 Gbps[7].

6.5 Mirai

Mirai va aparèixer el 2016 i és un dels malwares DDoS més predominants dels darrers anys. Ha protagonitzat algun dels atacs de denegació més grans de la història[8]. Molts dels seus membres són dispositius IoT als quals s'ha accedit utilitzant usuaris i paraules de pas per defecte.

7. Metodologia per registrar els atacs

Per tal de registrar els atacs als tres tipus de xarxes objecte d'estudi: una xarxa domèstica, una xarxa interna d'una universitat i una xarxa pública d'una universitat necessitem establir una metodologia. Tenint en compte:

7.1 Objectius

Els objectius són registrar els atacs dirigits als dispositius IoT i obtenir el màxim de dades sobre aquests: data, hora, duració, adreça IP d'origen, registre de les interaccions, recollir el payload si es possible, etcètera.

7.2 Definició dels escenaris

El registre dels atacs es realitzarà en tres tipus de xarxes:

- Xarxa domèstica: la xarxa domèstica consisteix d'una connexió de fibra òptica de 600 Mb simètrics de la companyia Movistar situada a la província de Barcelona.
- Xarxa externa d'una universitat: la xarxa externa d'una universitat consisteix en una connexió amb una IP externa el bloc d'adreces d'una universitat i no disposa de cap tipus de filtrat.

[6] https://en.wikipedia.org/wiki/Shellshock_(software_bug)
[7] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/
[8] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

- Xarxa interna d'una universitat: consisteix en una connexió amb una IP fixa, la qual esta filtrada per dos firewalls: primer pel Firewall perimetral i després pel firewall de la subxarxa. Si no tingués el filtrat dels Firewalls, aquesta adreça IP seria directament accessibles des d'internet.

7.3 Tipus de dispositiu

Per obtenir els objectius podem emprar dos tipus de dispositiu:

IDS

Un IDS (sistema de detecció d'intrusos) és un dispositiu que ens permet detectar i registrar els atacs que rebem dins d'una xarxa. Hi ha diversos tipus d'IDS i no és l'objectiu d'aquest treball enumerar-los tots ni les seves funcionalitats en profunditat.

En el cas que tenim en aquest treball, un IDS en pot permetre tenir una visió global dels atacs que es realitzen i poder obtenir més informació si l'atac que rebem està inclòs dins d'alguna de les regles de detecció de l'IDS.

Honeypot

Un honeypot es un dispositiu de xarxa que simula un dels serveis que s'ofereixen a la xarxa com a esquer per als atacants. Aquest dispositiu està monitoritzat i pretén obtenir informació sobre quins tipus d'atacs pot rebre l'organització i sobre les tècniques que utilitzen els atacants i sobre els propis atacants. Hi ha diversos tipus de honeypots, però en el cas objectiu d'aquest treball, un honeypot ens permetrà registrar els atacs, i recollir múltiple informació per després poder fer l'anàlisi corresponent.

7.4 Definició del mètode de captura

Per tal de simular un dispositiu IoT primer s'ha decidir quins serveis utilitza normalment. Un dels serveis més utilitzats i per tant atacat en els dispositius IoT és Telnet, pel que és important que el nostre mètode per registrar els atacs, contingui un honeypot d'alta interacció sobre aquest servei.

Altres serveis que no són a tots els dispositius IoT poden ser SSH i HTTP (tant en versió segura com no), per tant també seria interessant detectar o registrar aquests atacs. Aquests atacs, en dispositius IoT són més per força bruta que per prendre el control, per tant no necessitem un honeypot dedicat. Aquests serveis no són només de dispositius IoT pel que no tots els atacs rebuts seran destinats a aquests dispositius.

També seria interessant provar a detectar atacs sobre altres dispositius com IoT industrials, basats en SCADA, o en dispositius IoT d'eMobility.

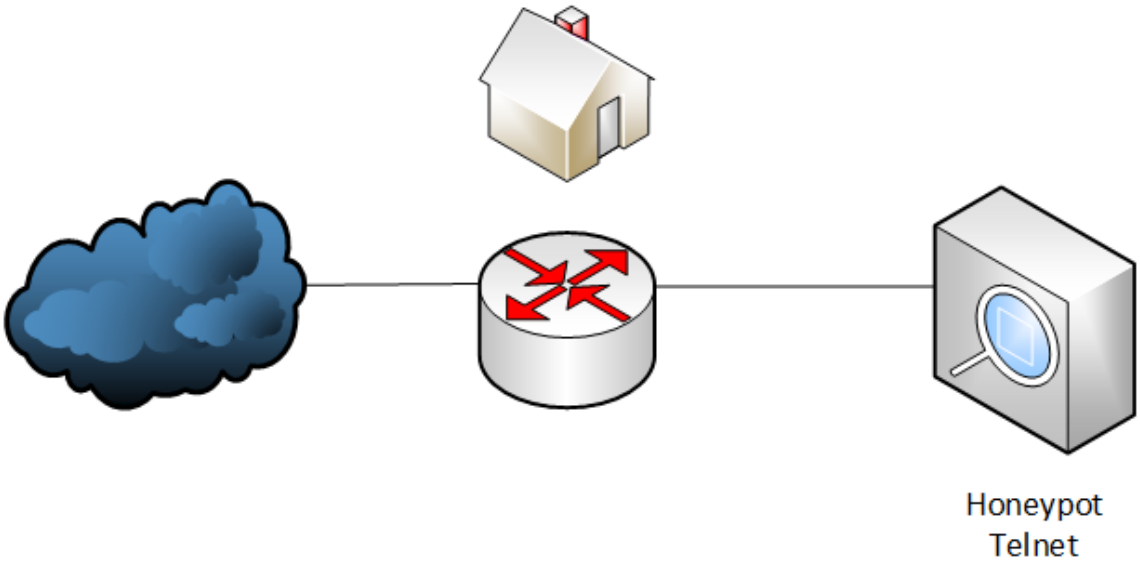
Per a realitzar totes aquestes accions, en totes les xarxes, hi ha un honeypot Telnet basat en python telnet-iot-honeypot de Phype[9]. Que permet fer un anàlisi dels atacs a dispositius IoT. Aquest honeypot està compost per un client i un servidor. El client és qui ofereix el "servei" de telnet i el servidor registra els atacs i emmagatzema els binaris. Aquest honeypot inclou una interfície web que permet fer un primer anàlisi de les dades de manera visual. Tot i això, emmagatzema les dades en una base de dades SQLite que permetrà explotar les dades generades.

En les xarxes de la universitat s'ha col·locat un IDS Suricata[10] + l'stack ELK (Elasticsearch[11], Logstash[12] i Kibana[13]) per visualitzar les alertes i atacs a tots els honeypots. Suricata és un dels IDS més populars (juntament amb Snort) i destaca per la seva capacitat d'utilitzar els sistemes multiprocessador. Elasticsearch és un motor de cerca, Logstash és un recol·lector/processador de logs i fonts de dades, i Kibana és un plugin de visualització de dades.

En la xarxa externa, a més del honeypot de Telnet, s'ha desplegat el multihoneypot t-pot[14] de Deutsche Telekom AG Honeypot Project amb tots els mòduls actius, per detectar possibles atacs a dispositius IoT industrials (conpot[15]) i d'eMobilitiy (emobility[16]) especialment, tot i que també s'utilitzaran la resta de honeypots per tractar d'obtenir dades d'atacs dirigits a dispositius IoT (cowrie[17], dionarea[18],...). L'eina t-pot inclou també un IDS Suricata i l'stack ELK per emmagatzemar, organitzar i visualitzar les dades generades per les diferents eines.

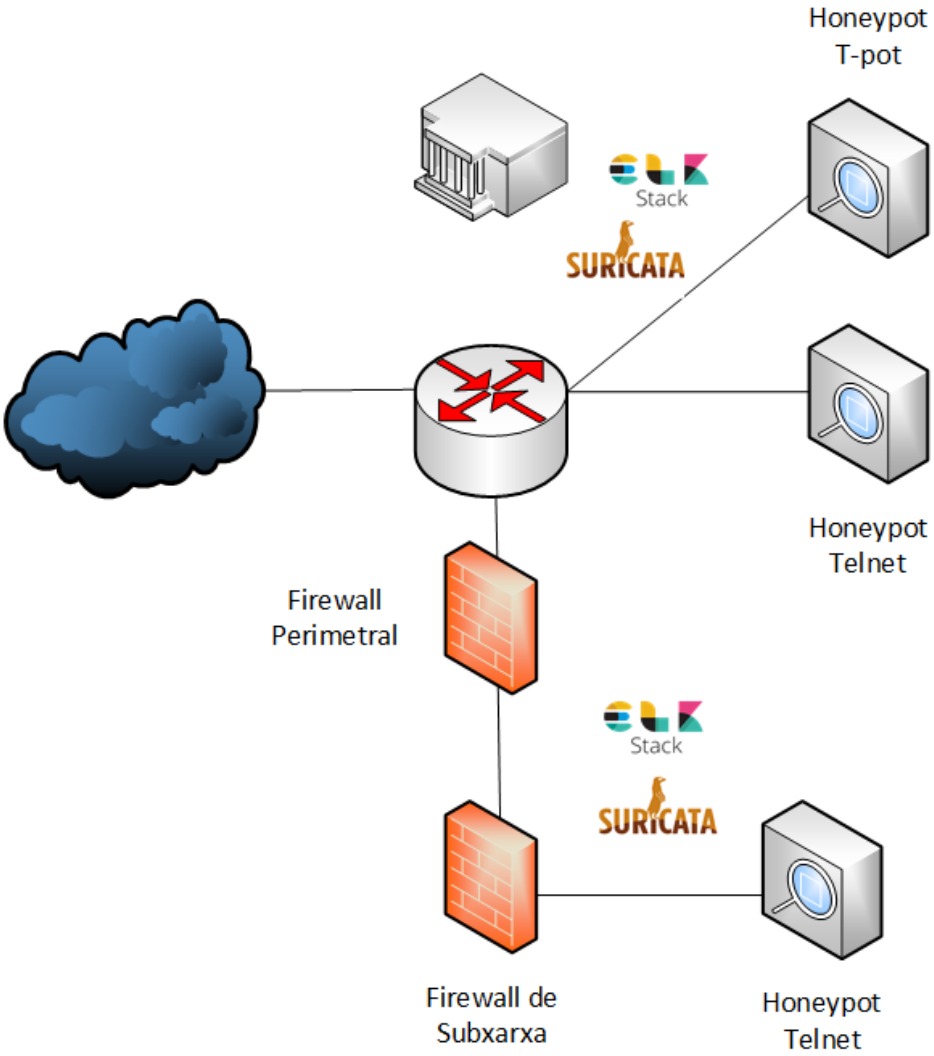
[9] https://github.com/Phype/telnet-iot-honeypot
[10] https://suricata-ids.org/
[11] https://www.elastic.co/products/elasticsearch
[12] https://www.elastic.co/products/logstash
[13] https://www.elastic.co/products/kibana
[14] http://dtag-dev-sec.github.io/mediator/feature/2015/03/17/concept.html
[15] http://conpot.org/
[16] https://github.com/dtag-dev-sec/emobility
[17] https://github.com/cowrie/cowrie
[18] https://github.com/DinoTools/dionaea

Per tant, la xarxa domèstica queda representada en la il·lustració 4:



Il·lustració 4 Xarxa domèstica

I la xarxa de la universitat, per la il·lustració 5:



Il·lustració 5 Xarxa de la universitat

8. Implementació i Registre dels atacs

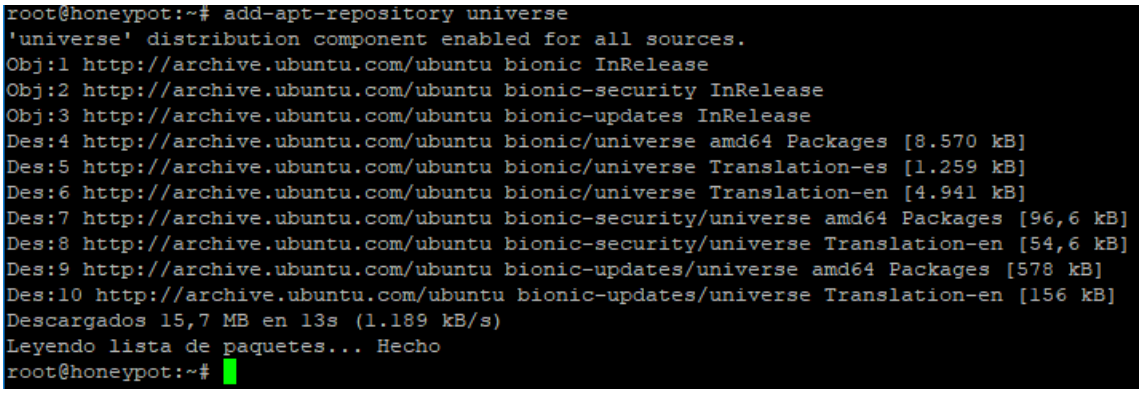
En aquest apartat es mostren quines passes s'han de seguir per crear un laboratori igual que l'utilitzat en aquest treball.

8.1 Implementació del sistema per detectar i capturar els atacs

Com s'ha indicat en l'apartat 7 d'aquest document, el laboratori consta de tres Honeypot Telnet, un Honeypot T-pot, i dos IDS Suricata amb l'ELK Stack per a visualitzar les dades.

8.2 Instal·lació de Honeypot Telnet

La maquina on s'instal·la el Honeypot Telnet és una Ubuntu Server 18.04. Per poder instal·lar el Honeypot Telnet primer s'ha d'activar el repositori *Universe* d'Ubuntu[19] :



Il·lustració 6 Activar repositori Universe

Un cop activat, es pot instal·lar els paquets necessaris per a que funcioni el Honeypot:

```
apt-get install -y python-pip libmysqlclient-dev python-mysqldb git sqlite3
```

[19] Per poder instal·lar el paquet python-pip

```
root@honeypot:~# apt-get install -y python-pip libmysqlclient-dev python-mysqldb git sqlite3
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
git ya está en su versión más reciente (1:2.17.1-1ubuntu0.3).
Se instalarán los siguientes paquetes adicionales:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-7 dpkg-dev fakeroot g++ g++-7 gcc
  gcc-7 gcc-7-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan4 libatomic1
  libbinutils libc-dev-bin libc6-dev libcc1-0 libcilkrts5 libdpkg-perl libexpat1-dev libfakeroot
  libfile-fcntllock-perl libgcc-7-dev libgomp1 libisl19 libitm1 liblsan0 libmpc3 libmpx2 libmysqlclient20
  libpython-all-dev libpython-dev libpython-stdlib libpython2.7 libpython2.7-dev libpython2.7-minimal
  libpython2.7-stdlib libquadmath0 libstdc++-7-dev libtsan0 libubsan0 linux-libc-dev make manpages-dev mysql-common
  python python-all python-all-dev python-asn1crypto python-cffi-backend python-crypto python-cryptography
  python-dbus python-dev python-enum34 python-gi python-idna python-ipaddress python-keyring python-keyrings.alt
  python-minimal python-pip-whl python-pkg-resources python-secretstorage python-setuptools python-six python-wheel
  python-xdg python2.7 python2.7-dev python2.7-minimal zlib1g-dev
Paquetes sugeridos:
  binutils-doc cpp-doc gcc-7-locales debian-keyring g++-multilib g++-7-multilib gcc-7-doc libstdc++6-7-dbg
  gcc-multilib autoconf automake libtool flex bison gdb gcc-doc gcc-7-multilib libgcc1-dbg libgomp1-dbg libitm1-dbg
  libatomic1-dbg libasan4-dbg liblsan0-dbg libtsan0-dbg libubsan0-dbg libcilkrts5-dbg libmpx2-dbg libquadmath0-dbg
  glibc-doc bzr libstdc++-7-doc make-doc python-doc python-tk python-crypto-doc python-cryptography-doc
  python-cryptography-vectors python-dbus-dbg python-dbus-doc python-enum34-doc python-gi-cairo gnome-keyring
  libkf5wallet-bin gir1.2-gnomekeyring-1.0 python-fs python-gdata python-keyczar default-mysql-server
  | virtual-mysql-server python-egenix-mxdatetime python-mysqldb-dbg python-secretstorage-doc python-setuptools-doc
  python2.7-doc binfmt-support sqlite3-doc
Se instalarán los siguientes paquetes NUEVOS:
  binutils binutils-common binutils-x86-64-linux-gnu build-essential cpp cpp-7 dpkg-dev fakeroot g++ g++-7 gcc
  gcc-7 gcc-7-base libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl libasan4 libatomic1
  libbinutils libc-dev-bin libc6-dev libcc1-0 libcilkrts5 libdpkg-perl libexpat1-dev libfakeroot
  libfile-fcntllock-perl libgcc-7-dev libgomp1 libisl19 libitm1 liblsan0 libmpc3 libmpx2 libmysqlclient-dev
  libmysqlclient20 libpython-all-dev libpython-dev libpython-stdlib libpython2.7 libpython2.7-dev
  libpython2.7-minimal libpython2.7-stdlib libquadmath0 libstdc++-7-dev libtsan0 libubsan0 linux-libc-dev make
  manpages-dev mysql-common python python-all python-all-dev python-asn1crypto python-cffi-backend python-crypto
  python-cryptography python-dbus python-dev python-enum34 python-gi python-idna python-ipaddress python-keyring
  python-keyrings.alt python-minimal python-mysqldb python-pip python-pip-whl python-pkg-resources
  python-secretstorage python-setuptools python-six python-wheel python-xdg python2.7 python2.7-dev
  python2.7-minimal sqlite3 zlib1g-dev
0 actualizados, 81 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 77,1 MB de archivos.
Se utilizarán 249 MB de espacio de disco adicional después de esta operación.
Des:1 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 libpython2.7-minimal amd64 2.7.15~rc1-1ubuntu0.1 [3
34 kB]
Des:2 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 python2.7-minimal amd64 2.7.15~rc1-1ubuntu0.1 [1.30
4 kB]
Des:3 http://archive.ubuntu.com/ubuntu bionic/main amd64 python-minimal amd64 2.7.15~rc1-1 [28,1 kB]
Des:4 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 libpython2.7-stdlib amd64 2.7.15~rc1-1ubuntu0.1 [1.
912 kB]
Des:5 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 python2.7 amd64 2.7.15~rc1-1ubuntu0.1 [238 kB]
Des:6 http://archive.ubuntu.com/ubuntu bionic/main amd64 libpython-stdlib amd64 2.7.15~rc1-1 [7.620 B]
Des:7 http://archive.ubuntu.com/ubuntu bionic/main amd64 python amd64 2.7.15~rc1-1 [140 kB]
Des:8 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 binutils-common amd64 2.30-21ubuntu1~18.04 [193 kB]
Des:9 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 libbinutils amd64 2.30-21ubuntu1~18.04 [502 kB]
Des:10 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 binutils-x86-64-linux-gnu amd64 2.30-21ubuntu1~18.0
4 [1.855 kB]
Des:11 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 binutils amd64 2.30-21ubuntu1~18.04 [3.392 B]
Des:12 http://archive.ubuntu.com/ubuntu bionic/main amd64 libc-dev-bin amd64 2.27-3ubuntu1 [71,8 kB]
Des:13 http://archive.ubuntu.com/ubuntu bionic-security/main amd64 linux-libc-dev amd64 4.15.0-39.42 [1.008 kB]
Des:14 http://archive.ubuntu.com/ubuntu bionic/main amd64 libc6-dev amd64 2.27-3ubuntu1 [2.587 kB]
Des:15 http://archive.ubuntu.com/ubuntu bionic-updates/main amd64 gcc-7-base amd64 7.3.0-27ubuntu1~18.04 [18,9 kB]
Des:16 http://archive.ubuntu.com/ubuntu bionic/main amd64 libisl19 amd64 0.19-1 [551 kB]
Des:17 http://archive.ubuntu.com/ubuntu bionic/main amd64 libmpc3 amd64 1.1.0-1 [40,8 kB]
```

