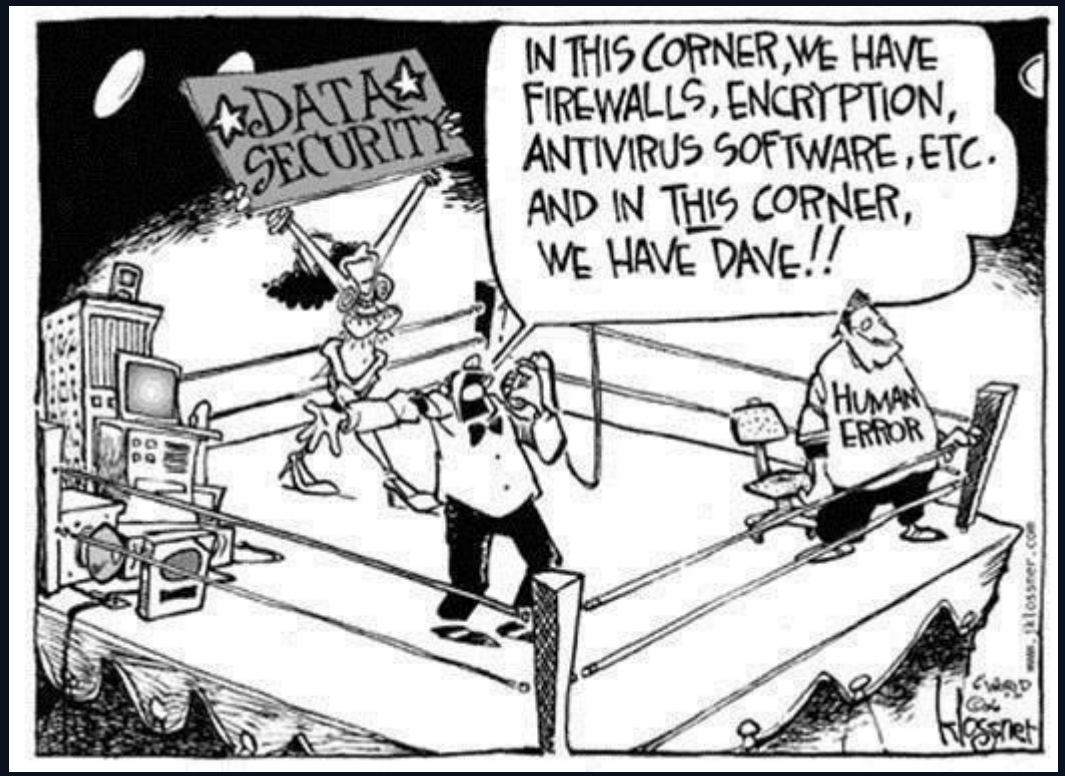
Tan fuerte como el eslabón mas debil

Seguridad como parte de la cibercultura

FUNDACION 8 CAPA OCHO


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com

FUNDACION 8 CAPA OCHO

VISION

Lograr un desarrollo de **propuestas**, en un **espacio colaborativo** y **multidisciplinario**, para el más amplio marco de las problemáticas actuales, incluyendo, pero no limitando, a los aspectos **técnicos**, **jurídicos**, **normativos**, **políticos** y **comunicacionales**.

Nuestra visión radica en el desarrollo de **actividades efectivas** y **productivas** para incrementar destrezas y **mejorar la prevención y protección del ciberespacio**.

OBJETIVO

Tenemos como principales objetivos la promoción de estudios, contenidos e iniciativas entorno al ciberespacio desde una perspectiva de **derechos, seguridad y protección** de la información para disponer de un ciberespacio fiable y resiliente. El conjunto de incentivos serán desarrollados en un marco multidisciplinario para la concientización social, **especialización profesional** y la adopción de nociones de primer nivel convergentes a cada estrato de la comunidad.

Manuel
DE CAMPOS
Pre

Pedro
JANICES
Sec

Arturo
BUSLEIMAN
Tes

COMISION DIRECTIVA

Adrian
ACOSTA
.INT

Irma
LLANO
.PY

Santiago
VAZQUEZ
.PY

César
MOLINE
.DO

Mateo
MARTINEZ
.Uy

COMISION INTERNACIONAL

Pablo
LAZARO
PSA

Victor
CHANENKO
PFA

Marisol
MANCINI
DEF

Eduardo
MALVACIO
EA

Pablo
SORRENTINO
AR

COMISION SEGURIDAD Y DEFENSA

Luis
PAPAGNI
BUE

Juan Pablo
DUSSO
CAT

Marcos
KABALA
SAL

COMISION INTERIOR

Escuela de Suboficiales de la Policia Federal Argentina

CharruaCon Security Conference - Uruguay

La Plata – Prov. Bs As
en conjunto con ACTIBA

En Pergamino con Junin, Trenque Lauquen, Ramallo
invitados por RECIA

DIPUTADOS
ARGENTINA

Taller de Seguridad de Infraestructura de nube y servicios DNS

De que hablamos cuando decimos

CIBERSEGURIDAD ?

CERBER RANSOMWARE

YOUR DOCUMENTS, PHOTOS, DATABASES AND OTHER IMPORTANT FILES
HAVE BEEN ENCRYPTED!

The only way to decrypt your files is to receive
the private key and decryption program.

To receive the private key and decryption program
go to any decrypted folder - inside there is the special file (*_READ_THIS_FILE_*)
with complete instructions how to decrypt your files.

If you cannot find any (*_READ_THIS_FILE_*) file at your PC,
follow the instructions below:

1. Download "Tor Browser" from https://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:

[redacted]

Note! This page is available via "Tor Browser" only.

AlphaBay Market

http://pwoah7foa6au2pul.onion/register.php?aff=41211

Valhalla

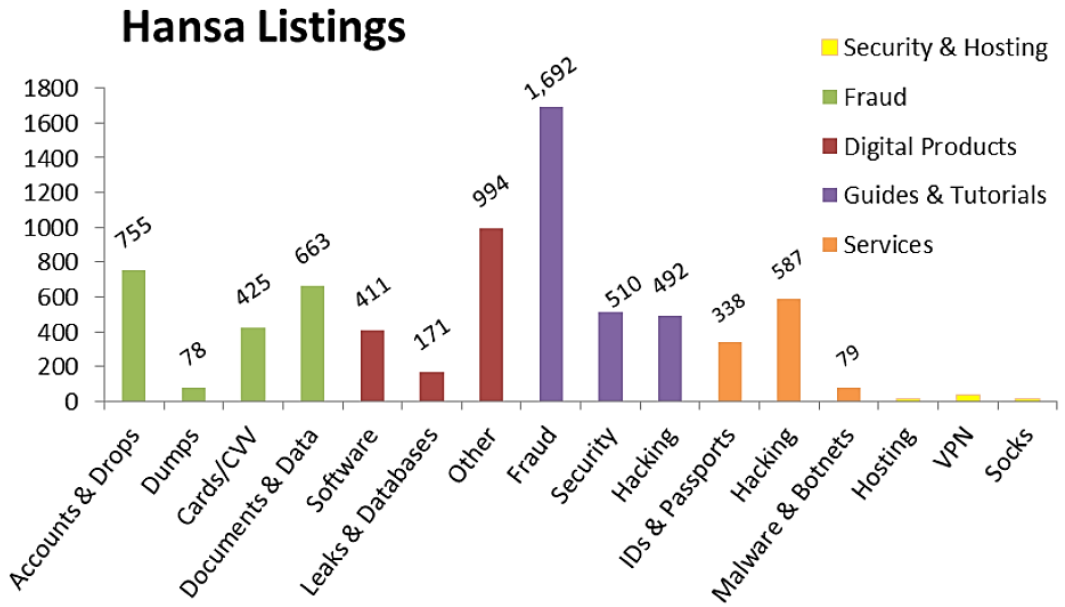
http://valhallaxmn3fydu.onion/register/E3we

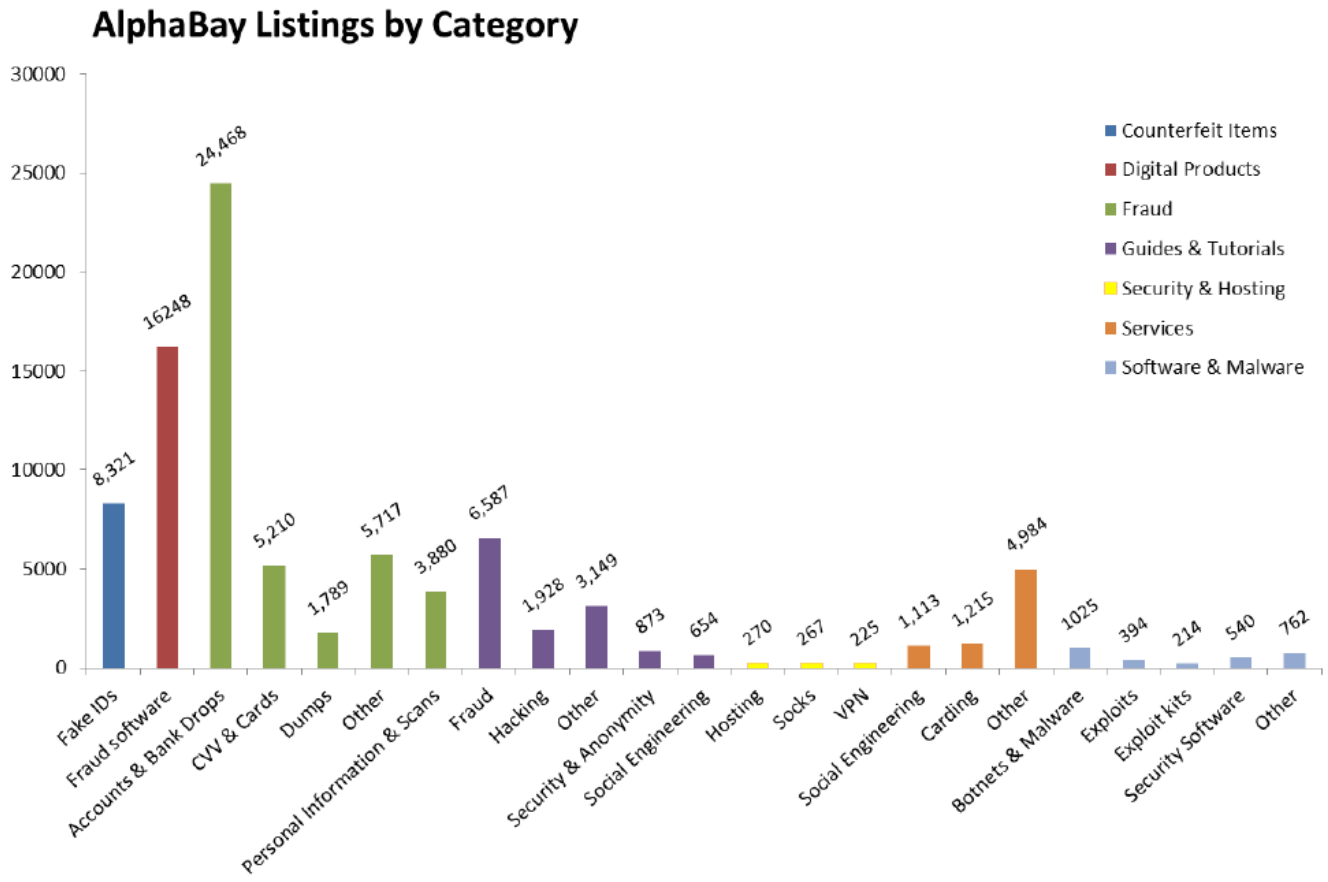
Dream Market

http://lchudifyeqm4ldjj.onion/?ai=1675

HANSA

http://hansamkt2rr6nfg3.onion/affiliate/110





Fuente: European Cybercrime Centre – 1Q 2017

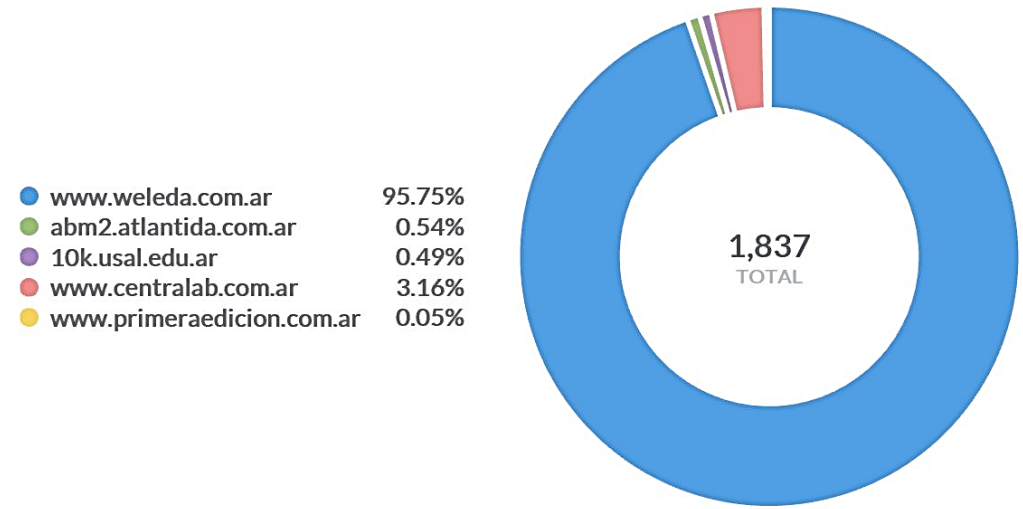
Últimos ataques a Argentina

Ataques a Argentina

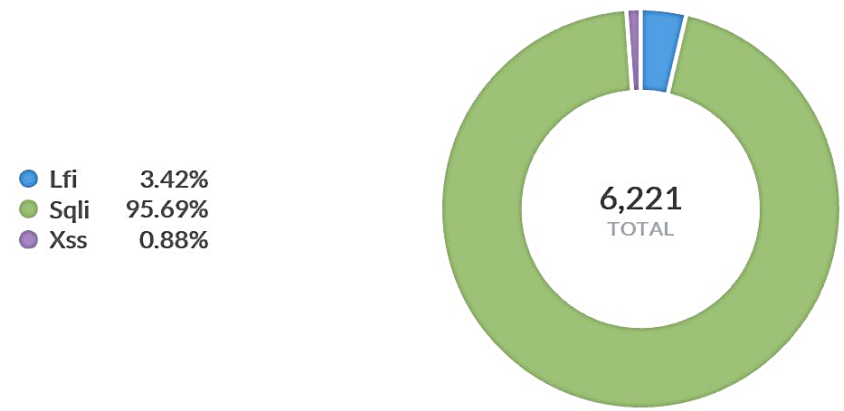
Fecha	Type	Http Host	Http URL	Http Query
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#KtkyGKyOT\n/*!00000AND#BwZyhpqUc\nEXTRACTVALUE(9407,CONCAT(0x5c
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#Qzauudfz\n/*!00000AND#sBppZM\nEXTRACTVALUE(6970,CONCAT(0x5c,0x71
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#yWYEVVafeH\n/*!00000AND#WWjbVoADz\nEXTRACTVALUE(8972,CONCAT(0
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#blzxsia\n/*!00000AND#dvQjYD\nEXTRACTVALUE(2408,CONCAT(0x5c,0x71626
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#lHkaBlyynqQ\n/*!00000AND#PcopNc\nEXTRACTVALUE(7262,CONCAT(0x5c,0x
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#DgBDVBHtPdk\n/*!00000AND#aQYMeV\nEXTRACTVALUE(8433,CONCAT(0x5c
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#ITSbiMroQGe\n/*!00000AND#MumGduoBwqV\nEXTRACTVALUE(7103,CONCA
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#uSCYnTqQ\n/*!00000AND#bfumMRcnSBzn\nEXTRACTVALUE(5438,CONCAT((
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#mpHSZb\n/*!00000AND#xEtJUxdWqB\nEXTRACTVALUE(8236,CONCAT(0x5c,(
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#mIHkrYVT\n/*!00000AND#DeOeFiofFwu\nEXTRACTVALUE(6520,CONCAT(0x5c
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#GZumpHCvNIG\n/*!00000AND#ojieOZm\nEXTRACTVALUE(9661,CONCAT(0x5c
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#roIdbJ\n/*!00000AND#dtTyMb\nEXTRACTVALUE(8872,CONCAT(0x5c,0x71626
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#cRnqDv\n/*!00000AND#WxEHNrXDMeZ\nEXTRACTVALUE(9547,CONCAT(0x5c
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#UVgGcv\n/*!00000AND#yDhkBZvJiQ\nEXTRACTVALUE(6857,CONCAT(0x5c,0x
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#LXSIMRle\n/*!00000AND#oORTSm\nEXTRACTVALUE(1169,CONCAT(0x5c,0x7
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#BsmXnDgkNG\n/*!00000AND#tUOToQfrbahT\nEXTRACTVALUE(2443,CONCAT
12-09-2017 15:34	Sqli	www.weleda.com.ar	index.php	{"Get": ["b=12345'#KmoLzOr\n/*!00000AND#oBbgoMz\nEXTRACTVALUE(5570,CONCAT(0x5c,0x7

Rows 1-17 of 2000

Ataques a Argentina última semana



Últimos ataques a Argentina por tipo



NO CRIMINALIZAR LA DEEP WEB

DATA RECORDS ARE LOST OR STOLEN AT THE FOLLOWING FREQUENCY

EVERY DAY

5,253,104

Records

EVERY HOUR

218,879

Records

EVERY MINUTE

3,648

Records

EVERY SECOND

61

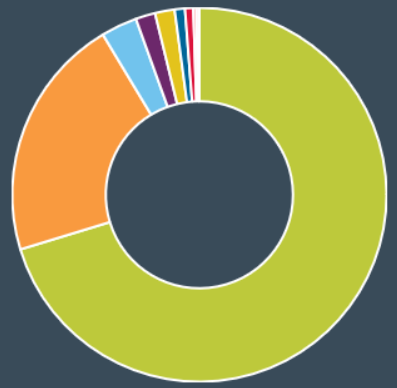
Records

Fuente: http://www.breachlevelindex.com 2017

DATA RECORDS STOLEN OR LOST BY INDUSTRY

Shows percentage of total records, hover over pie chart for record totals.

2017 | 2016 | 2015 | 2014 | 2013 | ALL-TIME

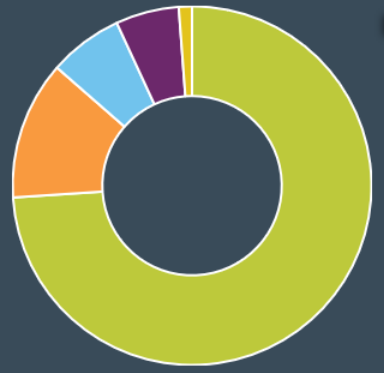


Entertainment	70.28%
Government	21.10%
Technology	3.11%
Healthcare	1.70%
Education	1.69%
Social Media	0.89%
Other	0.71%
Financial	0.26%
Retail	0.19%

NUMBER OF BREACH INCIDENTS BY TYPE

Attackers use a variety of techniques against organizations.

2017 | 2016 | 2015 | 2014 | 2013 | ALL-TIME



Identity Theft	73.95%
Financial Access	12.49%
Account Access	6.67%
Existential Data	5.71%
Nuisance	1.18%

NUMBER OF BREACH INCIDENTS BY SOURCE

Source of data breaches causing problems can vary.

2017 | 2016 | 2015 | 2014 | 2013 | ALL-TIME

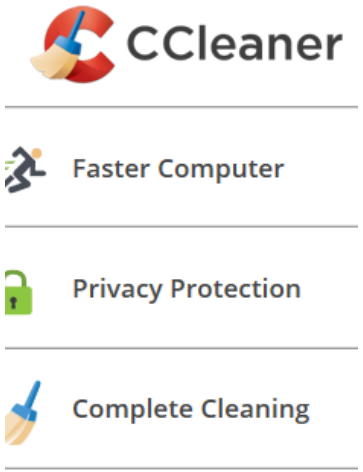
Malicious Outsider	73.41%
Accidental Loss	18.30%
Malicious Insider	8.07%
Unknown	0.11%
State Sponsored	0.11%

Fuente: http://www.breachlevelindex.com 2017

Hackers compromised free CCleaner software, Avast's Piriform says

September 18, 2017 - Reuters

"No hay nada que un usuario podría haber notado", dijo Williams, señalando que el software de optimización tenía un certificado digital adecuado, lo que significa que otras computadoras confían automáticamente en el programa



The malicious program was slipped into legitimate software called CCleaner, which is downloaded for personal computers and Android phones as often **as five million times a week**. It cleans up junk programs and advertising cookies to speed up devices.

CCleaner is the main product made by London's Piriform, which was bought in July by Prague-based Avast, one of the world's largest computer security vendors. At the time of the acquisition, the company said **130 million people used CCleaner**.

A version of CCleaner downloaded in August **included remote administration tools that tried to connect to several unregistered web pages, presumably to download additional unauthorized programs**, security researchers at Cisco's (CSCO.O) Talos unit said.

CCleaner does not update automatically, so each person who has installed the problematic version **will need to delete it and install a fresh version**, he said.

Williams said that Talos detected the issue at an early stage, when the hackers appeared to be collecting information from infected machines, rather than forcing them to install new programs.

http://www.reuters.com/article/us-security-avast/hackers-compromised-free-ccleaner-software-avasts-piriform-says-idUSKCN1BT0R9

Unpatched Windows Kernel Bug Could Help Malware Hinder Detection

Sunday, September 17, 2017 Mohit Kumar

A 17-year-old programming error has been discovered in Microsoft's Windows kernel that could prevent some security software from detecting malware at runtime when loaded into system memory.

El problema de seguridad, descrito por el investigador de seguridad de enSilo, Omri Misgav, reside en la rutina del kernel "***PsSetLoadImageNotifyRoutine***", que aparentemente afecta todas las versiones de los sistemas operativos Windows desde Windows 2000.

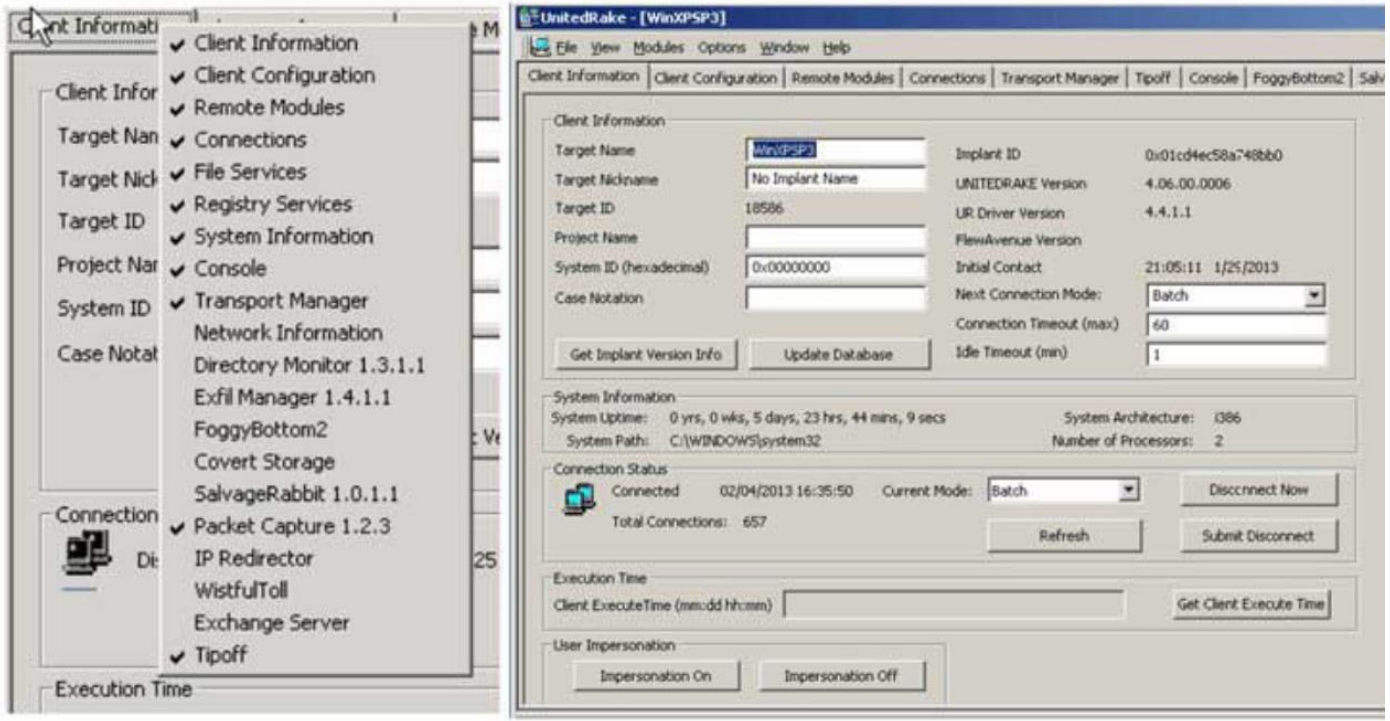
Windows tiene una API incorporada, llamada PsSetLoadImageNotifyRoutine, que ayuda a los programas a supervisar si se ha cargado cualquier módulo nuevo en la memoria. Una vez registrado, el programa recibe una notificación cada vez que se carga un módulo en la memoria. Esta notificación incluye la ruta al módulo en el disco. Sin embargo, Misgav encontró que debido a "comportamiento de almacenamiento en caché, junto con la forma en que el controlador de sistema de archivos mantiene el nombre de archivo y un grave error de codificación", la función no devuelve siempre la ruta correcta de los módulos cargados.

¿Qué es lo malo? Parece que Microsoft no tiene planes de abordar este problema, ya que el gigante del software no lo considera como una vulnerabilidad de seguridad.

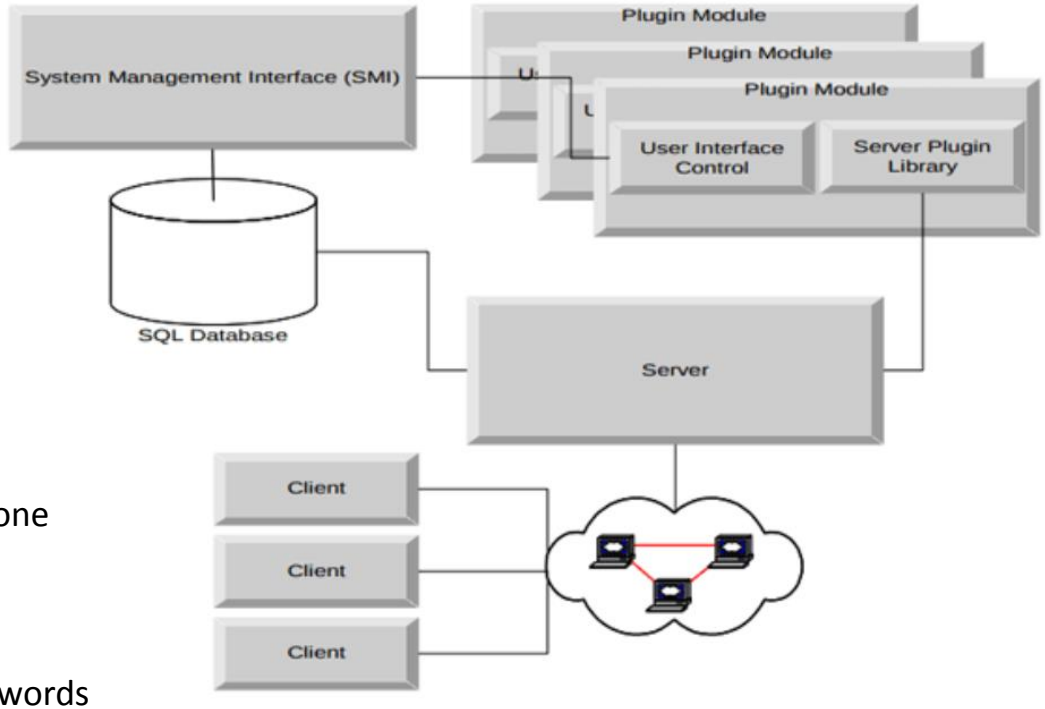
"Este error podría tener implicaciones de seguridad para aquellos que no son conscientes de su existencia. Creemos que si Microsoft no planea arreglar este error, deben por lo menos advertir explícitamente a los desarrolladores acerca de ello en su documentación", dice Tal Liberman, jefe del equipo de investigación de enSilo.

Los investigadores creen que este "error programático" **podría ser teóricamente utilizado por los autores de malware para evitar la detección de antivirus** -especialmente aquellos productos de seguridad que dependen de esta API para comprobar si se ha cargado algún código malicioso en la memoria- mediante una "serie de operaciones de archivo" inducir a error el motor de exploración a mirar el archivo equivocado

http://www.reuters.com/article/us-security-avast/hackers-compromised-free-ccleaner-software-avasts-piriform-says-idUSKCN1BT0R9
https://breakingmalware.com/documentation/windows-pssetloadimagenotifyroutine-callbacks-good-bad-unclear-part-1/



UNITEDRAKE, the implant is a "fully extensible remote collection system" that comes with a number of "plug-ins,"



CAPTIVATEDAUDIENCE is for recording conversations via the infected computer's microphone

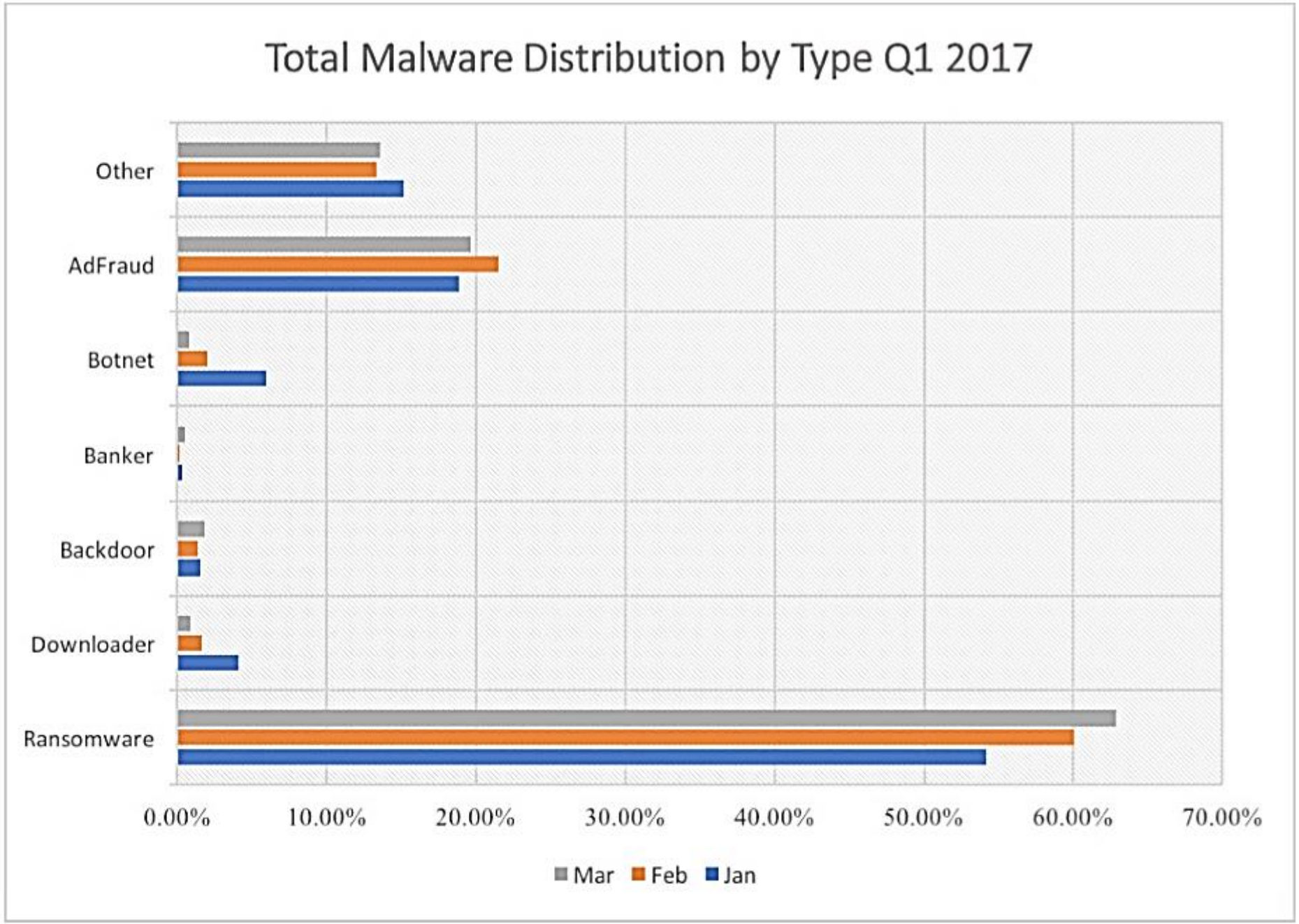
GUMFISH is for covertly taking control over a computer's webcam and snap photographs

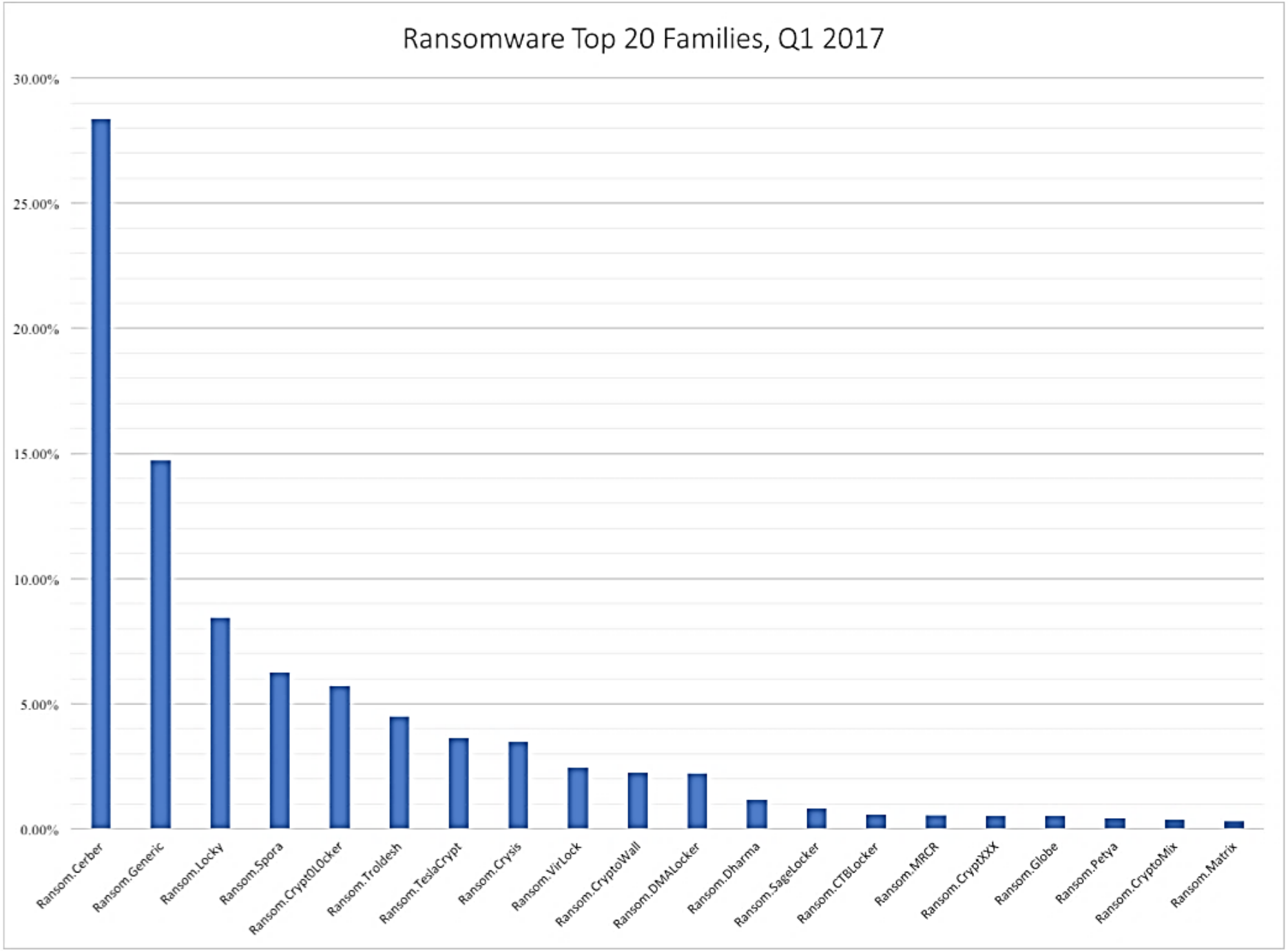
FOGGYBOTTOM for exfiltrating Internet data like browsing histories, login details and passwords

GROK is a Keylogger Trojan for capturing keystrokes

SALVAGERABBIT is for accessing data on removable flash drives that connect to the infected computer.

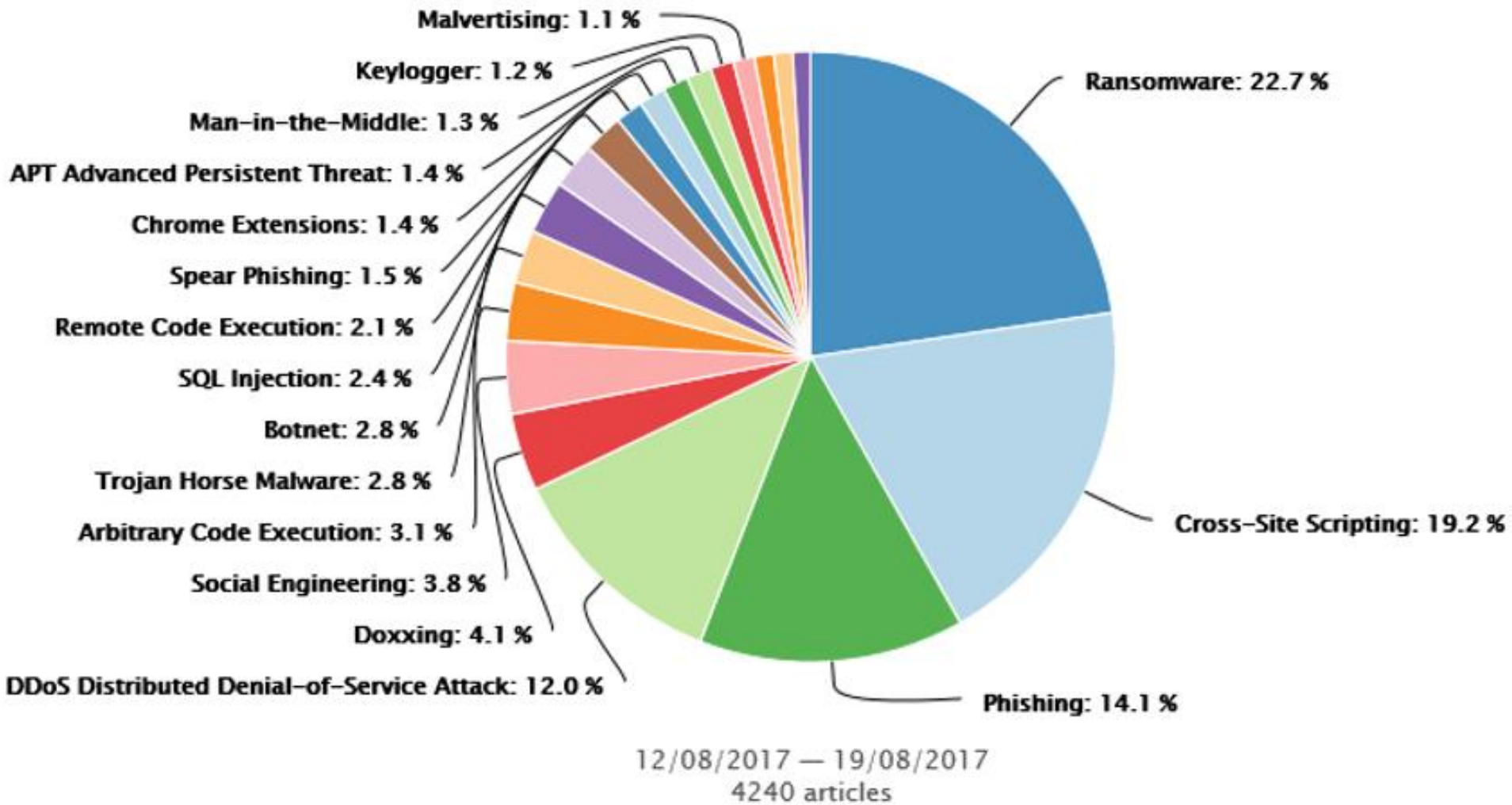
Fuente: thehackernews


Total Malware Distribution by Type Q1 2017
Other
AdFraud
Botnet
Banker
Backdoor
Downloader
Ransomware
0.00%
10.00%
20.00%
30.00%
40.00%
50.00%
60.00%
70.00%
Mar
Feb
Jan


Ransomware Top 20 Families, Q1 2017
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
Ransom.Cerber
Ransom.Generic
Ransom.Locky
Ransom.Spora
Ransom.CryptOLOcker
Ransom.Troldesh
Ransom.TeslaCrypt
Ransom.Crysis
Ransom.VirLock
Ransom.CryptoWall
Ransom.DMALocker
Ransom.Dharma
Ransom.SageLocker
Ransom.CTBLocker
Ransom.MRCR
Ransom.CryptXXX
Ransom.Globe
Ransom.Petya
Ransom.CryptoMix
Ransom.Matrix

Incidents

Attack Types by Mentions Graph



Fuente: European Cybercrime Centre – 1Q 2017

Hacker Claims He Hacked 150,000 Printers to 'Raise Awareness' About Hacking

Eve Peyser
2/06/17 8:46pm • Filed to: HACKERS!

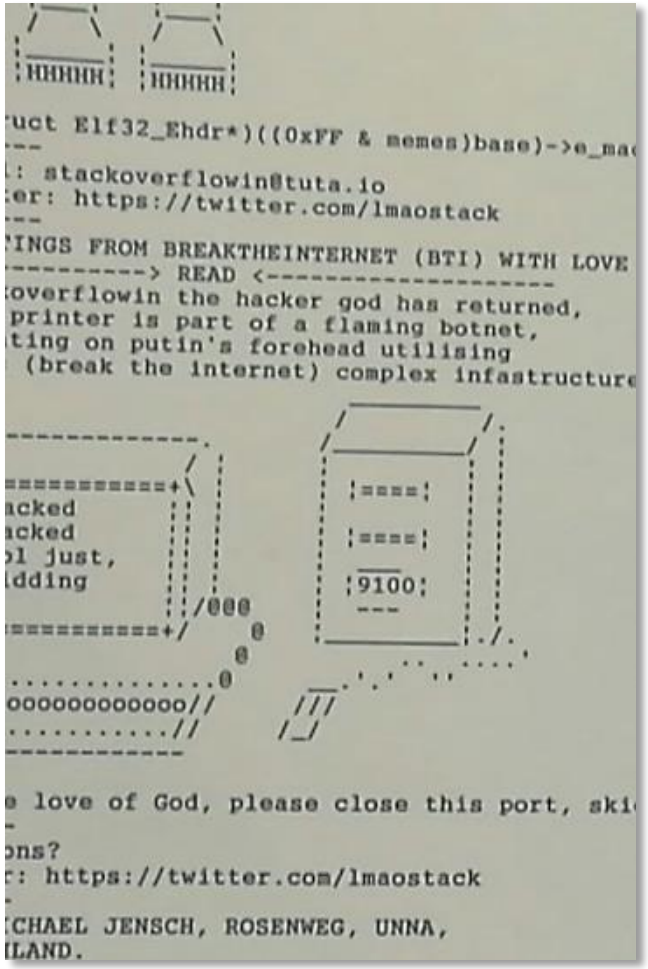
GIZMODO

Durante el fin de semana, un hacker que lleva el nombre de Stackoverflowin afirmó que hackeó 150.000 impresoras inseguras en un esfuerzo para "**aumentar la conciencia de todos sobre los peligros de dejar impresoras expuestas en línea sin un cortafuegos u otras configuraciones de seguridad habilitadas**".

Utilizando su propio **script automatizado**, Stackoverflowin detectó impresoras inseguras fabricadas por una amplia gama de empresas, incluyendo XX, XXX, XXXX y XXXXX. Instruyó a las máquinas para que imprimieran un documento **informando a las víctimas** del hack con arte ASCII entremezclado, entre otras cosas.

Stackoverflowin dijo a Bleeping Computer que el guión que escribió "apunta a dispositivos de impresión que tienen puertos **IPP (Internet Printing Protocol), puertos LPD (Line Printer Daemon) y puerto 9100 abiertos a conexiones externas**".

Esto viene de los talones de un estudio publicado la semana pasada de la Universidad de Ruhr Bochum, que encontró una serie de vulnerabilidades de seguridad de las máquinas hechas por 20 grandes marcas.



id **Show device information.**
status Enable status messages.
version **Show firmware version or serial number (from 'info config').**
pagecount Manipulate printer's page counter: pagecount <number>
printenv Show printer environment variable: printenv <VAR>
env Show environment variables (alias for 'info variables').
set Set printer environment variable: set <VAR=VALUE>

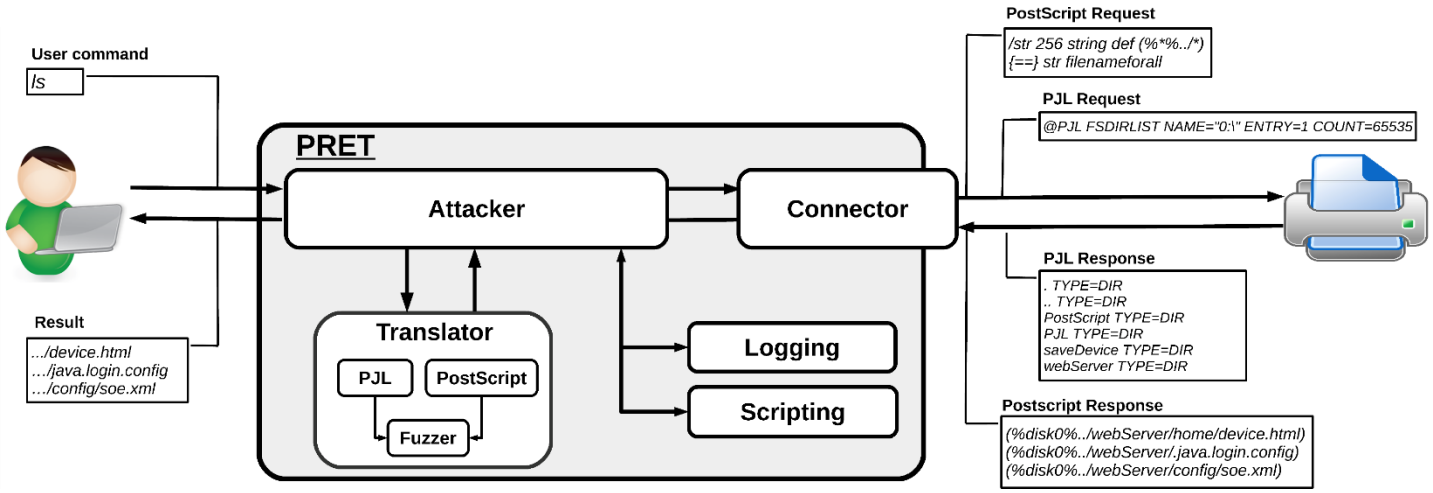
display Set printer's display message: display <message>
offline Take printer offline and display message: offline <message>
restart Restart printer.
reset **Reset to factory defaults.**
selftest Perform various printer self-tests.
disable Disable printing functionality.
destroy Cause physical damage to printer's NVRAM.
flood **Flood user input, may reveal buffer overflows.**

lock Lock control panel settings and **disk write access**.
unlock Unlock control panel settings and **disk write access**.
hold Enable job retention.

nvram NVRAM operations: nvram <operation>
nvram dump [all] - Dump (all) NVRAM **to local file**.
nvram read addr - Read single byte from address.
nvram write addr value - Write single byte to address.

info Show information: info <category>
info config - Provides configuration information.
info filesys - Returns PJL file system information.
info id - Provides the printer model number.
info memory - Identifies amount of memory available.
info pagecount - Returns the number of pages printed.
info status - Provides the current printer status.
info ustatus - Lists the unsolicited status variables.
info variables - Lists printer's environment variables.

Printer Exploitation Toolkit - The tool that made dumpster diving obsolete.



overlay
Put overlay eps file on all hardcopies: overlay <file.eps>
cross
Put printer graffiti on all hardcopies: cross <font> <text>
replace
Replace string in documents to be printed: replace <old> <new>
capture
Capture further jobs to be printed on this device.

Tools

- P[redacted]F

Fundamentals

- **Printer languages**
  - PJL, PCL, PostScript
- **Network protocols**
  - LPD, IPP, Raw, SMB

Attack Carriers

- USB drive or cable
- Port 9100 printing
- Cross-site printing

CATEGORIA	ATAQUE	Protocolo	Testeo
Denegación de Servicio	Transmission channel	TCP	while true; do nc printer 9100; done
	Document processing	PS	PRET commands: disable, hang
		PJL	PRET commands: disable, offline
	Physical damage	PS	PRET command: destroy
		PJL	PRET command: destroy
Escalada de privilegios	Factory defaults	SNMP	snmpset -v1 -c public printer 1.3.6.1.2.1.43.5.1.1.3.1 i 6
		PML	PRET command: reset
		PS	PRET command: reset
	Accounting bypass	TCP	Connect to printer directly, bypassing the print server
		IPP	Check if you can set a username without authentication
		PS	Check if PostScript code is preprocessed on print server
		PJL	PRET command: pagecount
	Fax and Scanner	multiple	Install printer driver and (ab)use fax/scan functionality
Acceso a trabajos de impresion	Print job retention	PS	PRET command: capture
	Print job manipulation	PS	PRET commands: cross, overlay, replace
Filtración de información	Memory access	PJL	PRET command: nvram dump
	File system access	PS	PRET commands: fuzz, ls, get, put, …
		PJL	PRET commands: fuzz, ls, get, put, …
	Credential disclosure	PS	PRET commands: lock, unlock
		PJL	PRET commands: lock, unlock
Ejecucion de codigo	Buffer overflows	PJL	PRET command: flood
		LPD	./lpdtest.py printer in "`python -c 'print "x"*3000'`"
	Firmware updates	PJL	Flip a bit, check if the modified firmware is still accepted
	Software packages	multiple	Obtain an SDK and write your own proof-of-concept application

last modified on 2 July 2017

Que tan dificil es buscar un patio de juegos?

Shodan Developers Book View All...

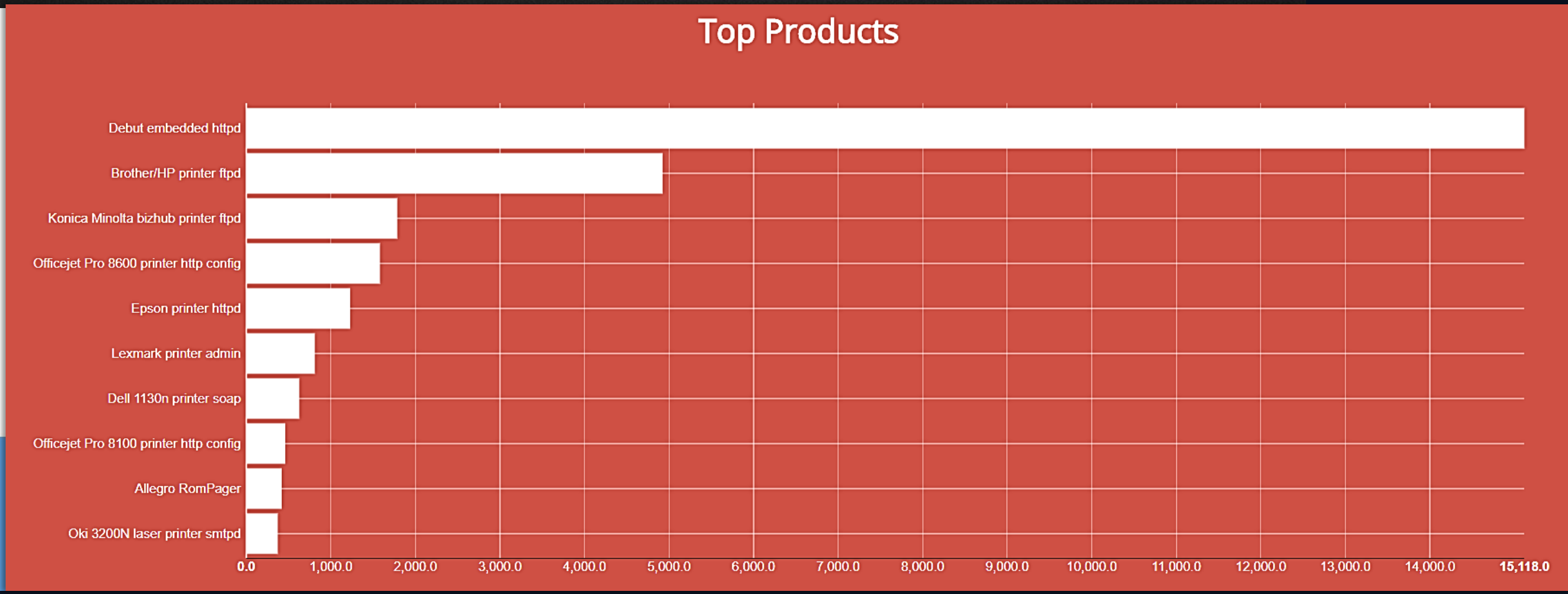
SHODAN

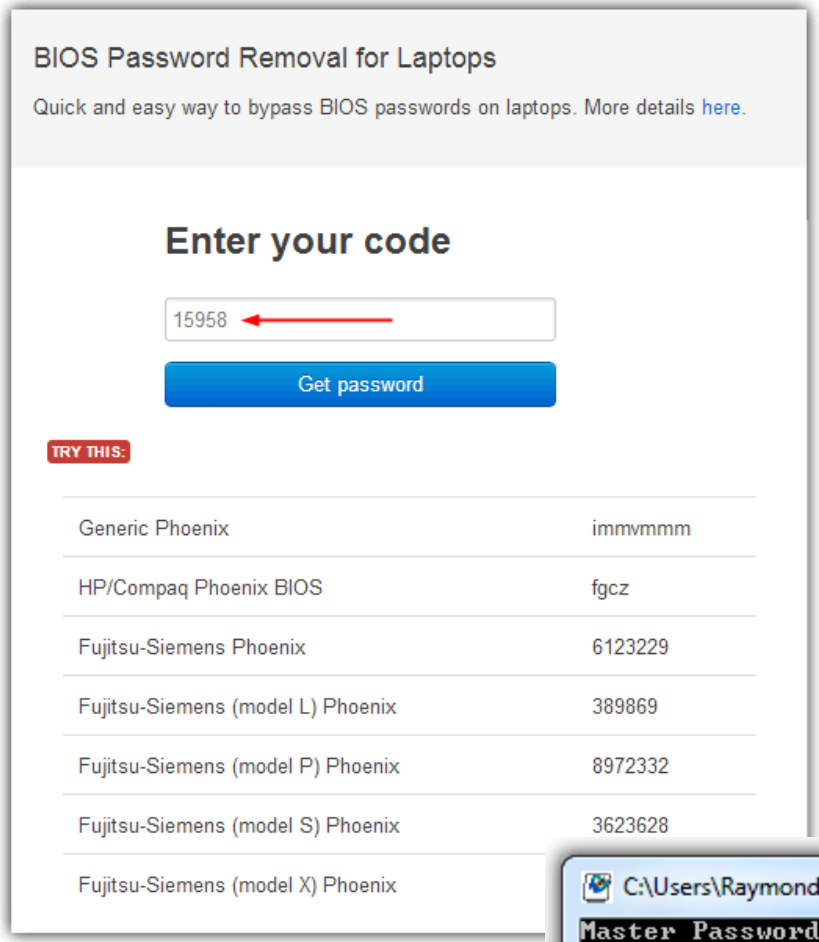
Explore Enterprise Access Contact Us New to Shodan? Login or Reg

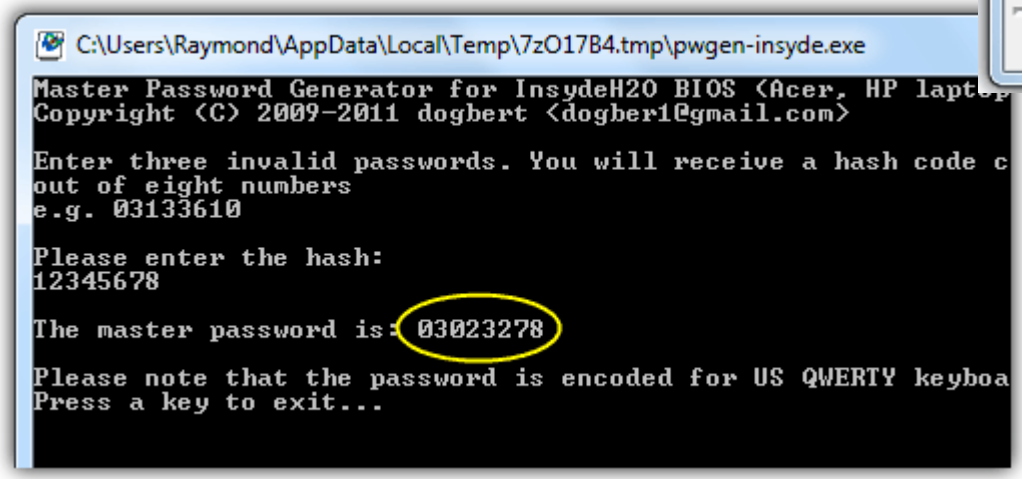
Internet connected printers

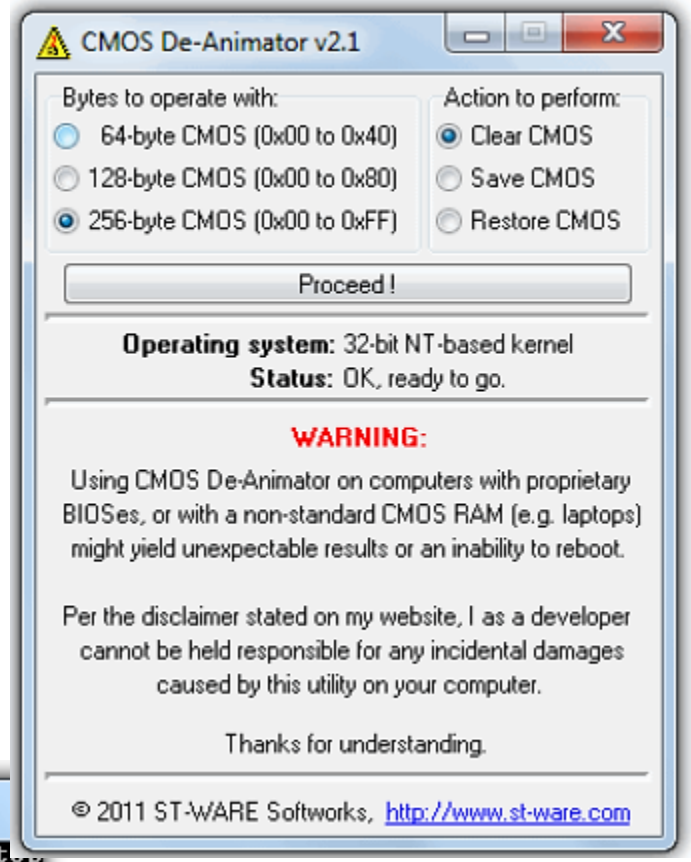
Search for device:printer returned 35,851 results on 30-01-2017

Top Products




BIOS Password Removal for Laptops
Quick and easy way to bypass BIOS passwords on laptops. More details here.
Enter your code
15958
Get password
TRY THIS:
Generic Phoenix immvmmm
HP/Compaq Phoenix BIOS fgcz
Fujitsu-Siemens Phoenix 6123229
Fujitsu-Siemens (model L) Phoenix 389869
Fujitsu-Siemens (model P) Phoenix 8972332
Fujitsu-Siemens (model S) Phoenix 3623628
Fujitsu-Siemens (model X) Phoenix


C:\Users\Raymond\AppData\Local\Temp\7zO17B4.tmp\pwgen-insyde.exe
Master Password Generator for InsydeH2O BIOS (Acer, HP laptop
Copyright (C) 2009-2011 dogbert <dogbert1@gmail.com>
Enter three invalid passwords. You will receive a hash code c
out of eight numbers
e.g. 03133610
Please enter the hash:
12345678
The master password is: 03023278
Please note that the password is encoded for US QWERTY keyboa
Press a key to exit...


CMOS De-Animator v2.1
Bytes to operate with:
64-byte CMOS (0x00 to 0x40)
128-byte CMOS (0x00 to 0x80)
256-byte CMOS (0x00 to 0xFF)
Action to perform:
Clear CMOS
Save CMOS
Restore CMOS
Proceed !
Operating system: 32-bit NT-based kernel
Status: OK, ready to go.
WARNING:
Using CMOS De-Animator on computers with proprietary BIOSes, or with a non-standard CMOS RAM (e.g. laptops) might yield unexpectable results or an inability to reboot.
Per the disclaimer stated on my website, I as a developer cannot be held responsible for any incidental damages caused by this utility on your computer.
Thanks for understanding.
© 2011 ST-WARE Softworks, http://www.st-ware.com

DECISIÓN

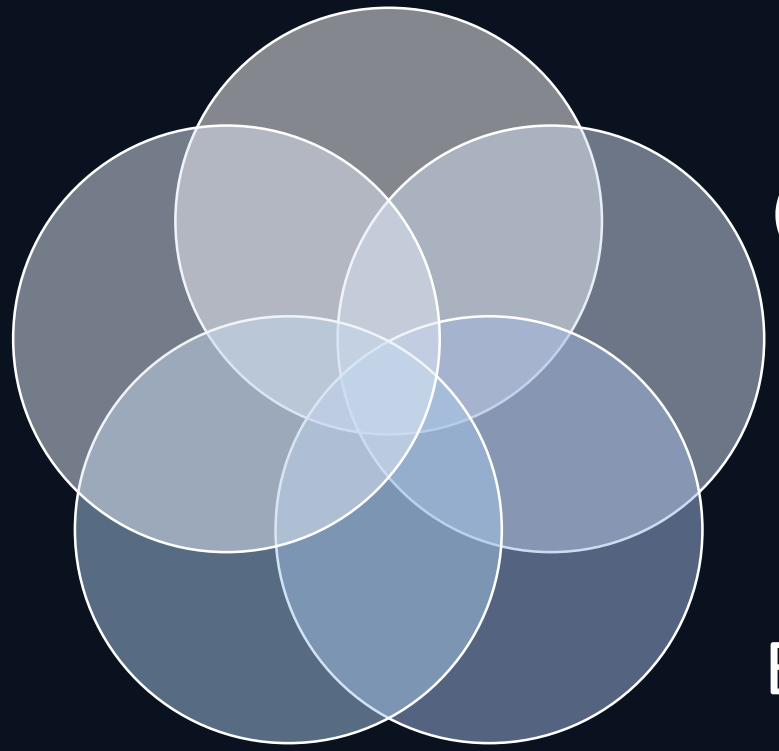
(política)

COMUNICACIÓN

(medios, familia, escuela, empresa)

CAPACITACIÓN

(academia, org.civ., fund, etc)



NORMAS

(leyes, protocolos)

EJECUCIÓN

(organismos, fuerzas, icia)


POLITICOS
JURIDICOS
CONOCIMIENTO
TECNICOS
NORMATIVOS

MINISTERIO DE MODERNIZACION

SEC PAIS DIGITAL

DNICIC – COMISION - CERT

MINISTERIO DE SEGURIDAD

PFA – PSA – PNA - GNA

CIBERCRIMEN/TERRORISMO

DROGAS/OPER-SESP

MINISTERIO DE DEFENSA

SUBSECRETARIA DE CIBERDEFENSA

EMC/EA/AA

MINISTERIO DE JUSTICIA

COORD GRAL DE CIBERDELITOS

Resol JGM 580/11 - Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad

- Elaborar y proponer normas destinadas a incrementar los esfuerzos orientados a elevar los umbrales de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Publico Nacional
- Establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad, asegurando la implementación de los últimos avances en tecnología para la protección de las infraestructuras críticas
- Investigar nuevas tecnologías y herramientas en materia de seguridad informática
- Incorporar tecnología de última generación para minimizar todas las posibles vulnerabilidades de la infraestructura digital del Sector Público Nacional

Dispo ONTI 3/2013 - Política de Seguridad de la Información Modelo

- Todo Organismo se encuentra expuesto a riesgos en materia de seguridad de la información. No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al cual se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos.

- 10.4 Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc. Los usuarios deben estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes deben introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

- Desconectar de la red/sistema/servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso

Dec 577/2017- Comité de Ciberseguridad

- Créase el COMITÉ DE CIBERSEGURIDAD en la órbita del MINISTERIO DE MODERNIZACIÓN, que estará integrado por representantes del citado Ministerio, del MINISTERIO DE DEFENSA y del MINISTERIO DE SEGURIDAD, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

- Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.

- Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

- Impulsar el dictado de un marco normativo en materia de Ciberseguridad.

Artículo 255

Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

CODIGO PENAL

Ley 26.388
Modificación. Art. 13

Sancionada:
Junio 4 de 2008

Promulgada de Hecho:
Junio 24 de 2008

Artículo 153 bis

Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

Artículo 173

15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.

CODIGO PENAL

(Inciso incorporado por art. 1° de la Ley N° 25.930 B.O. 21/9/2004)

16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

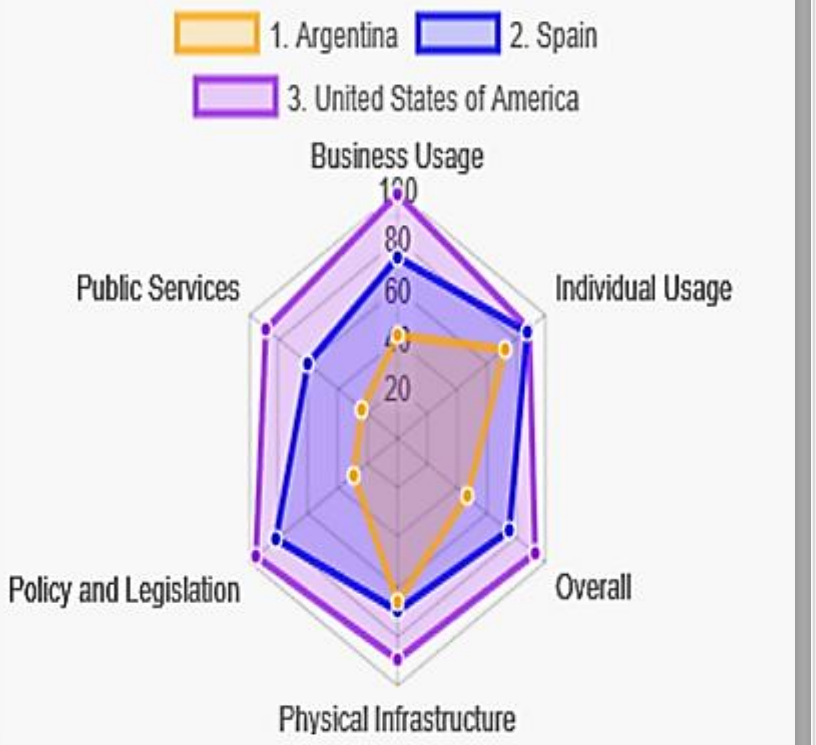
(Inciso incorporado por art. 9° de la Ley N° 26.388, B.O. 25/6/2008)

Artículo 174

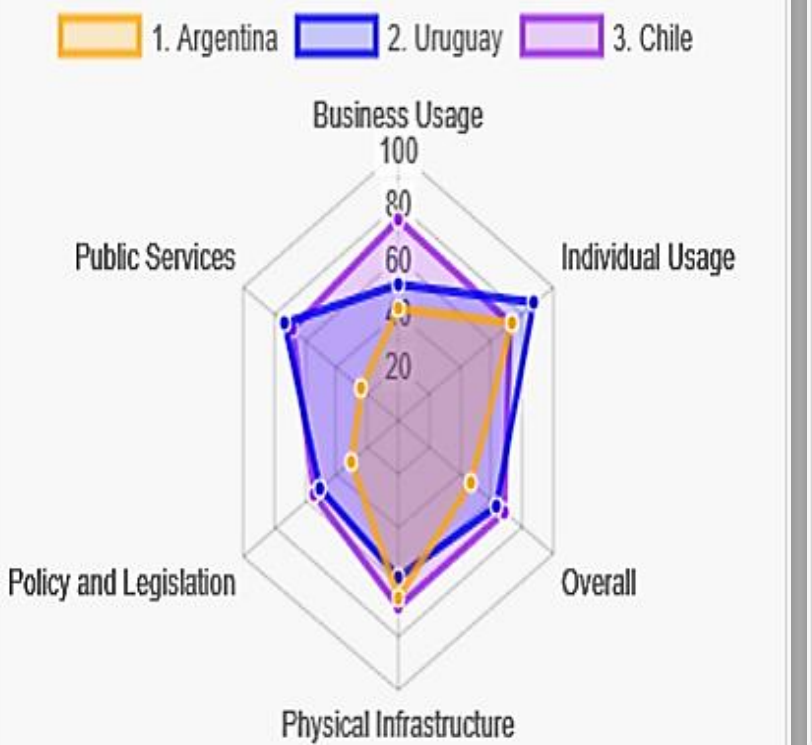
6°.- El que maliciosamente afectare el normal desenvolvimiento de un establecimiento o explotación comercial, industrial, agropecuaria, minera o destinado a la prestación de servicios; destruyere, dañare, hiciere desaparecer, ocultare o fraudulentamente disminuyere el valor de materias primas, productos de cualquier naturaleza, máquinas, equipos u otros bienes de capital. (Inciso incorporado por art. 2° de la Ley N° 25.602 B.O.20/6/2002)

En los casos de los tres incisos precedentes, el culpable, si fuere funcionario o empleado público, sufrirá además inhabilitación especial perpetua.

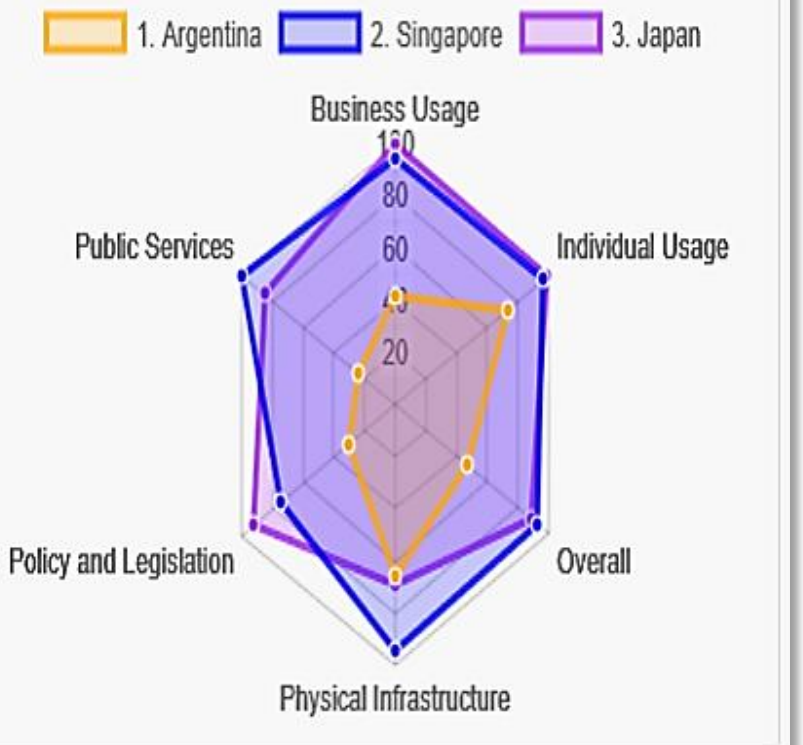
Comparison: composites



Comparison: composites



Comparison: composites



Source GFCE Cybermonitor – agosto 2017

Y a nivel técnico?

Se deben identificar las necesidades de información, lo que debe ser conocido para salvaguardar la nación.

Las necesidades de inteligencia son establecidos por …… de acuerdo con las instrucciones recibidas del …… y los asesores de seguridad nacional.

Los requisitos se desarrollan en base a la información crítica necesaria para proteger a …… de la seguridad nacional y amenazas criminales.

El …… y el ……participan en la formulación de las necesidades del proyecto.

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Es la gestión de todo el esfuerzo, desde la identificación de la necesidad de información para la entrega de un producto de inteligencia a un consumidor.

Se trata de los planes de ejecución para satisfacer los requerimientos impuestos a la ……., así como la identificación de los requisitos específicos de las colecciones basadas en las necesidades del …….

Planificación y dirección también es sensible al final del ciclo, porque la inteligencia actual y finalizada, que soporta la toma de decisiones, genera nuevos requisitos.

El ……. lleva la planificación y la dirección del proyecto para el organismo.

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Es la recopilación de información en bruto sobre la base de requisitos.

Las actividades tales como ……., ……. técnicas y físicas, funcionamiento de la fuente humana, búsquedas y relaciones de enlace dan lugar a la colección de inteligencia

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Es la conversión de la gran cantidad de información recopilada en una forma utilizable por los analistas.

Esto se hace a través de una variedad de métodos, incluyendo el ……, ……. , y la reducción de datos.

El procesamiento incluye la entrada de datos sin procesar en las bases de datos en los que puede ser explotado para su uso en el proceso de análisis.

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Es la conversión de la información en bruto, en inteligencia.

Incluye la integración, evaluación y análisis de los datos disponibles, y la preparación de productos de inteligencia.

La fiabilidad, validez y pertinencia de la información se evalúa y se “pesa”. La información se integra lógicamente, se pone en contexto, y se utiliza para producir la inteligencia.

Esto incluye tanto la inteligencia en bruto como los terminados. La inteligencia en bruto se refiere a menudo como "los puntos" – piezas individuales de información difundida de forma individual.

Los informes de inteligencia terminados son los que "conectan los puntos", poniendo la información en su contexto y proponiendo conclusiones sobre sus implicaciones.

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

El último paso es la distribución de la inteligencia en bruto o finalizada a los consumidores, cuyos requerimientos han iniciado las necesidades de inteligencia.

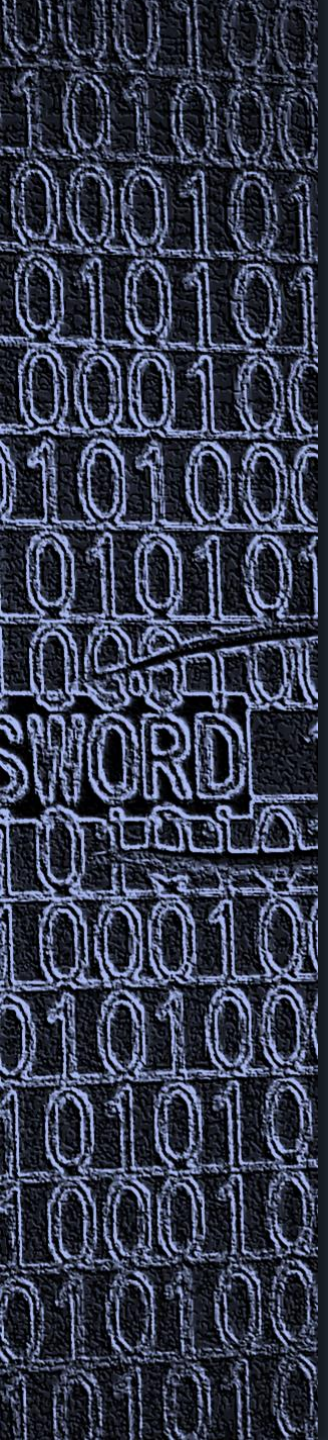
El …… difunde información en tres formatos estándar: Reportes de Información …… , el Boletín de ……., y la Evaluaciones de ……

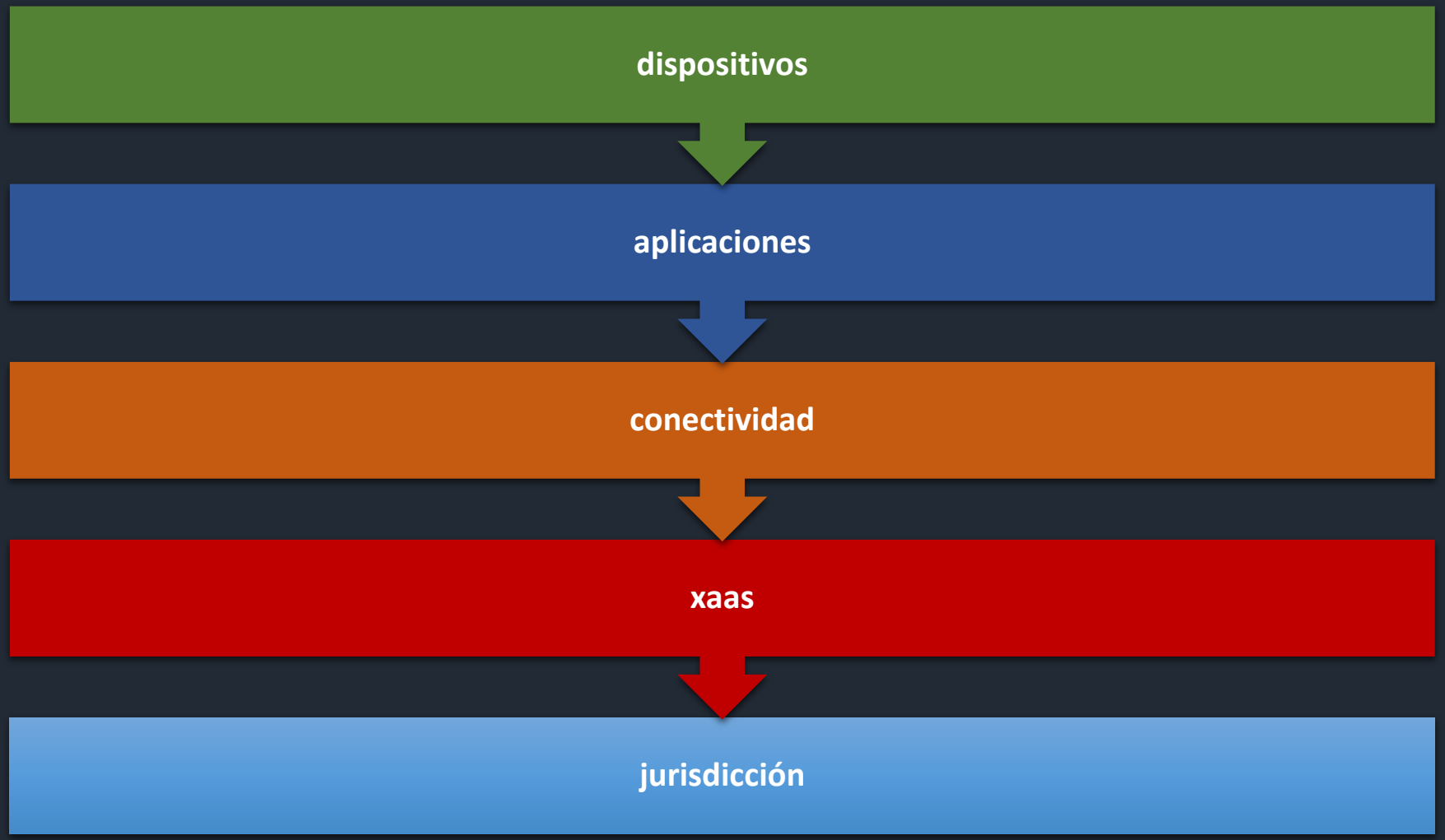
Los productos de inteligencia se proporcionan diariamente al ……., al ……., y para los clientes en todo el …… y en otros departamentos.

Estos clientes de ……. toman decisiones operativas, estratégicas, y políticas basadas en la información. Estas decisiones pueden dar lugar a la exigencia de más requerimientos, continuando así el ciclo de productos.

En base al https://www.fbi.gov/about-us/intelligence/intelligence-cycle

Qué podemos hacer?




dispositivos
aplicaciones
conectividad
xaas
jurisdicción

dispositivos

- Mobile phones, tablets, notebooks, etc
- Almacenamiento (discos ext, pendrives, etc.)
- PC escritorio, servidor, firewall
- Access point, router, switch, repeaters
- Impresoras, scanners
- IoT (cardio, pulseras, TV, etc.)
- Gadgets, Consolas de juego
- GPS, cámaras, drones

dispositivos

Conocemos las opciones de seguridad del equipo?

Documentamos el proceso de update y patchs?

Podemos asegurar quien utilizó/manipuló el dispositivo?

aplicaciones

Sistema operativo

Mensajería instantánea

Redes sociales

Correos corporativos

Correos “gratuitos”

App especificas o boutiques

buscadores

Sanidad?

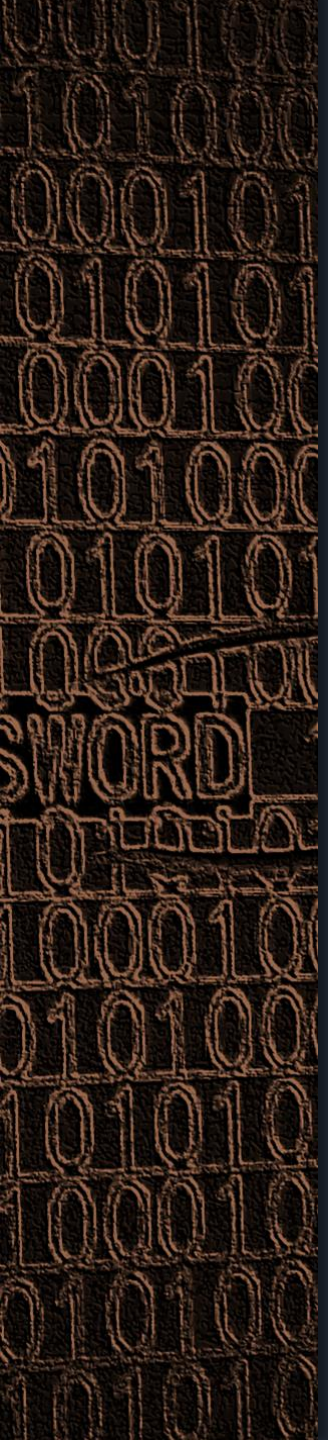
aplicaciones

Conocemos y analizamos la cantidad de datos que se colectan?

Sabemos dónde encontrar esa información?

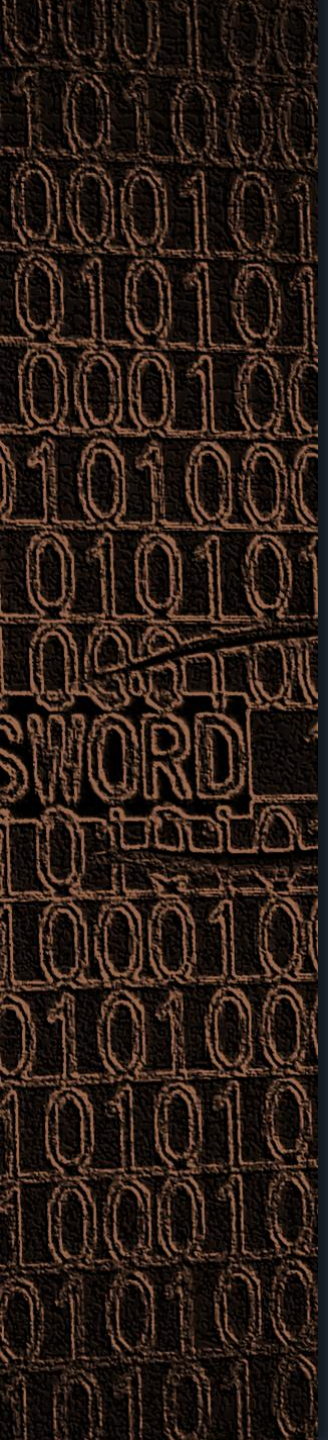
Sabemos cuál es el protocolo de requerimiento?

Y el protocolo de preservación y validación de la evidencia, existe en esa empresa? nos sirve?



conectividad

- Proveedores de Servicio de Internet (1 o +)
- IP (dirección fija/dinámica, IMEI/IMSI, MAC, etc.)
- Tipo de conexiones (TCP, NFC, Bluethooth, etc.)
- Rangos horarios, tipos de dispositivos, rutas, etc
- Cantidad de dispositivos (registro de conexiones)



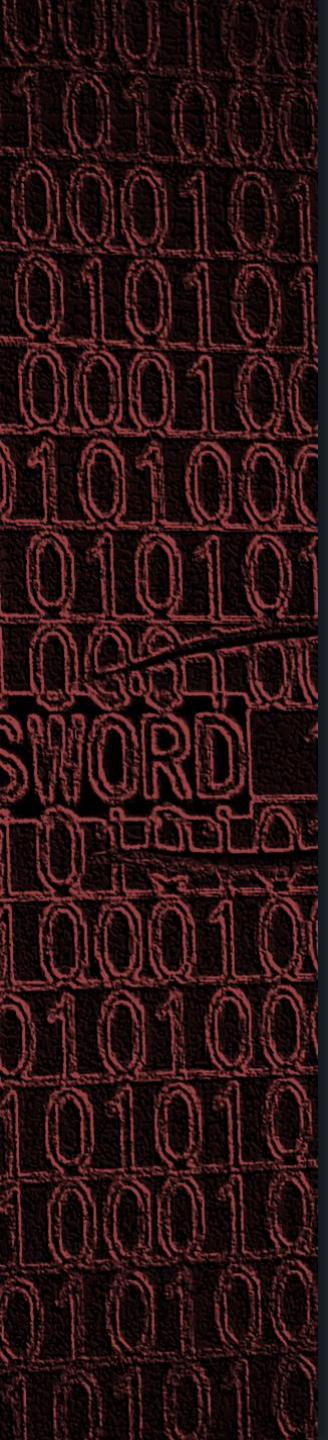
conectividad

Conocemos las políticas de resguardo de datos de los ISP?

Conocemos que datos colectan o pudieren colectar los ISP?

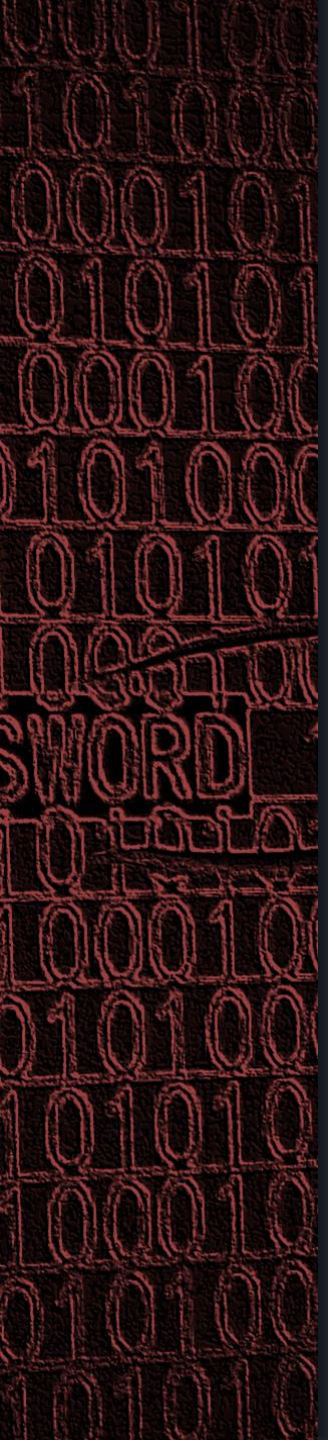
Sabemos donde consultar los IMEI y los IMSI?

Los ISP tienen TODA la información o se les puede escapar/ocultar parte?



xaas

- Infraestructura
- Almacenamiento
- Aplicaciones
- Inteligencia de negocios / Marketing
- Gestión de Identidades



xaas

…no entran todas las preguntas ;)

Qué información tiene el proveedor del servicio y que otra información comparte o delega a terceros que desconocemos y que podrían sernos de utilidad (o punto débil)?

Logs, backups, otros.. Conocemos las políticas y estrategias que tienen productivas y donde podríamos tener mas información?

Ubicación / Jurisdicción

- Nacional
- Acuerdos binacionales
- Otro país
- Acuerdos a través de organizaciones o convenios multinacionales
- Multinacional (varios países, cloud)

Ubicación / Jurisdicción

Qué jurisdicción se aplica?

Es delito en esa jurisdicción?

Cuál es la ley aplicable?

Cuál es el método o proceso de cadena de custodia de la evidencia en esa jurisdicción?

La cantidad de información en cada eslabón es enorme y compleja,
requiere de una capacitación y un entrenamiento constante,
Pero por sobre todo, de la cooperación y acción conjunta
Público - Privado

UNA INTERNET LIBRE ABIERTA Y SEGURA

SOLO LA PODEMOS CONSTRUIR ENTRE TODOS

gracias

STOP | THINK | CONNECT™

RECIA
Red de Ciudades Inteligentes de Argentina

UAI