



Poltergeist en tu edificio

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL







Eduardo Arriols Nuñez

- Red Team Leader en Innotec System
- eduardo_arriols@innotecsystem.com

Evolución de los edificios



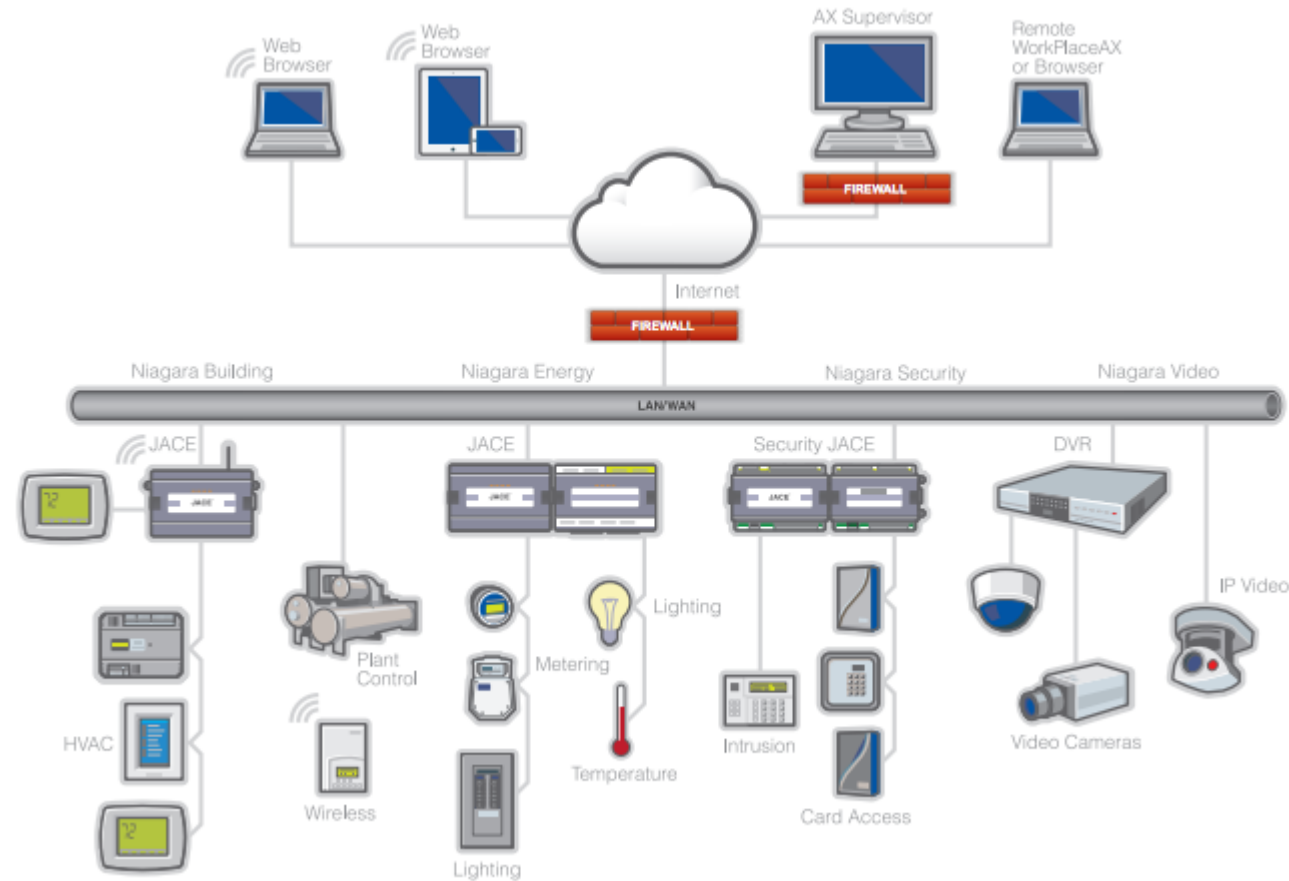
Building Management System (BMS)



