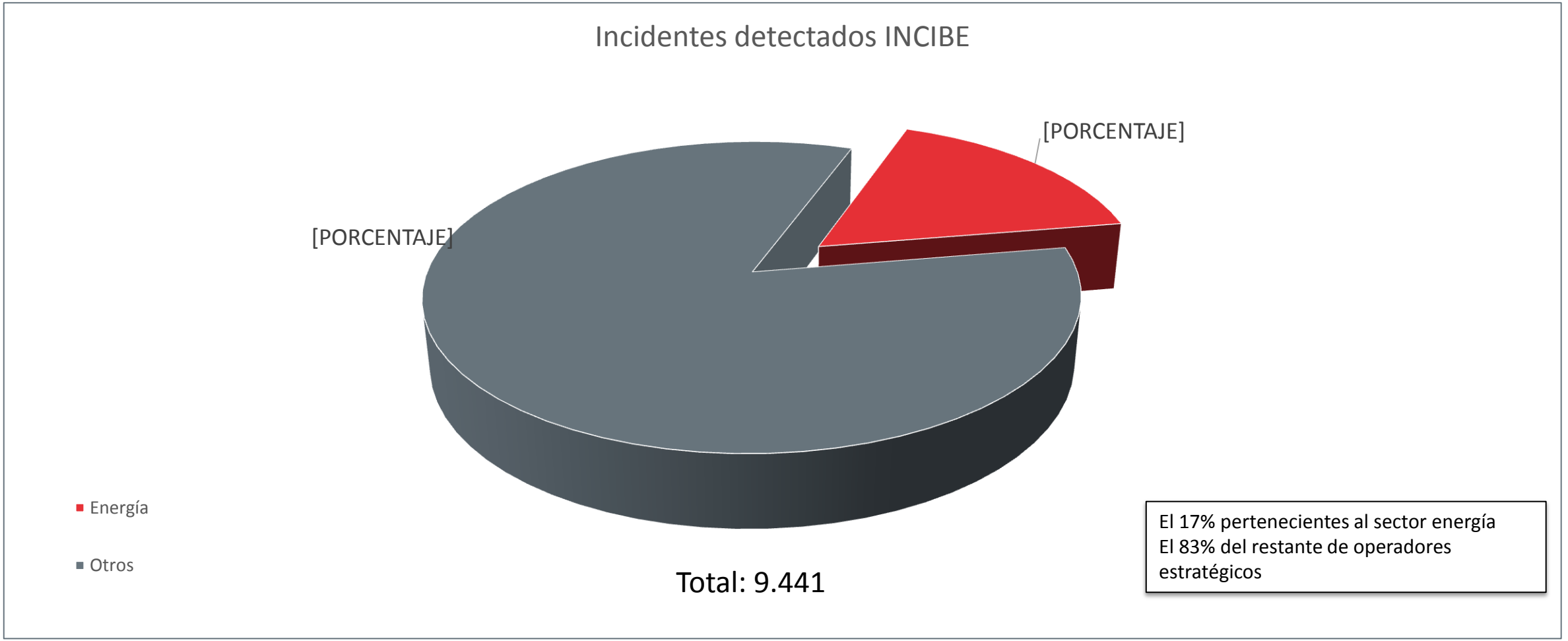
Los retos de la eólica ante la ciberseguridad

