How to prepare your renewable energy assets for the new cybersecurity threats

29 October 2020

Global technology provider

More efficient and profitable renewable energy plants

Making the most of energy

Advanced technology for monitoring, control, and management of renewable assets

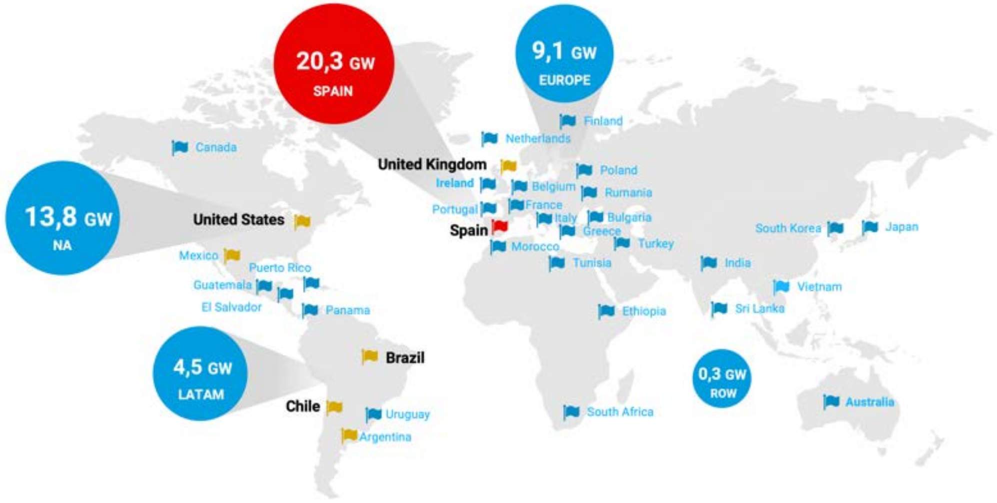
Renewables

Trading

Grid Integration

✓ + 45 Gigawatts

GLENNMONT PARTNERS	PleniumPartners	EDF	Naturgy	enel Green Power	acciona	RED ELÉCTRICA DE ESPAÑA
saetayield	FRV	GRUPOMEXICO	IBERDROLA	edp	enel	viesgo
Genneia	elawan energy	AES	finerge	Southern Company		Brookfield



Are we safe?

About ICS

Industrial control systems are essential to the operation of various critical infrastructure. These systems are now becoming increasingly more networked and remotely accessible as organizations transform to meet the digital age. This development potentially exposes industrial control systems to digital threats as never before.

New age…

Since COVID-19, with a world-wide exodus of people in remote work, remote connections are intensively used.

…new threats

This implies that cybercrime is increasing its skills in accessing remote locations, for instance power generation facilities.

Threats

Trojan horse

Viruses

DoS

Espionage

Malware

Spoofing

Session hijacking

Worms

Man in the Middle

Main renewable energy threats and risks

Phishing

The act of sending email that falsely claims to be from a legitimate organization.

Social Engineering

The act of exploiting human weaknesses to gain access to personal information and protected systems.

Ransomware

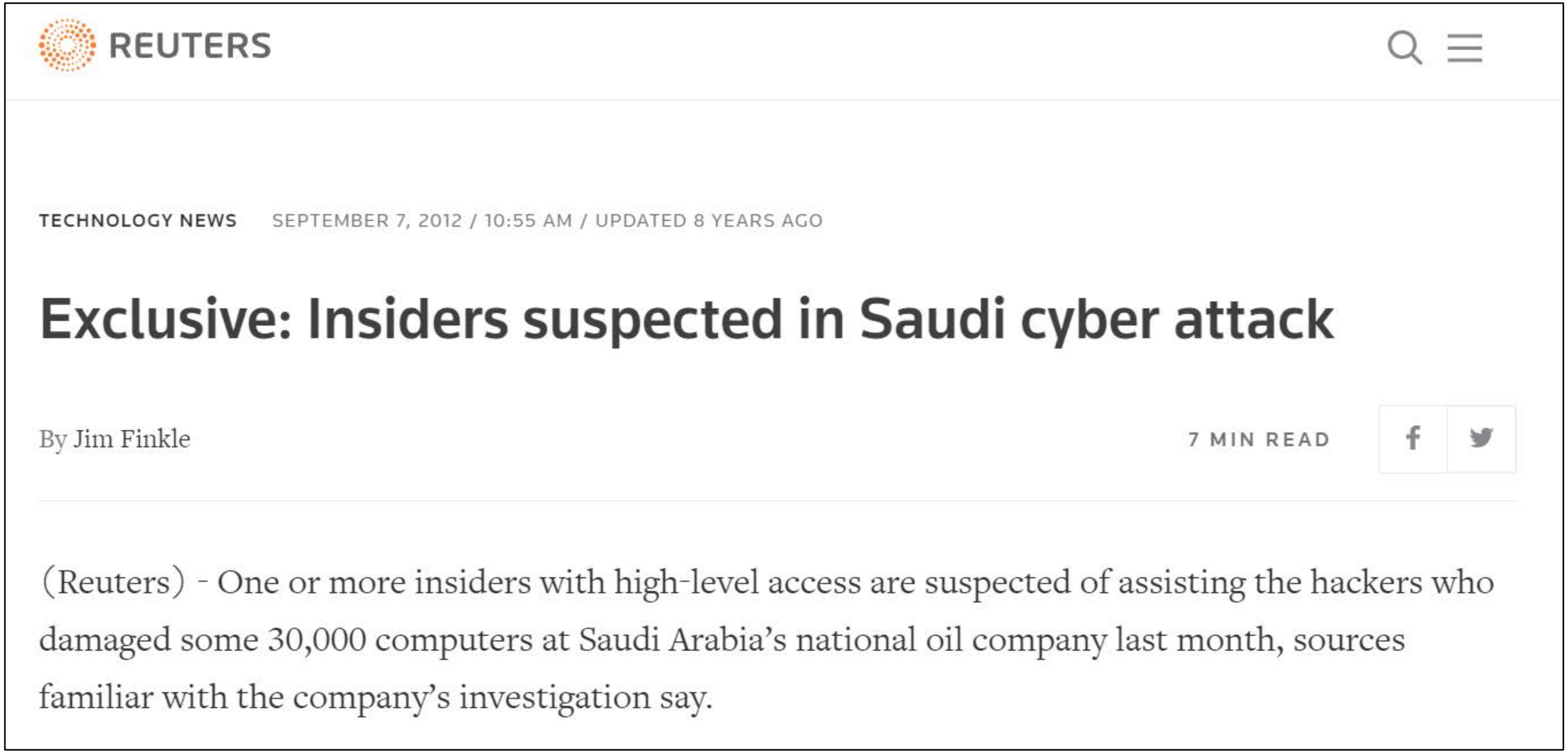
Is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Unpatched devices

An unpatched device has well known vulnerabilities that can be exploited on the wild.