Il·lustració 7 Instal·lació de paquets Honeypot Telnet

Clonem el repositori git del projecte:

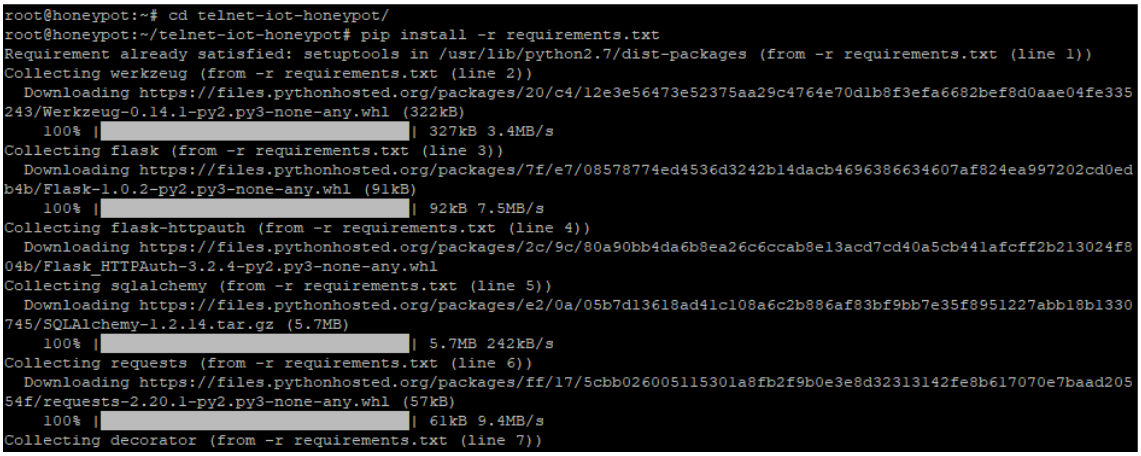
```
git clone https://github.com/Phype/telnet-iot-honeypot.git
```

```
root@honeypot:~# git clone https://github.com/Phype/telnet-iot-honeypot.git
Cloning into 'telnet-iot-honeypot'...
remote: Enumerating objects: 1338, done.
remote: Total 1338 (delta 0), reused 0 (delta 0), pack-reused 1338
Receiving objects: 100% (1338/1338), 2.07 MiB | 2.23 MiB/s, done.
Resolving deltas: 100% (684/684), done.
```

Il·lustració 8 Clonació del repositori Honeypot Telnet

Entrem dins el directori Telnet-iot-honeypot i instal·lem els paquets necessaris:

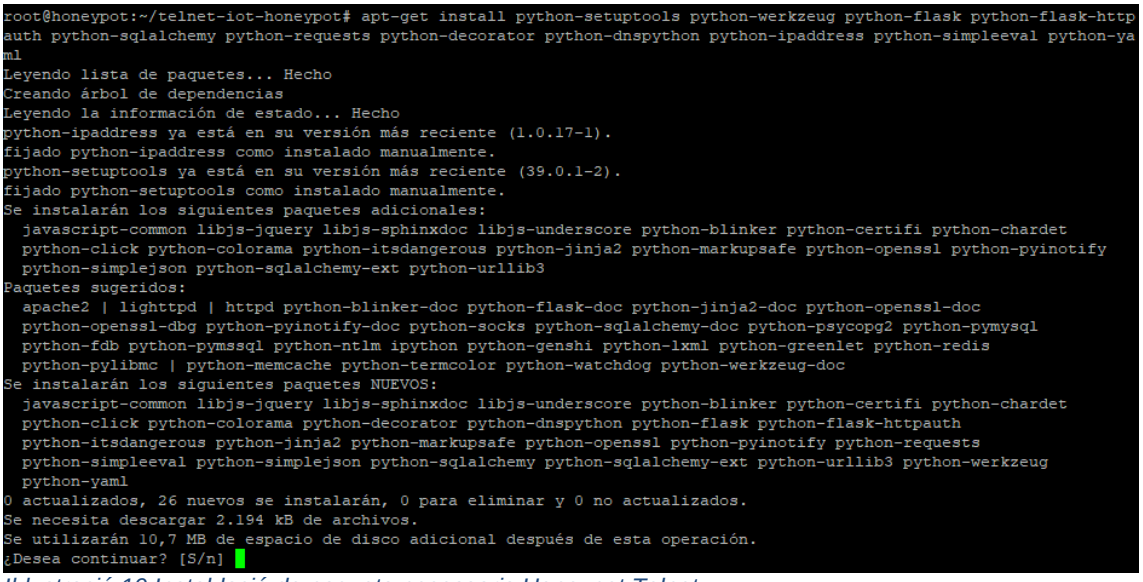
```
cd telnet-iot-honeypot/
pip install -r requirements.txt
```



Il·lustració 9 Instal·lació de paquets necessaris Honeypot Telnet

Afegim més paquets necessaris:

```
apt-get install python-setuptools python-werkzeug python-flask python-flask-httpauth python-sqlalchemy python-requests python-decorator python-dnspython python-ipaddress python-simpleeval python-yaml
```



Il·lustració 10 Instal·lació de paquets necessaris Honeypot Telnet

La configuració del Honeypot està en el fitxer config.dist.yaml. En aquest fitxer podem configurar, l'usuari i password del backend (si no s'especifiquen, es generen automàticament)la IP el port del backend, per defecte localhost:5000, el tipus de base de dades on emmagatzemarem les connexions (sqlite o mysql), el nombre màxim de connexions simultànies (per defecte una, millor posar 4), en quin directori s'emmagatzemaran les mostres capturades (per defecte samples),

la clau l'API de Virustotal[20] per si volem que analitzi les mostres capturades amb el motor de Virustotal, activar la resolució de noms, i si volem que les mostres passin per Cuckoo Sandbox[21].

```
# Backend URL to which honeypot will connect to to store data
backend: "http://localhost:5000"

# Write raw data to logfile, can be imported into backend db later
#   does include everything EXCEPT sample contents
log_raw: null

############################################
# Backend configuration

# sqlalchemy sql connect string
# examples:
# using sqlite: "sqlite:///database.db"
# using mysql:  ""mysql+mysqldb://USER:PASSWORD@MYSQL_HOST/DATABASE_NAME","
sql: "sqlite:///database.db"

# Max connections to sql db, maybe restricted in some scenarios
max_db_conn: 4

# Directory in which samples are stored
sample_dir: "samples"

# Virustotal API key
vt_key:       "[redacted]"
submit_to_vt: true

# Enable or Disable IP to ASN resolution
# Disabling will fasten up importing big amounts of data
do_ip_to_asn_resolution: true

cuckoo_enabled:  false,
cuckoo_url_base: "http://127.0.0.1:8090"
cuckoo_user:     "user"
cuckoo_passwd:   "passwd"
cuckoo_force:    0
```

Il·lustració 11 config.dist.yaml Honeypot Telnet

Hi ha un problema amb un parell de fitxers que fa que el Honeypot no funcioni correctament. Per arreglar-ho s'ha d'editar el fitxer honeypot/session.py i canviar a la línia 81 parse(1) per run(1):

```
try:                                try:
        tree = parse(1)                     tree = run(1)
        tree.run(self.env)                  tree.run(self.env)
```

Il·lustració 12 Canvis a fitxer honeypot/session.py Honeypot Telnet

[20] https://www.virustotal.com

[21] https://cuckoosandbox.org/

I editar el fitxer honypot/sample.py i afegir global _BACKEND a la línia 12:

```
_BACKEND = None
def get_backend():
        if _BACKEND:
                return _BACKEND
        elif config.get("backend", optional=True) != None:
                _BACKEND = client.Client()
                return _BACKEND
```

```
_BACKEND = None
def get_backend():
        global _BACKEND
        if _BACKEND:
                return _BACKEND
        elif config.get("backend", optional=True) != None:
                _BACKEND = client.Client()
                return _BACKEND
```

Il·lustració 13 Canvis al fitxer honeypot/sample.py

En aquest punt ja tenim el Honeypot llest. Per engegar-lo, primer arrenquem el backend:

`python backend.py`

```
root@honeypot:~/telnet-iot-honeypot# python backend.py
Creating/Connecting to DB
DB Setup done
Creating admin user "admin" see config for password
 * Serving Flask app "backend.backend" (lazy loading)
 * Environment: production
   WARNING: Do not use the development server in a production environment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://0.0.0.0:5000/ (Press CTRL+C to quit)
```

Il·lustració 14 Arranc backend

I després executem el honeypot:

`python honeypot.py`

```
root@honeypot:~# cd telnet-iot-honeypot/
root@honeypot:~/telnet-iot-honeypot# python honeypot.py
2018-11-26 13:55:33   telnet.py:57      Socket open on port 2223
```

Il·lustració 15 Arranc Honeypot

Com es pot observar, el honeypot escolta en el port 2223, per canviar el port d'escolta, s'ha d'editar el fitxer honeypot.py i modificar la línia 58:

```
if action == None:
        srv = Telnetd(2223)
        signal.signal(signal.SIGINT, signal_handler)
        srv.run()
```

```
if action == None:
        srv = Telnetd(23)
        signal.signal(signal.SIGINT, signal_handler)
        srv.run()
```

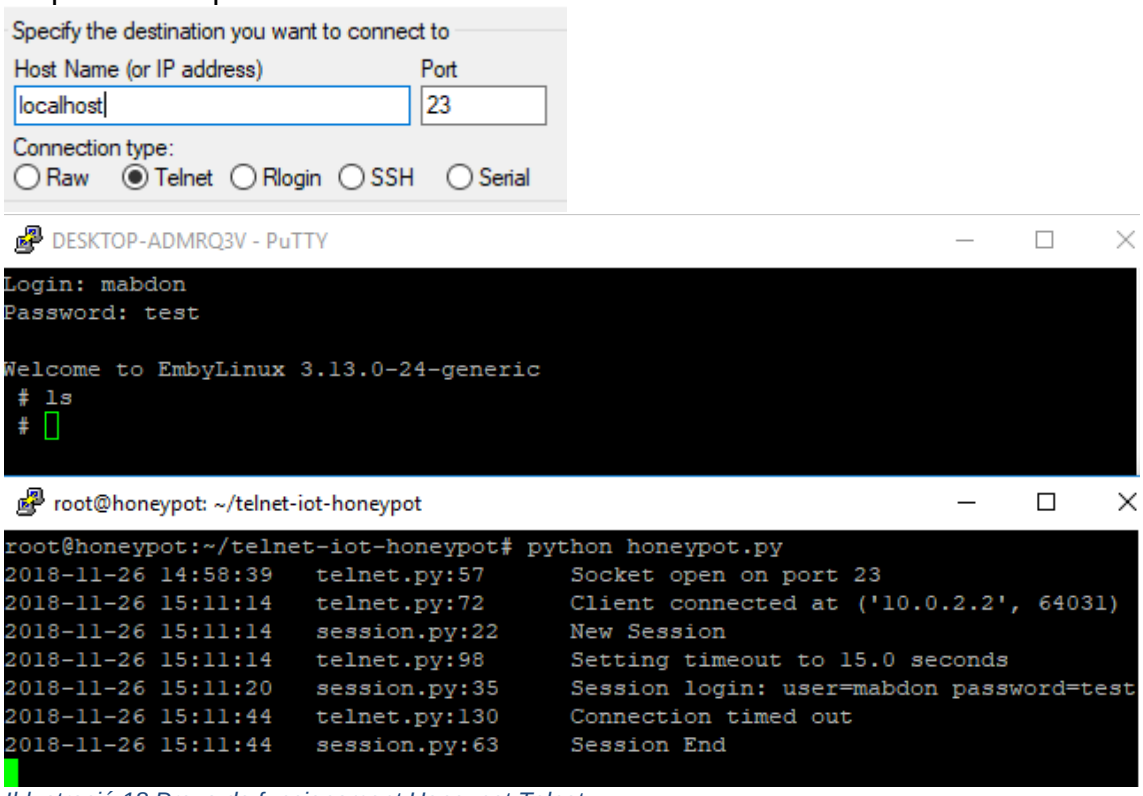
Il·lustració 16 Canvi de port del Honeypot

I d'aquesta manera escoltarà en el port 23:

```
root@honeypot:~/telnet-iot-honeypot# python honeypot.py
2018-11-26 14:58:39    telnet.py:57      Socket open on port 23
```

Il·lustració 17 Honeypot escoltant al port 23

Es pot fer una prova:



Il·lustració 18 Prova de funcionament Honeypot Telnet

8.2.1 Instal·lació del servidor web

Si volem accedir la web del backend des de fora del Honeypot hem d'instal·lar un servidor web:
apt install apache2

```
root@honeypot:~/telnet-iot-honeypot# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill-dbd-sqlite3 libaprutill-ldap liblua5.2-0
  ssl-cert
Paquetes sugeridos:
  www-browser apache2-doc apache2-suexec-pristine | apache2-suexec-custom openssl-blacklist
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-bin apache2-data apache2-utils libaprl libaprutill libaprutill-dbd-sqlite3 libaprutill-ldap
  liblua5.2-0 ssl-cert
0 actualizados, 10 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 1.730 kB de archivos.
Se utilizarán 6.985 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
Des:1 http://archive.ubuntu.com/ubuntu bionic/main amd64 libaprl amd64 1.6.3-2 [90,9 kB]
```

Il·lustració 19 Instal·lació del servidor Apache

Entrem al directori telnet-iot-honeypot i copiem les dades de la web al directori del servidor web:

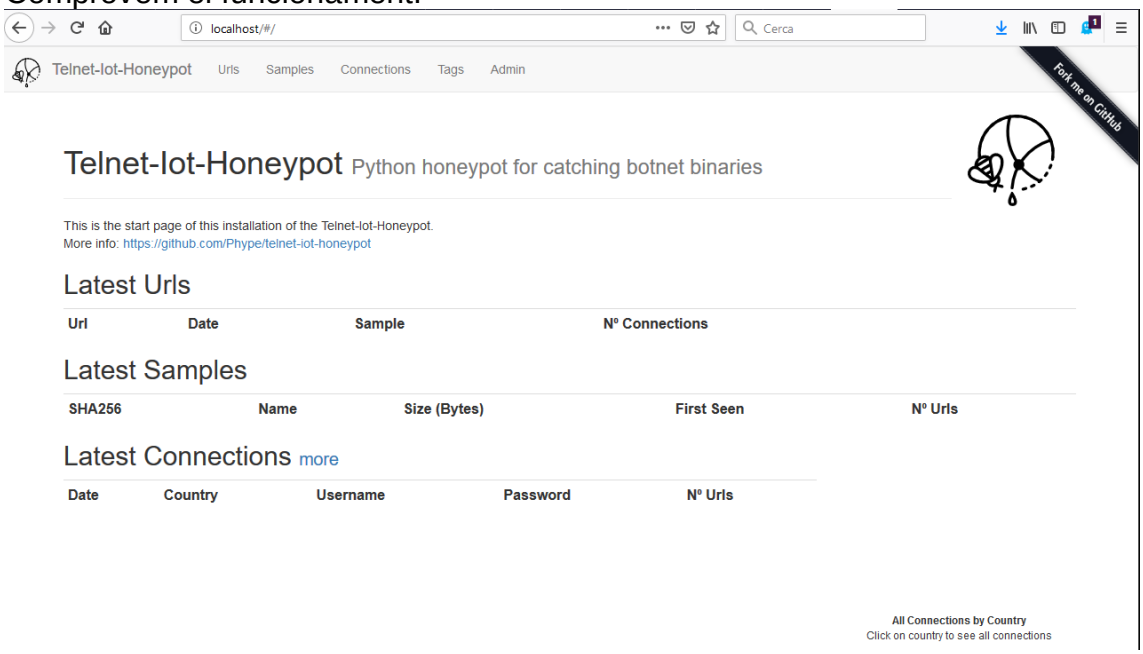
```
cd telnet-iot-honeypot
cp -R html /var/www
```

```
sudo chown www-data:www-data /var/www -R
```

```
root@honeypot:~# cd telnet-iot-honeypot/
root@honeypot:~/telnet-iot-honeypot# cp -R html /var/www/
root@honeypot:~/telnet-iot-honeypot# chown www-data:www-data /var/www -R
root@honeypot:~/telnet-iot-honeypot#
```

Il·lustració 20 Copia dels fitxers necessaris per la web

Comprovem el funcionament:



Il·lustració 21 Web del backend del Honeypot Telnet

8.2.2 Securització del Honeypot Telnet

Per securitzar el honeypot he configurat el Firewall ufw. Primer s'ha afegit una regla per permetre tot el tràfic des de la meva maquina (*ufw allow from *.*.*.**), després una per a que els "atacants" es puguin connectar al Honeypot (*ufw allow from any to 10.0.2.15 port 23*), i després s'ha activat el Firewall (*ufw enable*):

```
root@honeypot:~/telnet-iot-honeypot# ufw status
Status: inactive
root@honeypot:~/telnet-iot-honeypot# ufw allow from [redacted]
Rules updated
root@honeypot:~/telnet-iot-honeypot# ufw allow from any to 10.0.2.15 port 23
Rules updated
root@honeypot:~/telnet-iot-honeypot# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@honeypot:~/telnet-iot-honeypot#
```

Il·lustració 22 Regles del firewall del Honeypot Telnet

D'aquesta manera, des de la meva maquina puc accedir a la web del backend per veure els resultats i accedir a la maquina per SSH, i els "atacants" només poden accedir al Honeypot.