Raúl Riesco
Head of INTEL and ICS

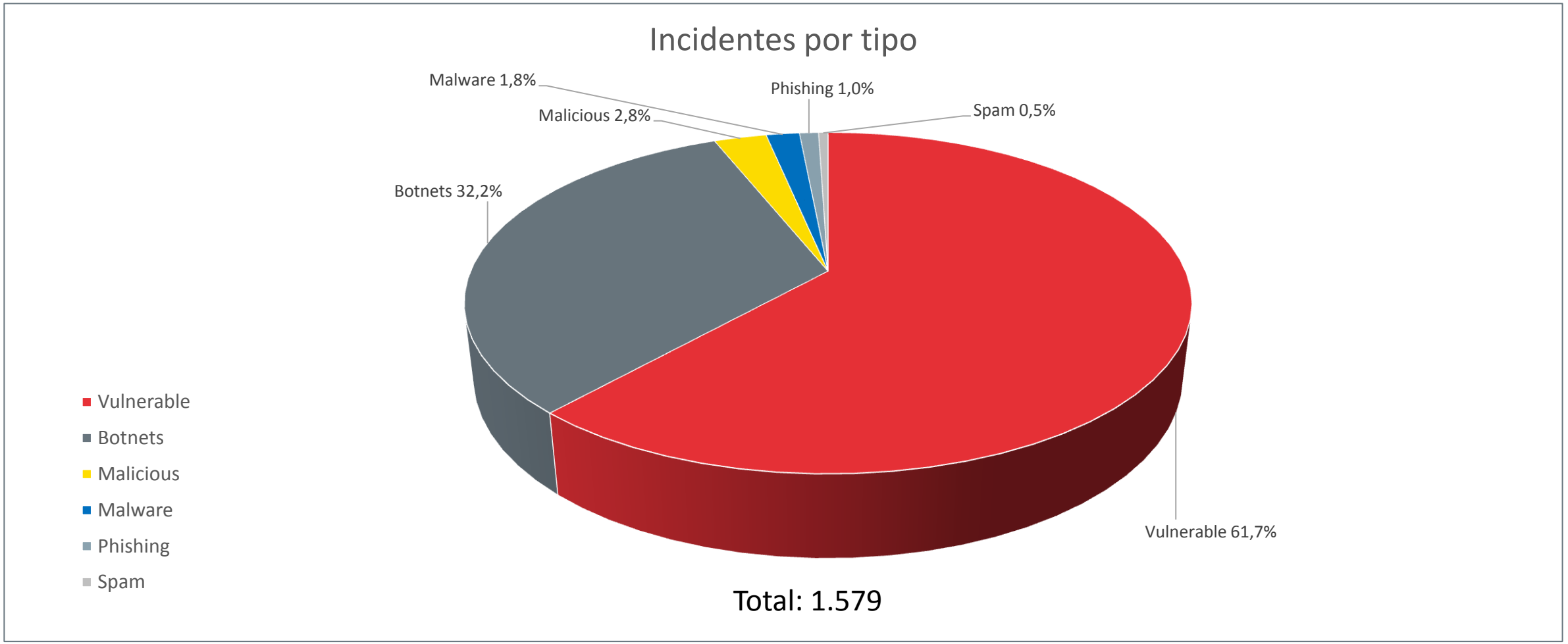
Agenda

1. Incidentes detectados por INCIBE en el sector energía 2017-18
2. Posibles ciber-ataques en parques eólicos
3. Vulnerabilidades conocidas en el sector eólico
4. Activos eólicos expuestos en internet
5. Buenas prácticas recomendadas

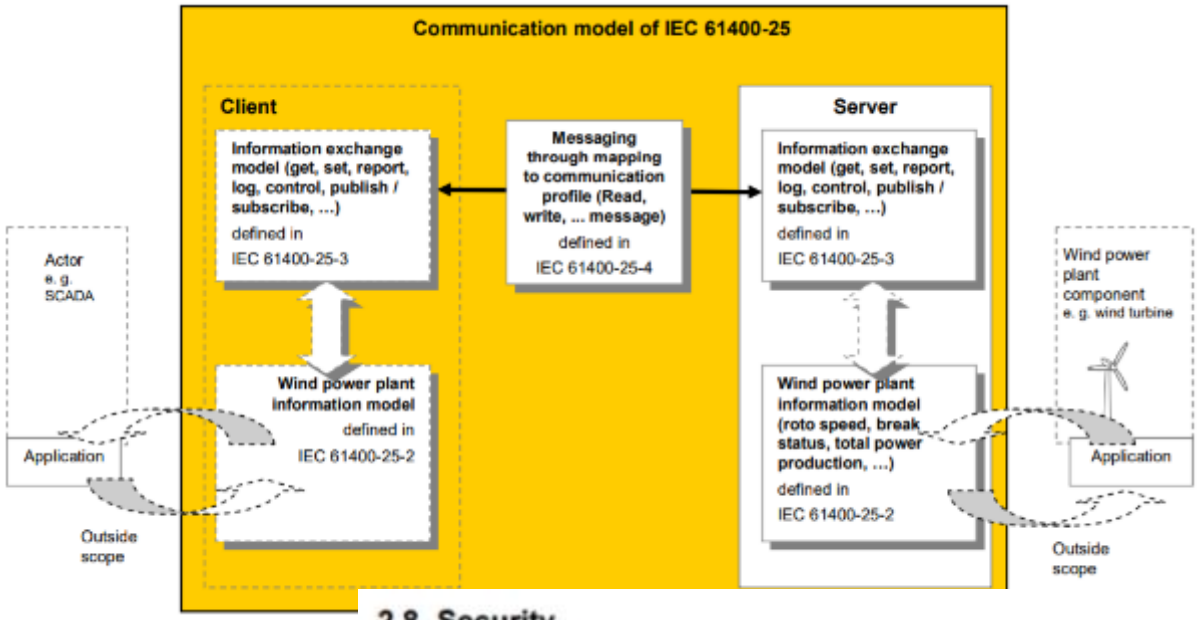
Incidentes detectados por INCIBE en operadores estratégicos durante 2017 y hasta el 04/06/2018



Clasificación de incidentes detectados por INCIBE en operadores del sector energía durante 2017 y hasta el 04/06/2018



IEC 61400-25 y OPC XML-DA Spec



OPC XML-DA Specification (Version 1.0) — **Released**

2.8 Security

The assumption that OPC XML-DA makes is that the transport will handle security, e.g., HTTPS

The OPC specifications define interfaces that provide open access to various forms of process control information. Such information can be of great importance to the operations of an enterprise and should therefore be protected. Vendors and end-users must work together to ensure that sensitive information is guarded against unauthorized access. Unauthorized access can include both data espionage and sabotage of critical control parameters.

