Tu información vale mucho: Cuídate, cuídanos!

Julio César Balderrama

Twitter **@juliobalderrama**
Profile: www.linkedin.com/in/juliocesarbalderrama

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

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/

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

¿Cualquier dispositivo puede ser hackeado?

¡Termómetro de sueño!

Algunas preguntas¿?


Quien NO
utiliza un
SmartPhone?

Utilizan una clave en el smartphone?

Quien posee un programa Antivirus en el smartphone?


Smartphone

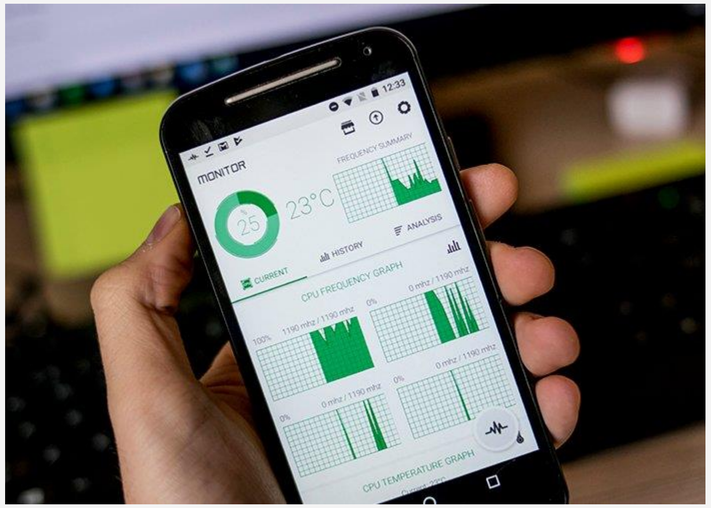
Algunas señales que indica que tu teléfono móvil podría estar poseído (hackeado)

- 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



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!

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

Cámaras IP - DVR

Múltiples vulnerabilidades en cámaras IP - DVR

"App-webs" "200 OK“

Al 17/10/2018

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

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

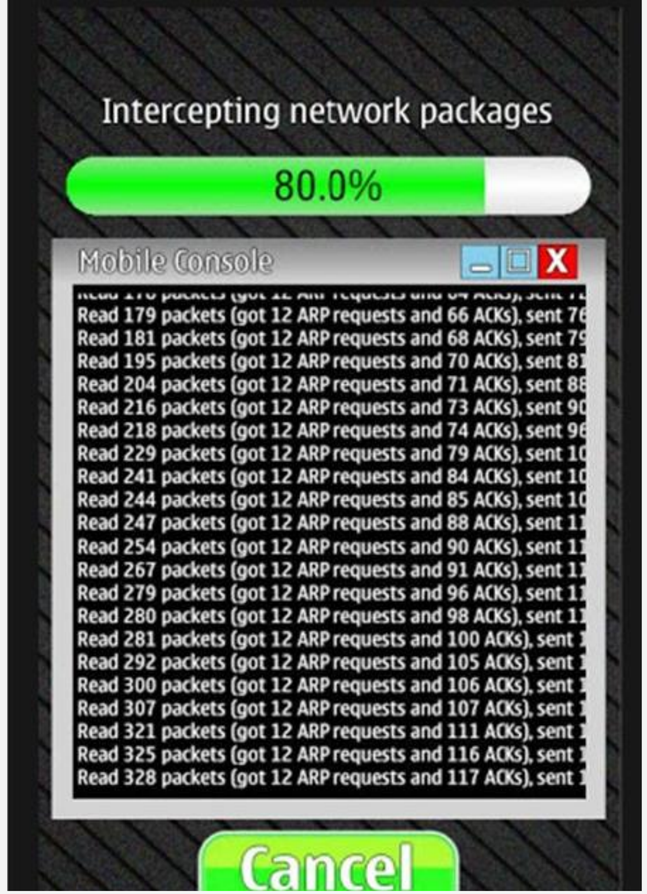
Heladeras, Lavarropas, Cafetera, …

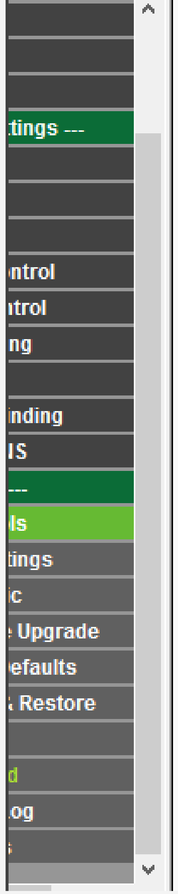
17 de octubre de 2018 - Jornada de Concientización en Ciberseguridad - *Fuerza Aérea Argentina*

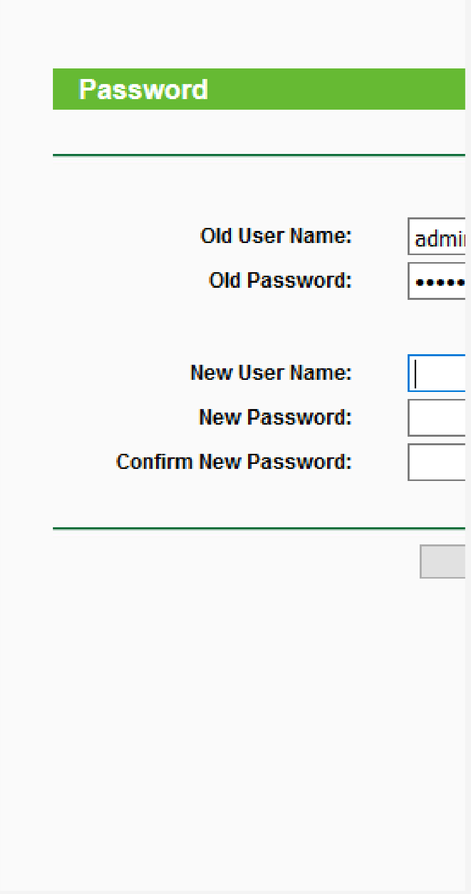
Consolas de juego

```
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?







WiFi inseguras

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

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 cibercriminales**
- **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

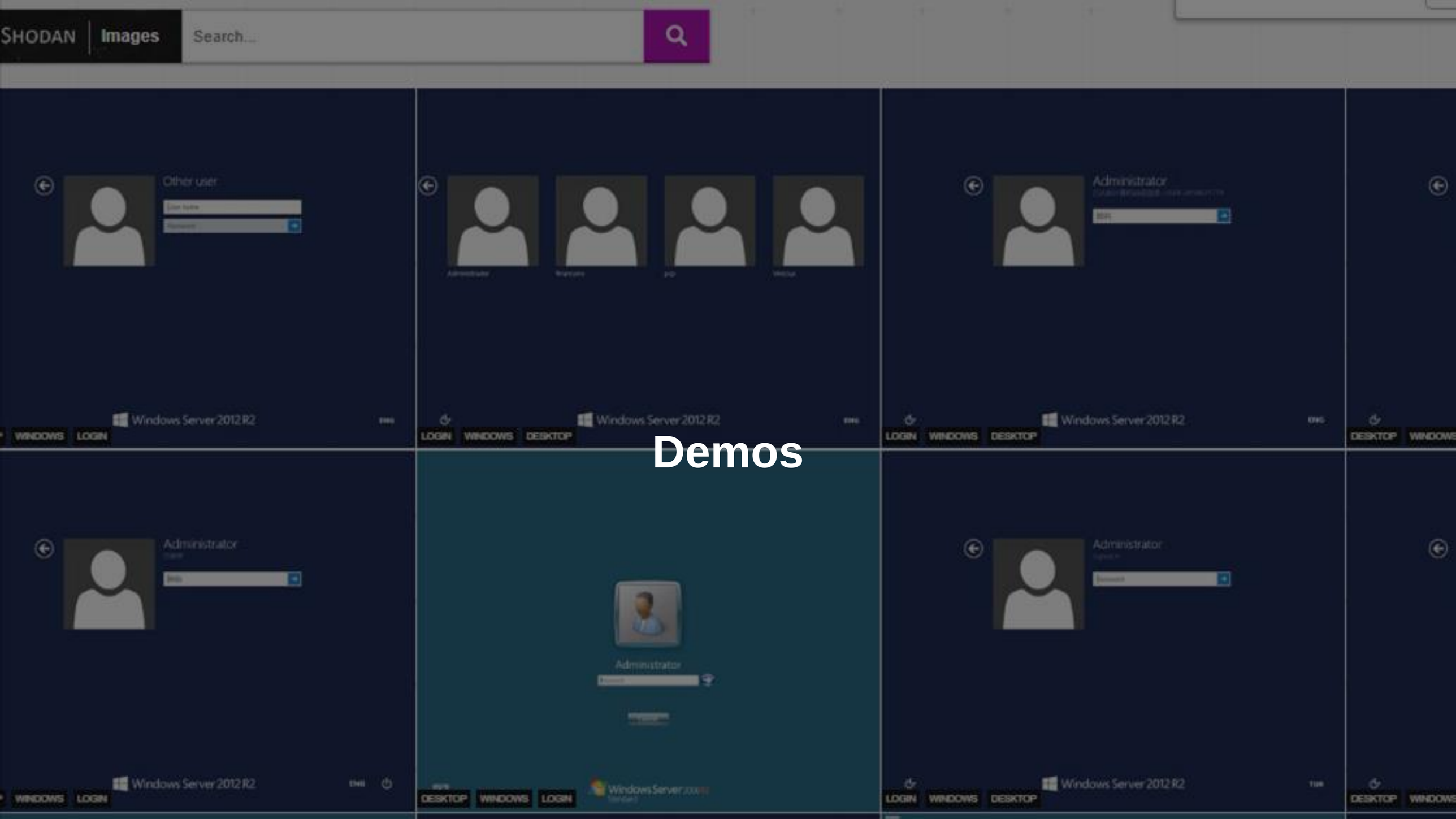
https://t.co/CCx9eQEbL2

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


SHODAN
Images
Search...
Other user
Windows Server 2012 R2
Administrator
Windows Server 2012 R2
Administrator
Windows Server 2012 R2
Administrator
Windows Server 2012 R2
Administrator
Windows Server 2012 R2

Demos

SHODAN | port:445 country:AR | Explore | Downloads | Reports | Developer Pricing

Exploits | Maps | Share Search | Download Results | Create Report

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
```

57.239.89

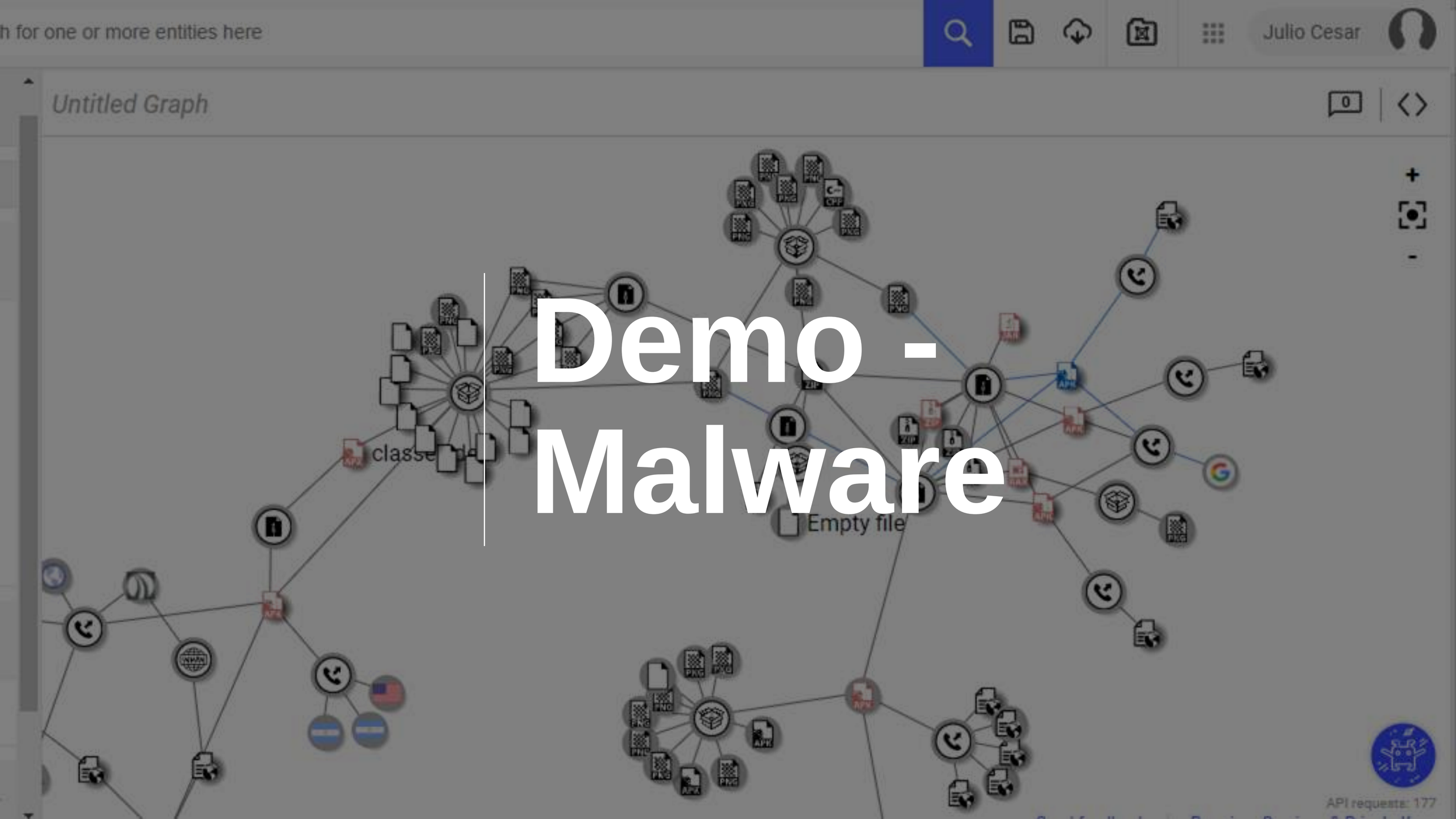
Added on 2018-10-17 10:32:58 GMT

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
---------------------------------------------------------------------------
```

Demos

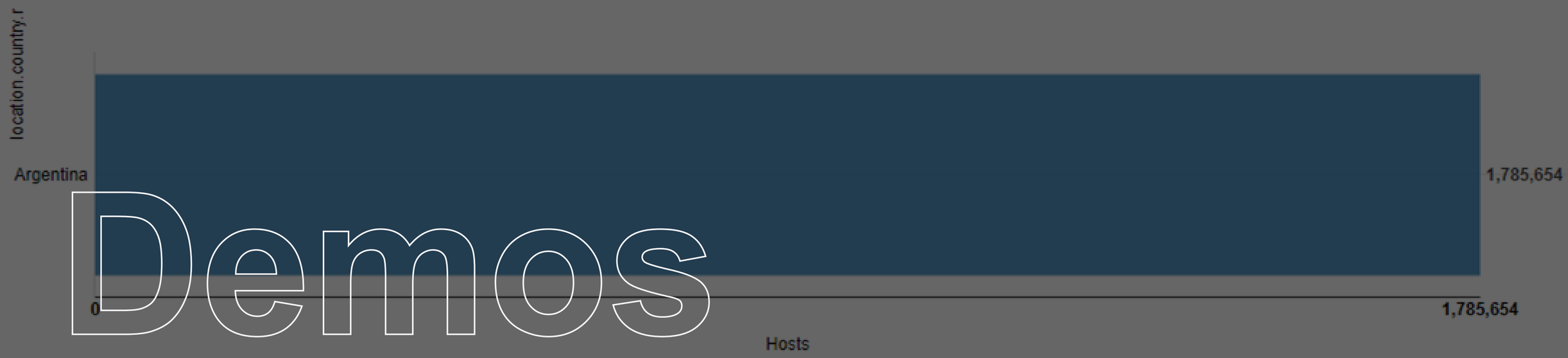

h for one or more entities here
Julio Cesar
Untitled Graph
Demo - Malware
Empty file
API requests: 177

censys

IPv4 Hosts

location.country_code:AR

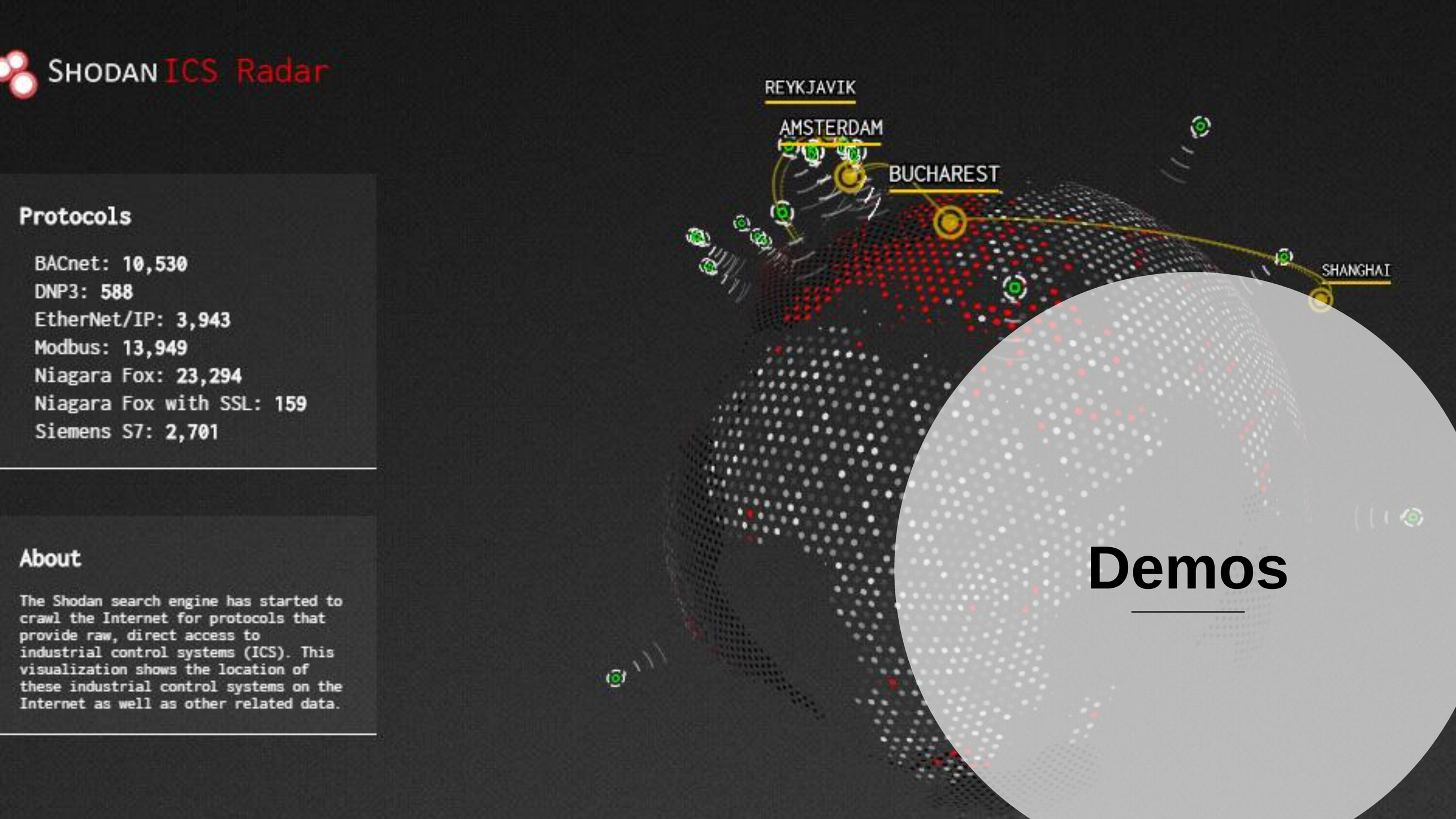
Host Report



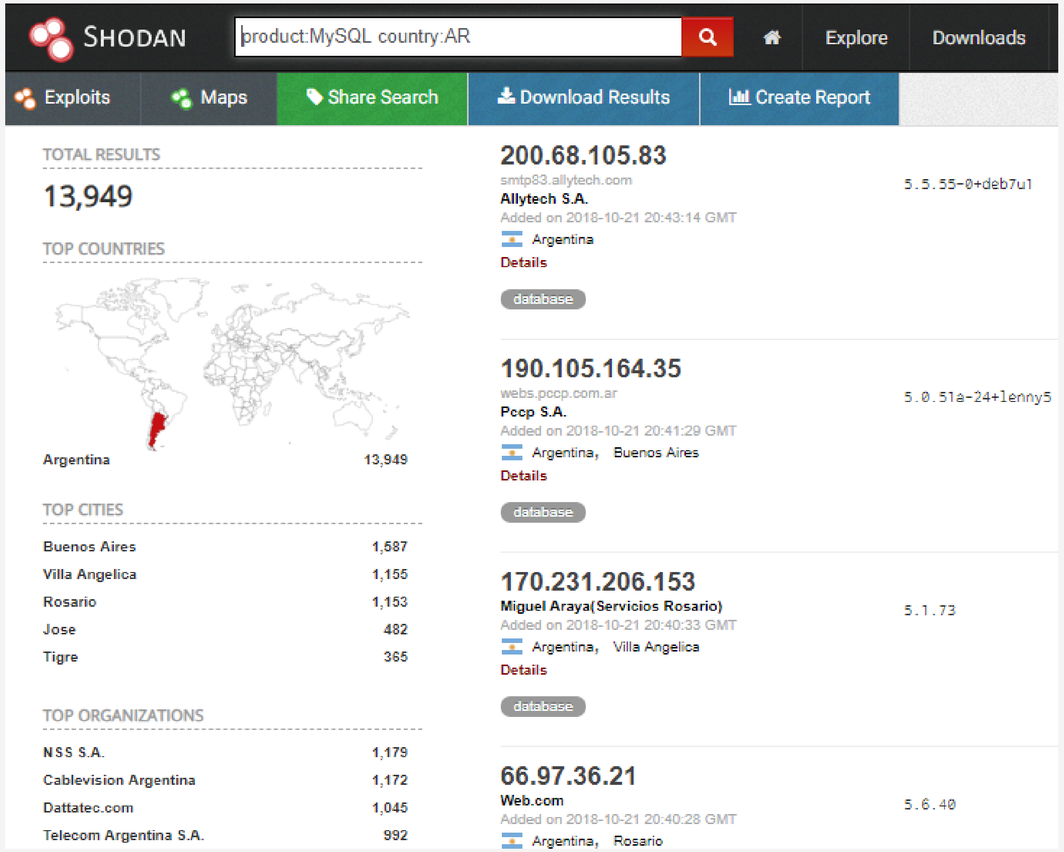
Demos

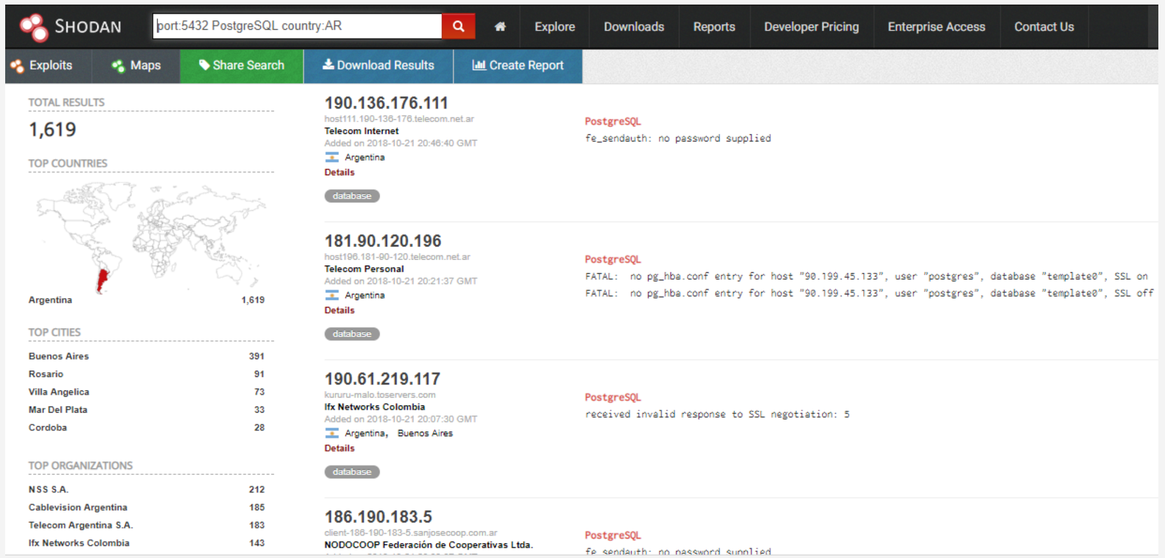
Raw Data

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


SHODAN ICS Radar
REYKJAVIK
AMSTERDAM
BUCHAREST
SHANGHAI
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






port:5555 country:AR
Search
Total Results: 2,688
Top Organizations
Telefonica de Argentina 428
Cablevision Argentina 233
Telecom Argentina S.A. 230
Ifx Networks Colombia 222
Cooperativa Telefonica ... 118
Bolivia
Paraguay
Rio de Janeiro
São Paulo
Uruguay
Santiago
Buenos
Argentina
Chile
Demos

SHODAN | "default password" country:AR | Explore | Downloads | Reports | Developer Pricing | Enterprise Access

Exploits | Maps | Share Search | Download Results | Create Report

Demo – Default Password

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: "[illegible]ec0a"
Accept-Ranges: bytes
Content-Length: 2546
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Type: text/html

<!DOCTYPE htm...
```

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...
```

```ruby
# auxiliary/scanner/smb/smb_ms_17_010

require 'msf/core'

class MetasploitModule < Msf::Auxiliary

  include Msf::Exploit::Remote::SMB::Client
  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 disclosure to determine if MS17-010 has been patched or not.
        Specifically, it connects to the IPC$ tree and attempts a transaction on FID 0.
        If the status returned is "STATUS_INSUFF_SERVER_RESOURCES", the machine does
        not have the MS17-010 patch.

        This module does not require valid SMB credentials in default server
        configurations. It can log on as the user "\" and connect to IPC$.
      },
      'Author'         => [ 'Sean Dillon <sean.dillon@risksense.com>' ],
      'References'     =>
        [
          [ 'CVE', '2017-0143'],
          [ 'CVE', '2017-0144'],
          [ 'CVE', '2017-0145'],
          [ 'CVE', '2017-0146'],
          [ 'CVE', '2017-0147'],
          [ 'CVE', '2017-0148'],
          [ 'MSB', 'MS17-010'],
          [ 'URL', 'https://technet.microsoft.com/en-us/library/security/ms17-010.aspx']
        ]
```

SHODAN | Exploits

MS17-010

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 ...
```

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 caígas 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/

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