Advanced Persistence Threats (APT)

A stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer or network and remains undetected for an extended period.



REUTERS

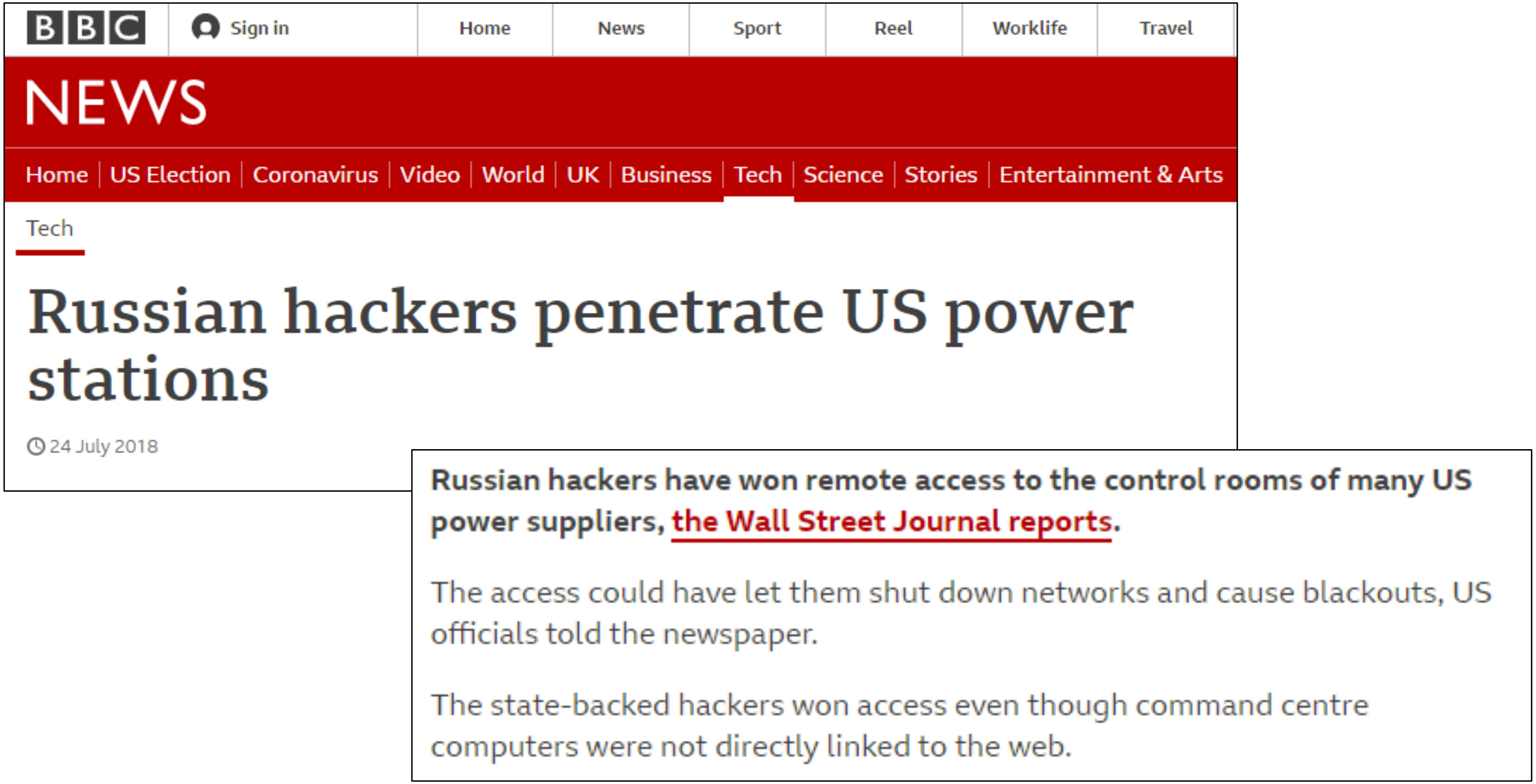
TECHNOLOGY NEWS SEPTEMBER 7, 2012 / 10:55 AM / UPDATED 8 YEARS AGO

Exclusive: Insiders suspected in Saudi cyber attack

By Jim Finkle

7 MIN READ

(Reuters) - One or more insiders with high-level access are suspected of assisting the hackers who damaged some 30,000 computers at Saudi Arabia's national oil company last month, sources familiar with the company's investigation say.


BBC
Sign in
Home
News
Sport
Reel
Worklife
Travel
NEWS
Home | US Election | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts
Tech