Nuestro escenario

Esquema típico de red

Implantadores

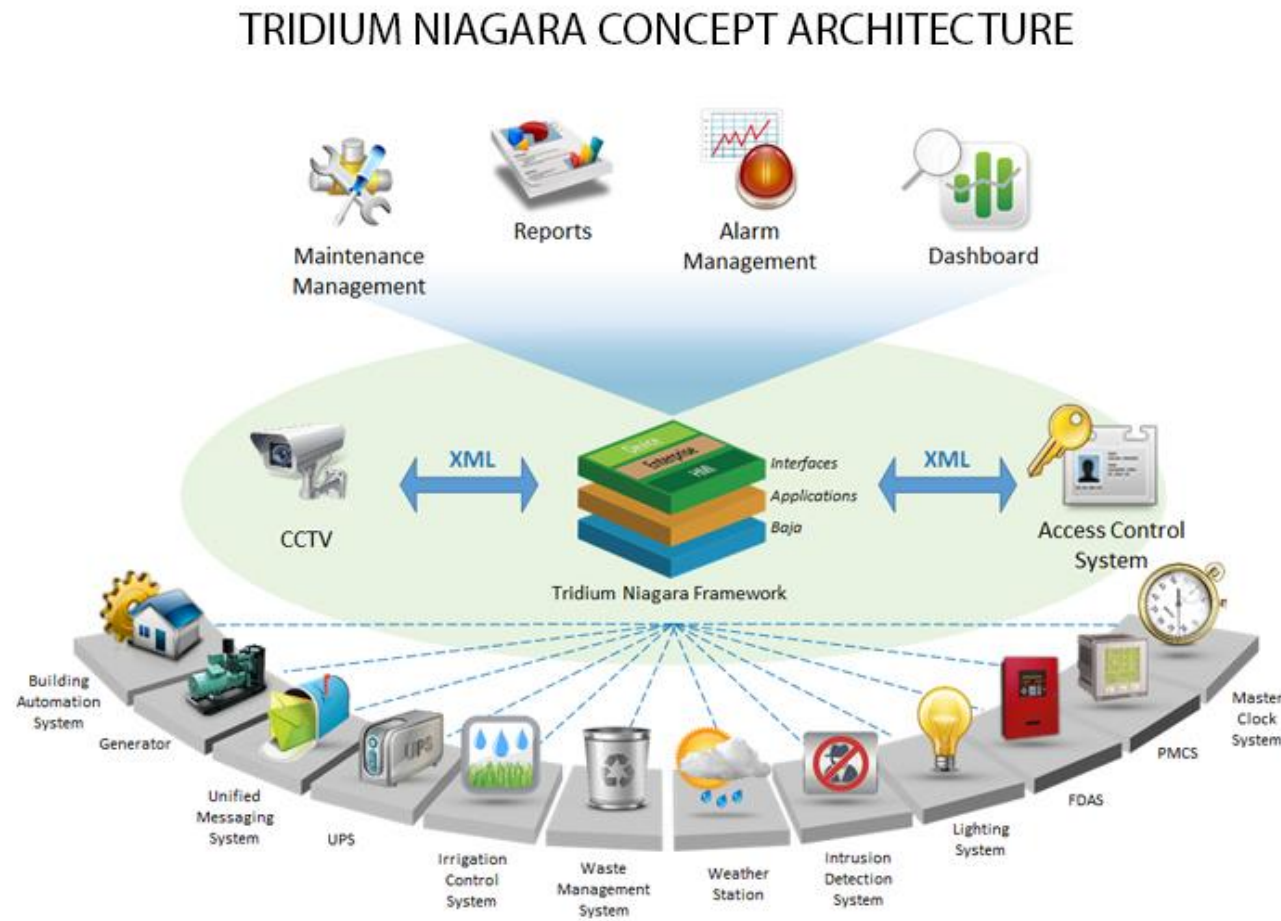


Fabricantes

TRIDIUM
SIEMENS
Honeywell

Sistema afectado

Versiones 1 y 2



1. Identificación de backdoor

Identificación de usuarios por defecto que según la versión de manual aparecían o no en el documento (**backdoor**)

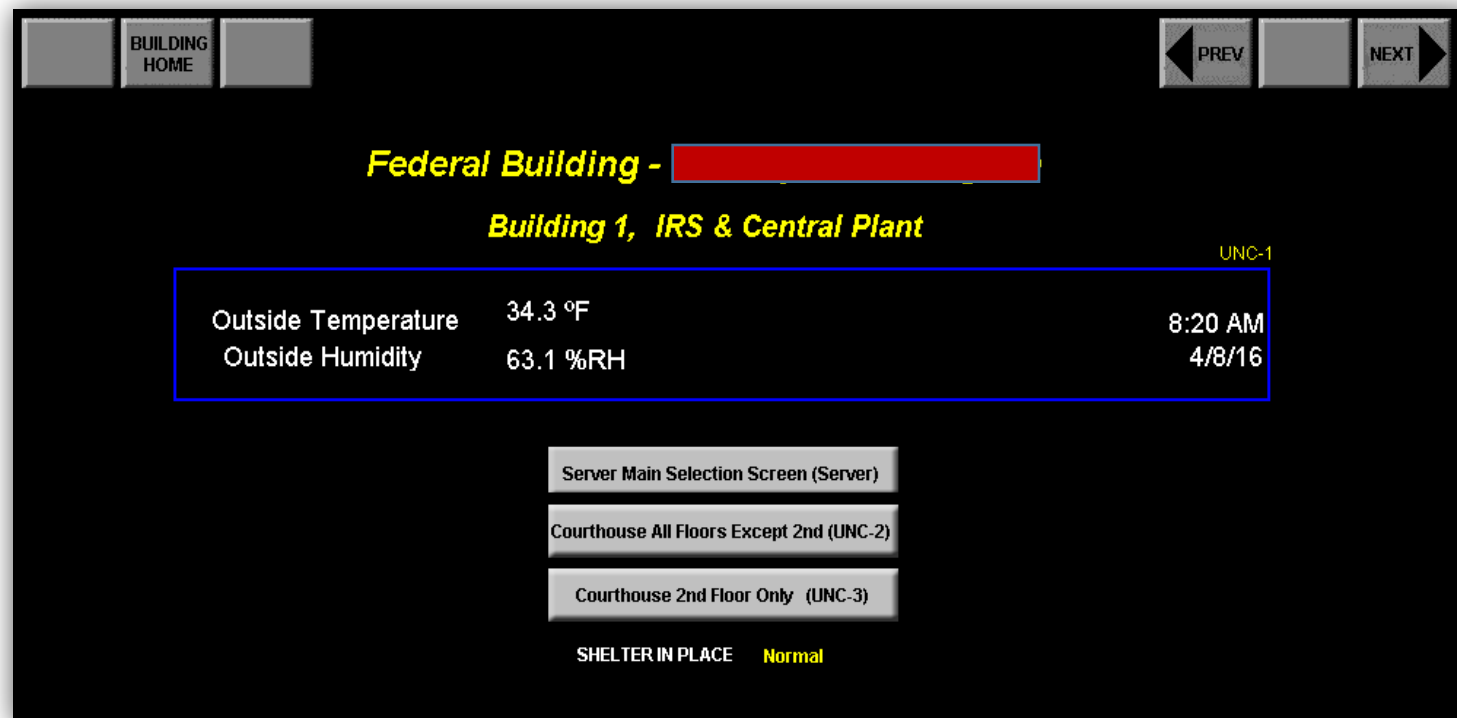
- guest / *****
- test / ****
- demo / ****
- admin / ***** (Directamente administrador)

En versiones mas modernas existen otros usuarios ampliamente utilizados por defecto

- default / *****
- tridium / *****
- ...