In the past, many companies have simply chosen to adopt a "wide-open" security policy for DCOM OPC servers and have relied on firewalls to protect from intruders. With the advent of web service technology, process control information is no longer restricted to the confines of a LAN. Web services are frequently deployed outside the firewall, potentially exposing important information to any person connected to the Internet.

End-users (network and site administrators) are responsible for enabling and properly configuring the security features of their selected web server components (for example, enabling the SSL capabilities of Microsoft IIS). This may include restricting access to web services to authorized users.

Vendors may also provide additional mechanisms to allow finer control over the types of operations that specific users are permitted to carry out on specific items (for example, using the Microsoft .NET security classes).

It is highly recommended that, as a minimum, vendors provide a means to globally disable the Server's "write" capabilities, putting it into a "read-only" mode.

If a vendor does choose to provide custom mechanisms, then that vendor must be certain that they do not compromise existing security mechanisms already in use. Custom mechanisms must be well integrated with existing security mechanisms. For example, client authentication and identification must be based on facilities supplied by the operating system (where available), rather than vendor-specific approaches.

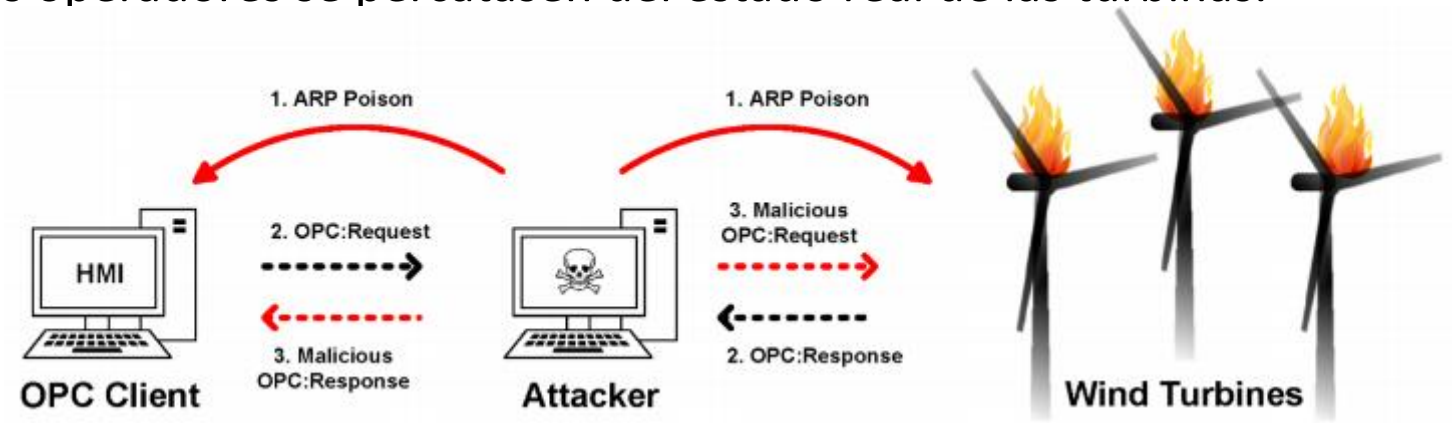
End-users are still responsible for configuring vendor-specific security mechanisms correctly. Vendors should provide assistance with configuration as necessary.

The OPC Foundation is not responsible for any damage relating to compromised security. Vendors and end-users must choose for themselves the security measures needed to ensure the safety of data exposed via OPC.

Please refer to OPC Security Custom Interface Standard for additional insight into security concepts.

Posibles ataques en parques eólicos
Control de la turbina

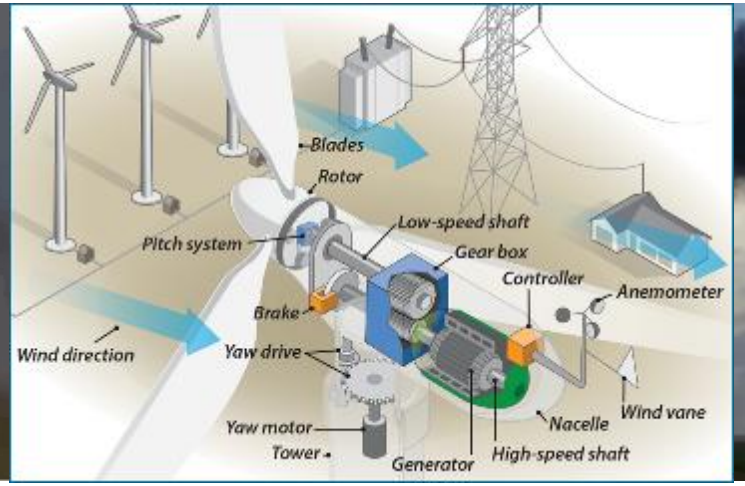
- En la BlackHat USA 2017 **Jason Staggs** demostró la **viabilidad de un ataque crítico** a una granja eólica utilizando como vector de entrada el **acceso físico** a una de las turbinas.
- PoC mediante una **Raspberry Pi + módulo Wi-Fi** conectado al **Switch ICS** permitiéndole acceder a todo el flujo de datos. Mediante una serie de scripts en Python consiguió **falsificar respuestas OPC-XML-DA** para ejecutar acciones dañinas sobre la turbina.
- Dicho ataque combinado con un ***man-in-the-middle*** permitiría encubrir dichas acciones evitando de este modo que los operadores se percatasen del estado real de las turbinas.