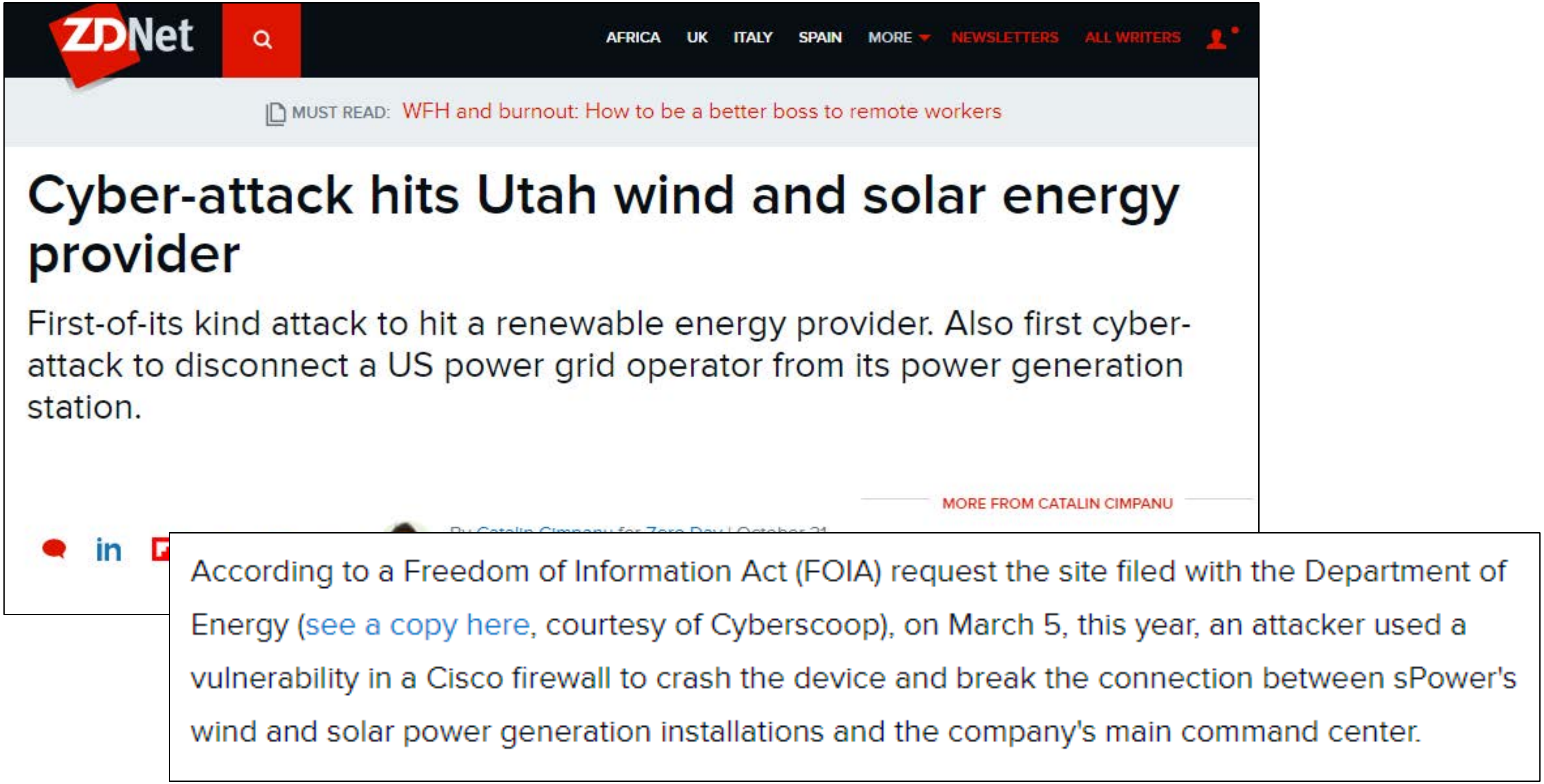
Russian hackers penetrate US power stations

24 July 2018

Russian hackers have won remote access to the control rooms of many US power suppliers, the Wall Street Journal reports.

The access could have let them shut down networks and cause blackouts, US officials told the newspaper.

The state-backed hackers won access even though command centre computers were not directly linked to the web.



MUST READ: WFH and burnout: How to be a better boss to remote workers

Cyber-attack hits Utah wind and solar energy provider

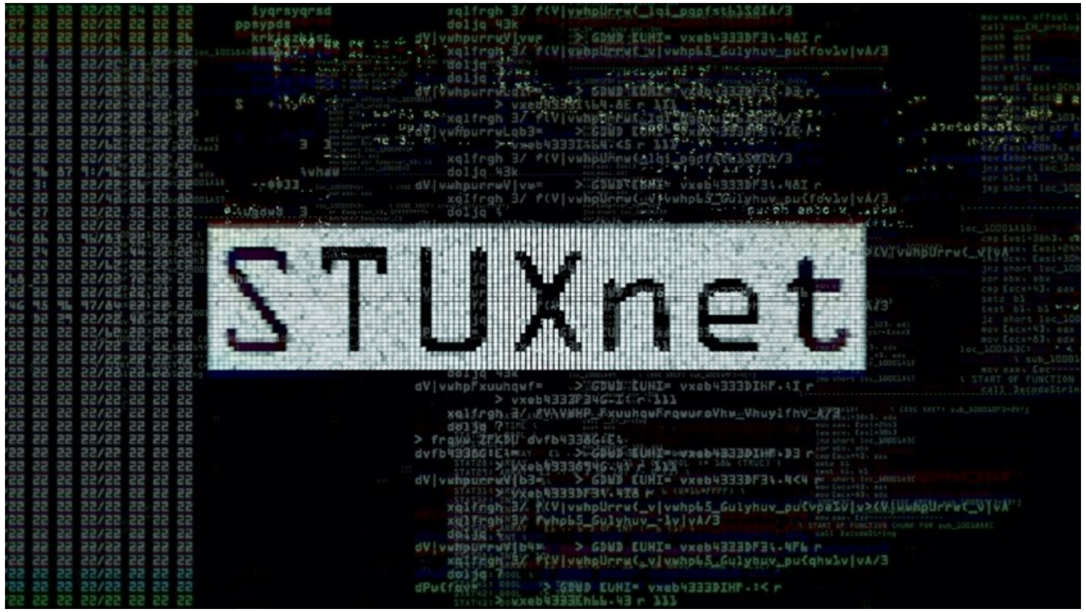
First-of-its kind attack to hit a renewable energy provider. Also first cyber-attack to disconnect a US power grid operator from its power generation station.

MORE FROM CATALIN CIMPANU

By Catalin Cimpanu for Zero Day | October 31

According to a Freedom of Information Act (FOIA) request the site filed with the Department of Energy (see a copy here, courtesy of Cyberscoop), on March 5, this year, an attacker used a vulnerability in a Cisco firewall to crash the device and break the connection between sPower's wind and solar power generation installations and the company's main command center.