2. Acceso con permisos de lectura

Se utiliza el acceso como el usuario identificado que únicamente tiene permisos de lectura. Esto impide la posibilidad de realizar acciones sobre el edificio.



3. Acceso a ficheros de configuración

Se analiza el sistema y se identifica la ruta del archivo de configuración (Existen varios). El usuario tiene **acceso de lectura a los archivos de configuración** donde se encuentran los **usuarios y su contraseña cifrada**.

```
<UserType>
  <userName>    </userName>
  <fullName>    </fullName>
  <workplaceHome>
  </workplaceHome>
  <browserHome>
  [REDACTED]
</browserHome>
<password>210    </password>
<securityMask>
  <mask radix="16">-fffffffff0001</mask>
</securityMask>
<enabled>true</enabled>
<logoffPeriod>0</logoffPeriod>
<userId>1</userId>
<securityAdmin>true</securityAdmin>
</UserType>
```

4. Identificación de librerías [no públicas]

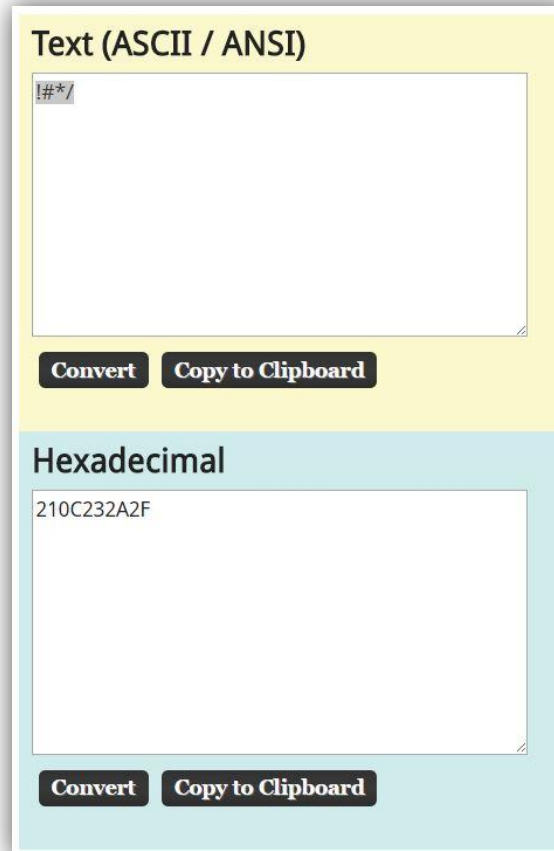
Se identifica el directorio donde se encuentran todas las librerías (no publicas) que utiliza el sistema. Entre las librerías, existe una que contiene funciones para cifrar y descifrar.



Name	Last Modified	Size
acInfini		341.3K
alm-2.30		46.4K
amerAuto		192.1K
andoverA		237.2K
bacnet-2		653.6K
bacnetWS		38.3K
bacxNdic		22.2K
basys-2.		232.2K
coreRunt		2954.2K
coreUi-2		2631.2K
csd-2.30		144.1K
dataAire		210.2K
dde-2.30		77.7K
dms-2.30		496.4K

5. Recuperación de credenciales

Creación de un simple script que haga uso de la librería para descifrar las claves cifradas.



The image shows a web interface for converting between text and hexadecimal. It is divided into two main sections: a yellow section for text and a light blue section for hexadecimal.

Text (ASCII / ANSI)