8.2.3 Configuració de la xarxa

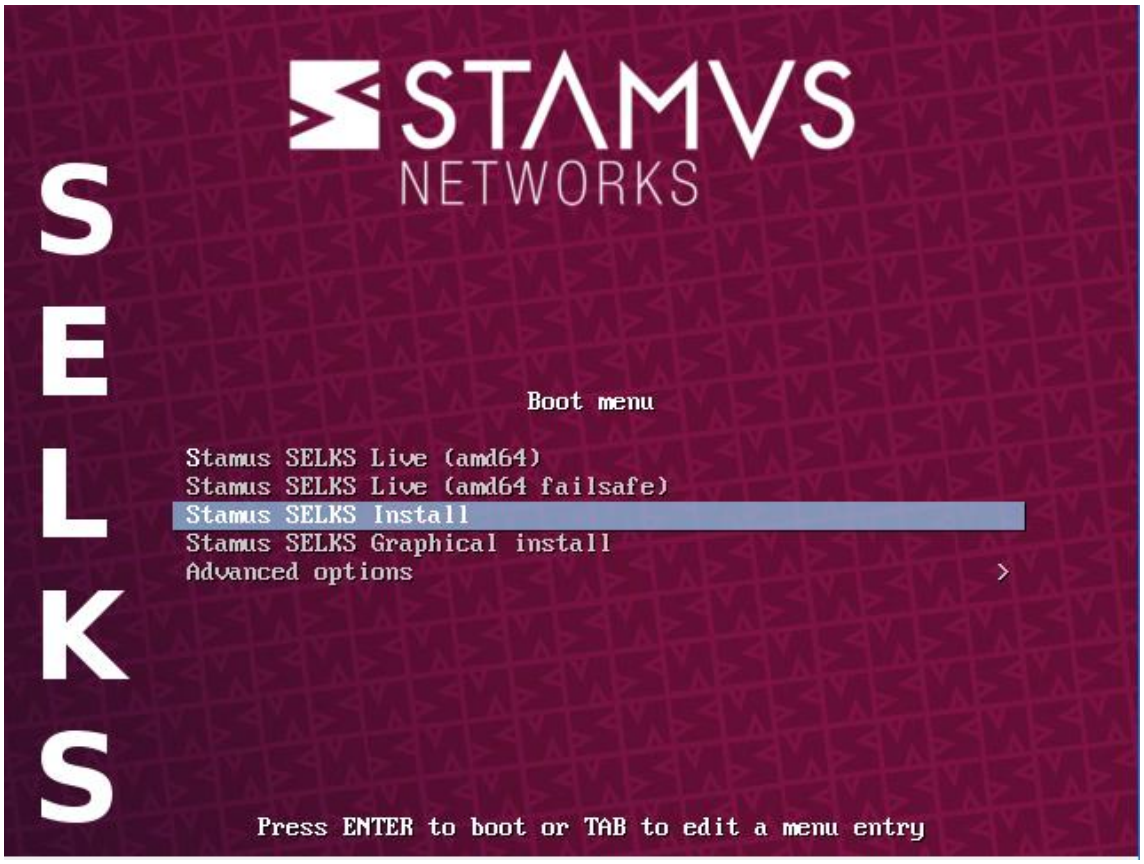
S'han desplegat tres Honeypots Telnet a tres xarxes diferents, tots ells han estat desplegats dins de màquines virtuals amb Virtualbox[22]. En el cas dels dos Honeypots desplegats a la xarxa de la universitat la interfície de xarxa ha estat configurada en mode "bridge" pel que la connexió era directa, no s'ha fet cap configuració apart d'establir la IP de manera estàtica. En el cas del Honeypot a la xarxa domèstica, també s'ha utilitzat una connexió "bridge", però en aquest cas s'ha obert el port 23 del router d'accés i s'ha redirigit cap al port 2223:

Il·lustració 23 Obertura de ports al router domèstic

8.3 Suricata + ELK

En aquest projecte s'ha utilitzat la distribució SELKS[23], concretament la versió SELKS without Desktop (SELKS-5.0beta1-nodesktop.iso), que integra Suricata amb l'ELK stack.

Un cop s'encén la màquina hem de triar Stamus SELKS Install:

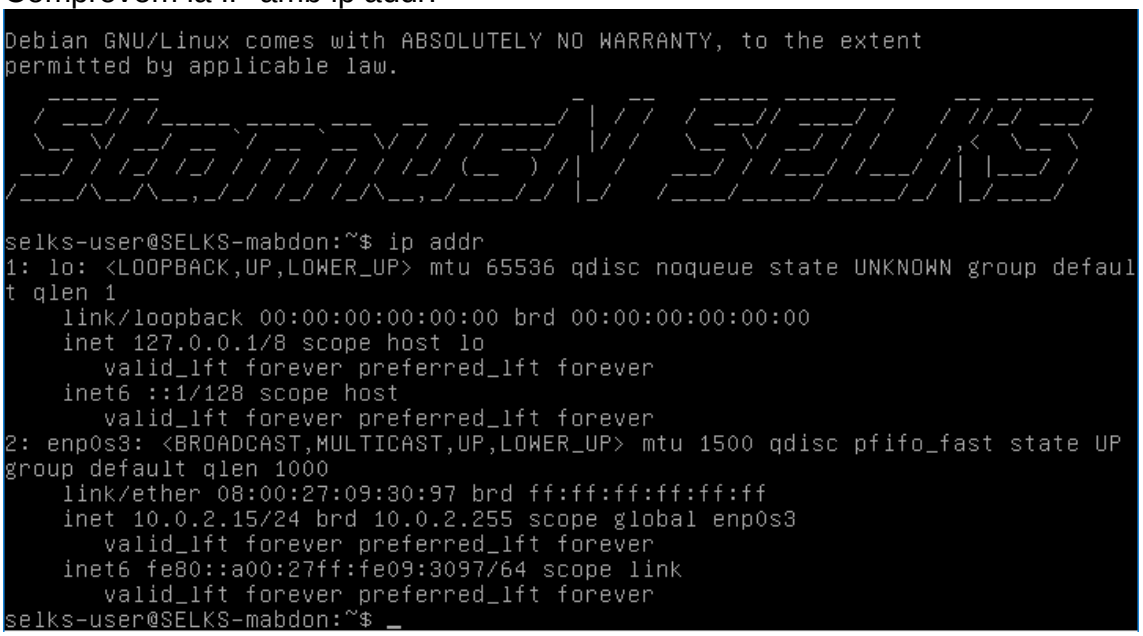


Il·lustració 24 Instal·lació de SELKS

[22] https://www.virtualbox.org/

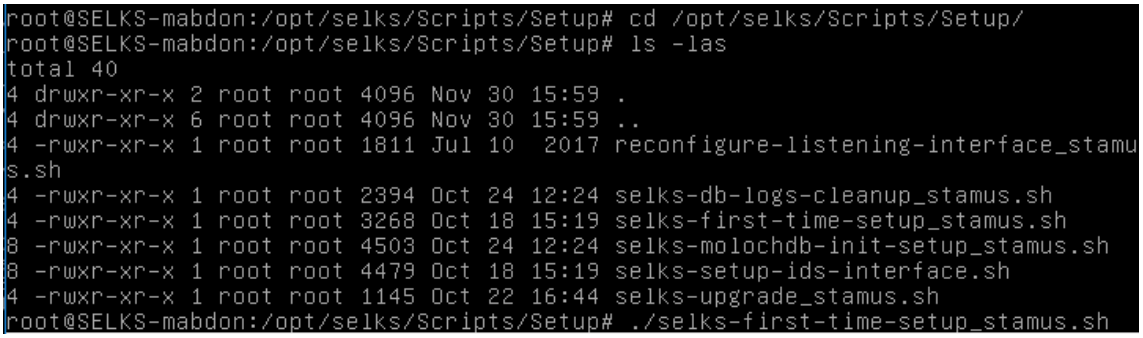
[23] https://www.stamus-networks.com/open-source/

Triem L'idioma, el país i el teclat, posem el nom de la maquina, definim el particionat del disc, esperem a que es copiïn els paquets i instal·lem el GRUB al disc dur. Reiniciem i entrem amb l'usuari selks-user paraula de pas selks-user. Comprovem la IP amb ip addr:



Il·lustració 25 Comprovar la xarxa

Fem sudo su – i entrem al directori /opt/selks/Scripts/Setup i executem l'script selks-first-time-setup-sh



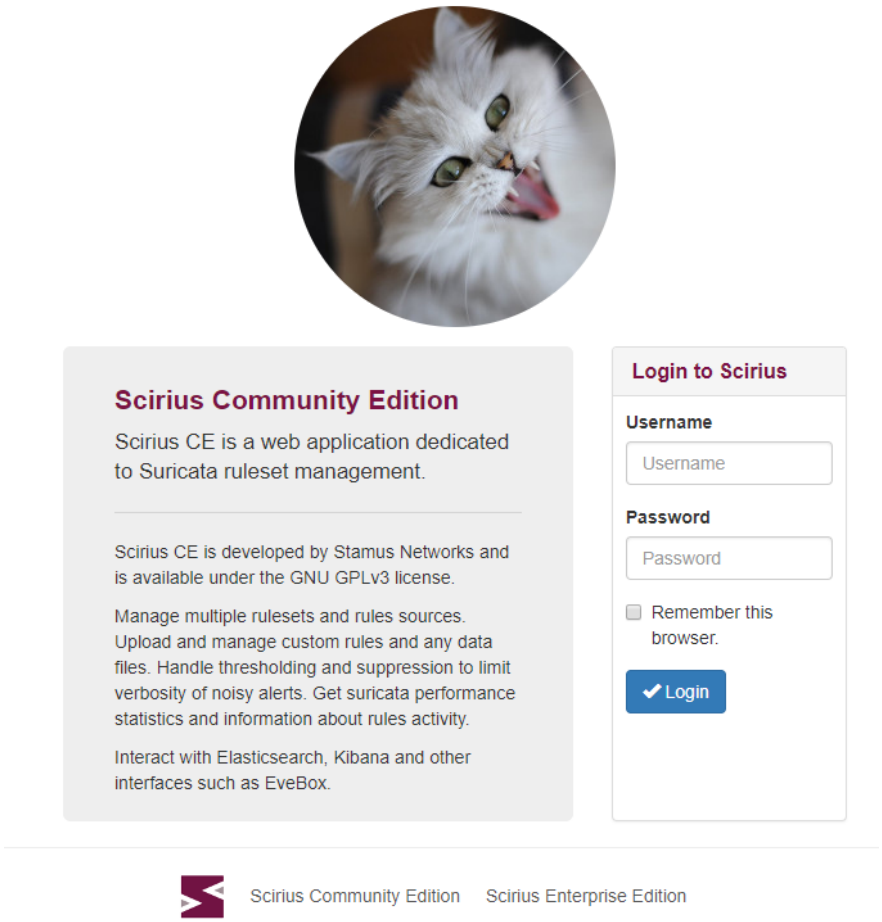
Il·lustració 26 Script de configuració

I definir la interfície que farà la captura:

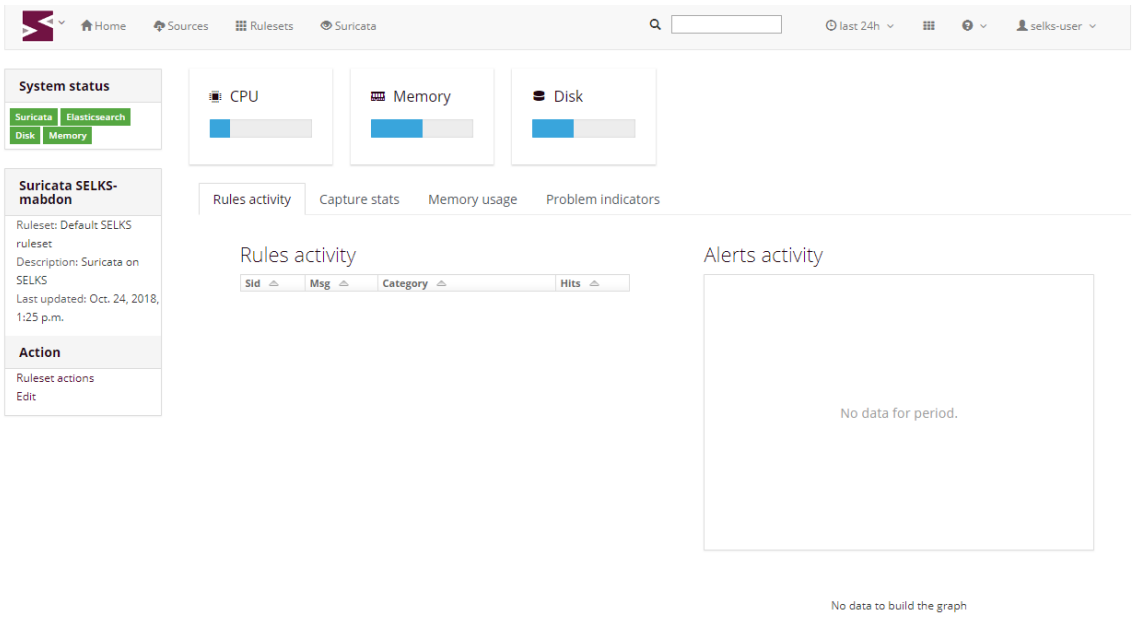
```
ion on
0: enp0s3
1: lo
Please type in interface or space delimited interfaces below and hit "Enter".
Example: eth1
OR
Example: eth1 eth2 eth3

Configure threat detection for INTERFACE(S):
enp0s3

The supplied network interface(s):  enp0s3

DONE!
FPC - Full Packet Capture. Suricata will rotate and delete the pcap captured fil
es.
FPC_Retain - Full Packet Capture with having Moloch's pcap retention/rotation. K
eeps the pcaps as long as there is space available.
None - disable packet capture

1) FPC
2) FPC_Retain
3) NONE
Please choose an option. Type in a number and hit "Enter" 3
```

Il·lustració 27 Definició d'interfície

Ara ja podem accedir a la interfície web anant a https:\\IP-SELKS i accedir amb l'usuari selks-user i paraula de pas selks-user:



Il·lustració 28 Interfície web de SELKS



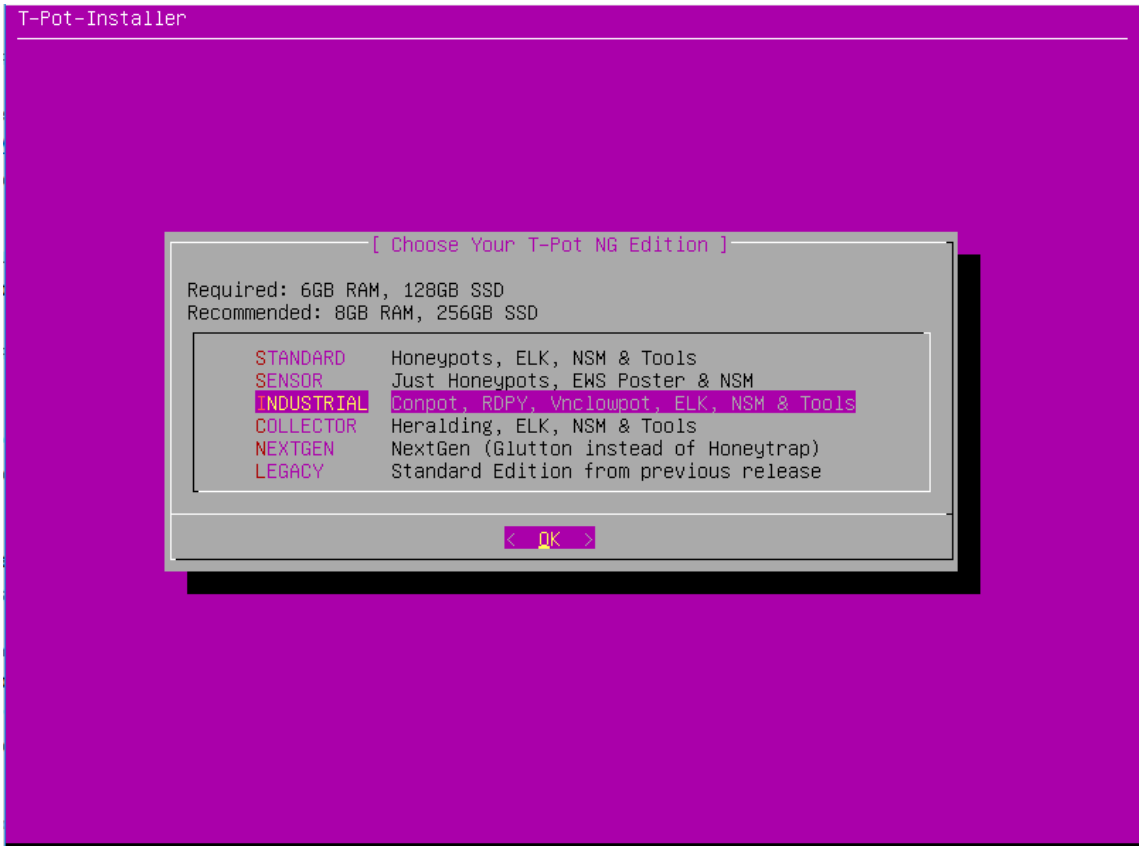
Il·lustració 29 Estat de SELKS

8.4 T-Pot

T-Pot es pot instal·lar en una maquina física o virtual. En aquest treball s'ha instal·lat en una maquina virtual amb VirtualBox. Per instal·lar T-Pot en VirtualBox, hem de donar d'alta al DHCP l'adreça MAC de la maquina virtual, afegir 8GB de RAM, 128 GB de disc dur i més d'un core del processador, en el cas d'aquest treball s'han posat 4 cores.
Un cop configurada la màquina s'ha de posar a la unitat de CD la imatge ISO t-pot[24].

