



Tu información vale mucho: Cuídate, cuídanos!

Julio César Balderrama

Twitter **@juliobalderrama**

Profile: www.linkedin.com/in/juliocesarbalderrama

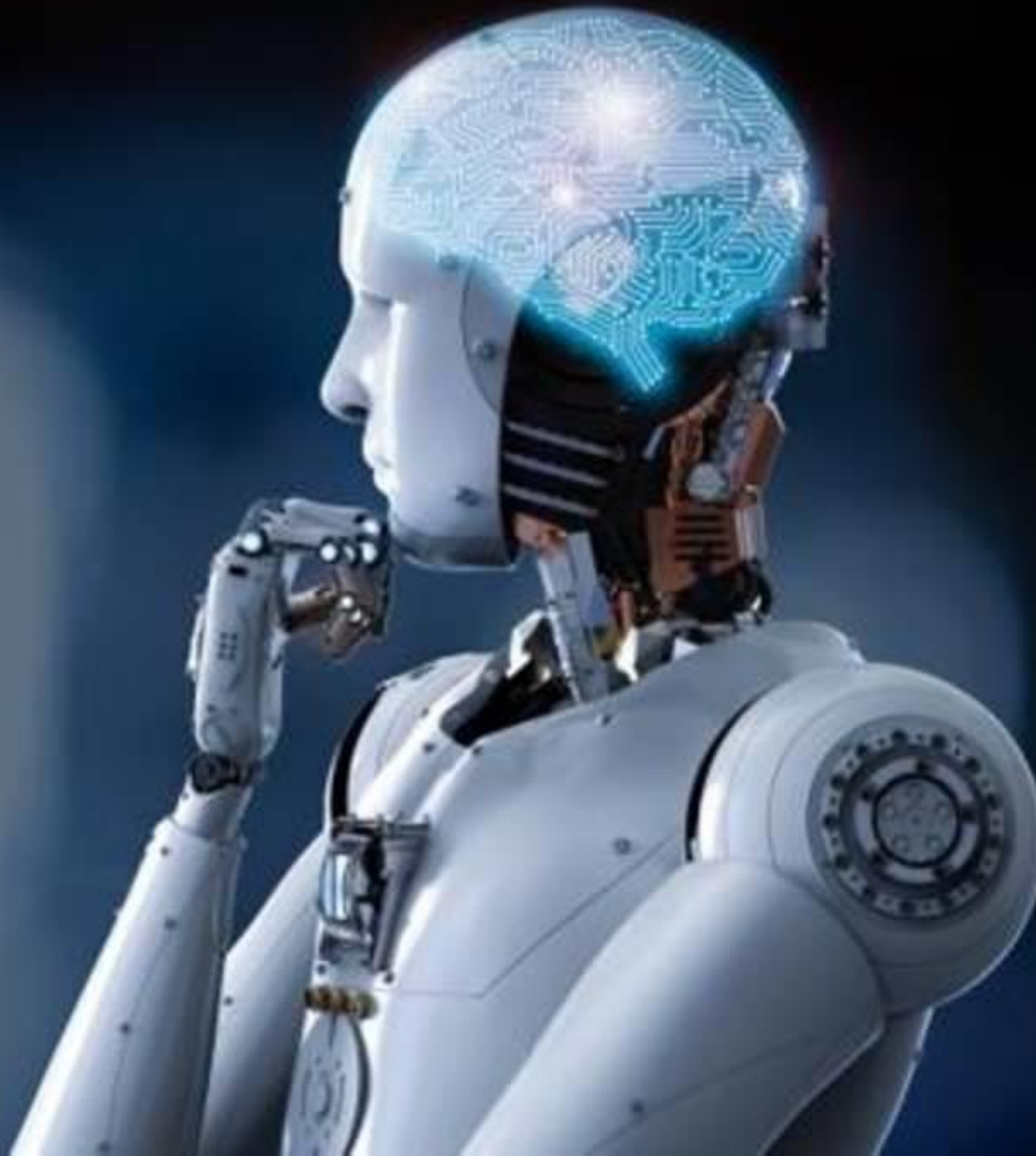
Las opiniones expresadas en esta presentación no reflejan necesariamente los puntos de vista de la Fuerza Aérea Argentina o de otros organismos del Estado.

Julio Cesar Balderrama

 @juliobalderrama

<https://www.linkedin.com/in/juliocesarbalderrama/>

**¿Cualquier
dispositivo
puede ser
hackeado?**





¡Termómetro de sueño!

Algunas preguntas¿?

A hand is holding a smartphone in the center of the frame. The phone's screen shows a street scene with yellow taxis and buildings. The background is a blurred city street with people walking. The text 'Quien NO utiliza un SmartPhone?' is overlaid in white, with 'NO' underlined.

Quien NO
utiliza un
SmartPhone?