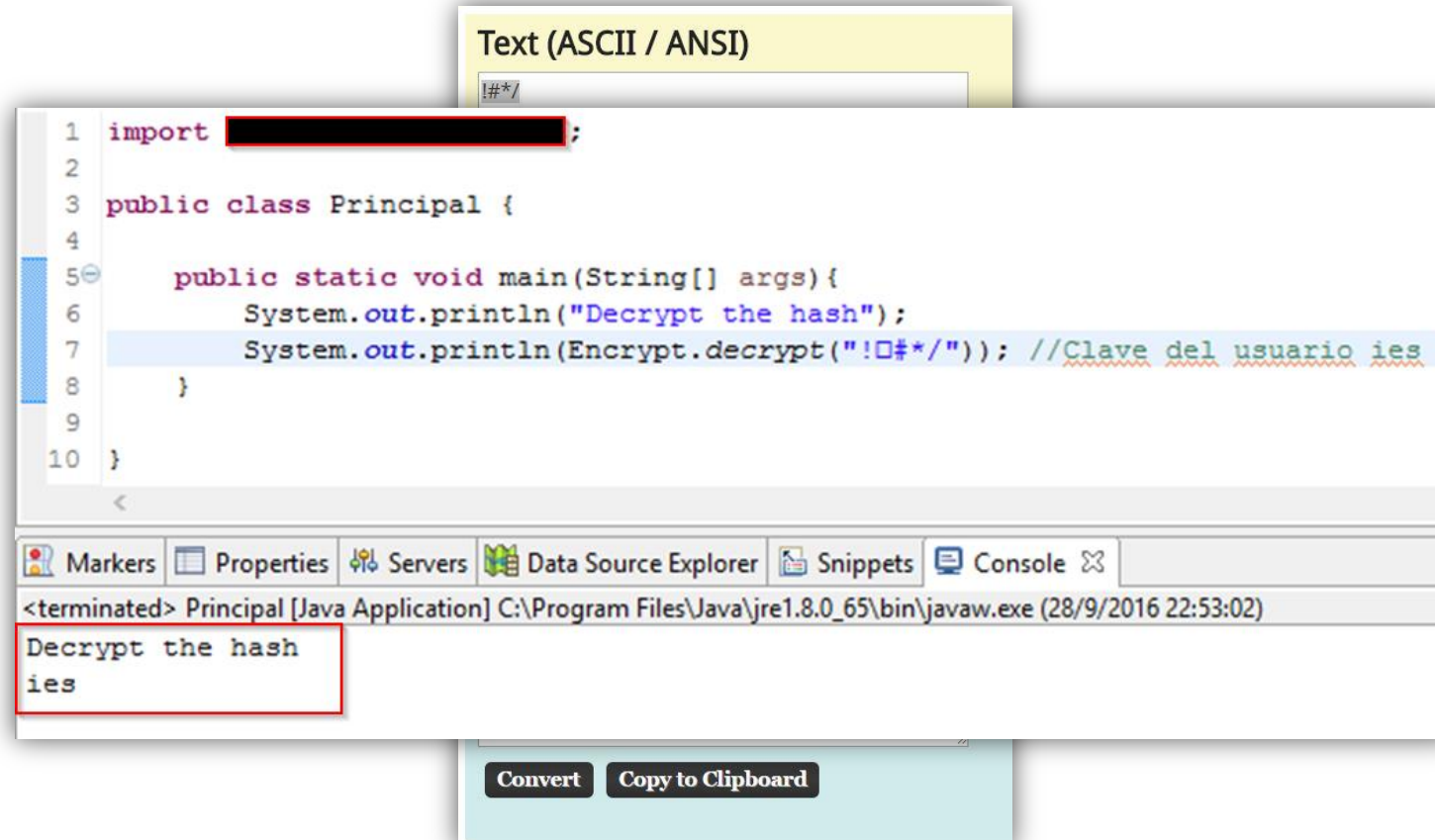
This section contains a text input field with the placeholder text `!@* /`. Below the input field are two buttons: **Convert** and **Copy to Clipboard**.

Hexadecimal

This section contains a hexadecimal input field with the placeholder text `210C232A2F`. Below the input field are two buttons: **Convert** and **Copy to Clipboard**.

5. Recuperación de credenciales

Creación de un simple script que haga uso de la librería para descifrar las claves cifradas.



The screenshot shows a Java IDE with a code editor and a console. The code editor contains the following Java code:

```
1 import [REDACTED];
2
3 public class Principal {
4
5     public static void main(String[] args) {
6         System.out.println("Decrypt the hash");
7         System.out.println(Encrypt.decrypt("![]#*/")); //Clave del usuario ies
8     }
9
10 }
```

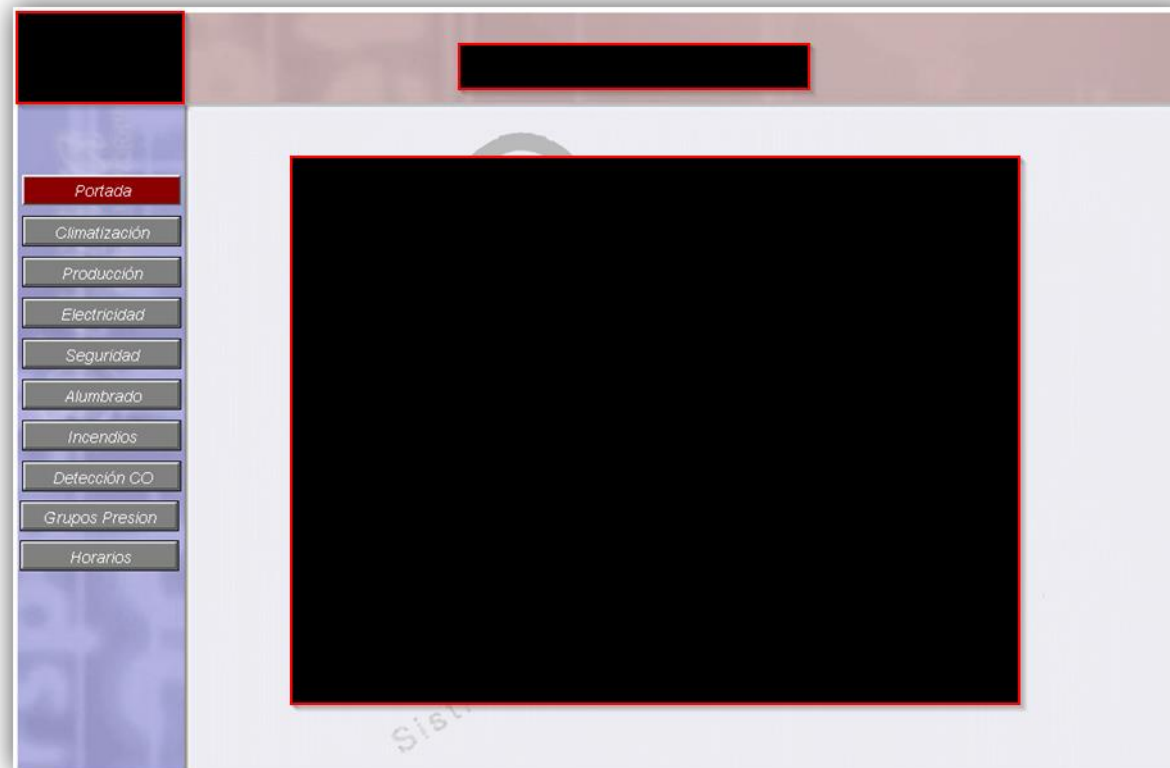
The console output shows the execution of the program:

```
<terminated> Principal [Java Application] C:\Program Files\Java\jre1.8.0_65\bin\javaw.exe (28/9/2016 22:53:02)
Decrypt the hash
ies
```

Below the console, there are two buttons: "Convert" and "Copy to Clipboard".