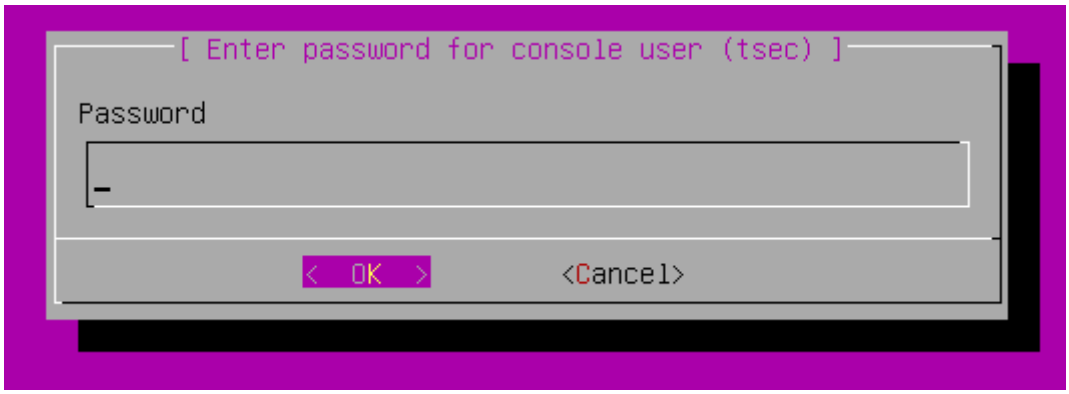
Quan arrenca, triar Install T-Pot, seleccionar el país, configurar el teclat. Esperar a que s'instal·lin els paquets i treure el cd de la unitat un cop reinicia. Quan reinicia demana quin perfil de T-Pot es vol instal·lar. Per aquest treball s'ha triat Standard:

[24] https://github.com/dtag-dev-sec/tpotce/releases



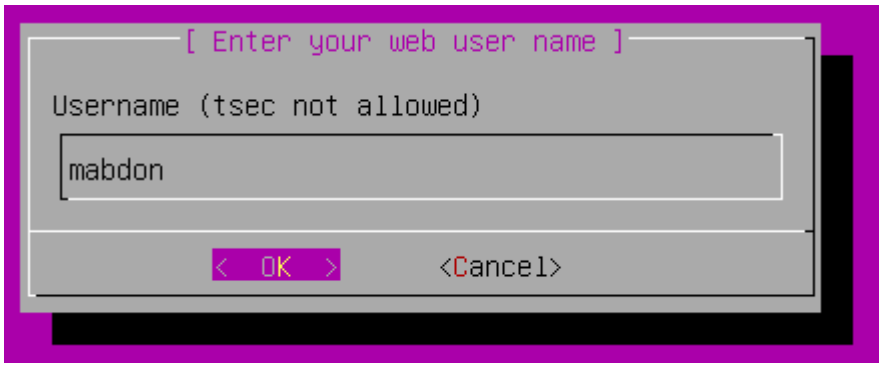
Il·lustració 30 Elecció del tipus de T-Pot a instal·lar

Després demana la paraula de pas de l'usuari tsec:



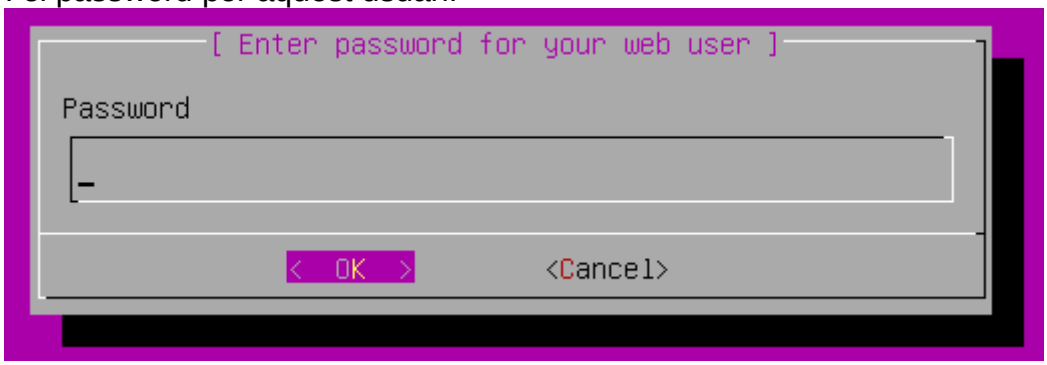
Il·lustració 31 Definició del password de l'usari local

Definim l'usuari web:



Il·lustració 32 Usuari web

I el password per aquest usuari:

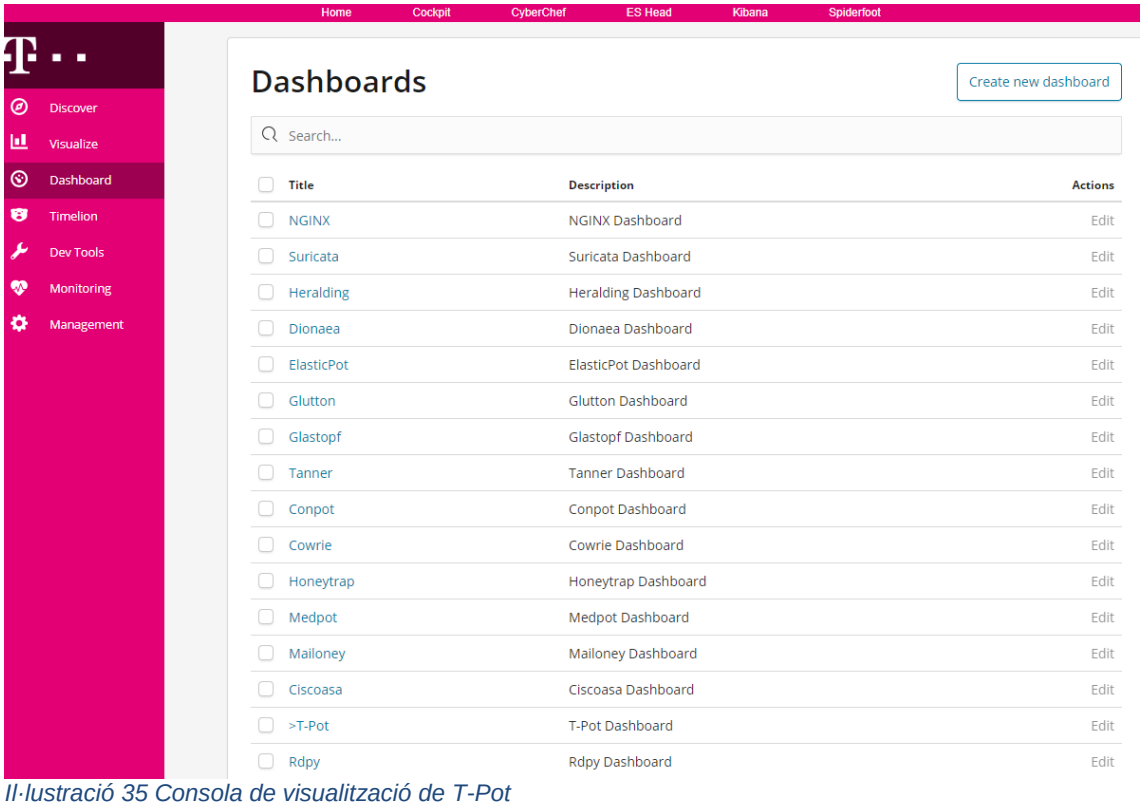


Il·lustració 33 Password de l'usuari web

Un cop finalitzada la instal·lació ens hem de connectar a la plana web indicada (https://10.0.2.15:64297):

Il·lustració 34 Arranc T-Pot amb la IP i el ports

Introduïm l'usari web i la seva paraula de pas creats anteriorment, i entrarem a kibana:



Il·lustració 35 Consola de visualització de T-Pot

Al menú DASHBOARD[25], podem triar el mòdul de visualització del honeypot que es vulgui. Si es tria T-Pot, es veu un resum de l'activitat de tots els honeypots alhora.

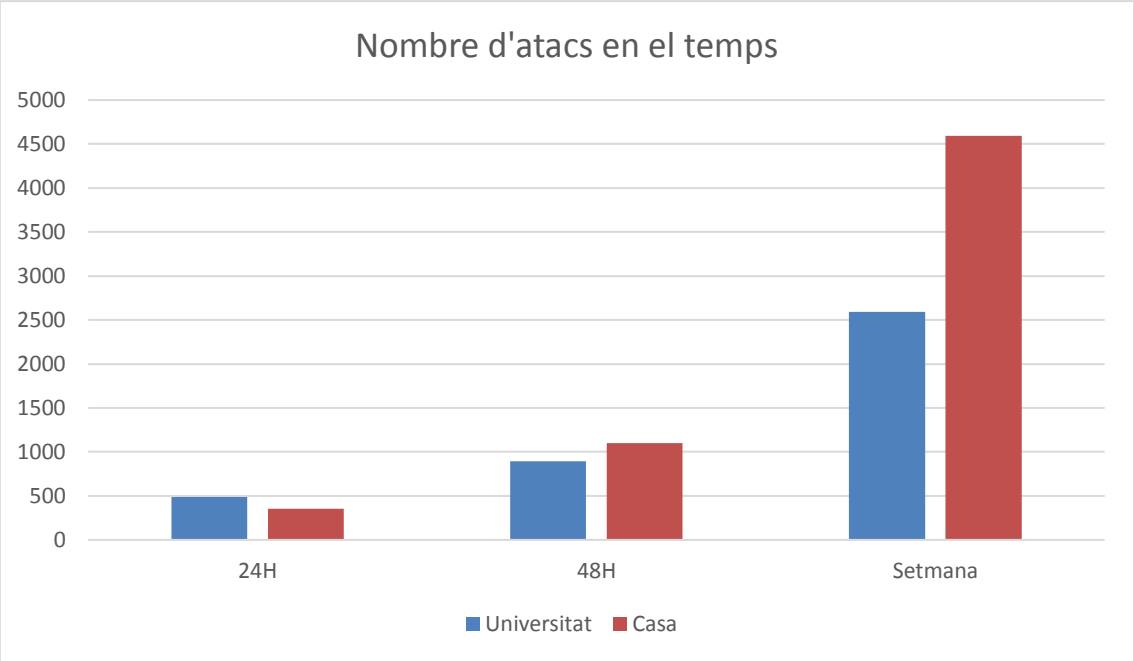
9 Anàlisi dels atacs rebuts

En aquest apartat s'analitzen els atacs rebuts durant una setmana a les diferents xarxes. L'equip situat a la xarxa interna d'una universitat no ha rebut cap tipus de connexió, gracies a les configuracions de seguretat de la pròpia xarxa, per tant, aquest anàlisi es centrarà en la sonda de la xarxa domèstica i la sonda de la xarxa externa de la universitat.

9.1 Honeypot Telnet

El Honeypot Telnet de la xarxa externa de la universitat ha registrat en les primeres 24 hores 486 connexions mentre que el de la xarxa domèstica ha registrat 354, durant les primeres 48 hores 891 la universitat i 1102 la domèstica, i en una setmana, la universitat ha rebut 2593 i la xarxa domèstica 4596.

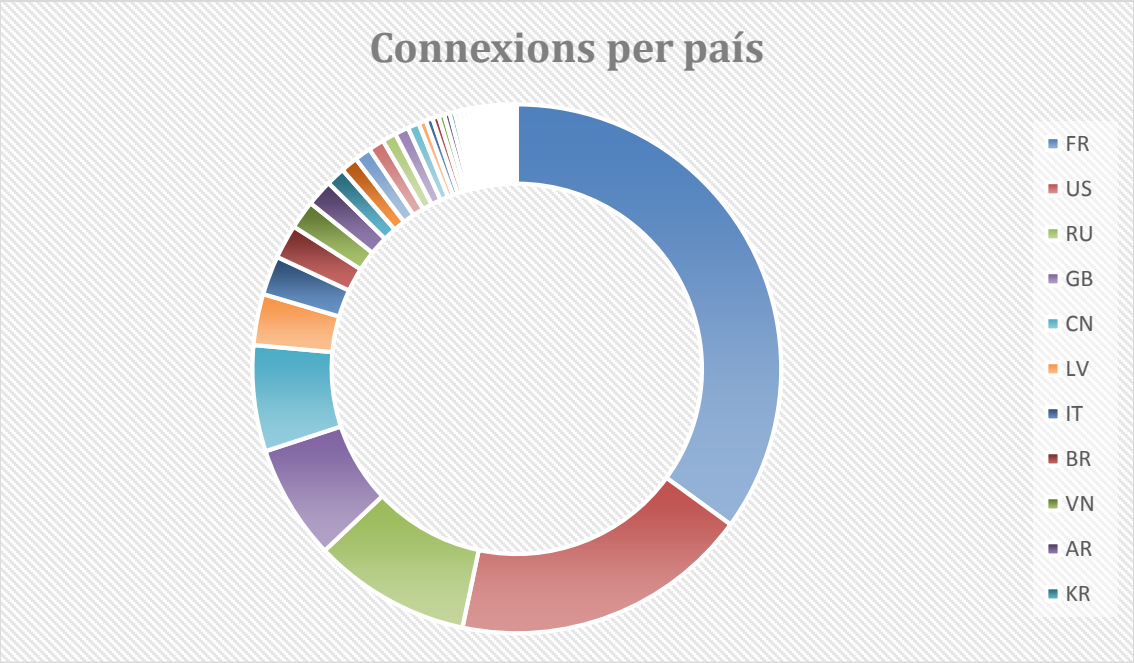
[25] Les imatges i la guia corresponen a T-Pot 18.11 publicat el 28/11/2018, tot i que aquest treball s'ha realitzat amb T-Pot 17.10.



Il·lustració 36 Nombre d'atacs en el temps Honeypot Telnet

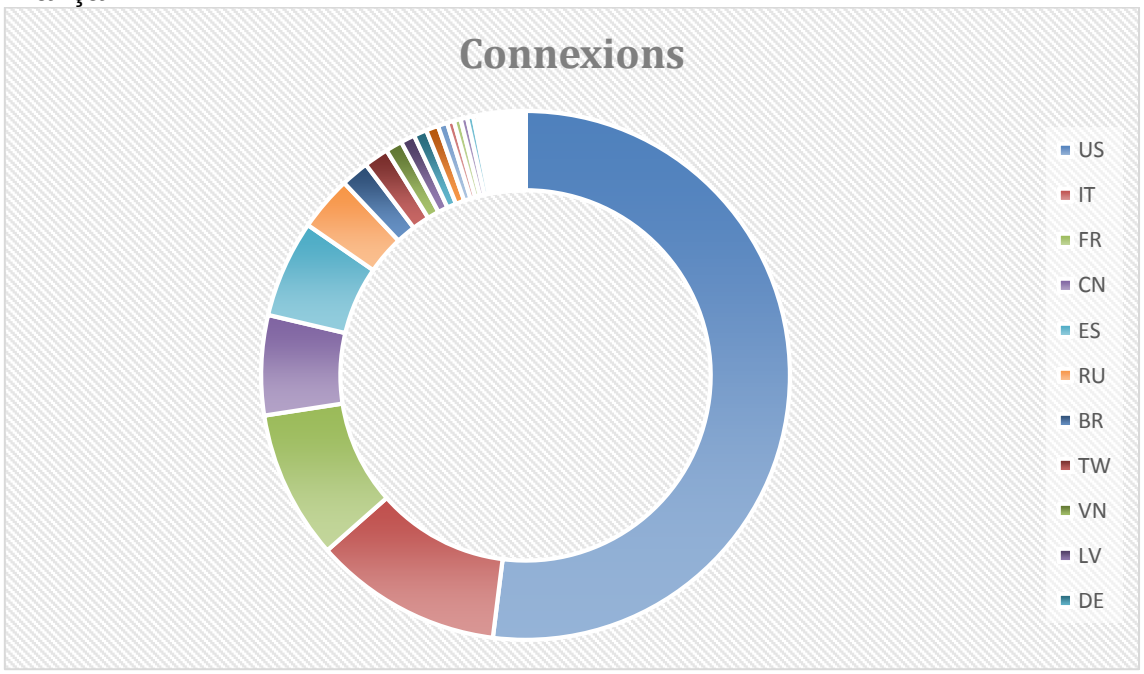
9.1.2 Països

En el Honeypot situat a la universitat ha estat contactat per 64 països. Els tres primers països per nombre de connexions són França, Estats Units i Rússia.



Il·lustració 37 Connexions per país Universitat

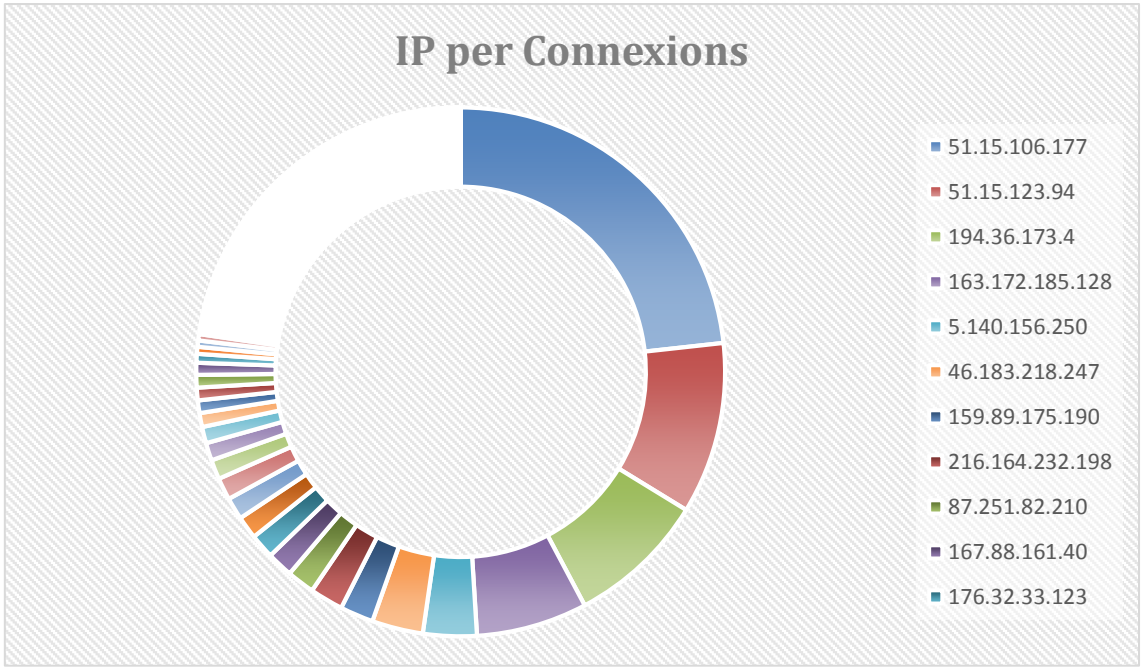
En el situat a la xarxa domèstica s'han rebut connexions des de 67 països i els tres primers països per nombre de connexions han estat Estats Units, Itàlia i França.