**Utilizan una
clave en el
smartphone?**



A hand is holding a smartphone. The screen is red and displays a yellow warning sign with a black exclamation mark. Below the sign, the words "VIRUS DETECTED" are visible in white, though partially obscured by the text overlay. The background is a plain, light-colored surface.

**Quien posee
un programa
Antivirus en el
smartphone?**

A close-up photograph of a person's hands holding a smartphone. The background is a blurred city street at night, with warm, out-of-focus lights creating a bokeh effect. The word "Smartphone" is overlaid in large, white, bold, sans-serif font across the center of the image. A thin white vertical line is positioned to the left of the text.

Smartphone

Algunas señales que indica que tu teléfono móvil podría estar poseído (hackeado)

- Funciona más lento
- Sobrecalentamiento
- La batería se agota antes de lo previsto
- Recibes y envías mensajes desconocidos
- Ventanas emergentes
- Compras y apps sospechosas
- Apariencia extraña y ruido de fondo
- Se apagan o activan funciones
- Encontramos procesos que **no** iniciamos
- El teclado escribe caracteres que **no** solicitamos
- Se abren Apps que **no** solicitamos

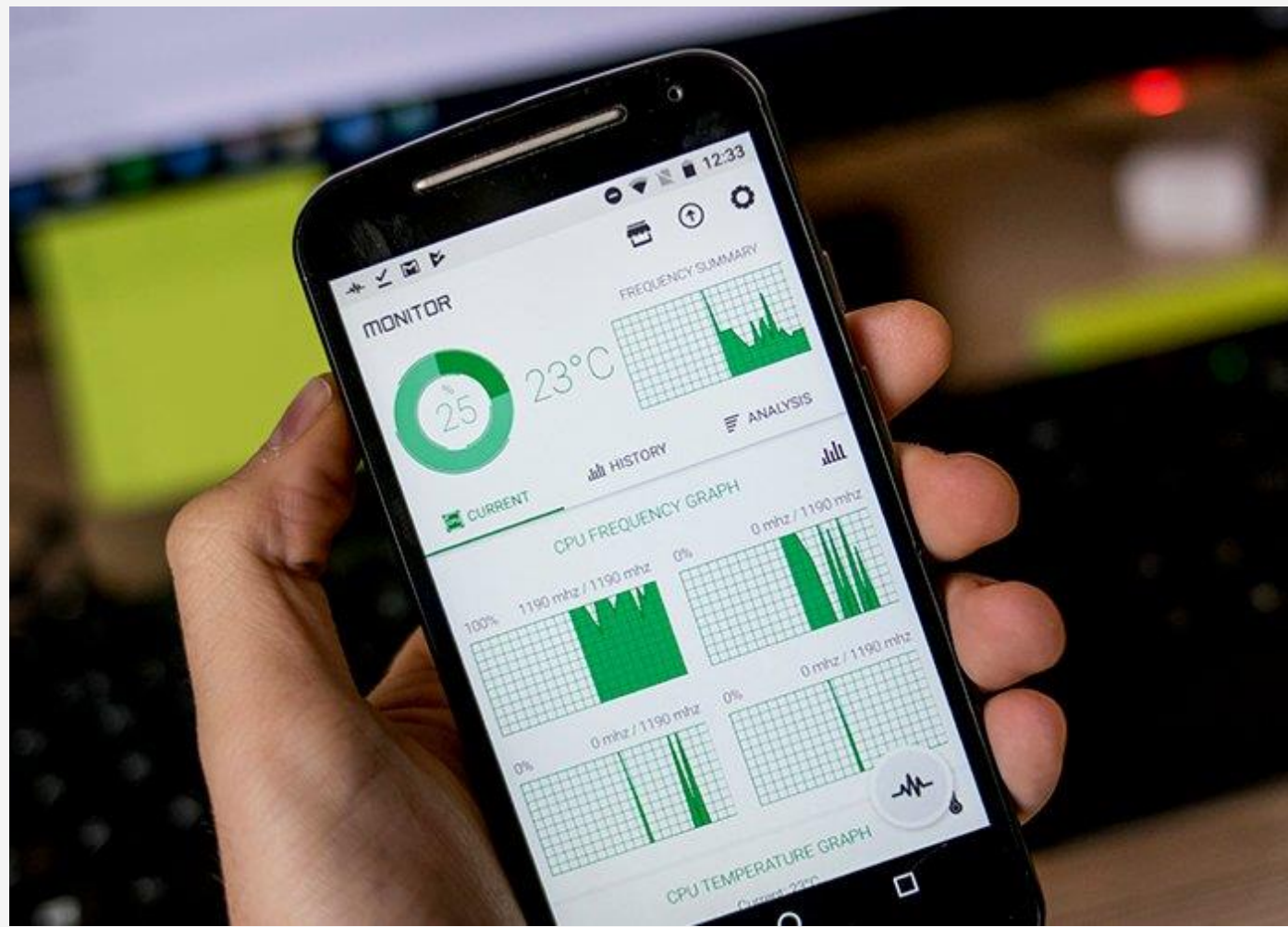


La botnet **Hide and Seek** empezado a secuestrar todo tipo de dispositivos Android **explotando el puerto ADB** (Android Debug Bridge) utilizado por los desarrolladores para programar y depurar las aplicaciones.