Fuente: https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf

Posibles ataques en parques eólicos
Daños a la turbina

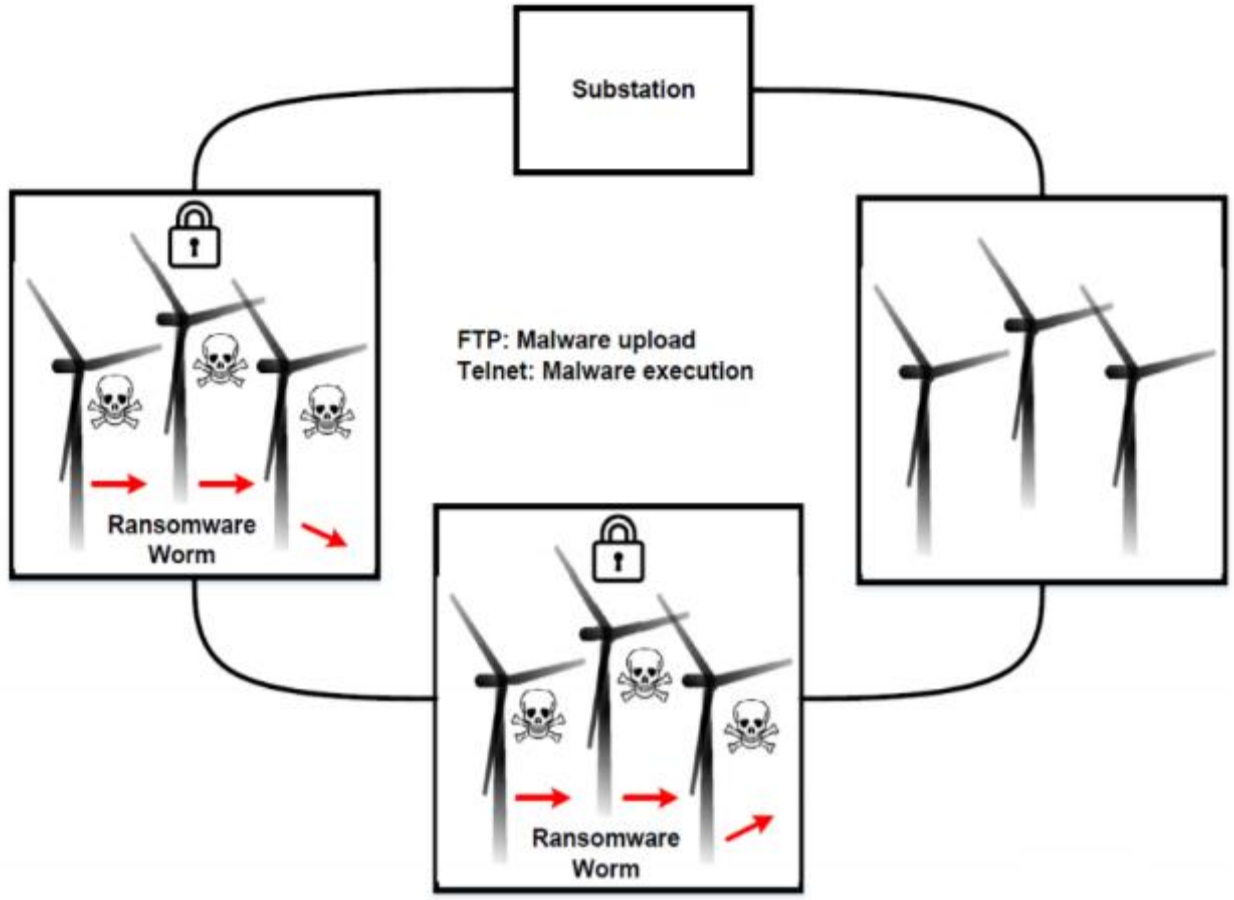
- El investigador demostró que **las acciones sobre la turbina pueden ser extremadamente graves si el servidor OPC no limita el uso de instrucciones de escritura (“*write request*”)**. Por ejemplo, el atacante puede forzar un “***Emergency shutdown***” (maniobra que genera un desgaste excesivo en determinados componentes mecánicos críticos).
- ***Un uso reiterativo de este tipo de acciones puede tener consecuencias impredecibles*.**