STUXnet



It is a malicious computer worm, first uncovered in 2010, thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran. Although no country has openly admitted responsibility, the worm is widely understood to be a cyberweapon built jointly by the United States and Israel (source: Wikipedia).

SHODAN

The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

The search engine for Security

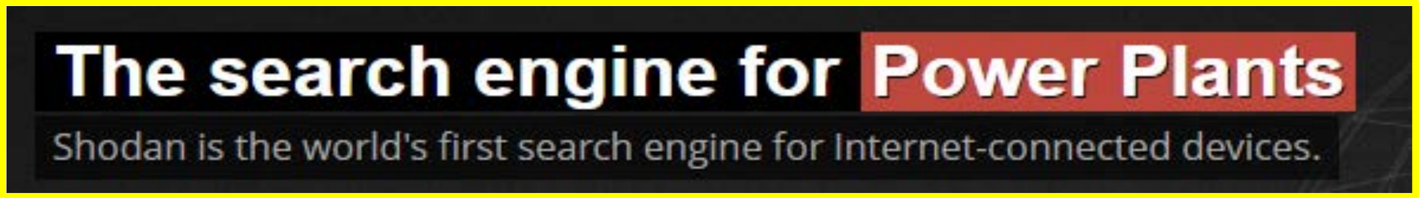
Shodan is the world's first search engine for Internet-connected devices.

The search engine for Refrigerators

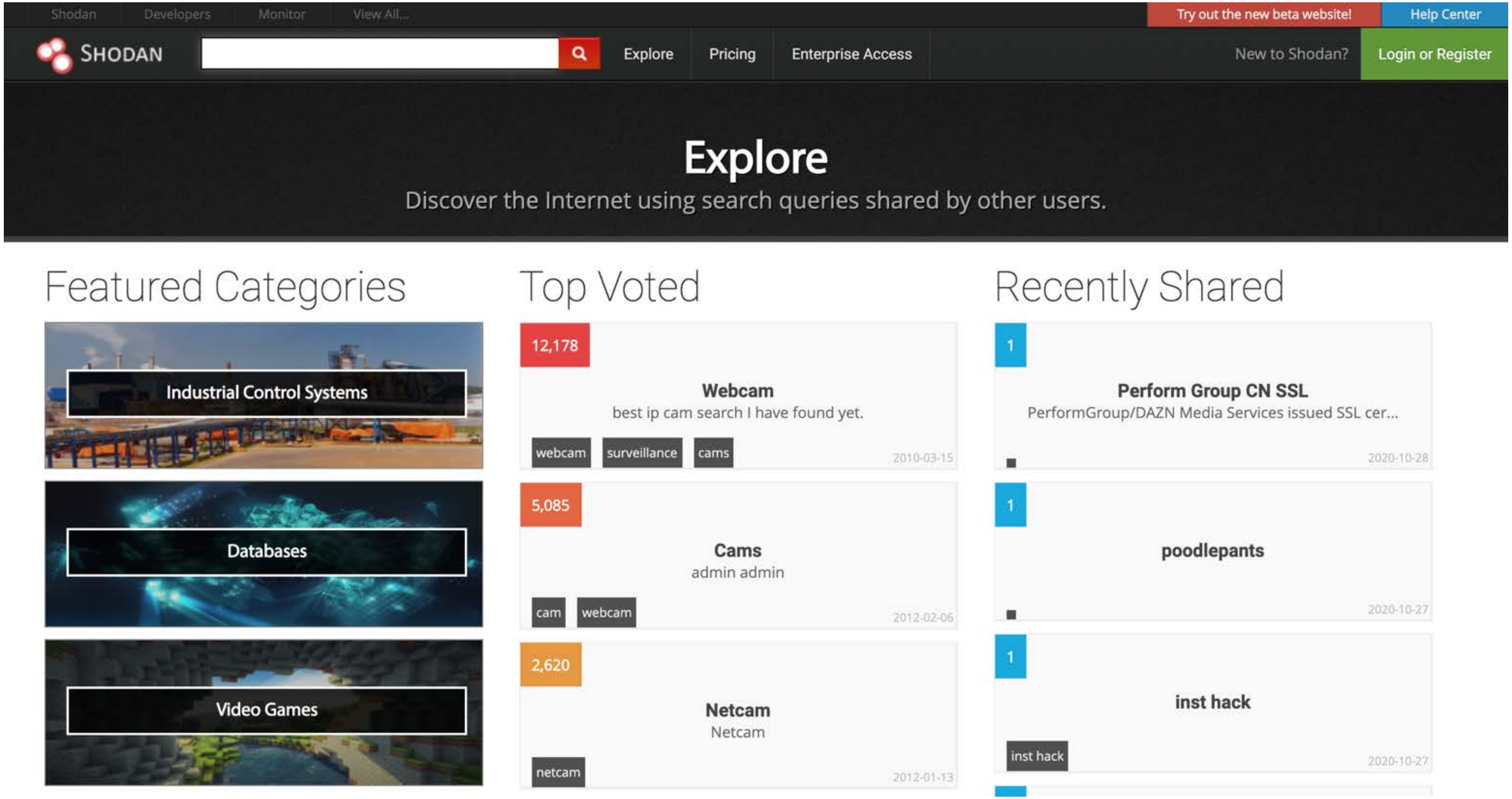
Shodan is the world's first search engine for Internet-connected devices.

The search engine for Buildings

Shodan is the world's first search engine for Internet-connected devices.


The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.



Shodan | Developers | Monitor | View All...

Try out the new beta website! | Help Center

SHODAN | Explore | Pricing | Enterprise Access | New to Shodan? | Login or Register

Explore

Discover the Internet using search queries shared by other users.