6. Control total del edificio

Acceso como usuario administrador al sistema BMS Tridium Niagara y control completo del edificio.



Localización de sistemas

The image displays two overlapping screenshots of search engines used for locating systems. The top screenshot is from ZoomEye, showing a search result for a specific IP address. The search type is set to 'Public Devices' and 'Web Services'. The results show 'Found about 28,561 results, 26,757 hosts (0.685 seconds)'. The search type is set to 'specialized'. The results show 'Canada North Vancouver' and 'Sept. 28, 2016'. The port list includes 80, 8080, 81, 443, 82, and 8081. The bottom screenshot is from Shodan, showing a search result for the same IP address. The search type is set to 'specialized'. The results show 'Total results: 1,946'. The results show 'Added on 2016-09-25 13:34:26 GMT' and 'Hong Kong, Central District'. The results show 'Details'.

ZoomEye Search Results:

- Search Type: Public Devices, Web Services
- Found about 28,561 results, 26,757 hosts (0.685 seconds)
- specialized
- Canada North Vancouver
- Sept. 28, 2016
- Port: 80 (21821), 8080 (1934), 81 (1644), 443 (690), 82 (643), 8081 (425)

Shodan Search Results:

- Total results: 1,946
- Added on 2016-09-25 13:34:26 GMT
- Hong Kong, Central District
- Details

Localización de sistemas

ZoomEy

Search Result

Global Vision

Found about 28,561 results, 26,757 hosts (0.685 seconds).

Search Type

Public Devices

Web Services

Port

80

21821

8080

1934

specialized

Canada North Vancouver

Sept. 28, 2016

SHODAN

Exploits

Maps

Share Search

SHODAN

country:"US"

Exploits

Maps

Share Search

Download Results

TOP COUNTRIES

United States

15,729

TOP CITIES

Los Angeles

1,161

South Lake Tahoe

516

San Francisco

386

Phoenix

245

Houston

187

Amazon.com

Added on 2016-09-27 23:55:39 GMT

United States, Ashburn

Details

SHODAN

country:"US"

Exploits

Maps

Share Search

Download Results

TOP COUNTRIES

United States

15,729

TOP CITIES

Los Angeles

1,161

South Lake Tahoe

516

San Francisco

386

Phoenix

245

Houston

187

Amazon.com

Added on 2016-09-27 23:55:39 GMT

United States, Ashburn

Details

Localización de sistemas

ZoomEy

Search Result

Global Vision

Found about 28,561 results, 26,757 hosts (0.685 seconds).

Search Type

Public Devices

Web Services

Port

80

21821

8080

1934

SHODAN

Exploits

Maps

Share Search

Download Results

SHODAN

country:"US"

Exploits

Maps

Share Search

Download Results

TOP COUNTRIES

United States

15,729

San Francisco

Phoenix

Houston

1,161

516

386

245

187

Linux 3.x

Enzu

Added on 2016-09-27 23:56:24 GMT

United States, Los Angeles

Details

HTTP/1.1 400 Bad Request\r\n

Amazon.com

Added on 2016-09-27 23:55:39 GMT

United States, Ashburn

Details

whose Niagara Framework runs an estimated 11 million devices and machines in 52 countries, has, it is

SHODAN

country:"US"