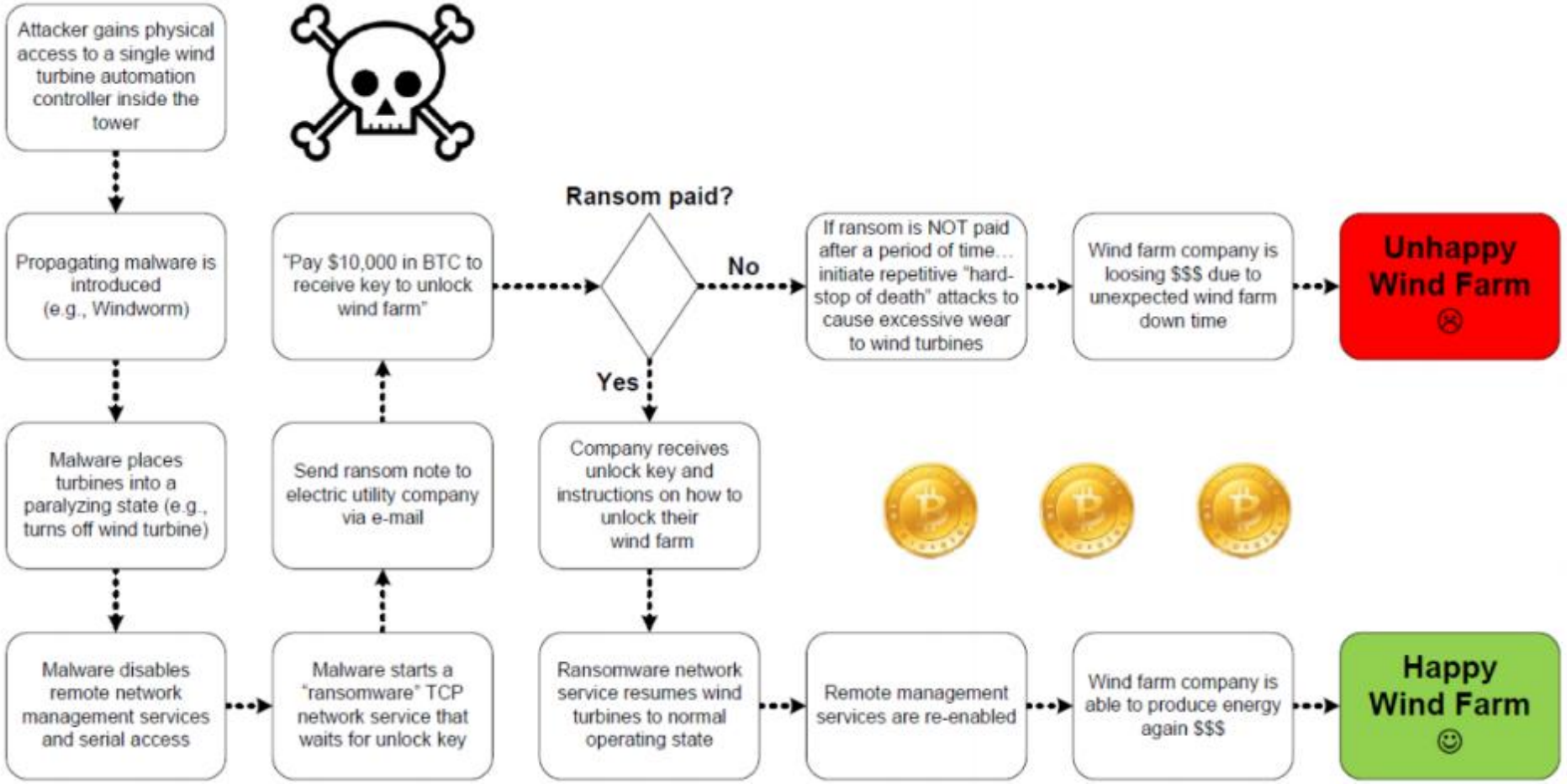
Posibles ataques en parques eólicos
Ransomware

- Jason Staggs desarrollo una prueba de concepto de un gusano, Windworm, que se aprovechaba de **credenciales por defecto** para **propagarse entre PACs (*Programmable Automation Controller*)** de diversas turbinas. El gusano, una vez infecta un dispositivo, **busca nuevos *targets* para subir una copia de si mismo** vía FTP y posteriormente **ejecutarse** mediante Telnet.

- El malware "***cross-compilado***" para diversos sistemas embebidos (windows, linux, RTOS) **permitiría modificar variables críticas asociadas al control de la turbina por medio de CANopen**.



Workflow de ataque ransom (extorsión)



Fuente: Jason Staggs (BlackHat USA 2017)

Lecciones aprendidas

- Los diversos ataques y pruebas de concepto expuestos por Jason Staggs **fueron posibles debido a carencias de seguridad** que podrían ser **fácilmente evitables**, por ejemplo, mediante:

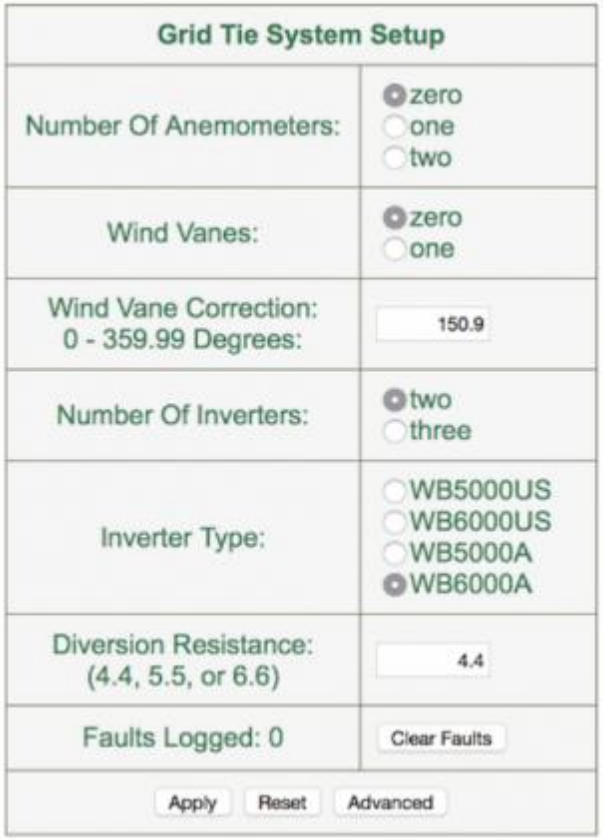
  - **Controles de seguridad física que impidan el acceso a la turbina**
  - **El uso de cifrado para la comunicación OPC (SSL/TLS).**
  - **Política robusta de contraseñas.**
  - **Segmentación de redes.**
  - **Limitación de solicitudes "read-only" en el servidor OPC.**

Vulnerabilidades conocidas en el sector eólico

- **Gestión remota de los activos a través de servicios inseguros**
- **Activos accesibles desde internet**
  - Gestión de configuración de turbinas
  - Diagnóstico de aerogeneradores
- **Turbinas eólicas y subestaciones suelen compartir la misma red de área local**

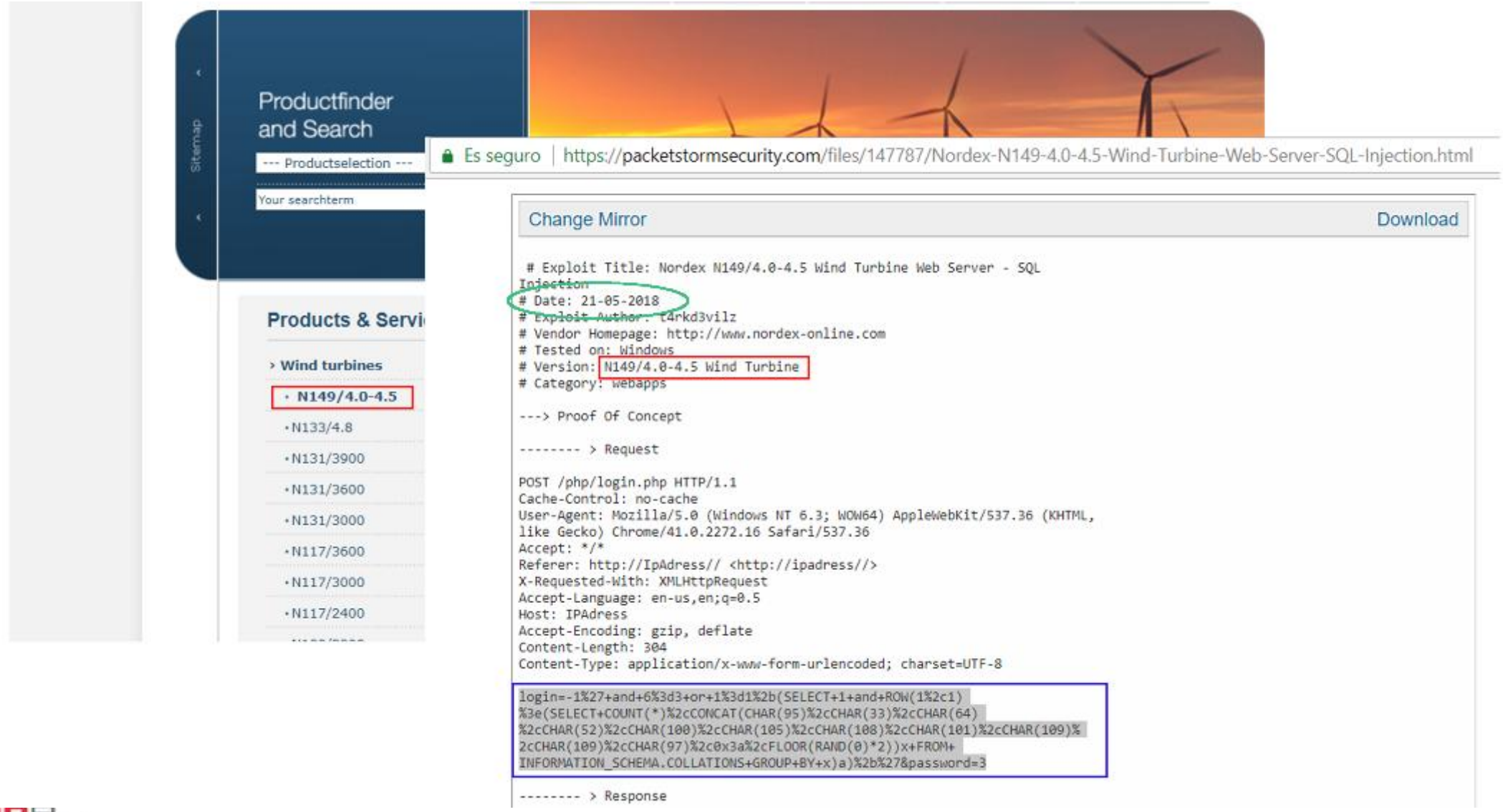
Vulnerabilidades en SW de control de turbinas eólicas

- En junio de 2015 el ICS-Cert publicaba una **vulnerabilidad CSRF** (*Cross-Site Request Forgery*) con un *CVSS v2 base score* de 10 en la interfaz de administración de la turbina XZERES 442SR Wind. La vulnerabilidad permitiría a un atacante **cambiar el *password* de administrador** del panel Web si un cliente era **engañado para hacer clic en un enlace malicioso**. En dicho caso, el atacante tendría acceso para **controlar la turbina** desde el panel de administración Web.
- Otra vulnerabilidad en el HMI de la turbina RLE Nova-Wind fue también reportada por el ICS-Cert en septiembre de 2015. En este caso, la vulnerabilidad se debía al **almacenamiento en claro de las credenciales para autenticarse con el HMI** lo que podría permitir a un atacante recuperar las mismas y ejecutar todo tipo de acciones sobre la turbina.



Más información: https://ics-cert.us-cert.gov/advisories/ICSA-15-155-01
https://ics-cert.us-cert.gov/advisories/ICSA-15-162-01A

Vulnerabilidades en SW de control de turbinas eólicas

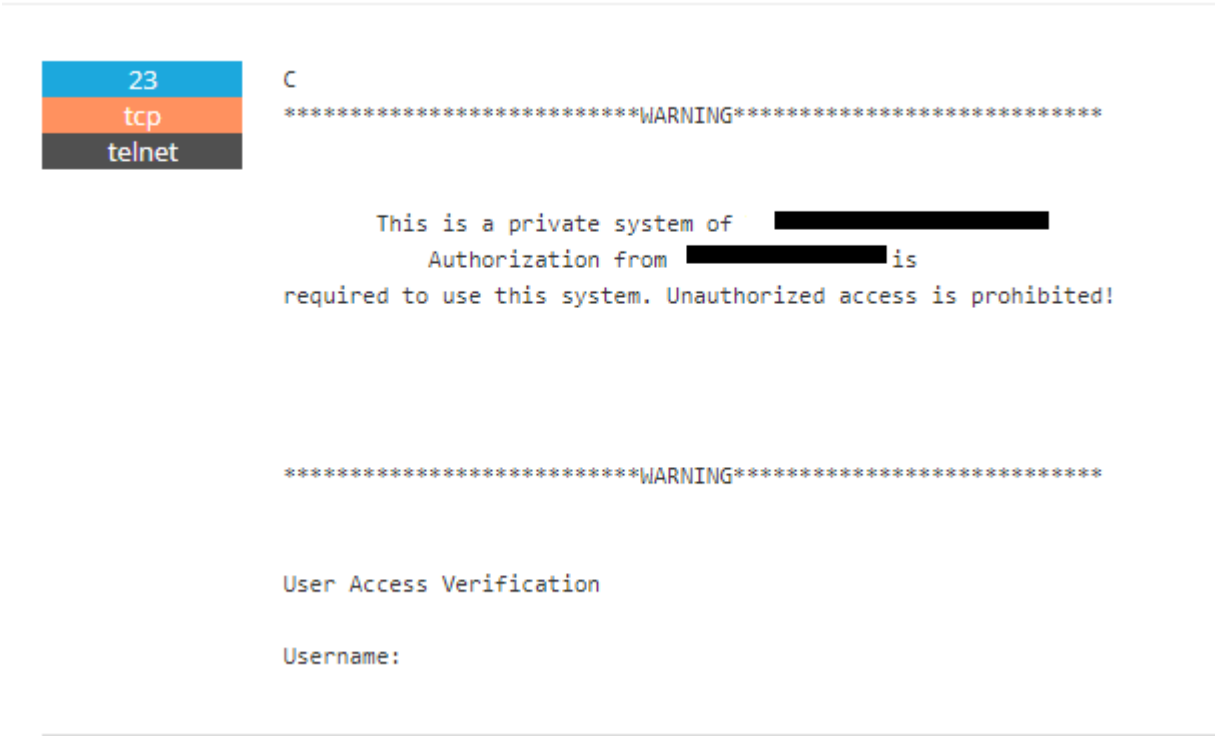


Más información: https://www.exploit-db.com/exploits/44684/

Activos eólicos expuestos en internet

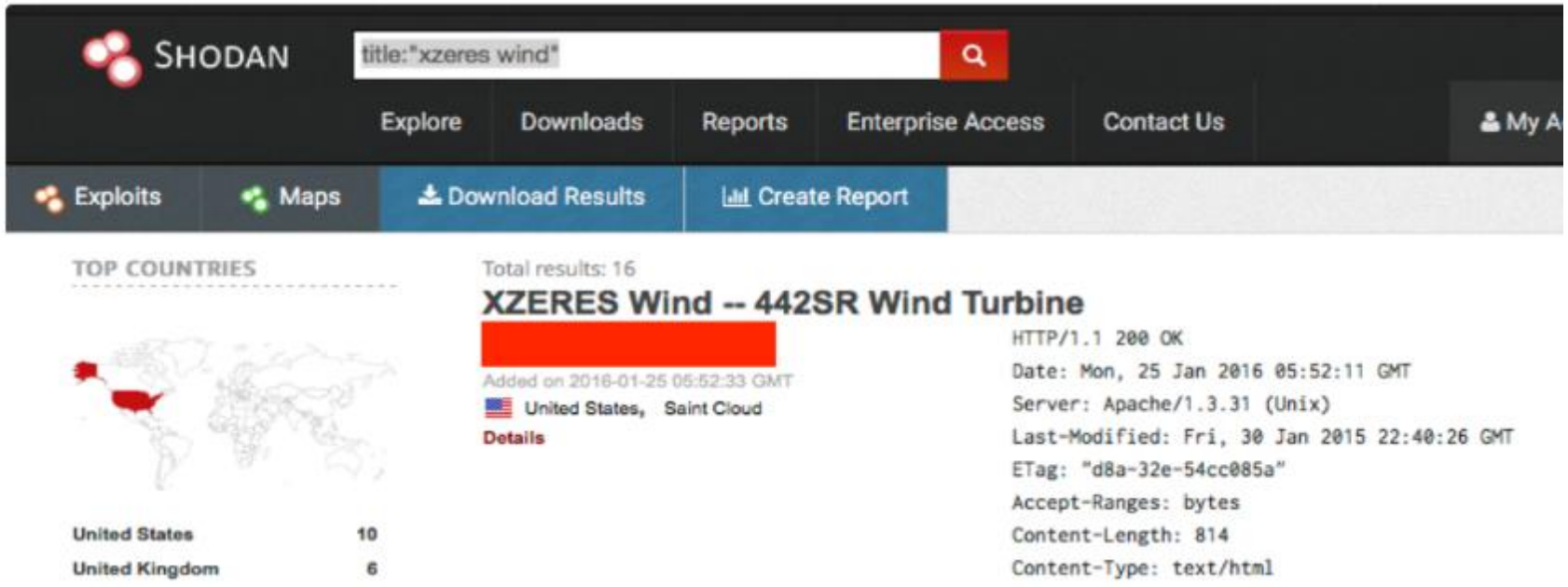
- **Utilizando el metabuscadores es posible identificar sistemas eólicos expuestos**

- **Búsqueda y análisis de posibles vulnerabilidades presentes en los sistemas para su posterior explotación**



Activos expuestos y riesgo de automatización de ataques

- Buscadores como ***Shodan*** o ***Censys*** así como herramientas de scanning como *Nmap*, *Masscan* o *Zmap* permiten rápidamente localizar y automatizar la explotación de vulnerabilidades como las descritas anteriormente.



Más información: https://workentin.wordpress.com/2016/01/26/shodan-and-serc-audits/

Buenas prácticas para mejorar la seguridad en el sector eólico y mitigar el efecto de brechas de seguridad

- **Mantener el software y el firmware actualizados y parcheados**
- **Limitar y controlar los puertos de red y servicios expuestos**
  - Desactivar interfaces de administración remota innecesarias
- **Configurar adecuadamente los dispositivos de red como puede ser un cortafuegos**
- **Diseño de red seguro**
  - Configurar adecuadamente los cortafuegos para cada torre
  - Establecer túneles VPN cifrados para cada torre

Buenas prácticas para mejorar la seguridad en el sector eólico y mitigar el efecto de brechas de seguridad

- **Contratar una compañía externa de ciberseguridad para realizar ejercicios de "red team" y detectar posibles brechas de seguridad y vectores de ataque**

- **Incrementar la seguridad de acceso a las torres**

- **Monitorizar la conectividad a los sistemas de control y generar eventos/alertas ante cualquier irregularidad o anomalía respecto de su "*baseline*" (por ejemplo, intentos de autenticación por fuerza bruta, accesos en horas no habituales, etc.)**

Gracias!

INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

raul.riesco@incibe.es

+34 987 877 189

www.incibe.es