Featured Categories

Industrial Control Systems

Databases

Video Games

Top Voted

12,178
Webcam
best ip cam search I have found yet.
webcam | surveillance | cams
2010-03-15

5,085
Cams
admin admin
cam | webcam
2012-02-06

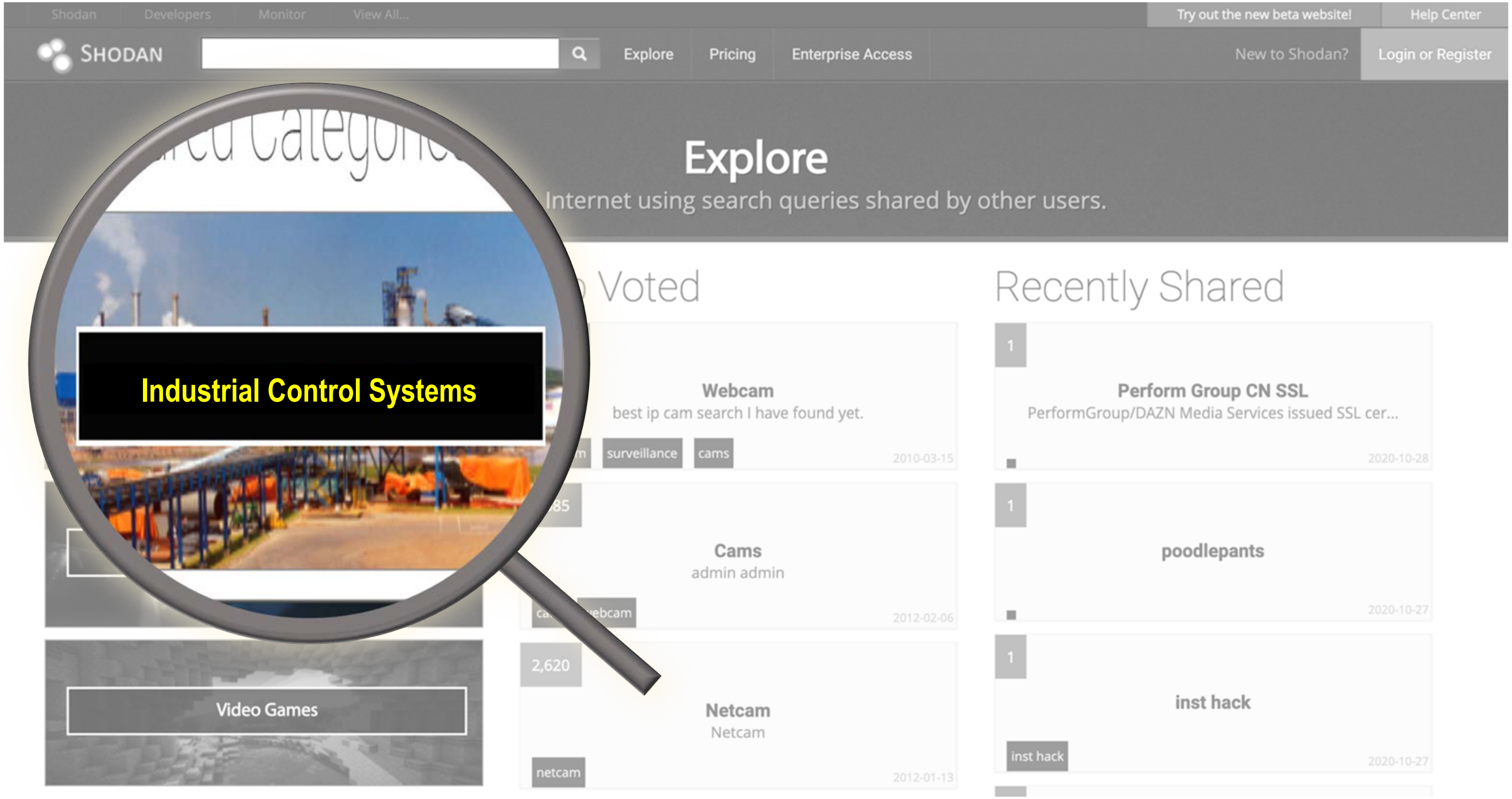
2,620
Netcam
Netcam
netcam
2012-01-13

Recently Shared

1
Perform Group CN SSL
PerformGroup/DAZN Media Services issued SSL cer...
2020-10-28

1
poodlepants
2020-10-27

1
inst hack
inst hack
2020-10-27



Explore

Internet using search queries shared by other users.

red Categorie

Industrial Control Systems

Video Games

Voted

Webcam
best ip cam search I have found yet.
m surveillance cams
2010-03-15

85
Cams
admin admin
ca webcam
2012-02-06

2,620
Netcam
Netcam
netcam
2012-01-13

Recently Shared

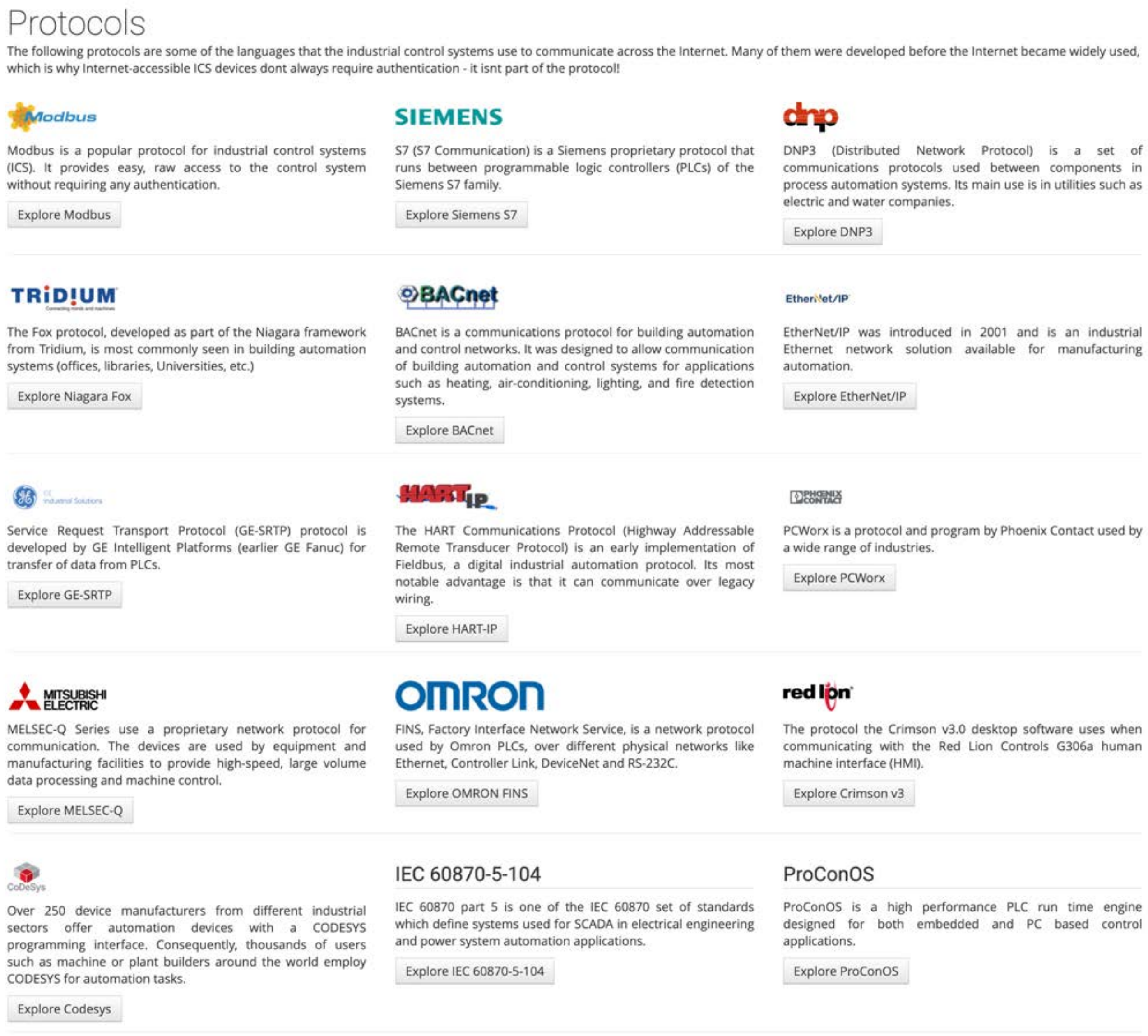
1
Perform Group CN SSL
PerformGroup/DAZN Media Services issued SSL cer...
2020-10-28

1
poodlepants
2020-10-27

1
inst hack
inst hack
2020-10-27

SHODAN

What we'll find in here?



Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices dont always require authentication - it isnt part of the protocol!

Modbus

Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

Explore Modbus

SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

dnp

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

TRIDIUM

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

Explore Niagara Fox

BACnet

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

Explore BACnet

EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

Explore GE-SRTP

HART IP

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

Explore HART-IP

PHOENIX CONTACT

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

Explore PCWorx

MITSUBISHI ELECTRIC

MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

Explore MELSEC-Q

OMRON

FINS, Factory Interface Network Service, is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

Explore OMRON FINS

red lion

The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G306a human machine interface (HMI).

Explore Crimson v3

CoDeSys

Over 250 device manufacturers from different industrial sectors offer automation devices with a CODESYS programming interface. Consequently, thousands of users such as machine or plant builders around the world employ CODESYS for automation tasks.

Explore Codesys

IEC 60870-5-104

IEC 60870 part 5 is one of the IEC 60870 set of standards which define systems used for SCADA in electrical engineering and power system automation applications.

Explore IEC 60870-5-104

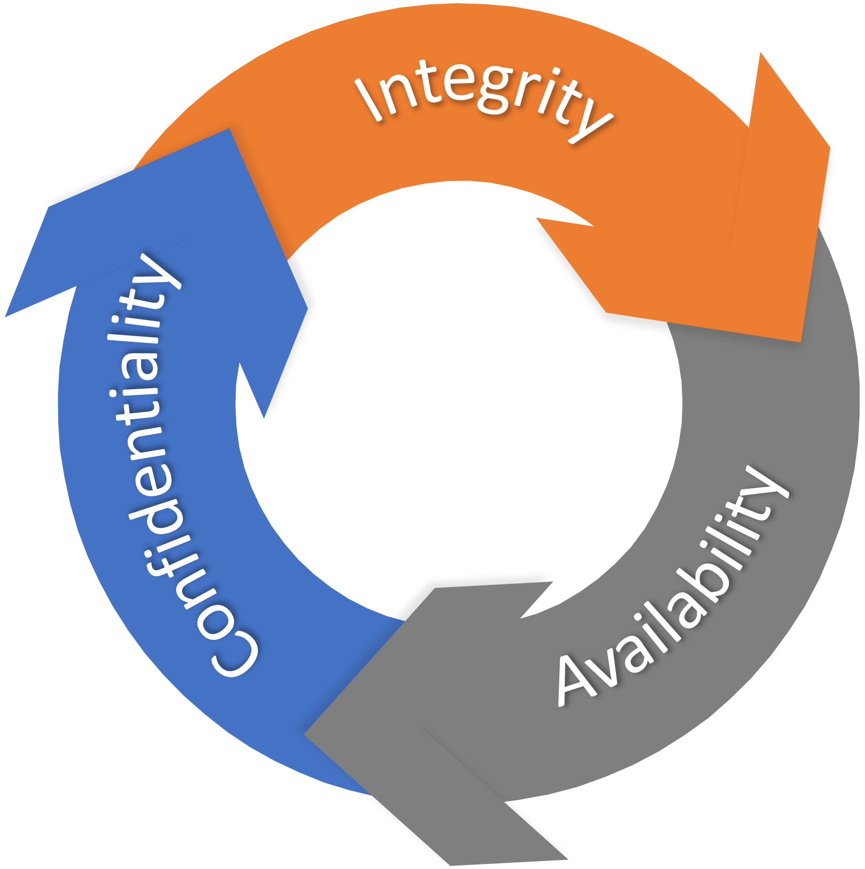
ProConOS

ProConOS is a high performance PLC run time engine designed for both embedded and PC based control applications.

Explore ProConOS

The CIA Security triangle

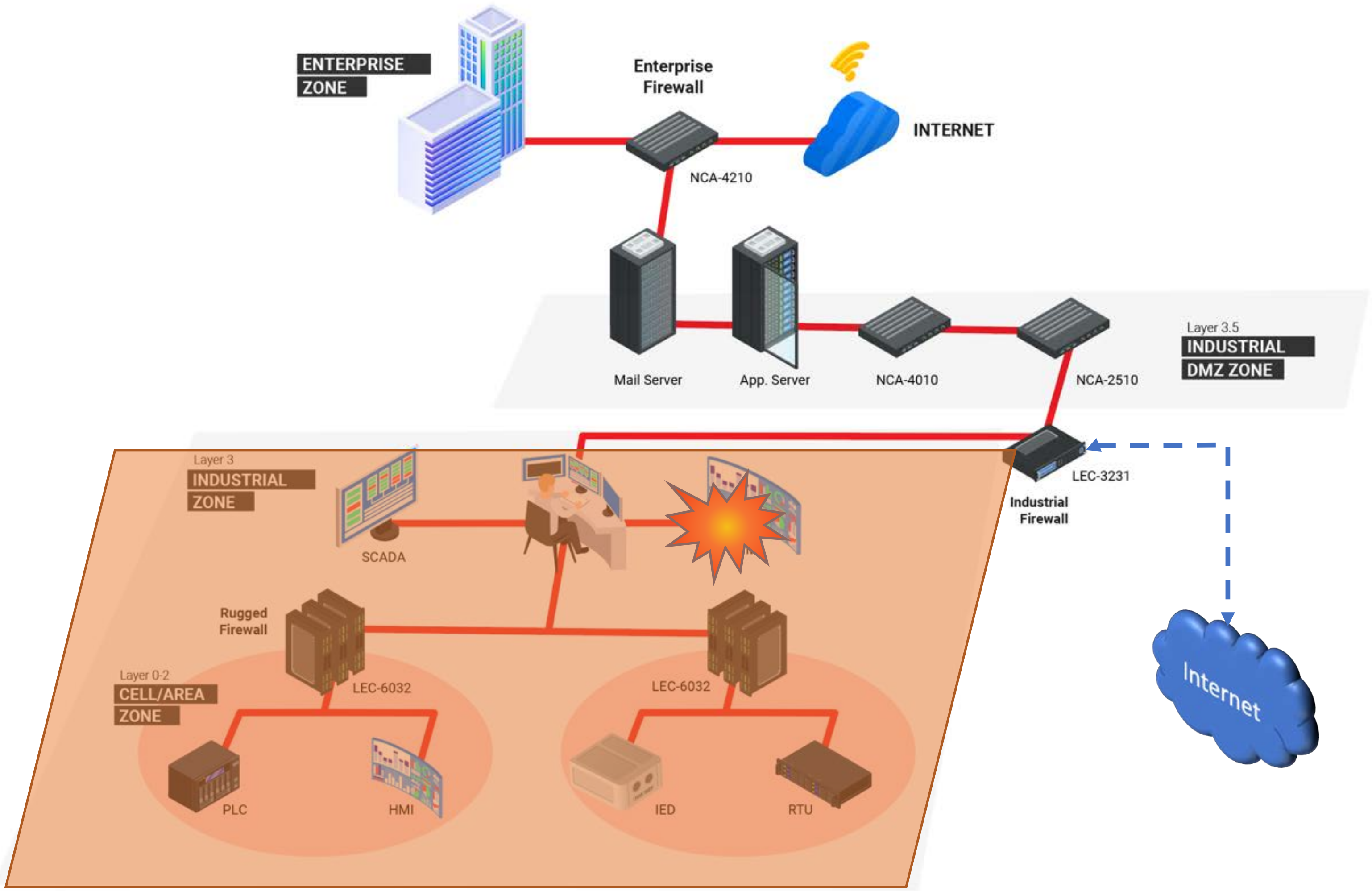
The accuracy and completeness
of data. No unauthorized changes.



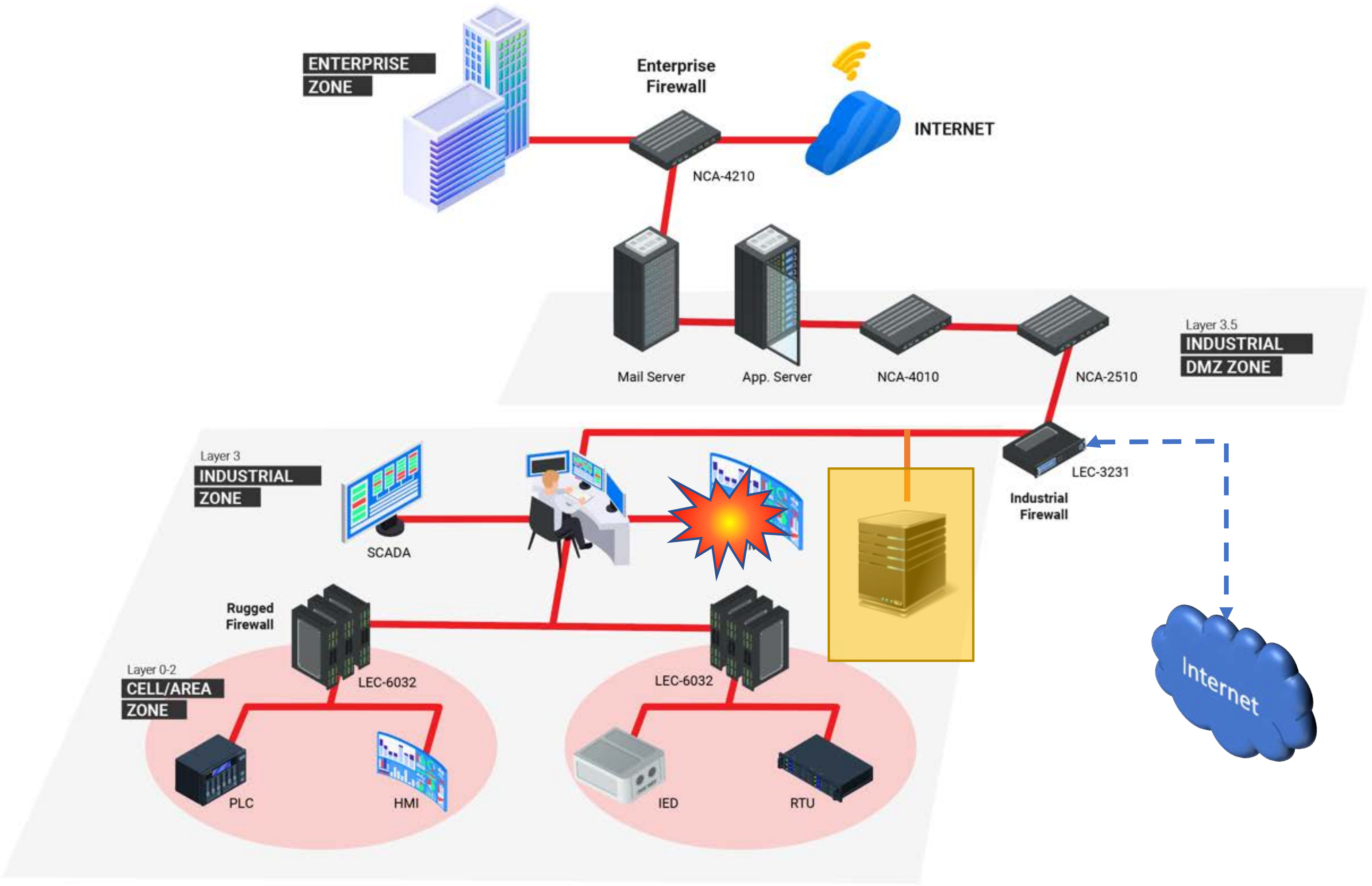
Protect the information
from being exposed to
an unauthorized party