Exploits

Maps

Share Search

Download Results

TOP COUNTRIES

United States

15,729

San Francisco

Phoenix

Houston

1,161

516

386

245

187

Linux 3.x

Enzu

Added on 2016-09-27 23:56:24 GMT

United States, Los Angeles

Details

HTTP/1.1 400 Bad Request\r\n

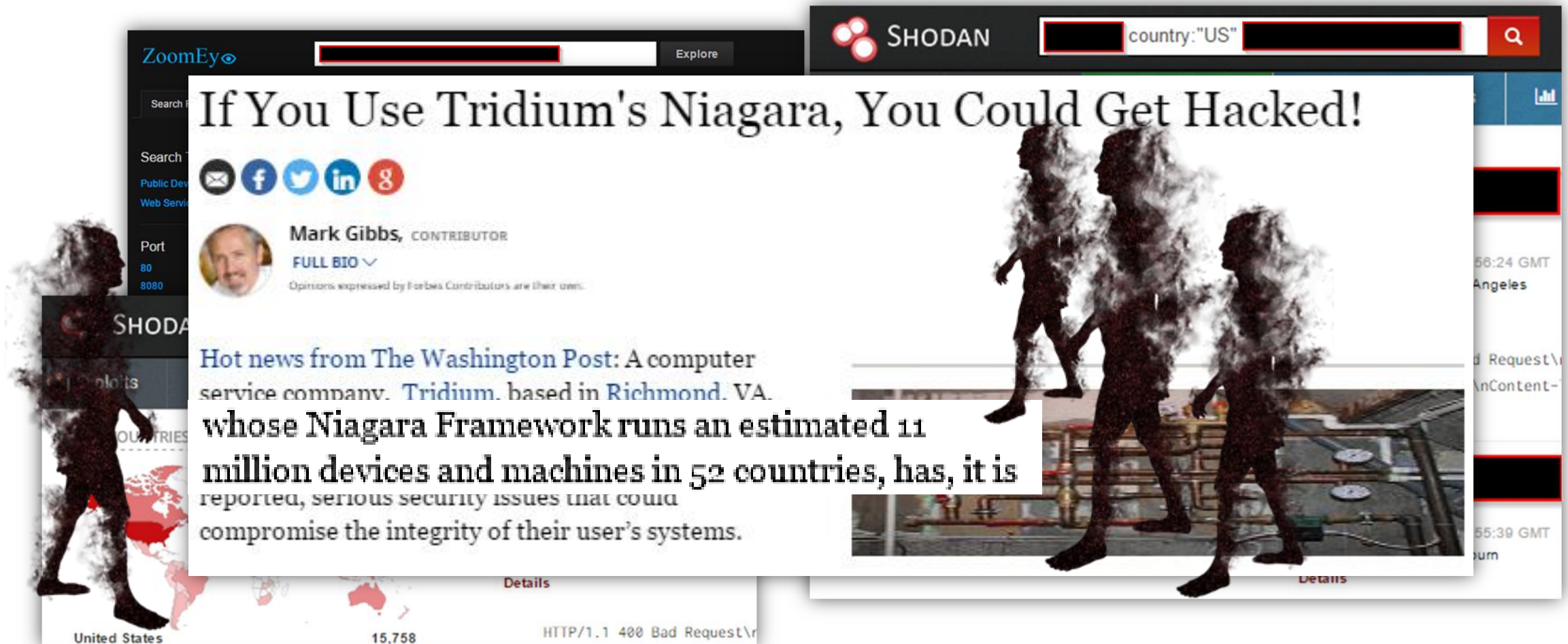
Amazon.com

Added on 2016-09-27 23:55:39 GMT

United States, Ashburn

Details

Localización de sistemas



ZoomEye **Explore**

SHODAN

If You Use Tridium's Niagara, You Could Get Hacked!

 **Mark Gibbs**, CONTRIBUTOR
[FULL BIO](#) 
Opinions expressed by Forbes Contributors are their own.

Hot news from The Washington Post: A computer service company, **Tridium**, based in **Richmond, VA**, whose Niagara Framework runs an estimated **11 million devices and machines in 52 countries**, has, it is reported, serious security issues that could compromise the integrity of their user's systems.

[Details](#)

SHODAN

United States 15,758 HTTP/1.1 400 Bad Request\r

56:24 GMT
Angeles

55:39 GMT
urn

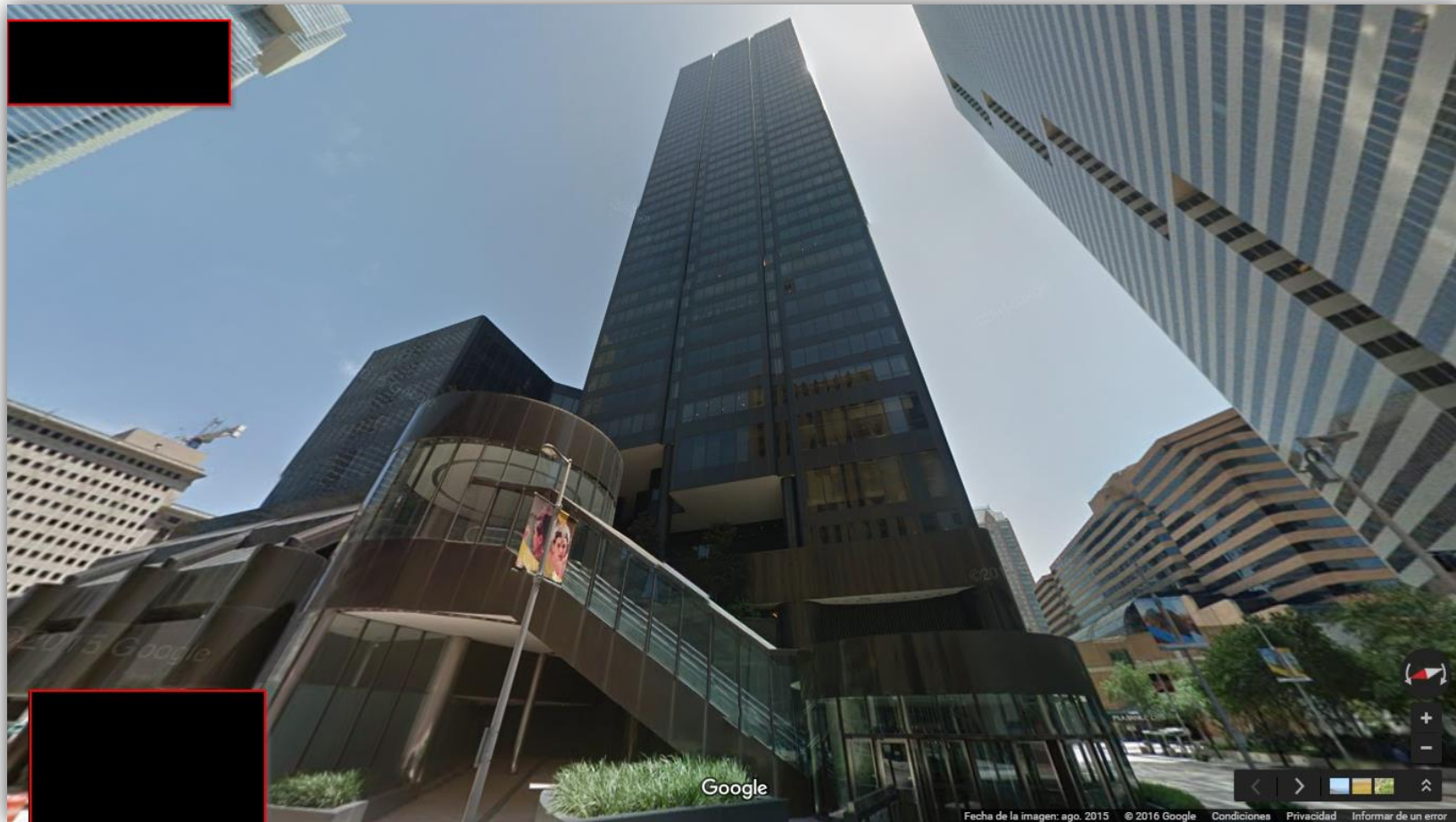
Edificios afectados

Empresas privadas



Edificios afectados

Entidades bancarias



Entornos industriales



Portada

Produccion

Calor

Frio

ACS

Climatizacion

CL-1

CL-2

Extraccion

Extraccion

Electricidad

Sotano-2

Sotano-1

Semiosotano

Planta

Terraza

C.T.