Il·lustració 38 Connexions per país xarxa domèstica

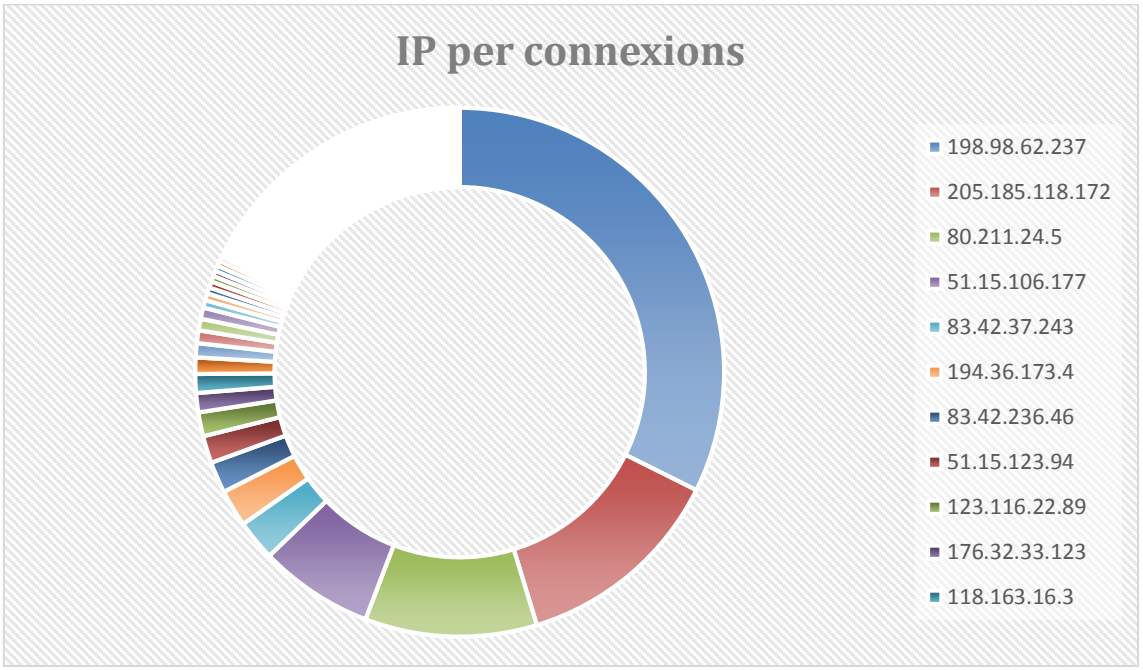
9.1.3 IPs

Les tres adreces IP que més han atacat a la xarxa de la universitat han estat 51.15.106.177 amb 603 connexions, 51.15.123.94 amb 272 connexions i 194.36.173.4 amb 220 connexions. En total s'han rebut connexions de 544 adreces IP diferents.



Il·lustració 39 IP per connexions Universitat

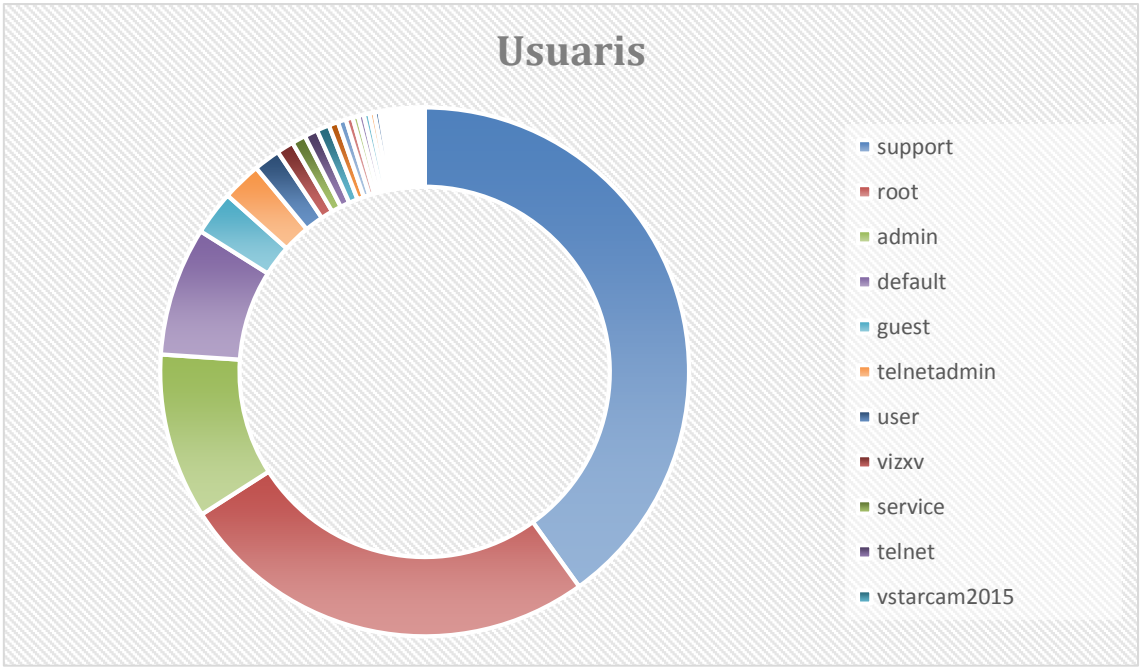
A la xarxa domèstica s'han rebut connexions des de 622 adreces IP diferents, i les tres adreces IP amb més connexions han estat 198.98.62.237 amb 1459 connexions, 205.185.118.172 amb 583 connexions i 80.211.24.5 amb 474 connexions.



Il·lustració 40 IP per connexions xarxa domèstica

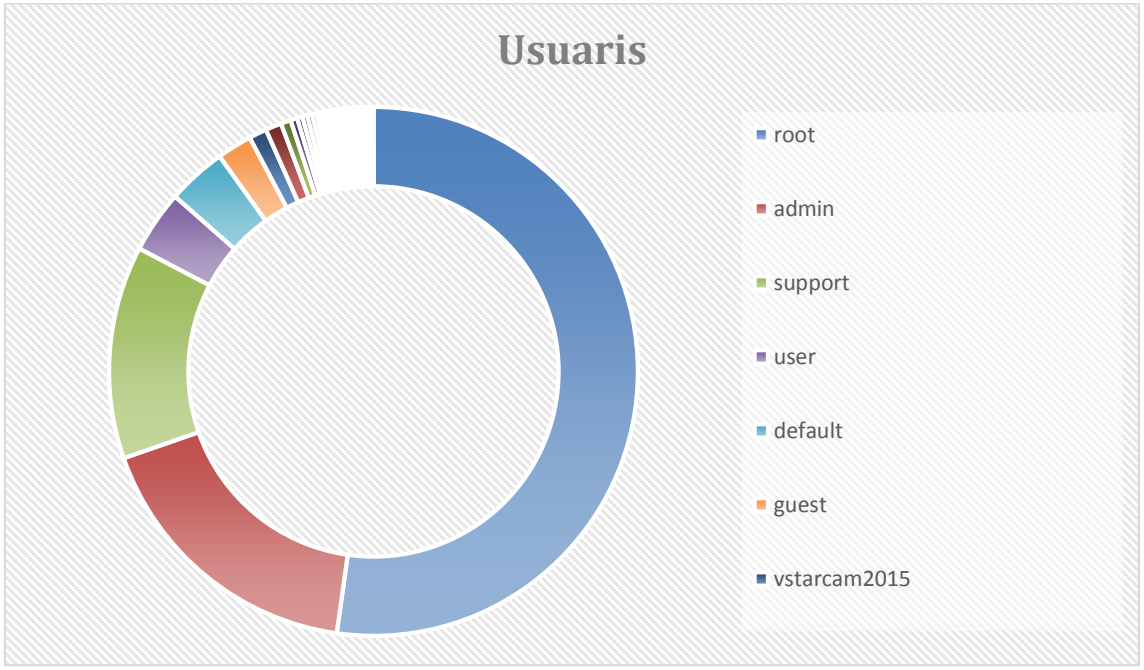
9.1.3 Noms d'usuari

A la xarxa de la universitat s'han utilitzat 42 noms d'usuari diferents, sent els tres més nombrosos suport amb 1039 intents, root amb 671 intents i admin amb 262 intents.



Il·lustració 41 Usuaris universitat

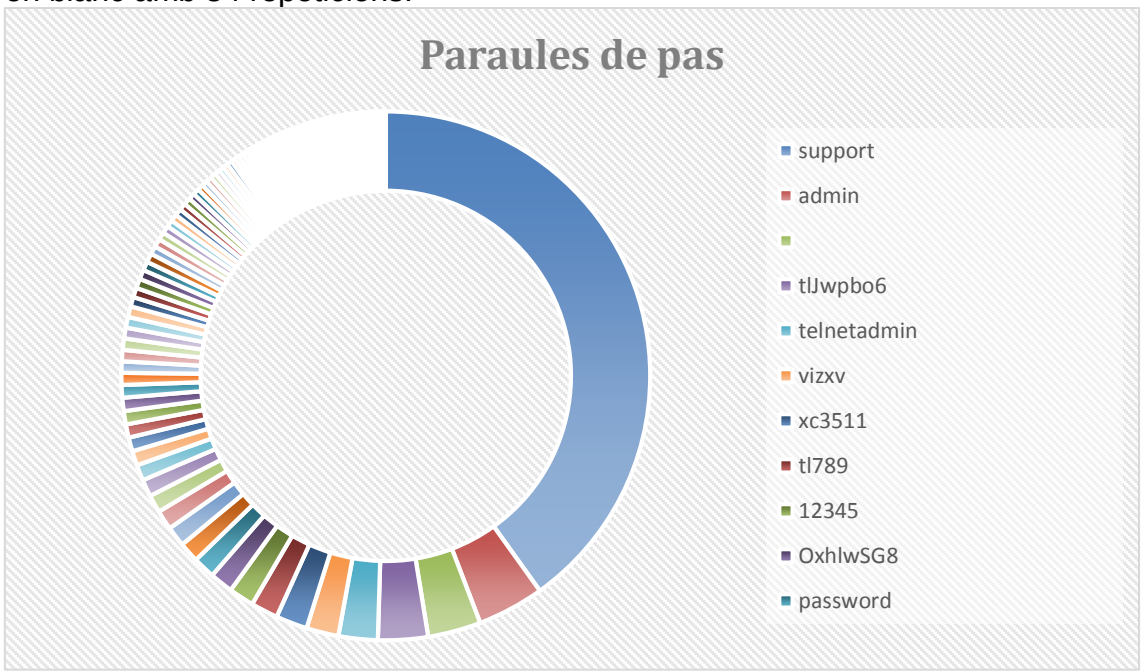
A la xarxa domèstica s'ha utilitzat 73 noms d'usuaris diferents, sent els tres més nombrosos root amb 2399 intents, admin amb 802 intents i suport amb 598 intents.



Il·lustració 42 Usuaris xarxa domèstica

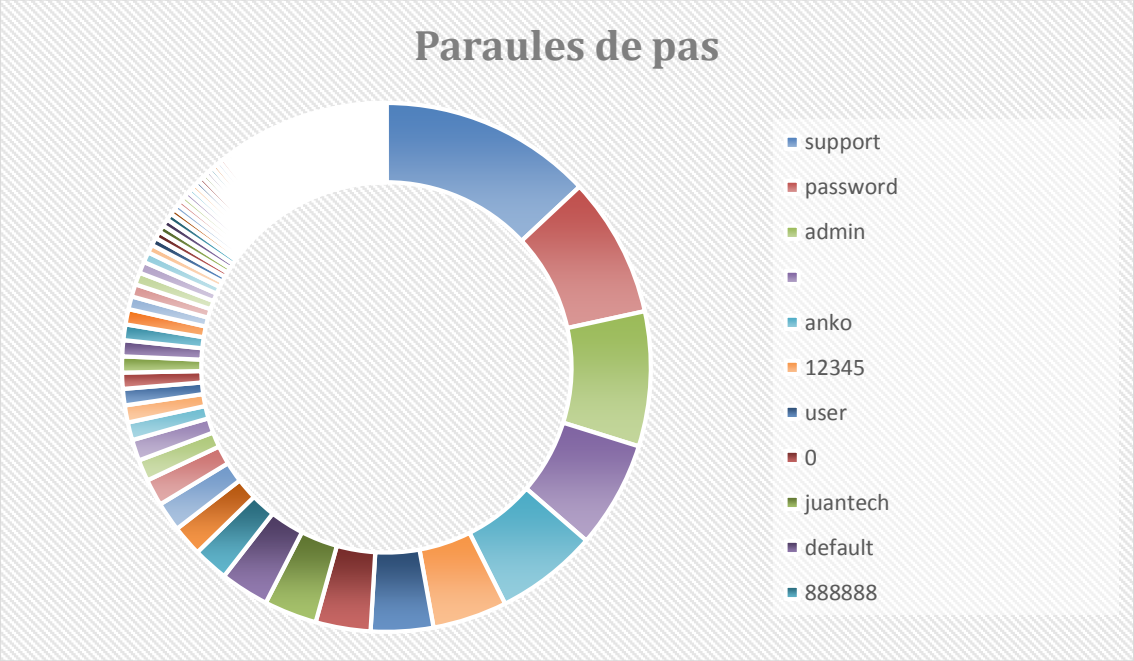
9.1.4 Paraules de pas

A la xarxa de la universitat s'han utilitzat 143 paraules de pas diferents, sent les tres més utilitzades, suport amb 1039 repeticions, admin amb 106 repeticions i en blanc amb 84 repeticions.



Il·lustració 43 Paraules de pas universitat

A la xarxa domèstica s'han utilitzat 189 paraules de pas diferents, sent les tres més utilitzades, suport amb 598 repeticions, password amb 393 repeticions i admin amb 378 repeticions.



Il·lustració 44 Paraules de pas xarxa domèstica

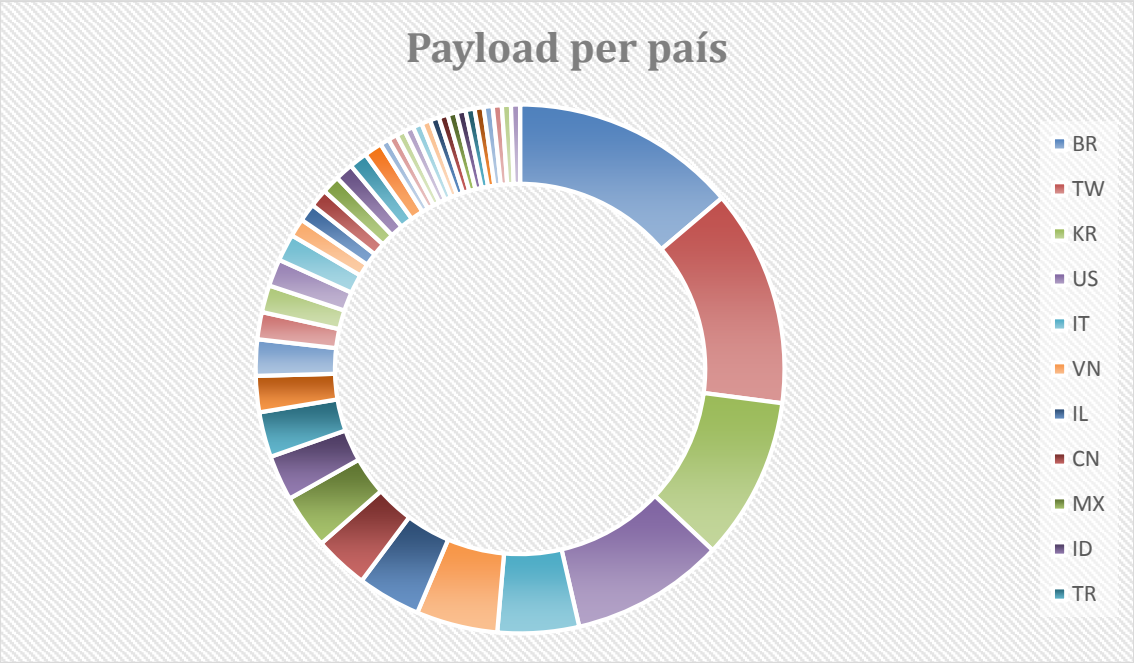
9.1.5 Mostres

A la xarxa externa de la universitat s'han capturat 60 mostres diferents des de 182 urls. La mostra identificada per virustotal[26] com Hajime a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3, s'ha descarregat des de 139 urls diferents, la mostra no identificada per virustotal 14049d077b887cbb8060d223ff9626664a044a8c3145f6a2b95a325df36b279b des de quatre urls diferents i la resta de mostres de d'una url.

Per països on estaven situades les urls, des d'on s'ha descarregat el payload, els tres primers països són Brasil, Taiwan i Korea.

26

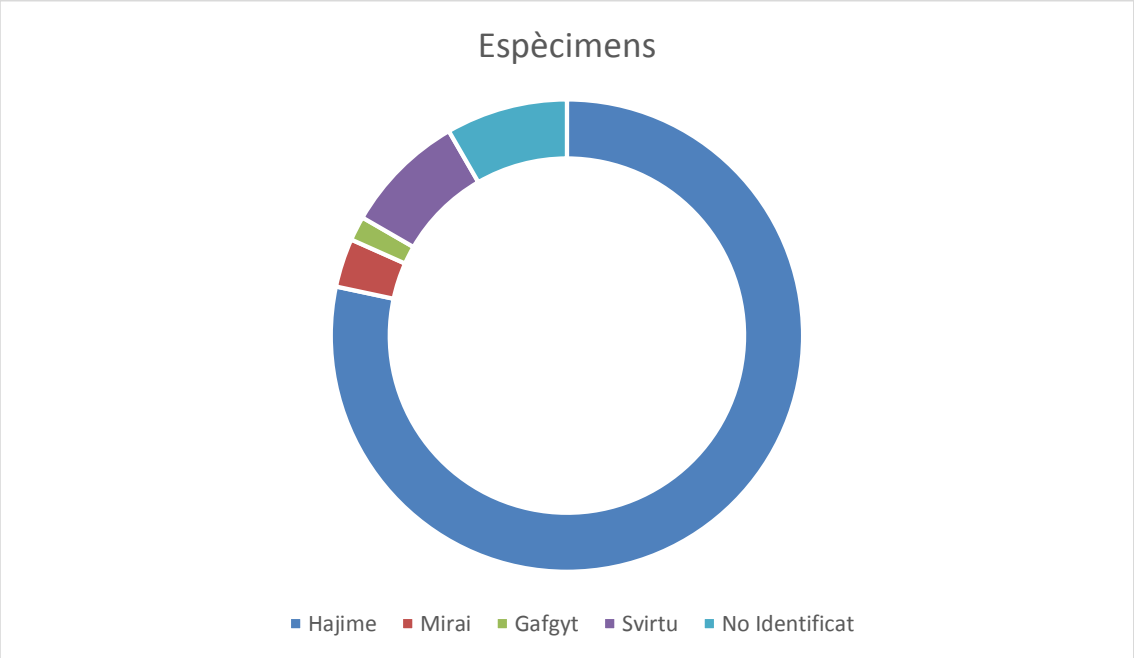
https://www.virustotal.com/#/file/a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3/detection



Il·lustració 45 Payload per país Universitat

De les 60 mostres 49 han estat identificades per l'antivirus Trend Internet Security 15.0.1212 amb el patró de virus actualitzat a 1/12/18. L'antivirus ha identificat 47 de les mostres com Hajime, 2 com Mirai, i 1 com Gafgyt.
La resta de mostres es passen per VirusTotal i, combinat amb el resultat de l'antivíric Trend, s'han identificat els següents espècimens:

	Hajime	Mirai	Gafgyt	Svirtu	No Identificat
Nombre	47	2	1	5	5



Il·lustració 46 Espècimens de la xarxa de la universitat

De les 5 mostres no identificades, una és un error 404 d'un bot que no està ben configurat[27] i no descarrega bé el payload:

```
# rm  # daddyl33t/dev/.t; rm  # daddyl33t/dev/.sh; rm  # daddyl33t/dev/.33af
# /bin/busybox wget http://159.89.130.69:80/8arm68 -O - > 5aA3; /bin/busybox chmod 777 5aA3; /bin/busybox yami
```

Il·lustració 47 daddyl33t

Una altre és un fitxer de text que conté la cadena gAt9W}c.