<https://www.shodan.io/search?query=port%3A5555>

Algunas recomendaciones




Códigos más útiles

- *#321# verificar si tus llamadas, mensajes u otros datos están siendo desviados
- *#62# averiguar a donde se redirigen las llamadas, los mensajes, los datos ...
- ##002# Código universal para deshabilitar todas las redirecciones ...(antes de roaming)
- *#21# verificar si la conectividad esta siendo desviada y los servicios desviados
- *#06# Cuales tu IMEI

Recuerda: tu smartphone contiene mucha ... información sensible ... cuídala

1. Utiliza clave “difícil” para el bloqueo
2. Encriptar el dispositivo y memorias
3. Utiliza un antivirus
4. Desinstalar aplicaciones sospechosas
5. No instalar aplicaciones de orígenes desconocidos
6. Anti Clic “pop-ups”
7. Mantener siempre actualizado
8. Verificar las facturas de consumo de datos
9. Anota el IMEI
<https://www.enacom.gob.ar/imei>
10. Si te lo robaron denunciá!

A close-up photograph of a dog's face, likely a golden retriever, with two black camera lenses overlaid on its eyes. The text "Cámaras IP - DVR" is written in white, bold, sans-serif font across the center of the image. A vertical white line is positioned to the left of the text.

Cámaras IP - DVR

Múltiples vulnerabilidades en cámaras IP - DVR

Mapa de cámaras Hikvision Hackeadas
<https://ipvm.com/reports/hik-hack-map>



"App-webs" "200 OK"

Al 17/10/2018

TOTAL RESULTS

709,413

TOP COUNTRIES



China	427,136
United States	29,422
Viet Nam	27,676
Russian Federation	19,303
India	15,168



Nuevas amenazas (botnet)

- Sora (variante de Mirai)
- Torii
- IoT_reaper
- Persirai

Algunas recomendaciones

- Utilizar marcas conocidas y que tengan garantía y soporte
- Cambiar la contraseña predeterminada de la cámara DVR o IP
- Cambiar los puertos por defecto
- Actualizar el firmware cuando hay nuevas versiones
- Separar la red wifi de la cámara
- Utilizar funciones adicionales de red
- Utilizar encriptación entre DVD o cámara y dispositivo remoto
- NO conectar directamente a internet, proteja con un firewall
- Si no conoce, contacte a un amigo cibernético para orientación sobre seguridad en la red





¡Cuidado! Aunque no lo creas pueden hackear tu Smart TV



Heladeras, Lavarropas, Cafetera, ...



Consolas de juego



```
Got packet from 50 0A 88 64
Packet type: Entry sensor closed
Data: 08 8C

Got packet from 50 0A 88 64
Packet type: Entry sensor closed
Data: 08 8C

Got packet from 50 0A 88 64
Packet type: Entry sensor opened
Data: 20 AC

Got packet from 50 0A 88 64
Packet type: Entry sensor opened
Data: 20 AC

Got packet from 50 0A 88 64
Packet type: Entry sensor opened
Data: 20 AC

Got packet from 50 A2 84 A8
Packet type: Enter menu

Got packet from 50 A2 84 A8
Packet type: PIN code
PIN bytes: 55 57
Mystery bits: 100
```

¿Es posible hackear y desactivar nuestra alarma de casa?



Intercepting network packages

80.0%

Mobile Console

```
Read 179 packets (got 12 ARP requests and 66 ACKs), sent 76
Read 181 packets (got 12 ARP requests and 68 ACKs), sent 79
Read 195 packets (got 12 ARP requests and 70 ACKs), sent 83
Read 204 packets (got 12 ARP requests and 71 ACKs), sent 88
Read 216 packets (got 12 ARP requests and 73 ACKs), sent 90
Read 218 packets (got 12 ARP requests and 74 ACKs), sent 96
Read 229 packets (got 12 ARP requests and 79 ACKs), sent 100
Read 241 packets (got 12 ARP requests and 84 ACKs), sent 104
Read 244 packets (got 12 ARP requests and 85 ACKs), sent 107
Read 247 packets (got 12 ARP requests and 88 ACKs), sent 110
Read 254 packets (got 12 ARP requests and 90 ACKs), sent 113
Read 267 packets (got 12 ARP requests and 91 ACKs), sent 116
Read 279 packets (got 12 ARP requests and 96 ACKs), sent 120
Read 280 packets (got 12 ARP requests and 98 ACKs), sent 123
Read 281 packets (got 12 ARP requests and 100 ACKs), sent 126
Read 292 packets (got 12 ARP requests and 105 ACKs), sent 130
Read 300 packets (got 12 ARP requests and 106 ACKs), sent 133
Read 307 packets (got 12 ARP requests and 107 ACKs), sent 136
Read 321 packets (got 12 ARP requests and 111 ACKs), sent 140
Read 325 packets (got 12 ARP requests and 116 ACKs), sent 144
Read 328 packets (got 12 ARP requests and 117 ACKs), sent 147
```