Alumbrado

Sotano-2

Sotano-1

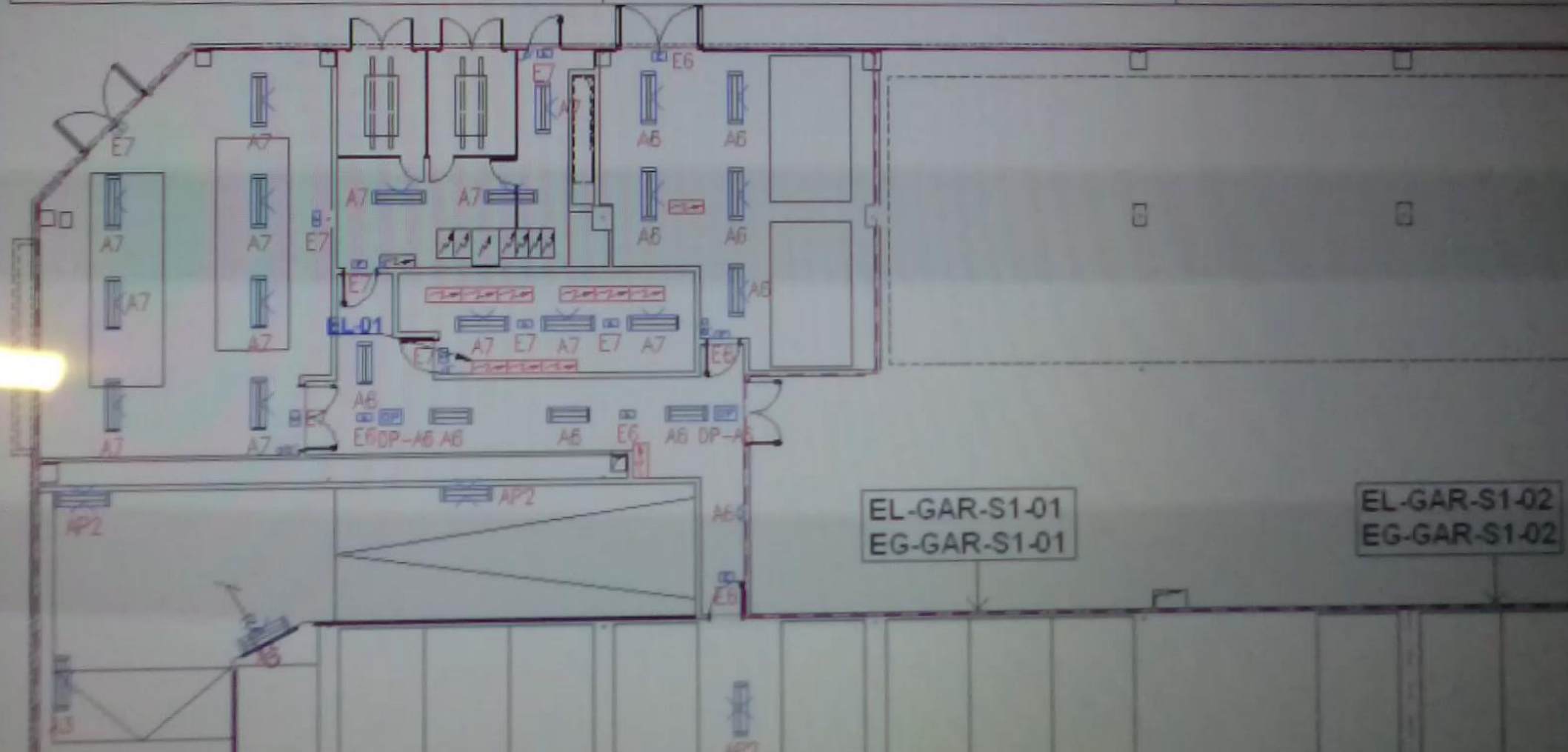
Semiosotano

Planta Baja

Terraza

Grupos De Presion

1 CTO: A1, A2, A3 (S1-01)		H: 3	5 CTO: AP1, AP2 (S1-01)		H: 3	9 CTO: A4 (S1-02)	
2 CTO: A5 (S1-01)		H: 10	6 CTO: AP3 (S1-01)		H: 10	10 CTO: A6 (S1-02)	
3 CTO: A6 (S1-01)		H: 10	7 CTO: AE1 (S1-01)		H: 5	11 CTO: AP1, AP2 (S1-02)	
4 CTO: A4 (S1-01)		H: 3	8 CTO: A1, A2, A3 (S1-02)		H: 3	12 CTO: AP3 (S1-02)	