En les altres, es va crear un binari amb la comanda echo, i les credencials per accedir van ser root:nas4free i root:f00b@r (en dues ocasions). Dos de les mostres es van generar des de la mateixa ip, pel que pot ser que generi un payload diferent cada cop que infecta una víctima. Les comandes executades són iguals en els tres casos, pel que es pot deduir que les tres mostres pertanyen a la mateixa botnet.

A la xarxa domèstica s'han capturat 130 mostres diferents capturades des de 272 urls diferents. La mostra a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3, identificada per virustotal[23] com Hajime, s'ha descarregat des de 139 urls diferents, la mostra 14049d077b887cbb8060d223ff9626664a044a8c3145f6a2b95a325df36b279b no identificada per virustotal des de tres urls diferents i la mostra b71a3c2eb44f3e04a535387e9d2ed2985718148b57c8b162289832dc898a9987 des de tres ubicacions diferents. La resta de mostres s'ha descarregat des d'una sola url cadascuna.

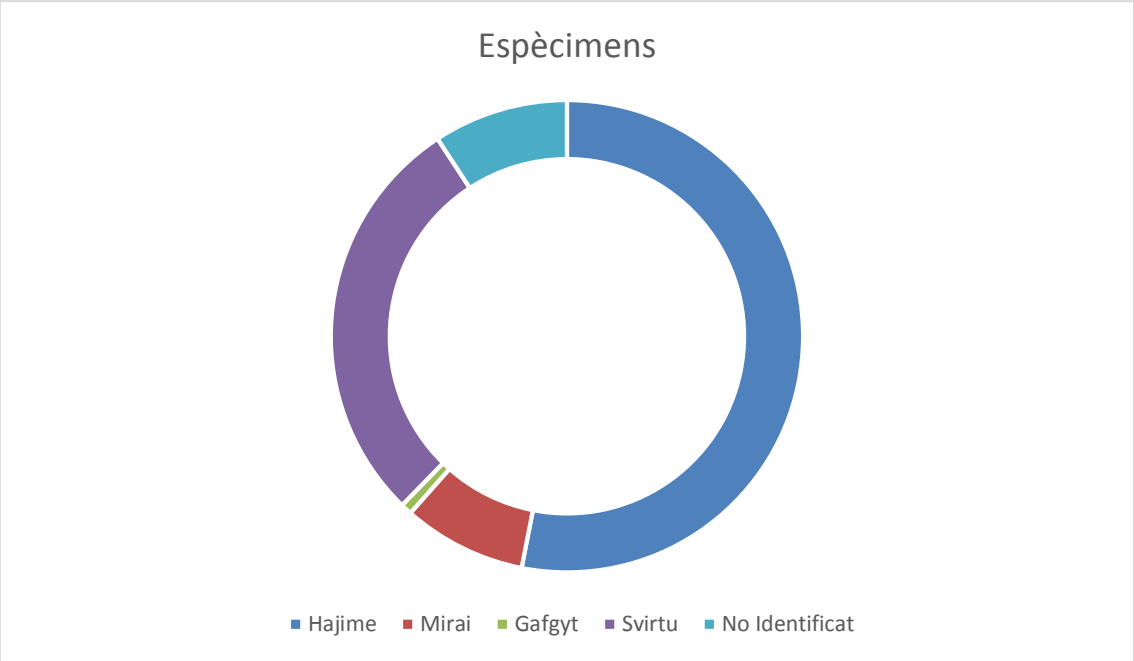
Per països on estaven situades les urls, des d'on s'ha descarregat el payload, els tres primers països són Xina, Estats Units i Korea.

De les 130 mostres 78 han estat identificades per l'antivirus Trend Internet Security 15.0.1212 amb el patró de virus actualitzat a 1/12/18. L'antivirus ha identificat 69 de les mostres com Hajime, 8 com Mirai, i 1 com Gafgyt.
La resta de mostres es passen per VirusTotal i, combinat amb el resultat de l'antivíric Trend, s'han identificat els següents espècimens:

	Hajime	Mirai	Gafgyt	Svirtu	No Identificat
Nombre	69	11	1	37	12

De les 12 mostres no identificades, 5 són planes web, 1 és un fitxer de text que conté la cadena gAt9W}c, 1 segons el nom del fitxer és mirai i, en les altres 5, es va crear un binari amb la comanda echo, i les credencials per accedir van ser root:nas4free i root:f00b@r (en quatre ocasions). Dos de les mostres es van generar des de la mateixa ip, pel que pot ser que generi un payload diferent cada cop que infecta una víctima. Les comandes executades són iguals en els tres casos, pel que es pot deduir que les tres mostres pertanyen a la mateixa botnet.

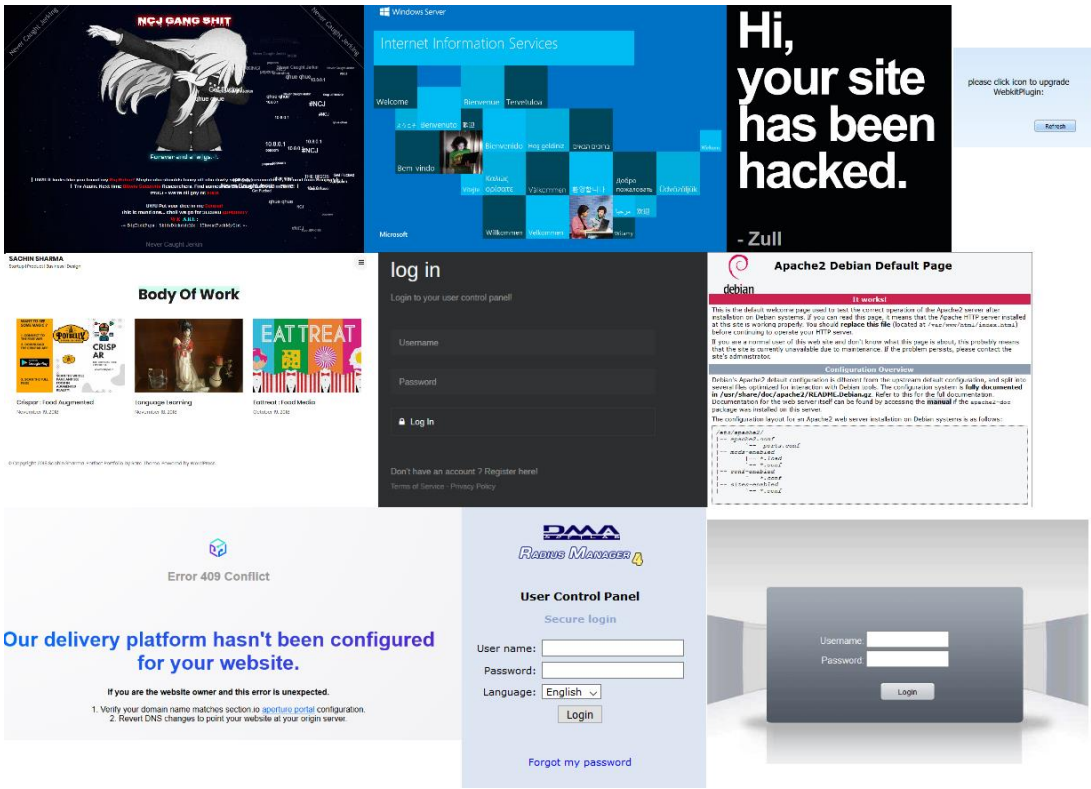
[27] https://www.bleepingcomputer.com/news/security/malware-author-uses-same-skype-id-to-run-iot-botnet-and-apply-for-jobs/



Il·lustració 48 Espècimens xarxa domèstica

9.1.5 Altres

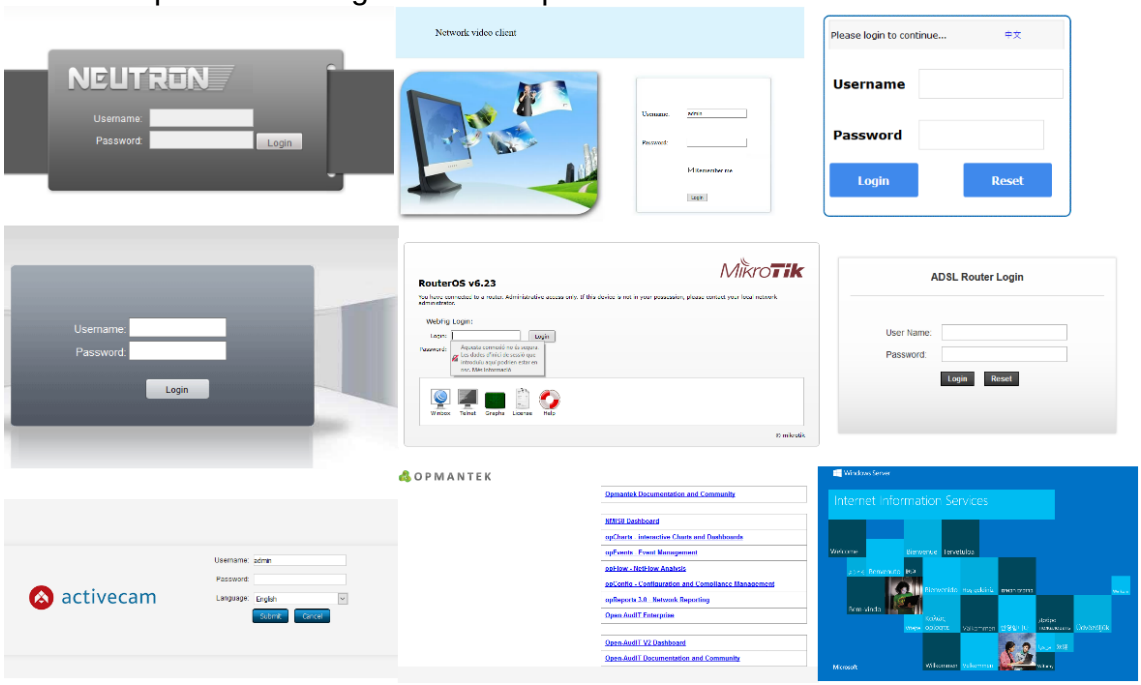
Algunes de les IP's que s'han connectat a la xarxa externa de la universitat tenen planes web (12), 139 tenen el port filtrat i 2 tancat. Una mostra de les planes web:



Il·lustració 49 Planes web a xarxa Universitat

Port	80	23	22	21
Obert	12	2	6	2
Filtrat	139	143	142	144
Tancat	2	9	5	7

A la xarxa domèstica hi ha 34 IP's amb el port 80 obert, 574 amb el port filtrat, i 15 amb el port tancat. Algunes de les planes web:

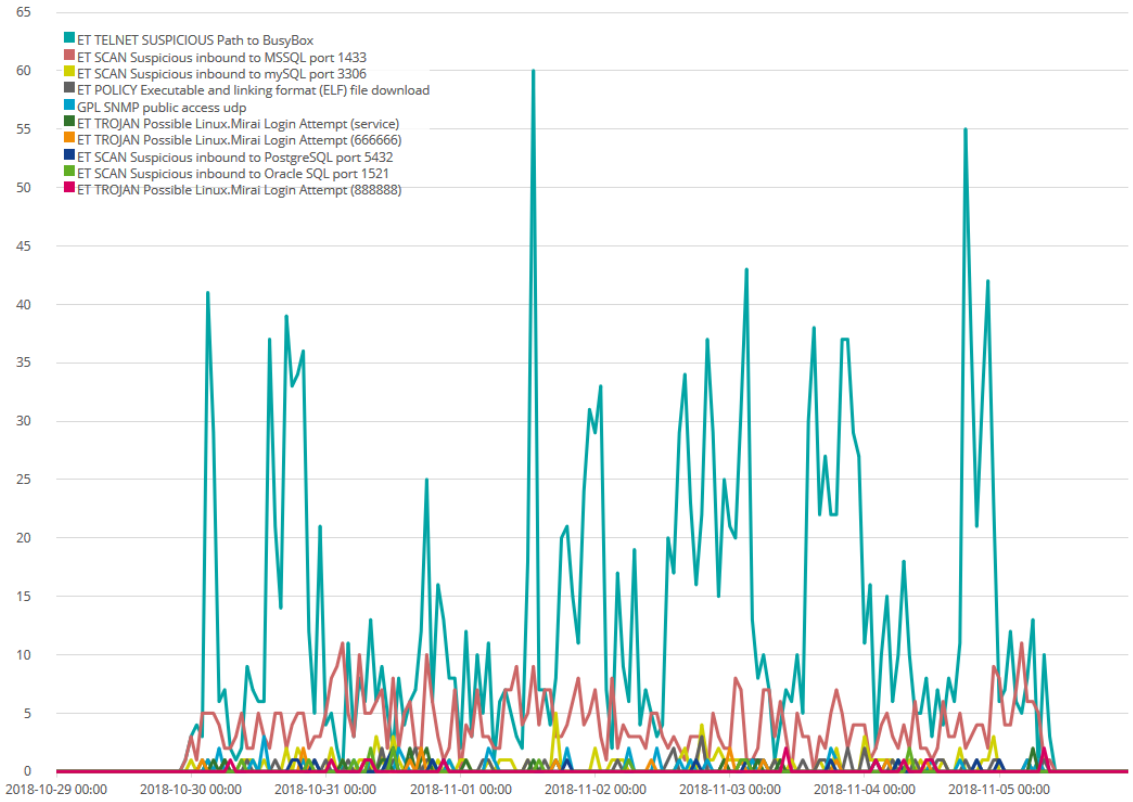


Il·lustració 50 Planes web a xarxa domèstica

Port	80	23	22	21
Obert	34	16	15	7
Filtrat	574	571	585	579
Tancat	15	36	23	37

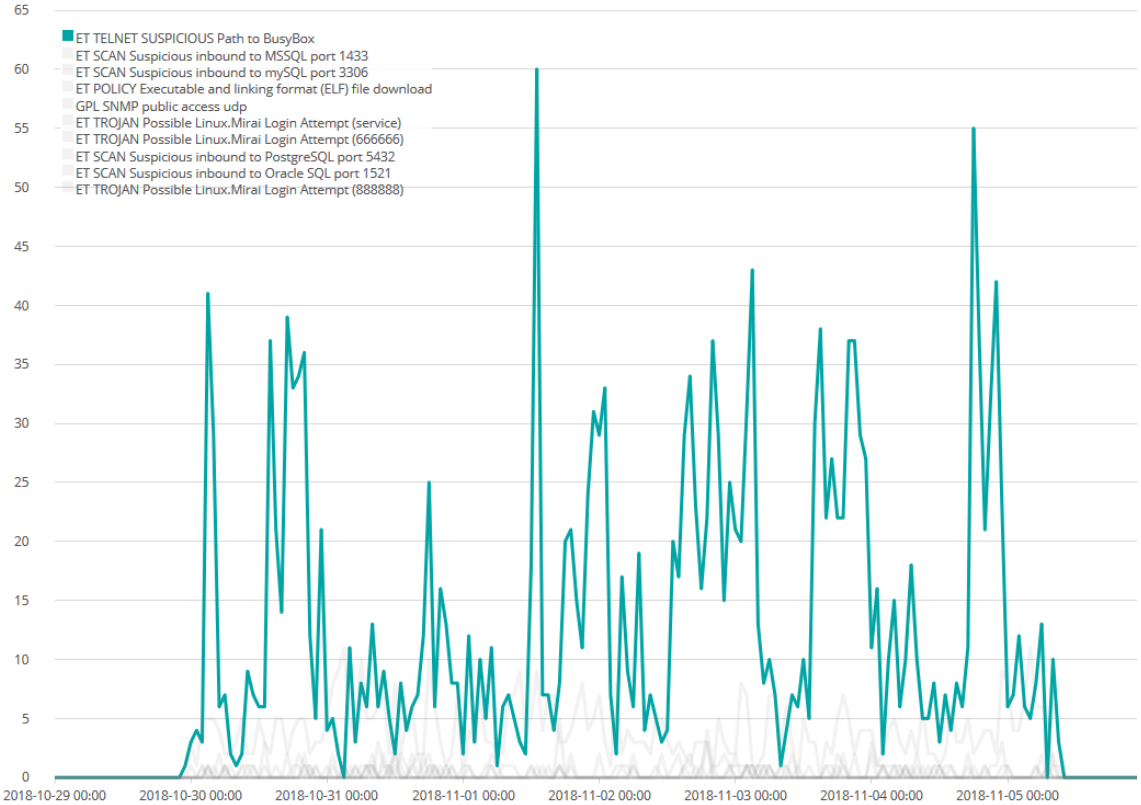
9.2 Suricata + ELKS a Honeypot Telnet

L'IDS Suricata ha generat 3315 alertes destinades al Honeypot Telnet de la xarxa externa de la universitat. No totes les alertes corresponen al servei de Telnet ofert. El sensor IDS ens permet veure la distribució i tipus dels atacs dirigits al Honeypot Telnet de la xarxa externa:



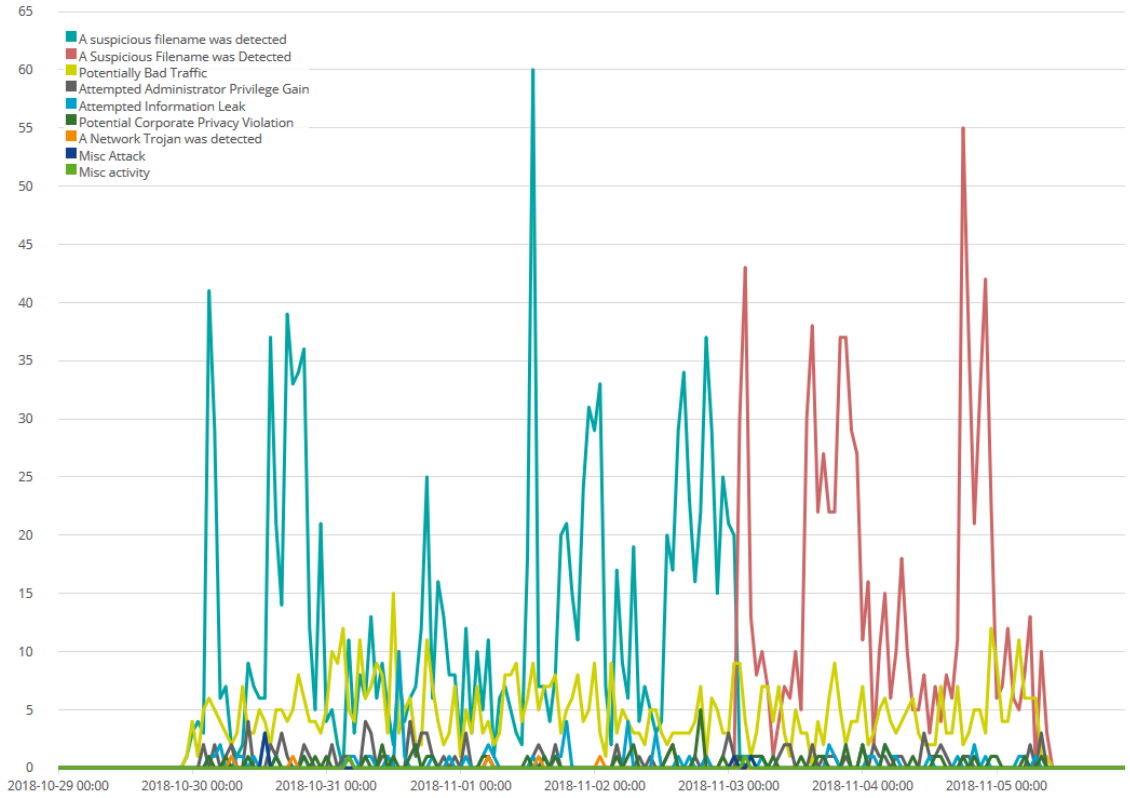
Il·lustració 51 Amenaces detectades per l'IDS

Filtrem les alertes cap al port 23 detectades per Suricata per veure la distribució dels accessos en el temps:



Il·lustració 52 Amenaces Telnet detectades per l'IDS

També es pot observar la distribució i el tipus d'alertes detectades:



Il·lustració 53 Tipus d'alertes detectades

Les 10 alertes amb destí al sensor Honeypot Telnet són:

ET TELNET SUSPICIOUS Path to BusyBox	2,183
ET SCAN Suspicious inbound to MSSQL port 1433	630
ET SCAN Suspicious inbound to mySQL port 3306	101
GPL SNMP public access udp	70
ET SCAN NMAP OS Detection Probe	56
ET POLICY Executable and linking format (ELF) file download	54
GPL SNMP private access udp	28
ET SCAN Suspicious inbound to PostgreSQL port 5432	27
ET TROJAN Possible Linux.Mirai Login Attempt (service)	20
ET TROJAN Possible Linux.Mirai Login Attempt (666666)	17

Il·lustració 54 Top ten d'alertes detectades

Es destacable el nombre d'intents d'accés a serveis que no s'estan servint, com MSSQL o MySQL.

9.3 t-pot

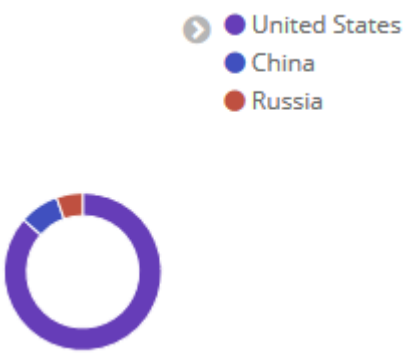
El honeypot t-pot disposa de diferents mòduls de honeypot.

9.3.1 Conpot

Conpot és un honeypot ICS/SCADA. Durant el període d'anàlisi, ha rebut 37 intents de connexió des de 5 adreces IP diferents, de tres països diferents, Estats Units, Xina i Rússia:

Source IP	CNT
71.6.146.185	28
107.170.213.78	3
125.64.94.200	3
185.156.177.144	2
196.52.43.101	1

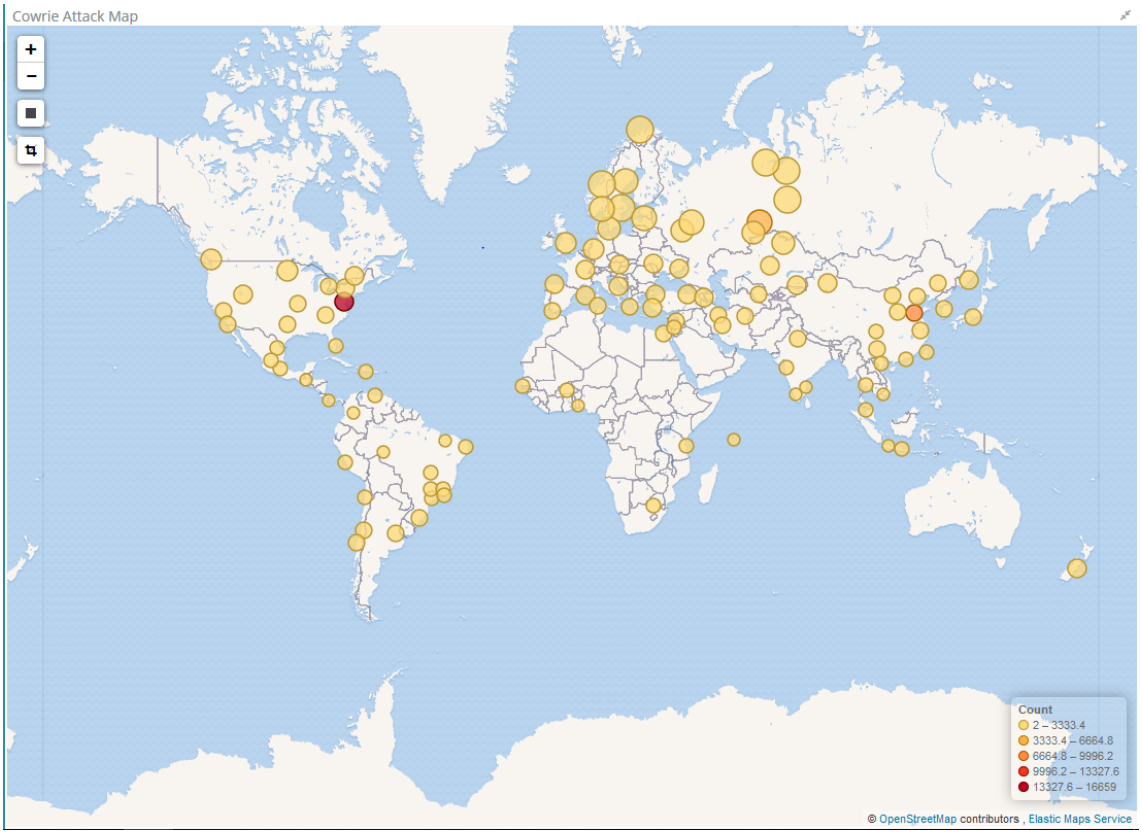
Il·lustració 55 Adreces IP Conpot



Il·lustració 56 Països Conpot

9.3.2 Cowrie

Cowrie és un honeypot Telnet/SSH/web. Durant el període de l'anàlisi s'han generat 69176 events des de molts països:



Il·lustració 57 Mapa d'atacs Cowrie

Per adreces IP d'origen, s'han de destacar les 16563 connexions d'es d'una sola adreça IP pertanyent a la xarxa d'Amazon i les 11479 connexions des del rang de Rostelcom amb exactament 637 connexions des de múltiples hosts:

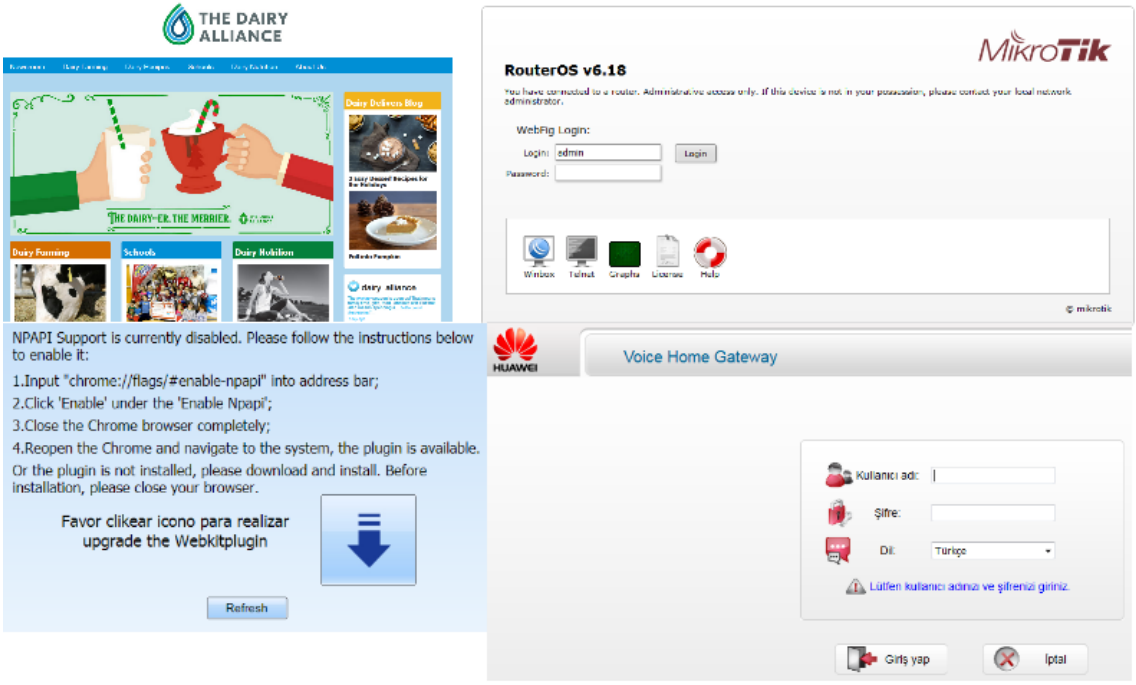
Source IP	CNT
34.228.113.27	16563
207.180.228.119	680
115.55.213.93	638
178.46.34.201	637
178.46.40.98	637
185.180.233.241	637
188.18.153.38	637
188.19.140.39	637
188.19.233.238	637
192.69.126.137	637

Il·lustració 58 Top ten d'adreces IP d'origen Cowrie

AS	ASN	CNT
14618	Amazon.com, Inc.	16563
12389	Rostelecom	11479
4837	CHINA UNICOM China169 Backbone	5201
4134	No.31,Jin-rong Street	2723
27699	TELEFÔNICA BRASIL S.A	2180
24444	Shandong Mobile Communication Company Limited	2055
9121	Turk Telekom	1193
3462	Data Communication Business Group	1102
4766	Korea Telecom	915
1267	Wind Telecomunicazioni SpA	830

Il·lustració 59 Top ten de proveïdors de xarxa origen dels atacs Cowrie

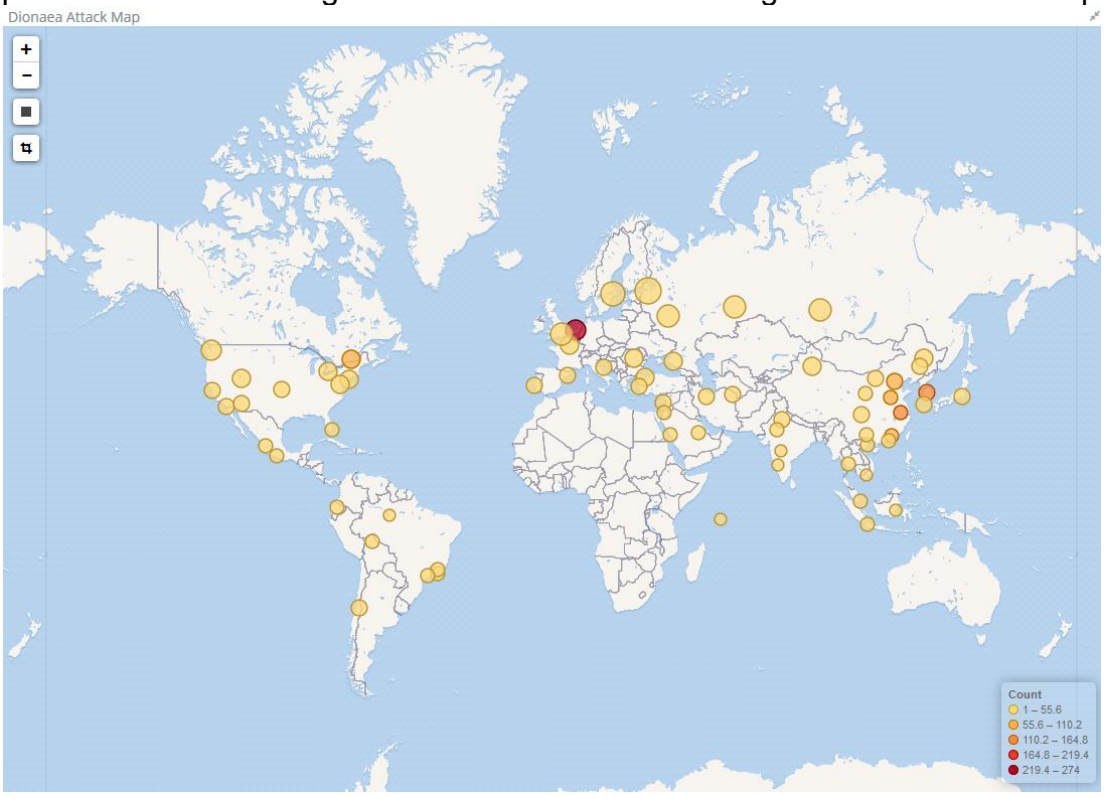
Provant amb a accedir amb el navegador a algunes de les IP's registrades, s'observa que entre els atacants hi ha càmeres, routers, servidors web, servidors vpx, etcètera:



Il·lustració 60 Plana web de dispositius compromesos que han atacat Cowrie

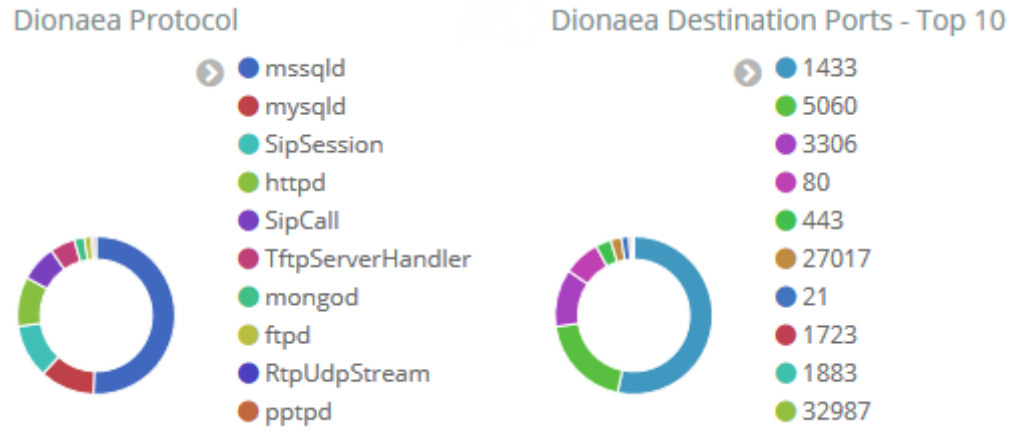
9.3.3 Dionaea

Dionaea és un honeypot que simula diversos serveis (ftp, web, tftp,...), durant el període de l'anàlisi ha generat 1357 events amb la següent distribució al mapa:



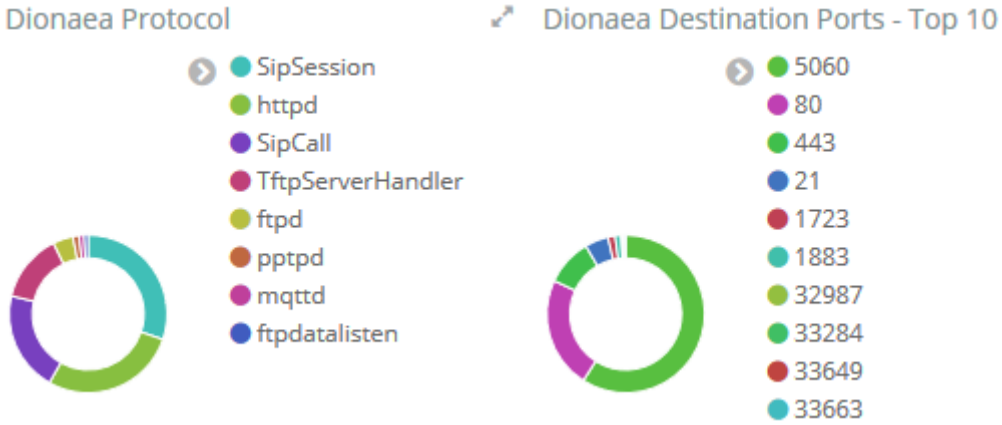
Il·lustració 61 Mapa d'atacs Dionaea

El tres serveis més atacats han estat MSSQL, sip, MySQL:



Il·lustració 62 Atacs capturats per Dionaea per protocol

Filtrant pels protocols que pot tenir un dispositiu IoT, la distribució dels atacs és la següent:



Il·lustració 63 Atacs a IoT capturats per Dionaea

Dionaea AS/N - Top 10

ASN	AS	CNT
4134	No.31,Jin-rong Street	227
199264	Estro Web Services Private Limited	180
4766	Korea Telecom	108
43350	NForce Entertainment B.V.	80
16276	OVH SAS	71
4837	CHINA UNICOM China169 Backbone	68
4808	China Unicom Beijing Province Network	59
63949	Linode, LLC	46
60781	LeaseWeb Netherlands B.V.	23
6939	Hurricane Electric LLC	17

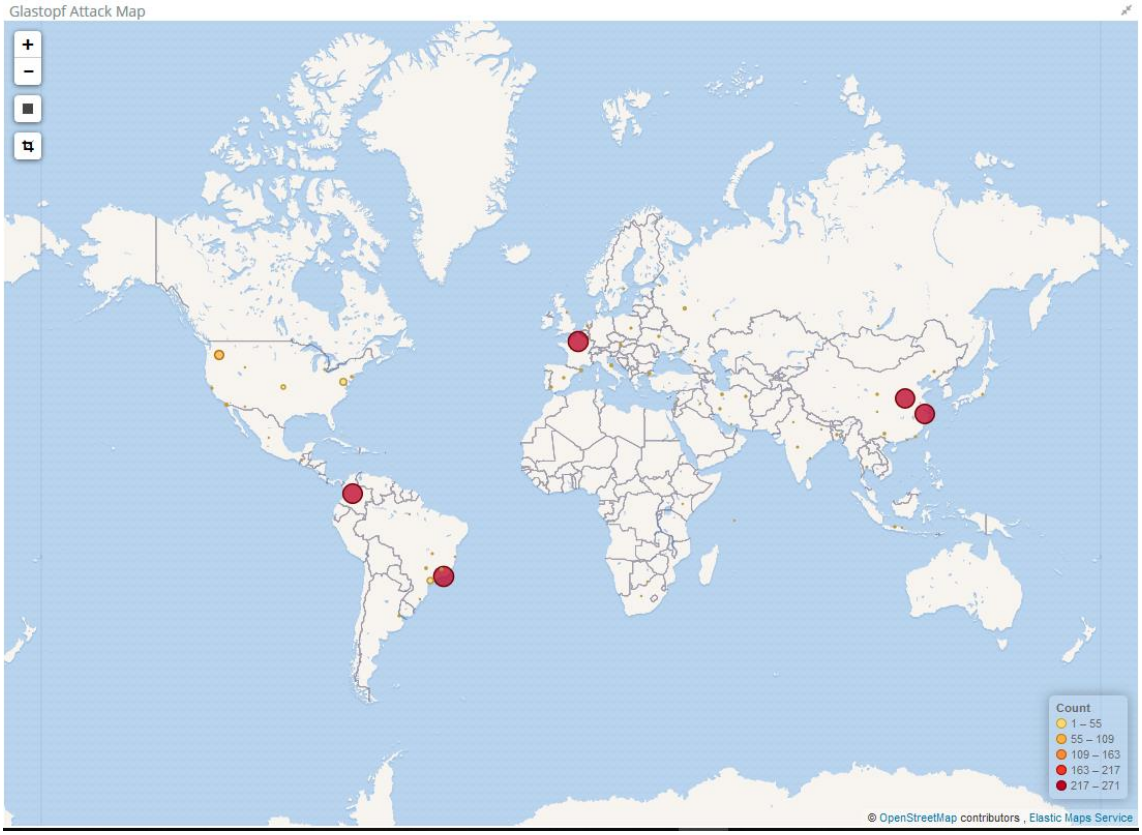
Dionaea Source IP - Top 10

Source IP	CNT
37.49.231.37	129
46.166.148.6	80
158.69.115.138	69
37.49.231.170	49
59.22.221.125	35
211.218.126.142	27
125.129.170.2	26
139.162.108.129	16
117.50.7.159	14
172.104.113.6	14

Il·lustració 64 Top ten per ASN i per IP Dionaea

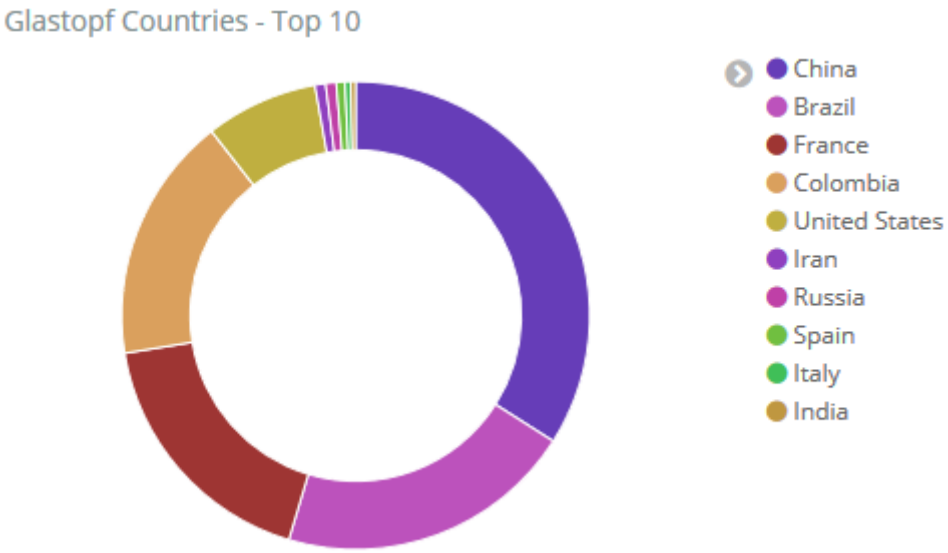
9.3.4 Glastopf

Glastopf és un honeypot d'aplicacions web. Durant el període de l'anàlisi, ha registrat 1553 events. La distribució dels atacs en el mapa és la següent:



Il·lustració 65 Mapa d'atacs Glastopf

Els atacs s'han generat majoritàriament, des de Xina, Brasil i França:



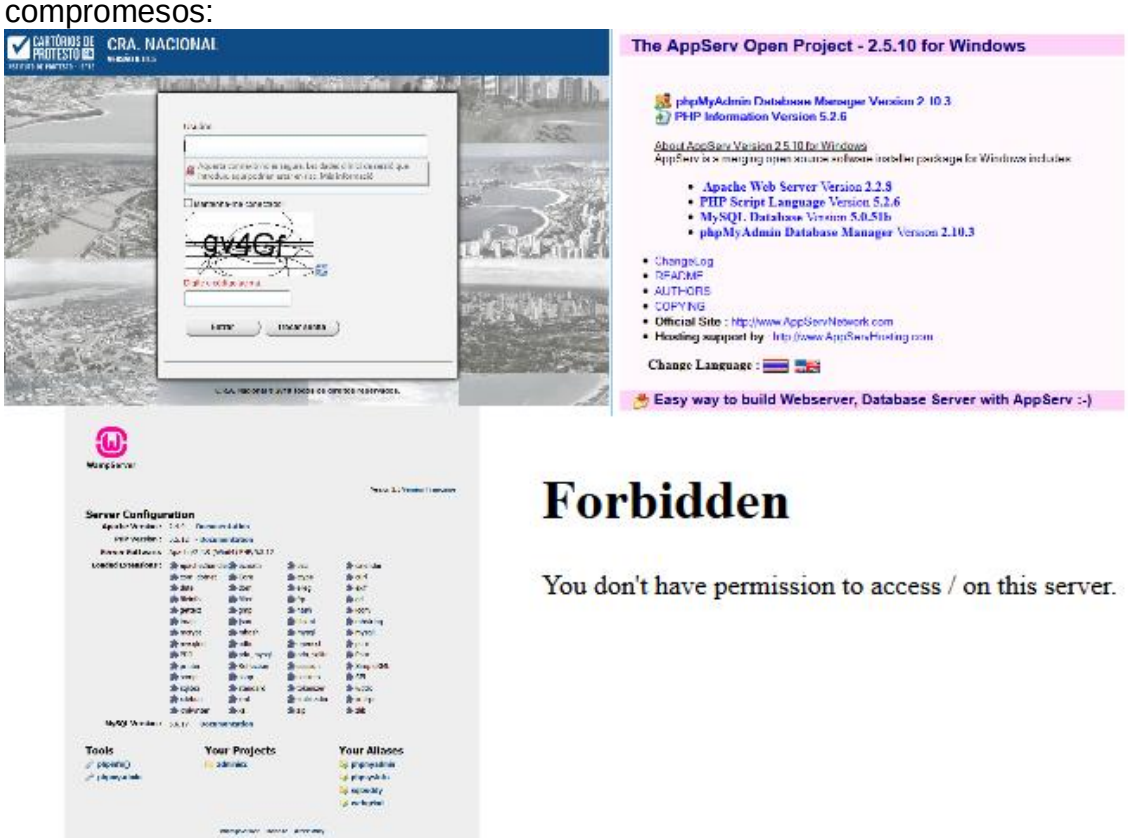
Il·lustració 66 Glastopf per Països

Aquestes són les IP's que han realitzat més connexions al honeypot Glastopf:

Source IP	CNT
200.155.8.34	266
62.210.203.16	266
186.113.253.51	256
123.56.229.74	245
116.255.154.114	244
54.172.118.182	7
18.206.159.236	6
34.214.188.65	6
34.217.59.241	6
34.220.40.173	6

Il·lustració 67 Atacs a Glastopf per IP

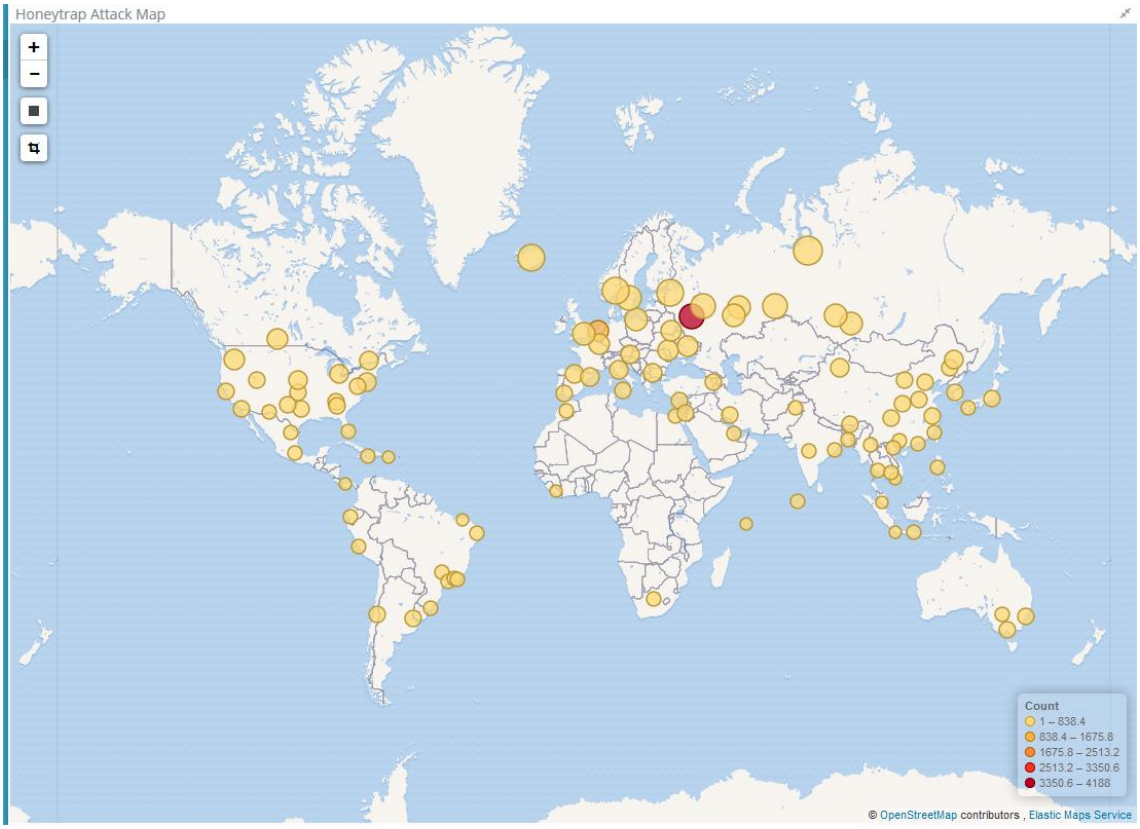
Algunes de les IP's tenen planes web, del que es desprèn que són servidors compromesos:



Il·lustració 68 Plana web de dispositius compromesos Glastopf

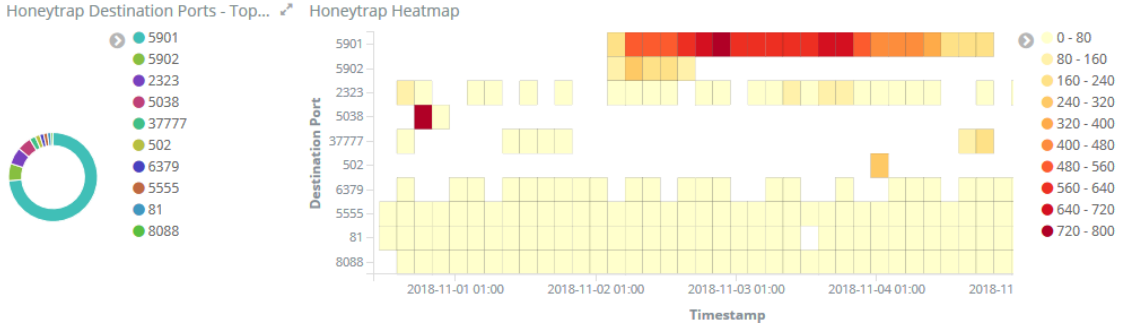
9.3.5 Honeytrap

Honeytrap és un honeypot que emula diferents serveis (VNC, Web,...). Durant el període de l'anàlisi, Honeytrap ha generat 27513 events, aquest ha estat el mapa dels atacs:



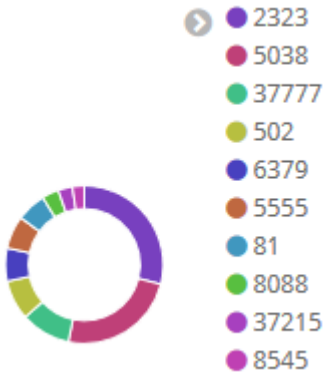
Il·lustració 69 Mapa d'atacs Honeytrap

Per ports es pot observar que la majoria dels atacs són al ports de VNC:



Il·lustració 70 Ports Honeytrap

Si filtrem els ports d'VNC ens queden els ports que podrien utilitzar un dispositiu IoT:



Il·lustració 71 Distribució d'atacs a ports IoT a Honeytrap

En la següent figura es mostren el top ten d'adreces IP que han accedit a Honeytrap i el top ten per ASN (autonomous system number):

AS	ASN	CNT	Source IP	CNT
57043	Hostkey B.v.	4232	185.156.177.144	2323
29073	Quasi Networks LTD.	1084	46.166.148.6	760
43350	NForce Entertainment B.V.	898	5.8.18.70	733
63949	Linode, LLC	756	185.156.177.81	634
50360	Tamatiya EOOD	585	185.156.177.131	485
12389	Rostelecom	551	185.143.223.239	416
14061	DigitalOcean, LLC	413	78.128.112.58	331
34300	JSC Internet-Cosmos	335	62.173.149.138	329
237	Merit Network Inc.	326	198.108.67.32	318
16276	OVH SAS	277	2.61.69.196	298

Il·lustració 72 top ten ASN i IP Honeytrap

10. Conclusions

Cada cop s'adquireixen més dispositius IoT tant en l'àmbit empresarial com al personal. En aquest escenari, conèixer l'estat de la seguretat en dispositius IoT és una competència necessària en pràcticament qualsevol xarxa
Amb aquest treball s'ha pretès mostrar quin és l'estat de la seguretat i a quins riscos i amenaces de seguretat s'enfronten els dispositiu IoT.
S'han definit mesures per reduir la superfície d'atac i millorar la seguretat d'aquests dispositius.

S'han vist quins usos poden fer els atacants, les definicions de l'estructura d'una botnet, i una història dels virus que tenen IoT com a objectiu.
S'ha definit un mètode per capturar i registrar els atacs que ha estat molt eficients, permetent recopilar tant els espècimens com la interacció de l'atacant amb el honeypot, i altres dades importants com la IP, la geolocalització o la duració de l'atac.

La captura i anàlisi dels atacs rebuts en dos tipus diferents de xarxes han permès tenir una visió de la quantitat d'atacs que es poden rebre en un curt període de temps i comprovar que no hi ha diferencies significatives en els tipus d'atacs rebuts, ni la seva metodologia. El nombre d'atacs, tot i que són automatitzats, és molt nombrós, el que certifica que s'ha de tenir molt en compte protegir aquests dispositius, especialment canviant les paraules de pas per defecte, ja que la major part dels atacs utilitzen les credencials per defecte.

La planificació indicada s'ha seguit rigorosament i ha estat adequada per assolir els objectius plantejats a l'inici d'aquest treball. No ha estat necessari introduir cap canvi ni mitigació contemplats en l'anàlisi de riscos.

11. Glossari

Bot: Un bot (Abreviatura de robot) és un programa informàtic que efectua automàticament tasques repetitives a través d'internet.
Botnet: Xarxa de d'ordinadors connectats a internet que poden ser controlats remotament de manera involuntària per realitzar tasques sense l'autorització del propietari i sense que aquest se n'adoni.
IoT: Internet of Things, la Internet de les coses es refereix, en termes d'informàtica, a una xarxa d'objectes de la vida quotidiana interconnectats.
Malware: Programari nociu dissenyat per inserir virus, cucs, troians, programari espia o fins i tot bots.

12. Bibliografia

- What Bots Do and How They Work | The Honeynet Project: http://www.honeynet.org/node/54 18/09/2018
- Uses of botnets | The Honeynet Project http://www.honeynet.org/node/52 18/09/2018
- Know your Enemy: Tracking Botnets | The Honeynet Project: http://www.honeynet.org/papers/bots 18/09/2018
- Honeypot Telnet https://github.com/Phype/telnet-iot-honeypot 23/10/2018
- 24 horas en la vida de mi router domestico: https://www.fwhibbit.es/24-horas-en-la-vida-de-mi-router-domestico 23/10/2018
- Mirai: https://securityaffairs.co/wordpress/52015/hacking/mirai-botnet.html 23/10/2018
- Routers MikroTik hackeados para reenviar tu trafico de red a ciberdelincuentes: https://www.redeszone.net/2018/09/04/miles-routers-mikrotik-hackeados-reenviar-trafico-red-ciberdelincuentes/ 23/10/2018
- T-Pot 18.11: https://hub.docker.com/r/dtagdevsec/kibana/ 30/11/2018
- Cripotminat IoT: https://securityintelligence.com/xmrig-father-zeus-of-cryptocurrency-mining-malware/ 25/11/2018
- Internet de les coses: https://ca.wikipedia.org/wiki/Internet_de_les_coses 23/09/2018
- Bot: https://ca.wikipedia.org/wiki/Bot_(Internet)
- Botnet: https://ca.wikipedia.org/wiki/Botnet 17/10/2018
- Botnet: https://en.wikipedia.org/wiki/Botnet 17/10/2018
- Botnets IoT: https://blog.radware.com/uncategorized/2018/03/history-of-iot-botnets/ 17/10/2018
- Hajime: https://www.pcworld.com/article/3190182/security/iot-malware-clashes-in-a-botnet-territory-battle.html 23/10/2018
- Honeypot: https://en.wikipedia.org/wiki/Honeypot_(computing) 23/10/2018
- IDS: https://en.wikipedia.org/wiki/Intrusion_detection_system 23/10/2018
- Malware per IoT: https://hakin9.org/the-history-and-evolution-of-malware/ 23/10/2018
- Malware per IoT: https://www.hindawi.com/journals/scn/2018/7178164/ 23/10/2018
- Malware, definició: https://ca.wikipedia.org/wiki/Programari_malici%C3%B3s 23/10/2018
- Passwords per defecte: https://www.grahamcluley.com/mirai-botnet-password/ 23/10/2018