Cancel

- tings ---
- ontrol
- ontrol
- ng
- inding
- IS
- ls
- tings
- c
- Upgrade
- defaults
- Restore
- d
- og

Password

Old User Name:

Old Password:

New User Name:

New Password:

Confirm New Password:

aircrack-ng : airodump-ng

Bookmarks Settings Help

apsed: 49 mins | 2013-08-28 11:07

	PWR	Beacons	#Data	#/s	CH	MB
C4:A8:E9	-1	26351	1	0	148	-1
:97:4F:48	-29	875	149	130	9	54e
B:74:22:76	-57	5653	0	0	6	54e
6C:D0:88:02	-62	937	65	0	11	54e
38:74:22:77	-62	2378	25	0	6	54
:28:26:81:58	-65	979	0	0	6	54
A:78:68:73:5C	-67	1985				
00:00:00:00:00:00	-70					

STATION

SSID	MAC	PWR	Rate
(not associated)	00:1E:8F:8D:18:25	-18	0 - 1
(not associated)	C0:9F:42:00:03:22	-71	0 - 1
(not associated)	D8:A2:5E:67:64:88	-72	0 - 1
(not associated)	38:AA:3C:79:7D:83	-73	0 - 1
(not associated)	0C:77:1A:83:1C:DF	-66	0 - 1
(not associated)	7C:C5:37:FB:41:7A	-68	0 - 1
(not associated)	E4:CE:8F:66:57:F2	-67	0 - 1
00:21:29:C4:A8:E9	44:6D:57:C8:5B:A0	-12	54e-5

ng : airodump-ng

WiFi inseguras



Asistentes virtuales para el hogar inteligente ¿estamos seguros?

17 de octubre de 2018 - Jornada de Concientización en Ciberseguridad - *Fuerza Aérea Argentina*

Principales amenazas asociadas en los asistentes virtuales



- Manejo de los asistentes por parte de ciberdelincuentes
- Robos y compras
- Hurto de datos sensibles
- Dophin Attacks
- Malware futuro

Los problemas de seguridad en IoT no lo arregla un antivirus





El hackeo de aires acondicionados provoca el apagón de toda una manzana


<https://t.co/CCx9eQEbL2>

A nighttime photograph of a city street. The scene is illuminated by streetlights, creating a bokeh effect in the background. Light trails from moving vehicles are visible on the road. On the right side, there is a modern bus stop with a glass and metal structure. The overall atmosphere is dark and urban.

Sensores de luz en el hogar y en la ciudad

**400 mil
pacientes
actualizaron su
marcapasos!**





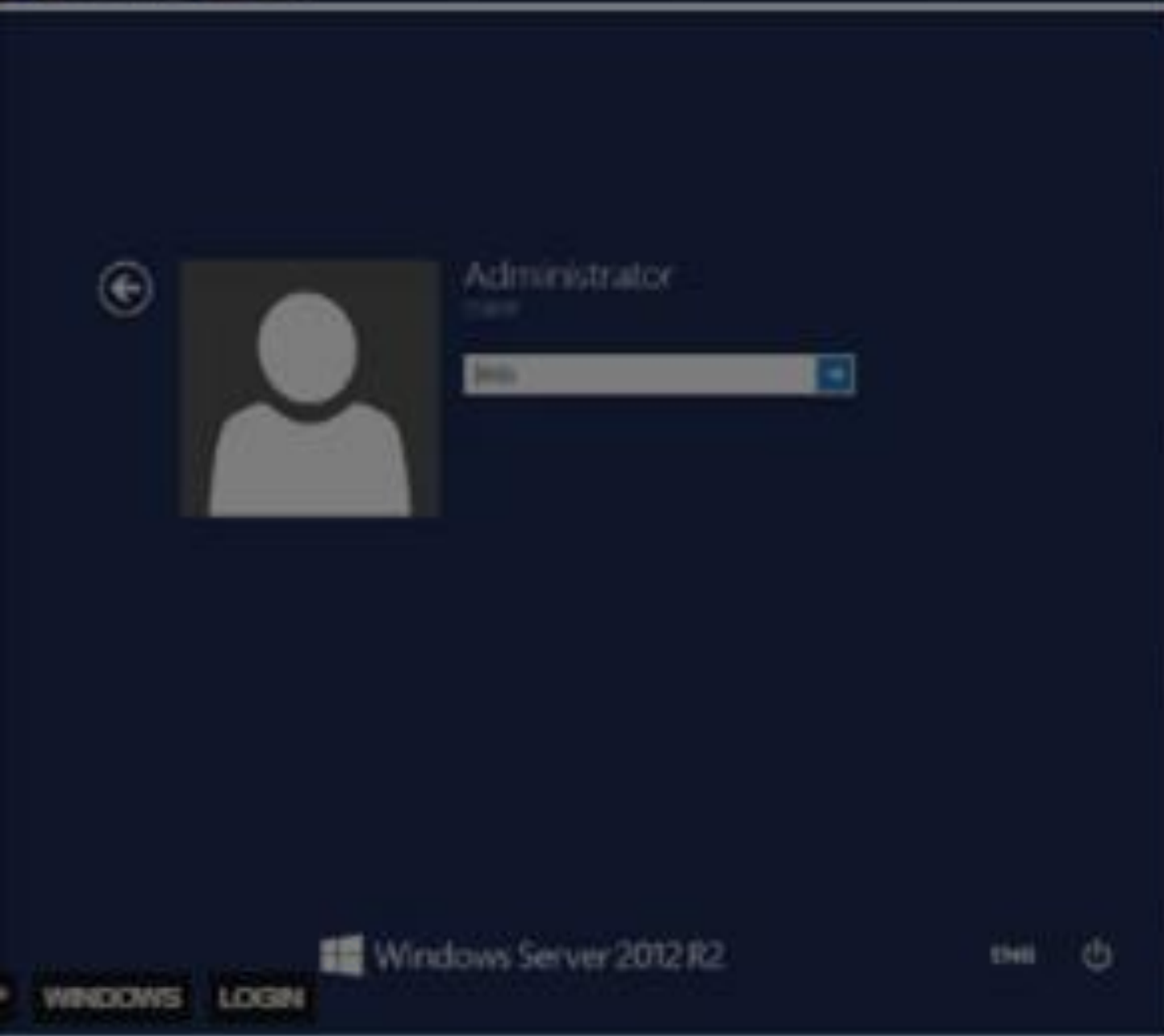
**Otra vez las
bombas de
Insulina ☹️**



**Hoteles Hackeados
– Secuestro del
sistema de tarjetas**



Demos



TOTAL RESULTS

13,265

TOP COUNTRIES



Argentina 13,265

TOP CITIES

Buenos Aires	1,440
Cordoba	872
Villa Angelica	734
Galvez	698
Tucuman	612

TOP ORGANIZATIONS

Telecom Argentina S.A. 4,600

181.110.71.80

host80.181-110-71.telecom.net.ar
Telecom Argentina S.A.
Added on 2018-10-17 10:37:14 GMT

Argentina

Details

SMB Status
Authentication: enabled
SMB Version: 2
Capabilities: raw-mode

90.57.239.89

reco.b...
ndov...
... S.A.

Argentina

Details

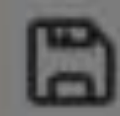
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,loc
itex,unix,extended-security

Shares

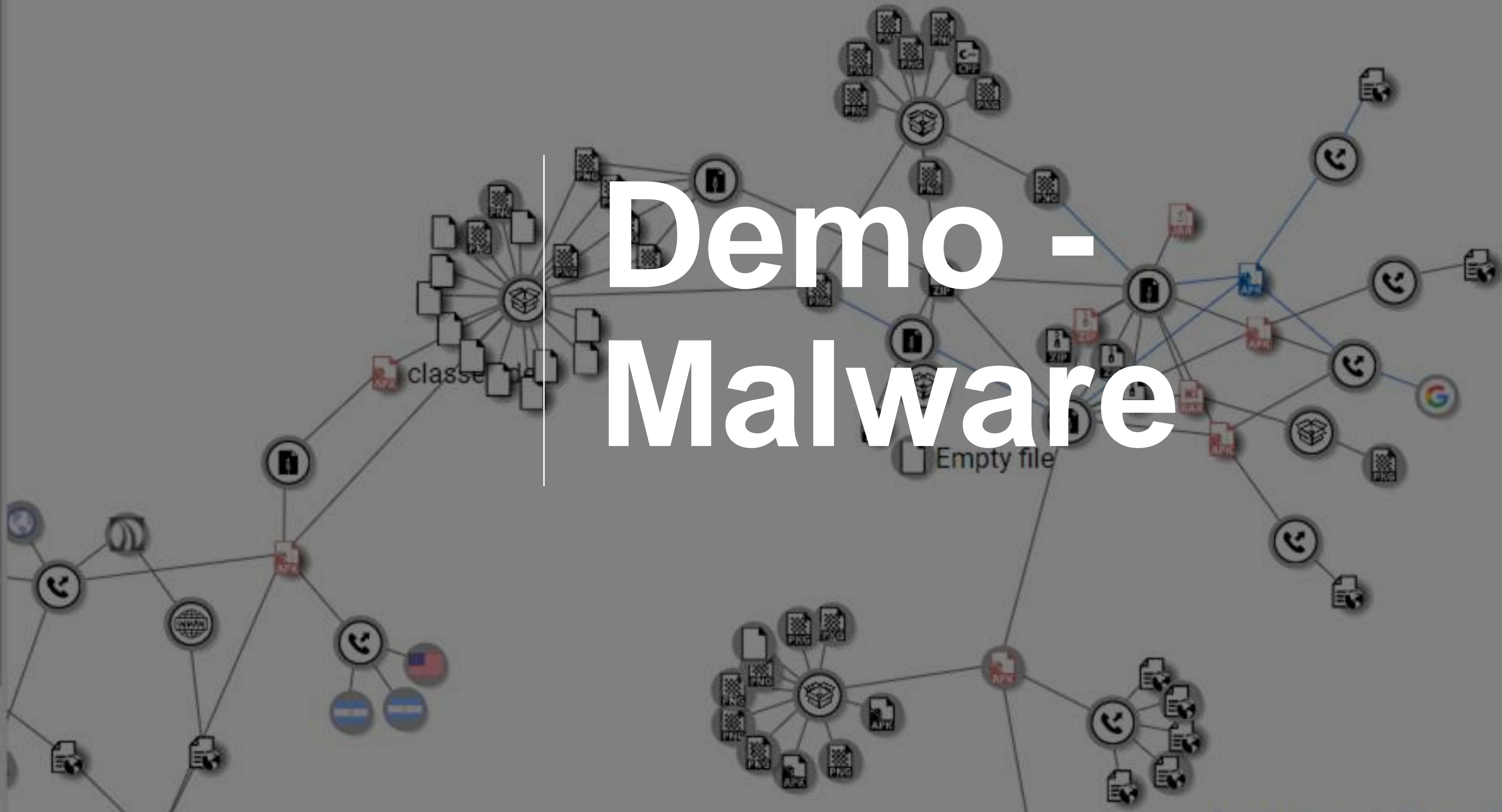
Name	Type	Comments
------	------	----------

print\$	Dirk	Printon Drivers
---------	------	-----------------

Demos



Untitled Graph



Demo - Malware

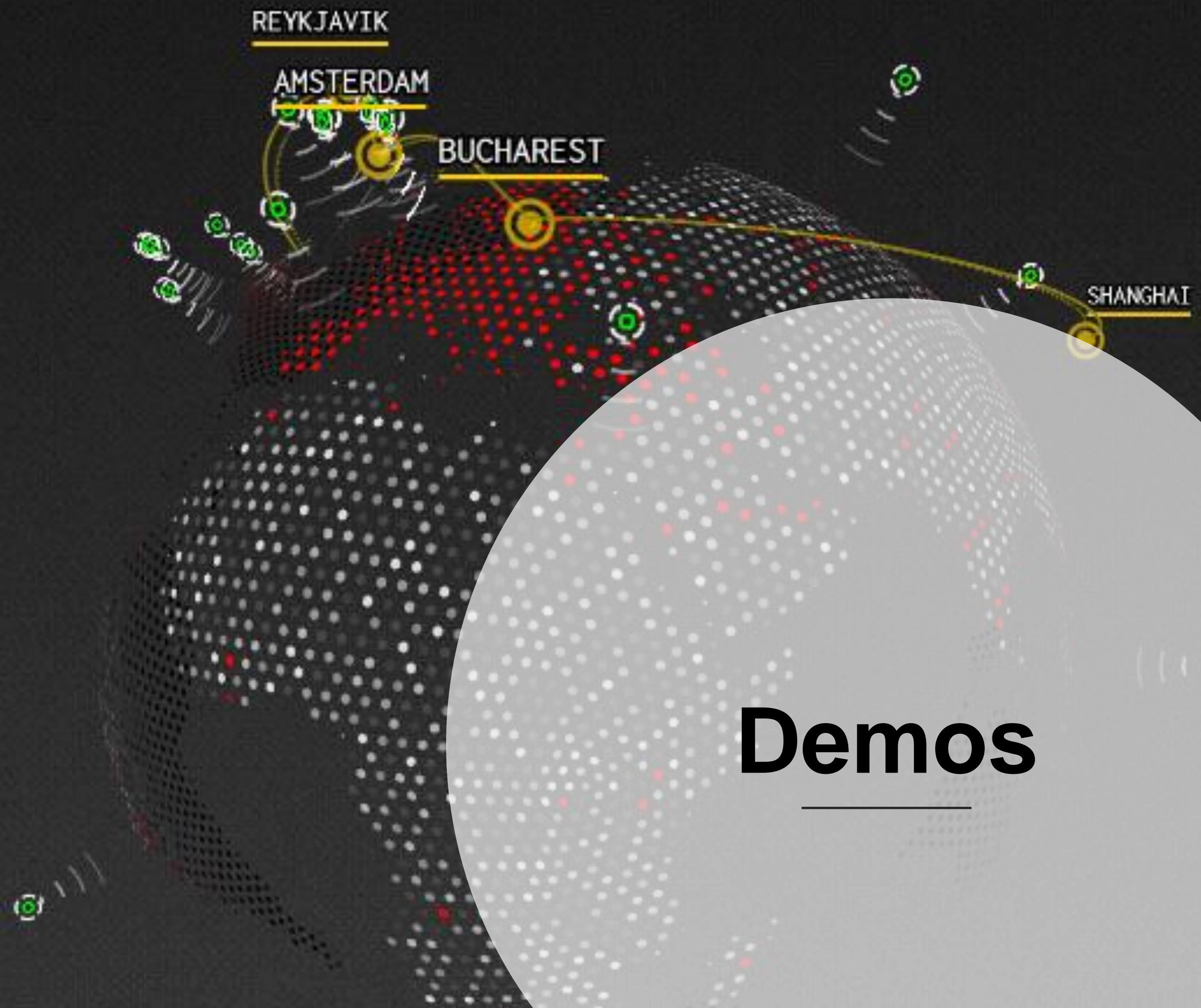


Host Report



Raw Data

location.country.raw	Hosts	
Argentina	1,785,654	100.0
Total	1,785,654	100.0



Protocols

BACnet: 10,530

DNP3: 588

EtherNet/IP: 3,943

Modbus: 13,949

Niagara Fox: 23,294

Niagara Fox with SSL: 159

Siemens S7: 2,701

About

The Shodan search engine has started to crawl the Internet for protocols that provide raw, direct access to industrial control systems (ICS). This visualization shows the location of these industrial control systems on the Internet as well as other related data.

Demos

Demo – Base de datos

SHODAN search results for `product:MySQL country:AR`. The interface shows a search bar with the query, navigation tabs (Exploits, Maps, Share Search, Download Results, Create Report), and a summary of 13,949 total results. A world map highlights Argentina. The results are categorized by top countries (Argentina: 13,949), top cities (Buenos Aires: 1,587, Villa Angelica: 1,155, Rosario: 1,153, Jose: 482, Tigre: 365), and top organizations (NSS S.A.: 1,179, Cablevision Argentina: 1,172, Dattatec.com: 1,045, Telecom Argentina S.A.: 992). Three specific IP addresses are listed with details:

- 200.68.105.83**: smtp83.allytech.com, Allytech S.A., Added on 2018-10-21 20:43:14 GMT, Argentina. Details: database.
- 190.105.164.35**: webs.poop.com.ar, Pccp S.A., Added on 2018-10-21 20:41:29 GMT, Argentina, Buenos Aires. Details: database.
- 170.231.206.153**: Miguel Araya(Servicios Rosario), Added on 2018-10-21 20:40:33 GMT, Argentina, Villa Angelica. Details: database.

SHODAN search results for `port:5432 PostgreSQL country:AR`. The interface shows a search bar with the query, navigation tabs (Exploits, Maps, Share Search, Download Results, Create Report), and a summary of 1,619 total results. A world map highlights Argentina. The results are categorized by top cities (Buenos Aires: 391, Rosario: 91, Villa Angelica: 73, Mar Del Plata: 33, Cordoba: 28) and top organizations (NSS S.A.: 212, Cablevision Argentina: 185, Telecom Argentina S.A.: 183, Ifx Networks Colombia: 143). Three specific IP addresses are listed with details:

- 190.136.176.111**: host111.190-136-176.telecom.net.ar, Telecom Internet, Added on 2018-10-21 20:46:40 GMT, Argentina. Details: database. PostgreSQL fe_sendauth: no password supplied.
- 181.90.120.196**: host196.181-90-120.telecom.net.ar, Telecom Personal, Added on 2018-10-21 20:21:37 GMT, Argentina. Details: database. FATAL: no pg_hba.conf entry for host "90.199.45.133", user "postgres", database "template0", SSL on. FATAL: no pg_hba.conf entry for host "90.199.45.133", user "postgres", database "template0", SSL off.
- 190.61.219.117**: kururu-malo.toservers.com, Ifx Networks Colombia, Added on 2018-10-21 20:07:30 GMT, Argentina, Buenos Aires. Details: database. PostgreSQL received invalid response to SSL negotiation: 5.

port:5555 country:AR

Search



Total Results: 2,688



Top Organizations



Telefonica de Argentina	428
Cablevision Argentina	233
Telecom Argentina S.A.	230
Ixf Networks Colombia	222
Cooperativa Telefonica ...	118

Demos



TOTAL RESULTS

1,825

TOP COUNTRIES



Argentina 1,825

TOP CITIES

Cordoba	101
Buenos Aires	51
Junin	36
La Plata	33
Olivos	21

TOP SERVICES

Telnet	1,235
8081	235
Automated Tank Gauge	154
HTTP (8181)	54
NAS Web Interfaces	16

190.16.228.171

171-228-16-190.fibertel.com.ar
Cablevision Argentina
 Added on 2018-10-21 20:41:22 GMT
 Argentina
[Details](#)

```
-----
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15...
```

181.30.67.132

132-67-30-181.fibertel.com.ar
Cablevision Argentina
 Added on 2018-10-21 20:37:22 GMT
 Argentina, Azul
[Details](#)

```
HTTP/1.1 200 OK
Date: Sun, 21 Oct 2018 20:42:33 GMT
Server: Apache/2.4.7 (Ubuntu)
Last-Modified: Fri, 23 Oct 2015 18:43:07 GMT
ETag: "0f2_522c05b01ec0a"
Accept-Ranges: bytes
Content-Length: 2546
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Type: text/html
```

Demo – Default Password

181.14.201.201

host201.181-14-201.telecom.net.ar
Telecom Argentina S.A.
 Added on 2018-10-21 20:15:37 GMT
 Argentina
[Details](#)

```
-----
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15...
```



```

6 # auxiliary/scanner/smb/smb_ms_17_010
7
8 require 'msf/core'
9
10 class MetasploitModule < Msf::Auxiliary
11
12   include Msf::Exploit::Remote::SMB::Client
13   include Msf::Exploit::Remote::SMB::Client::Authenticated
14
15   include Msf::Auxiliary::Scanner
16   include Msf::Auxiliary::Report
17
18   def initialize(info = {})
19     super(update_info(info,
20       'Name' => 'MS17-010 SMB RCE Detection',
21       'Description' => %q{
22         Uses information disclosure to determine if MS17-010 has been patched or not.
23         Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0.
24         If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does
25         not have the MS17-010 patch.
26
27         This module does not require valid SMB credentials in default server
28         configurations. It can log on as the user "" and connect to IPC$.
29       },
30       'Author' => [ 'Sean Dillon <sean.dillon@risksense.com>' ],
31       'References' =>
32         [
33           [ 'CVE', '2017-0143' ],
34           [ 'CVE', '2017-0144' ],
35           [ 'CVE', '2017-0145' ],
36           [ 'CVE', '2017-0146' ],
37           [ 'CVE', '2017-0147' ],
38           [ 'CVE', '2017-0148' ],
39           [ 'MSB', 'MS17-010' ],
40           [ 'URL', 'https://technet.microsoft.com/en-us/library/security/ms17-010.aspx' ]
41         ]
42     )
43   end
44 end

```

SHODAN
Exploits
MS17-010
Q

TOTAL RESULTS

6

PLATFORM

windows	4
windows_x86-64	2

TYPE

remote	5
dos	1

AUTHOR

sleepya	3
Sean Dillon	1
Metasploit	1
Juan Sacco	1

Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)

Sean Dillon

dos 445

...

```

include Msf::Exploit::Remote::SMB::Client::Authenticated

include Msf::Auxiliary::Scanner
include Msf::Auxiliary::Report

def initialize(info = {})
  super(update_info(info,
    'Name' => 'MS17-010 SMB RCE Detection',
    'Description' => %q{
      Uses information ...
    }
  )
end

```

Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)

Sean Dillon

dos 445

...

```

include Msf::Exploit::Remote::SMB::Client::Authenticated

include Msf::Auxiliary::Scanner
include Msf::Auxiliary::Report

```

Demos

Consejos para su hogar

- No utilizar la misma contraseña en múltiples sitios web o servicios en línea
- Utilizar administradores de contraseña (gratuitos / pagos)
- Activar la “autenticación de dos factores” (Google, Facebook, Twitter, etc.)
- Revisar la lista de aplicaciones y sitios web a los que concedieron permisos
- Eliminar cualquier aplicación o sitio web que no reconozcas o no confíes
- NO caigas en estafas que solicitan pago “el pariente nigeriano te lo agradece”
- No caigas en el engaño donde indican que tienen una contraseña que “reconozcan”
- Cubrir la cámara de la computadora SIEMPRE! que no la estés utilizando 😊



Consejos para su hogar

- Evite dispositivos IoT usados o de segunda mano (routers, cámaras) podrían tener malware instalado
- Cambiar con frecuencia la clave WiFi
- Realice automáticamente una copia de seguridad de sus datos (imágenes, contactos, documentos)
- Evalúe la salud cibernética en la familia, concientizar a los miembros de la familia
- Todos estos pasos en 1 o 2 horas pueden se pueden implementar
- Utilice programas legales, y programas antimalware reconocidos
- Configure los niveles de privacidad en las redes sociales



Thank you!
Merci
Gracias
Obrigado

Julio Cesar Balderrama

 @juliobalderrama

<https://www.linkedin.com/in/juliocesarbalderrama/>