The information is accessible
to authorized users in the
moment it is needed.

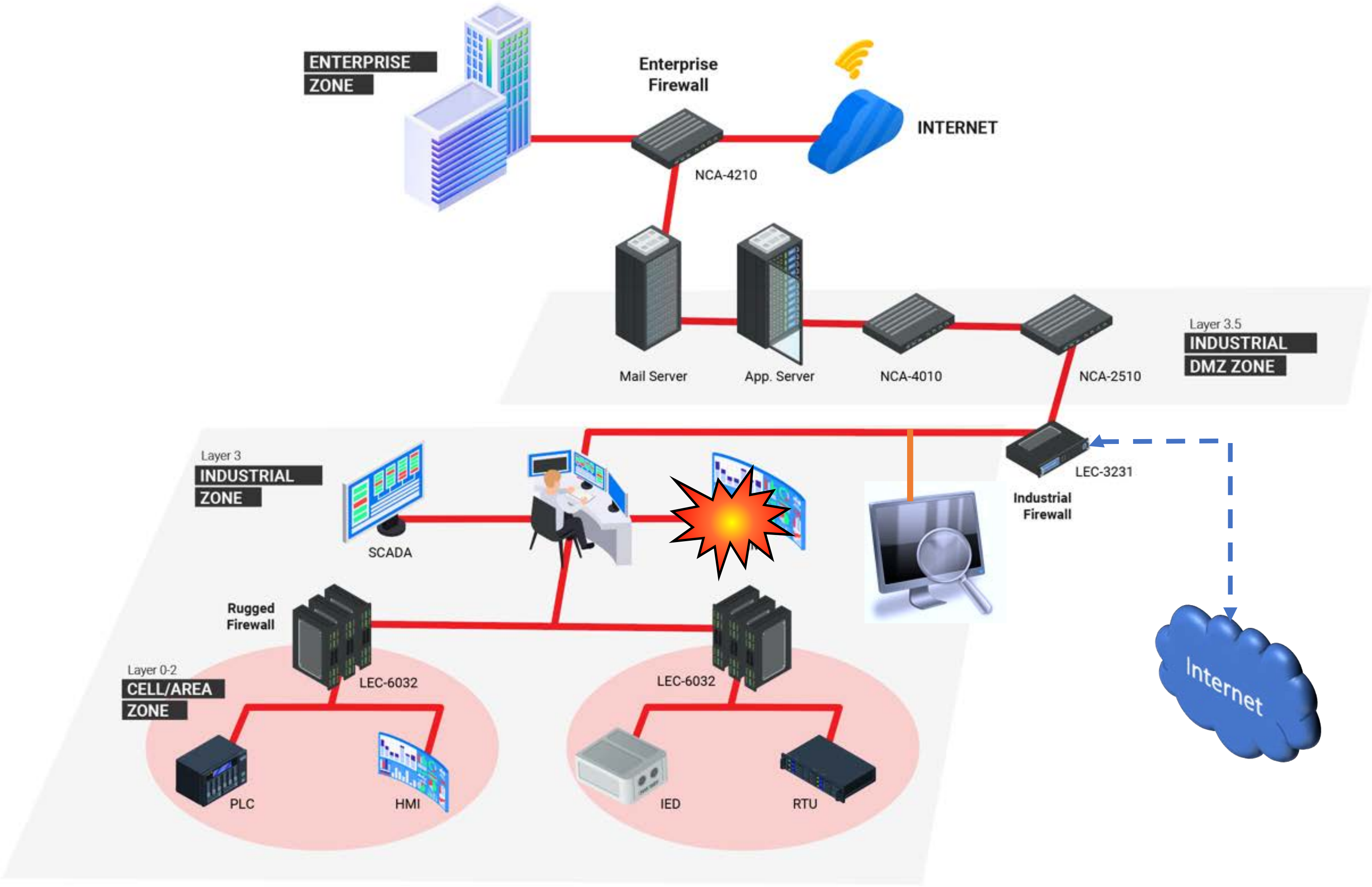
Current environments I. Firewall based



Current environments II. Honeypot based



New environments. Specialized IDS



In short

✓ 01

Modern power plants are using more and more IT infrastructures to control and access the plants

✓ 02

This implies that typical IT threats are now present in the ICS field

✓ 03

The cybercrime is now more than ever a sector-oriented threat, so power plants have become one of the most targeting sectors

✓ 04

Do not ask yourself if you are safe, ask yourself if you’ll be ready when you are attacked

Thanks!

Manuel Alguacil

CISO & ICT Director.

✉ malguacil@isotrol.com
☎ (+34) 955 036 800

Moisés Guerrero

Renewable Energy Consultant

✉ mguerrero@isotrol.com
☎ (+34) 955 036 800