Otros fenómenos paranormales

Alteración de señales



Database Index

ALERT.ALERTHISTORY	text/comma-se
ALERT.UNACKEDALERTS	text/comma-se
APP.MYDATA	text/comma-se
ARCHIVE.	AHU1 VAV BOXES ROOM 123 DAT
ARCHIVE.	AHU1 VAV BOXES ROOM 123 DAT
ARCHIVE.	AHU2 VAV BOXES ROOM 206 DAT
ARCHIVE.	AHU2 VAV BOXES ROOM 216A DAT
ARCHIVE.	AHU3 VAV BOXES ROOM E104K DAT
ARCHIVE.	AHU3 VAV BOXES ROOM E105M DAT
ARCHIVE.	AHU3 VAV BOXES ROOM E202B DAT
ARCHIVE.	AHU 1 DATA BLDGPRESS
ARCHIVE.	AHU 1 DATA CGVLV
ARCHIVE.	AHU 1 DATA DAFLO

Data

TSTAMP	VALUE	STATUS
11:00:01 19-Feb-2009 America/New York	125.119995	{ok}
10:45:01 19-Feb-2009 America/New York	127.18	{ok}
10:30:01 19-Feb-2009 America/New York	128.4	{ok}
10:15:01 19-Feb-2009 America/New York	123.54	{ok}
10:00:01 19-Feb-2009 America/New York	124.369995	{ok}
9:45:01 19-Feb-2009 America/New York	124.21999	{ok}
9:30:01 19-Feb-2009 America/New York	124.43	{ok}
9:15:01 19-Feb-2009 America/New York	131.23999	{ok}
9:00:01 19-Feb-2009 America/New York	123.61	{ok}
8:45:01 19-Feb-2009 America/New York	122.52	{ok}
8:30:01 19-Feb-2009 America/New York	122.0	{ok}
8:15:01 19-Feb-2009 America/New York	121.399994	{ok}
8:00:01 19-Feb-2009 America/New York	128.04	{ok}
7:45:01 19-Feb-2009 America/New York	115.439995	{ok}

Application Database Query

SQL Query

select * from ?

MIME Type

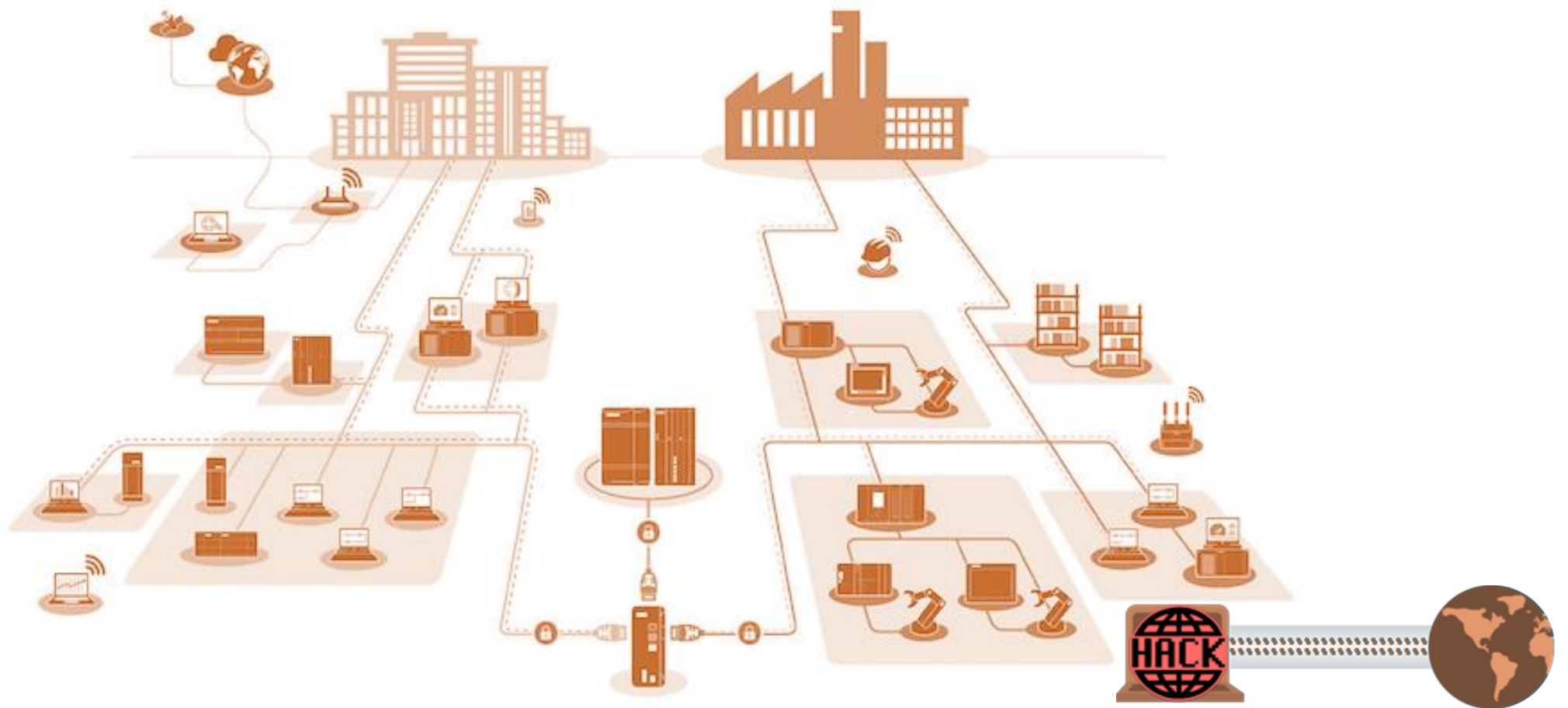
text/html

Execute

Reset

Otros fenómenos paranormales

Compromiso de redes internas



Otros fenómenos paranormales

Acceso a sistemas NO vulnerables

Schneider
Electric™

Honeywell

TRIDIUM

SIEMENS



Acciones coordinadas





DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL