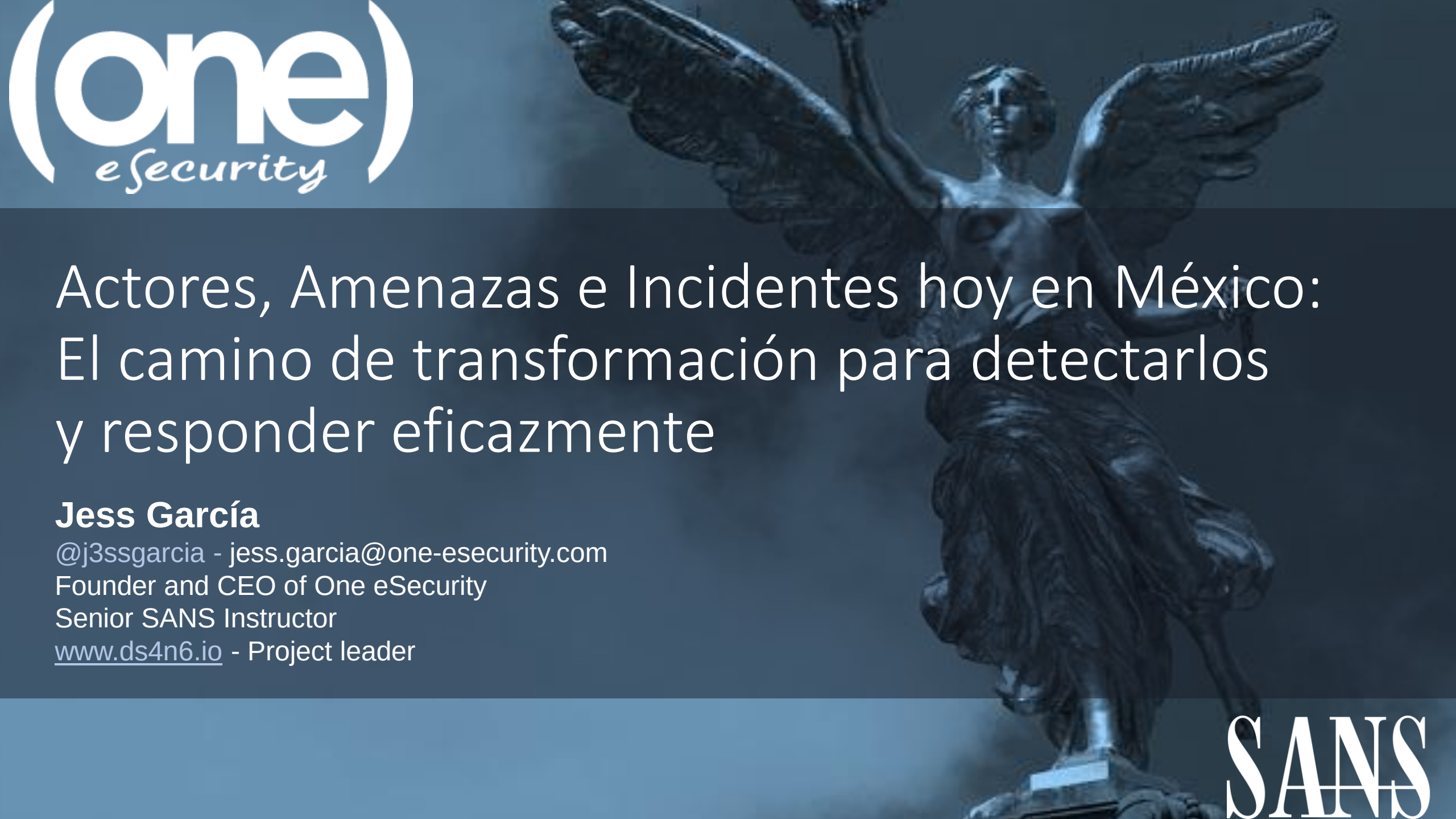


Actores, Amenazas e Incidentes hoy en México: El camino de transformación para detectarlos y responder eficazmente

Jess García
@j3ssgarcia - jess.garcia@one-esecurity.com
Founder and CEO of One eSecurity
Senior SANS Instructor
www.ds4n6.io - Project leader

WhoAmI

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

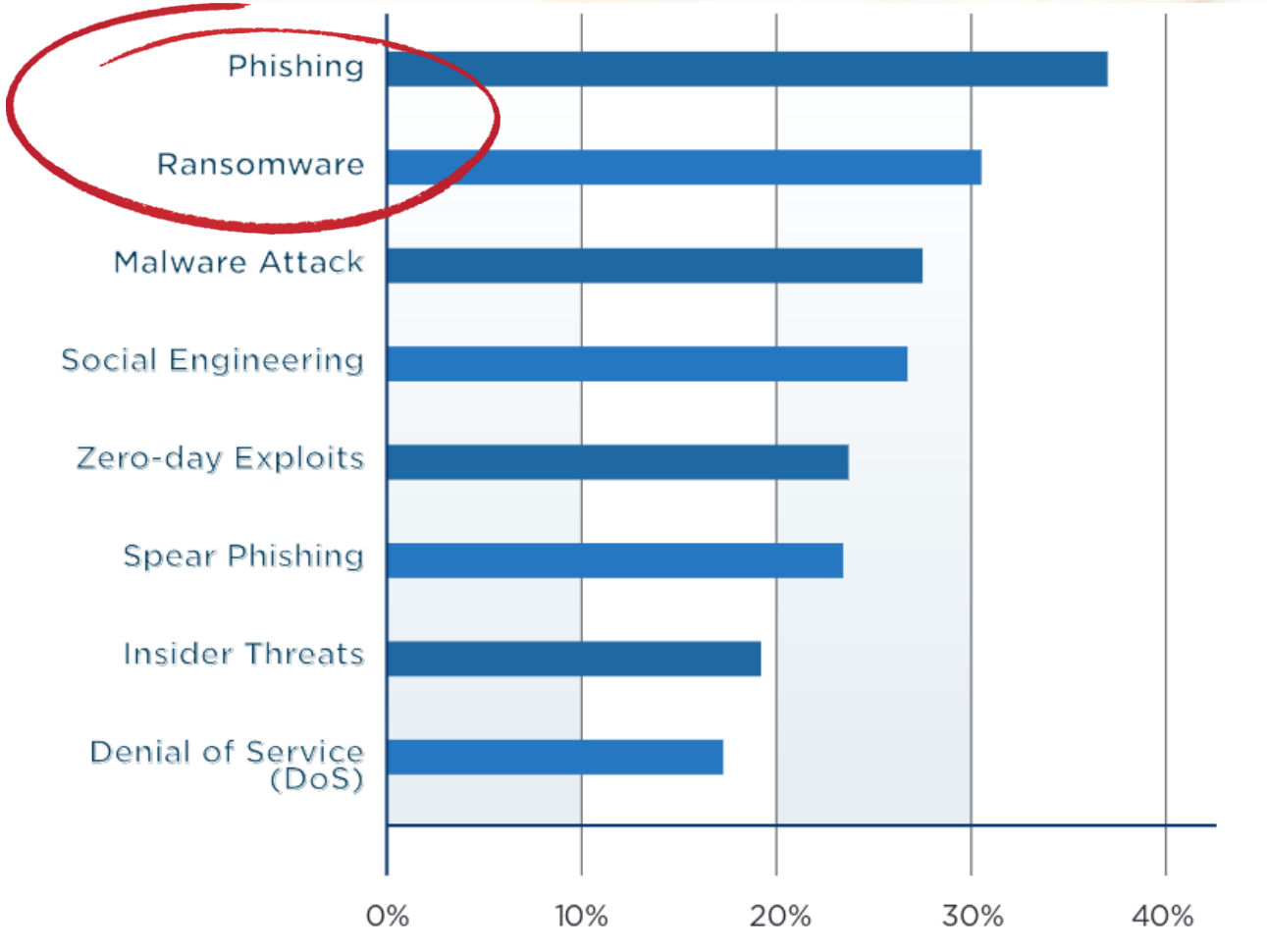
Índice

- Actores y amenazas en LATAM
- Casos reales
- Factores de éxito:
  Camino a la madurez

Actores y amenazas en LATAM

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

TOP 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

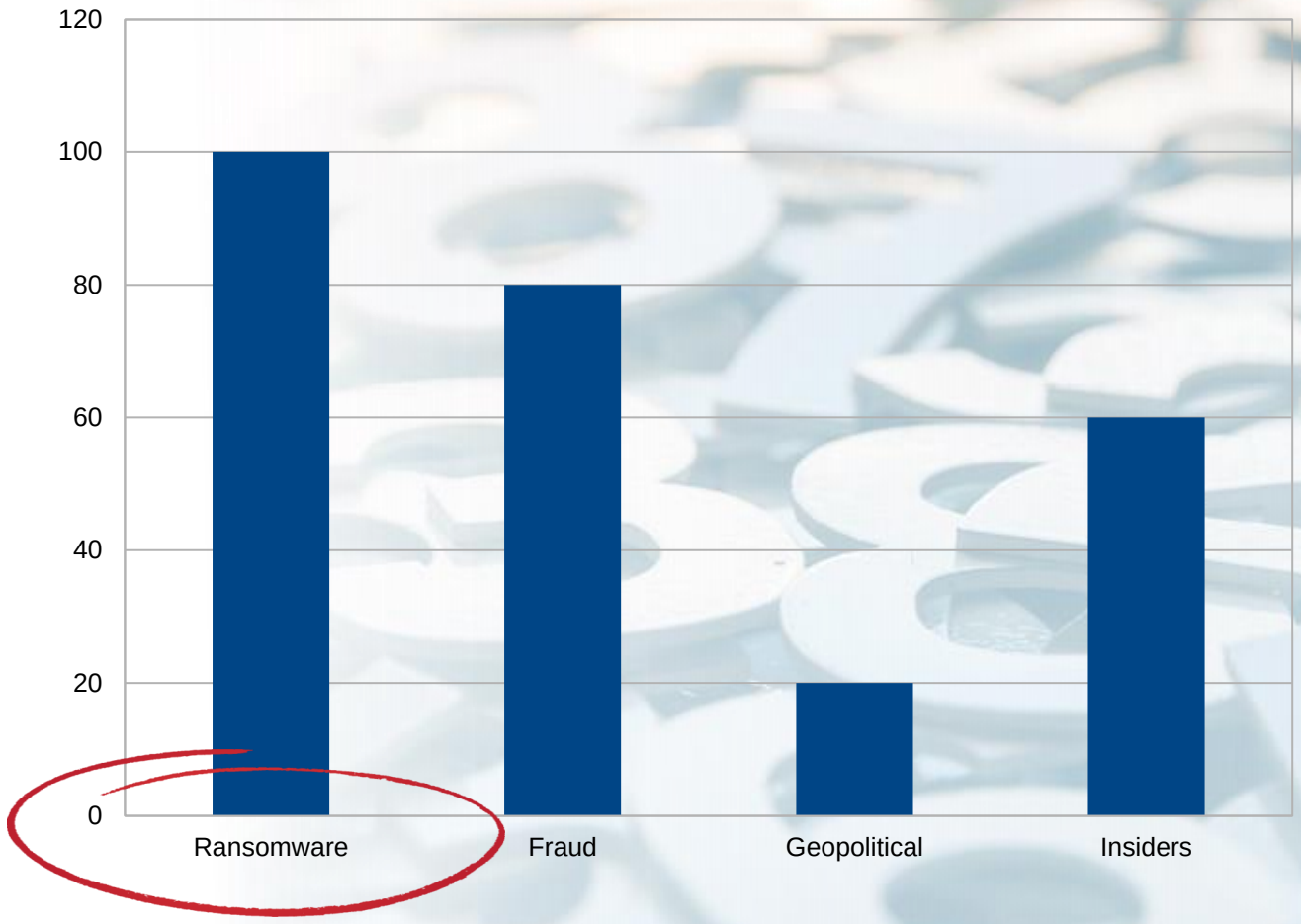


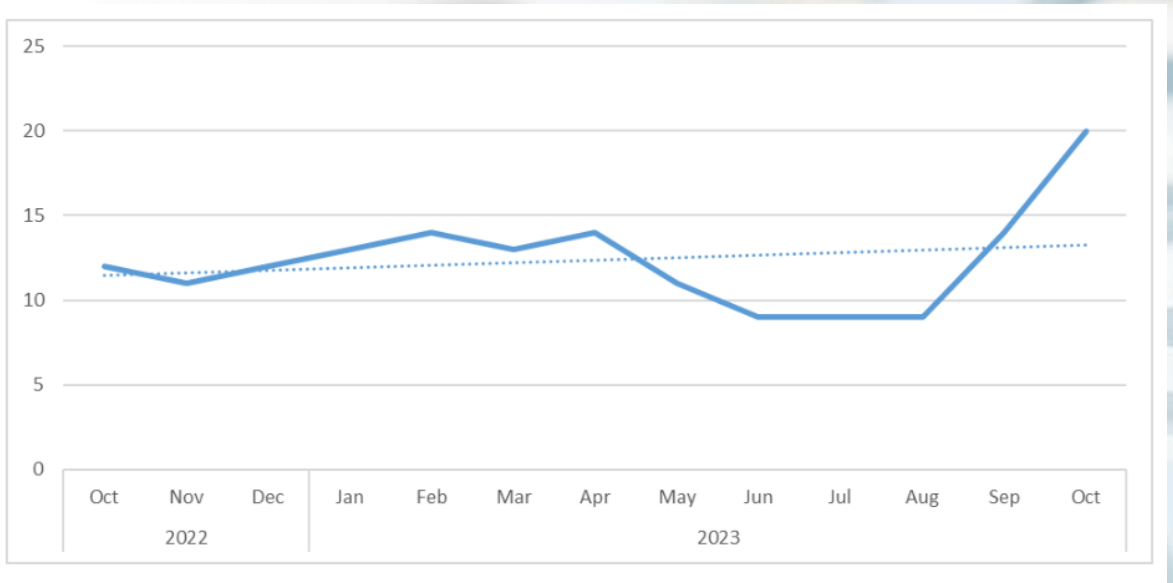
Gráfico de elaboración propia

Evolución del Ransomware

En 2024 el Ransomware continúa siendo la amenaza más crítica para organizaciones de todos los tamaños y se extiende mundialmente.

Tendencias:

- Ataques sin cifrado en aumento.
- Ataques de doble extorsión.
- Explotación de vulnerabilidades parcheadas recientemente
- RaaS (Ransomware as a Service)
- Mientras existan las criptomonedas, seguirá existiendo el ransomware.



Número de organizaciones afectadas por ataques de ransomware dirigidos confirmados, de octubre de 2022 a octubre de 2023

Referencia: The 2024 Ransomware Threat Landscape - Symantec

Threat actors en Mexico actualmente

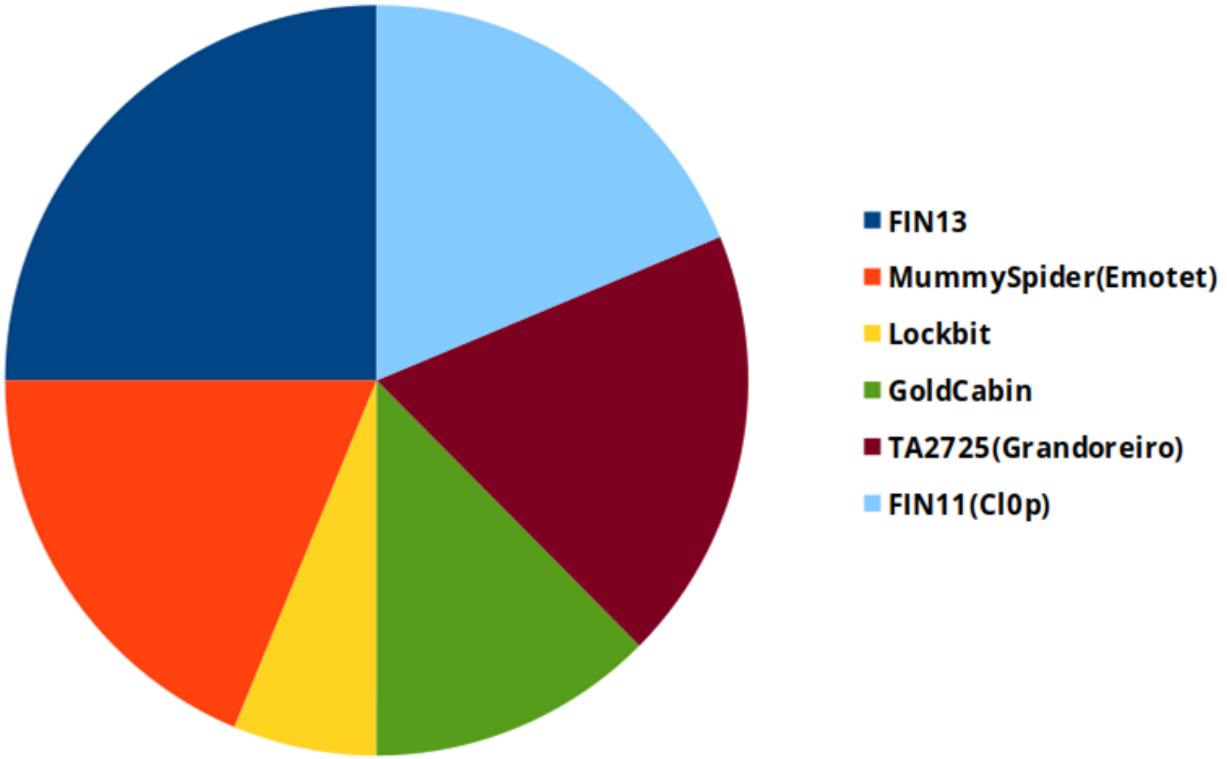
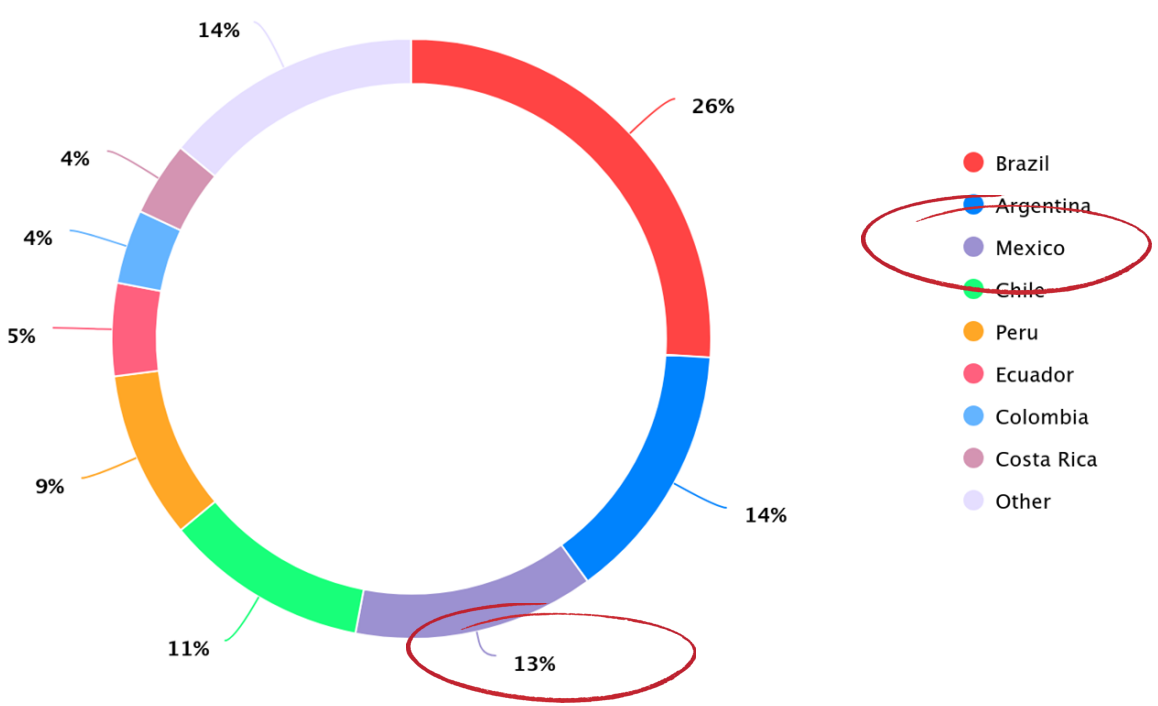


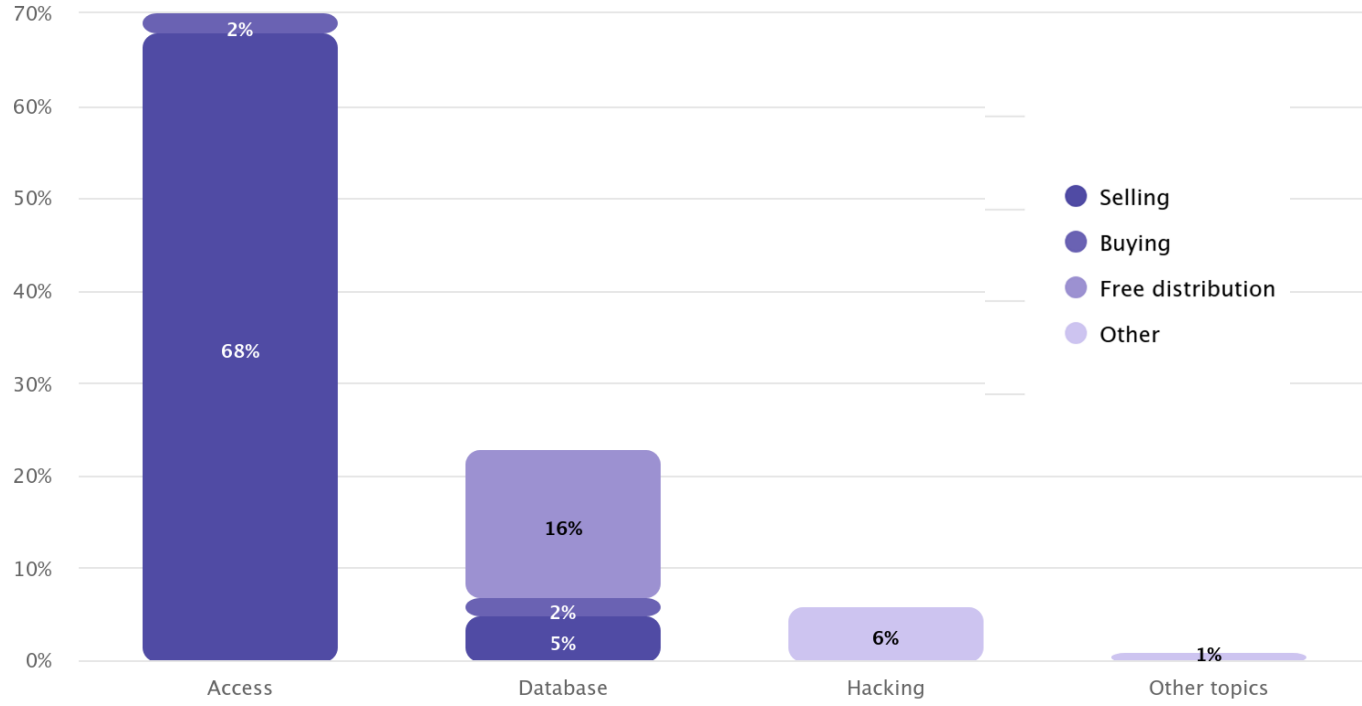
Gráfico de elaboración propia

- 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

Datos robados en LATAM 2023

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





Gráficos de elaboración propia

Casos reales en LATAM

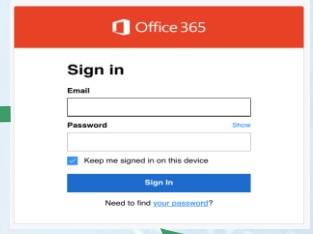
Caso 1:
Suplantación de identidad

Caso 1: ¿Qué ocurrió?

Ciberatacante

1. Envio de Phishing as a Service - PaaS

Colaborador

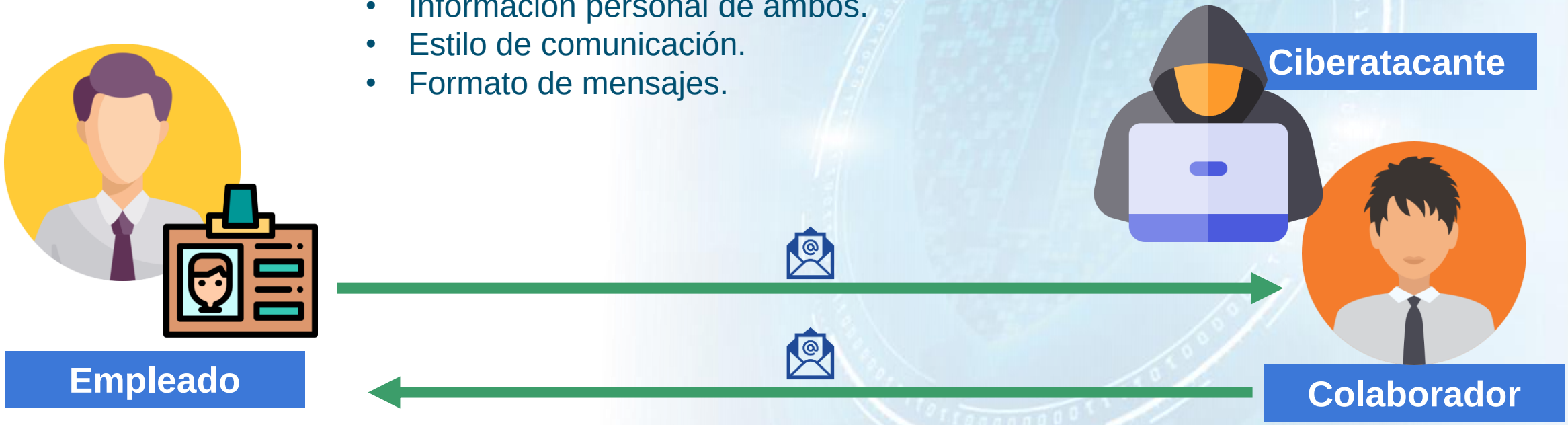


2. Ciberatacante consigue
Password
Token

Caso 1: ¿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.



Caso 1: ¿Qué ocurrió?

Empleado

Ciberatacante

Typosquatting: Ciberatacante envía un correo al Cliente con dominio: **colaborador@dominio_.com**

Servidor de correo de la empresa alerta de un **dominio desconocido**.

Colaborador

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

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

Caso 1: ¿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 1: ¿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 2: Ataque a la cadena de suministro

Caso 2: ¿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

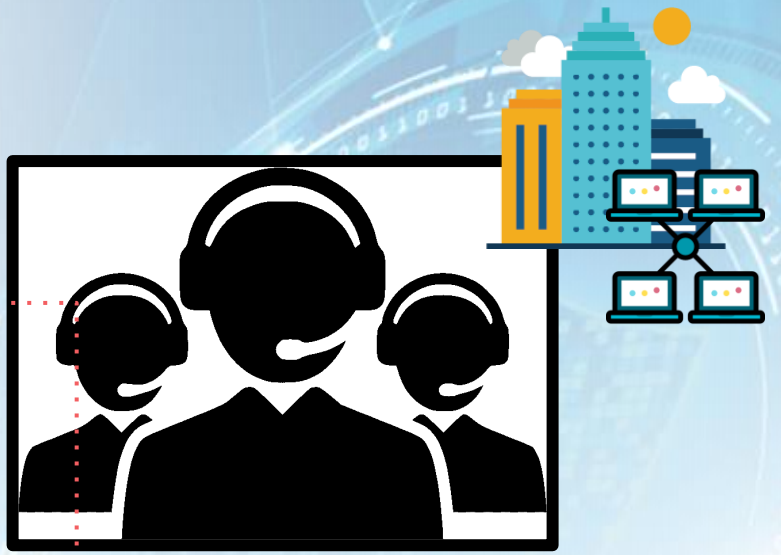
Caso 2: ¿Qué ocurrió?

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 credeciales de varios empleados del Call Center

Caso 2: ¿Qué ocurrió?

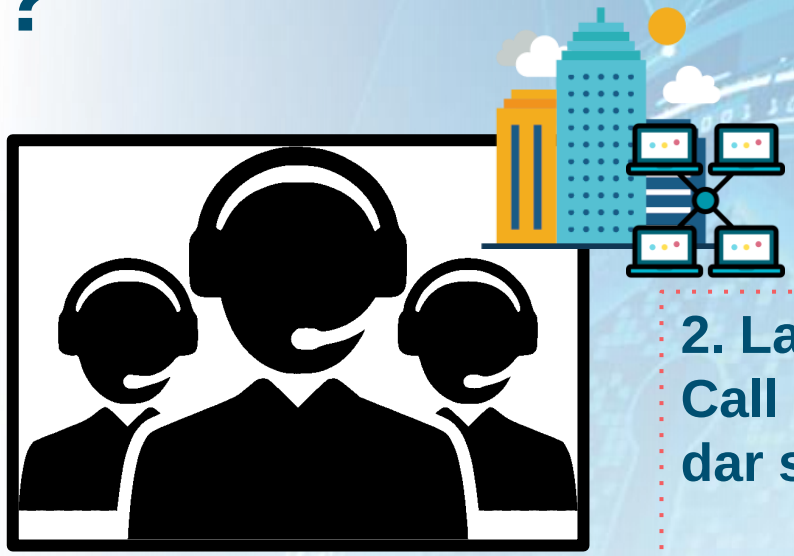
1. Atacante modifica condiciones de clientes de la empresa



2. Atacante intenta moverse lateralmente a la red de la empresa

ALERTA: Movimiento detectado

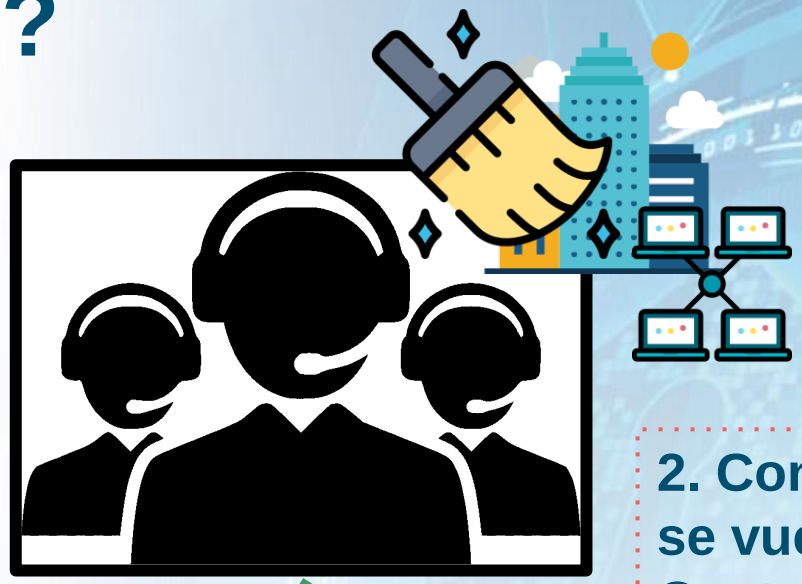
Caso 2: ¿Qué ocurrió?



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

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

Caso 2: ¿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 2: Medidas generales

Call center (proveedor):

- VPN con 2FA.
- Monitorización y alerta.
- Capacitación de usuarios.
- Antivirus con buena detección.

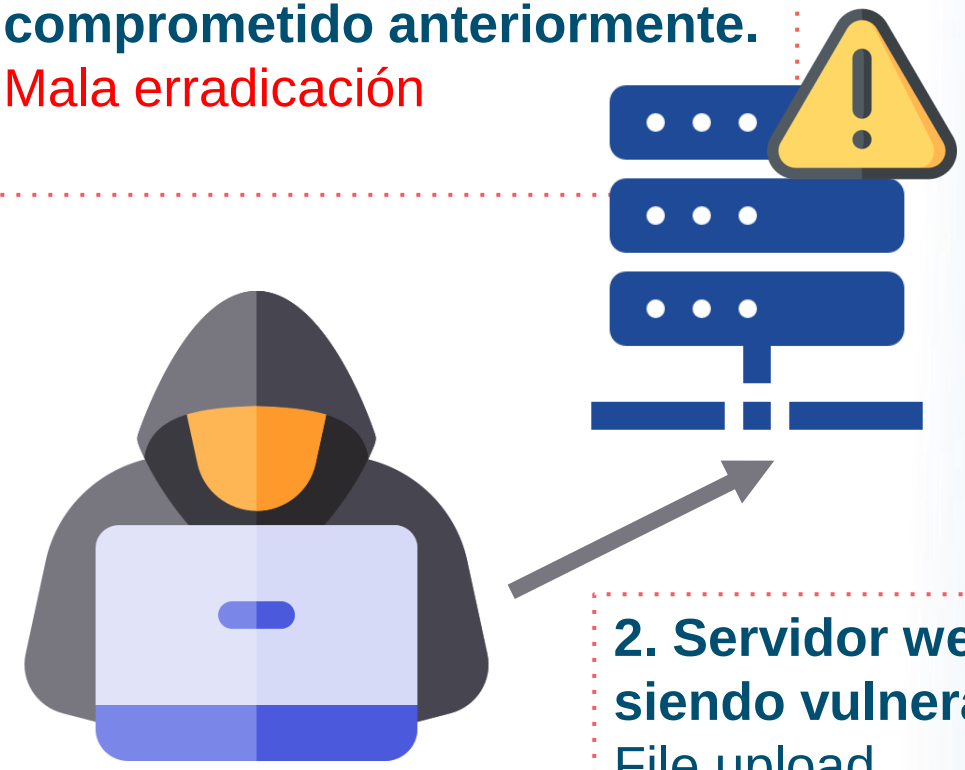
Empresa:

- Exigir buenas prácticas de seguridad a sus proveedores.

Caso 3: Fraude Transacciones fraudulentas como legítimas

Caso 3: ¿Qué ocurrió?

1. Servidor web comprometido anteriormente.
Mala erradicación



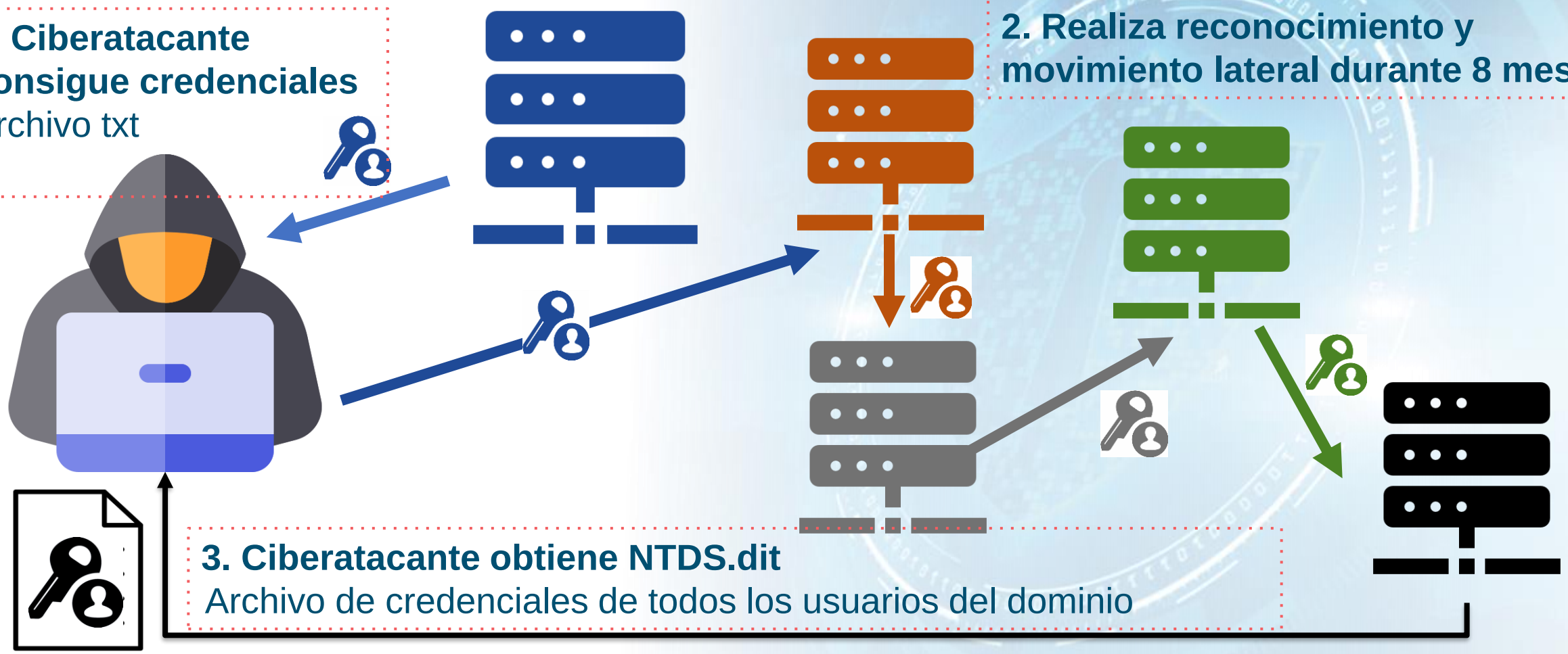
2. Servidor web continua siendo vulnerable
File upload

3. Meses después el atacante vuelve a aprovechar la misma vulnerabilidad
Despliegue de herramientas Webshells y backdoors para persistencia

Caso 3: ¿Qué ocurrió?

1. Ciberatacante consigue credenciales
Archivo txt

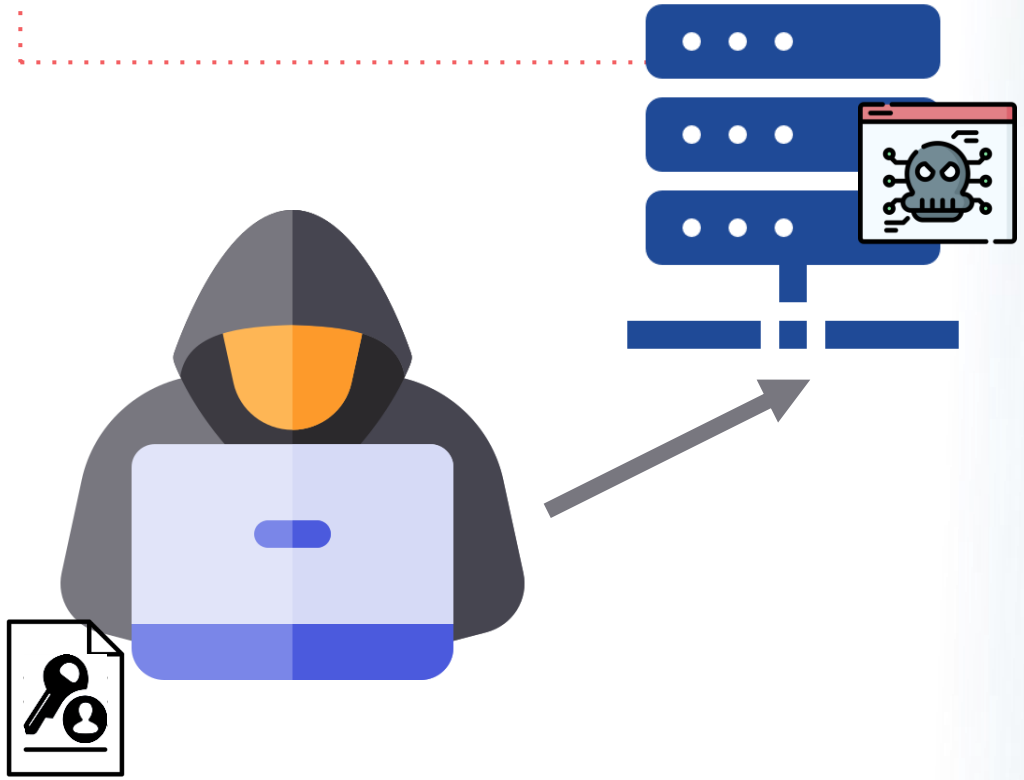
2. Realiza reconocimiento y movimiento lateral durante 8 meses



3. Ciberatacante obtiene NTDS.dit
Archivo de credenciales de todos los usuarios del dominio

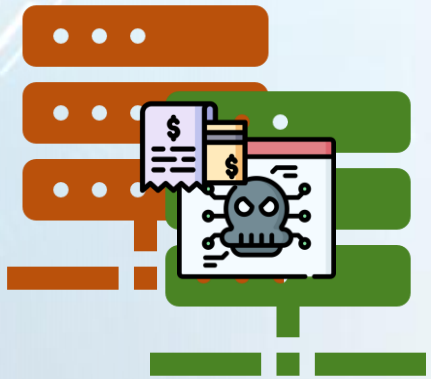
Caso 3: ¿Qué ocurrió?

1. Compromiso de file server



2. Ciberatacante exfiltra información sobre la operativa financiera

3. Compromiso de servidores SAP y transaccionales

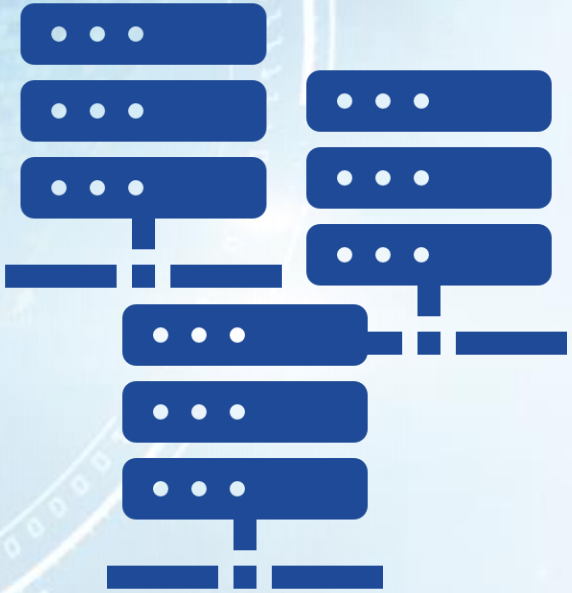


Caso 3: ¿Qué ocurrió?

1. Modificación de archivos de transacciones legítimas

3. Ejecución de transacciones con cambios en el destinatario

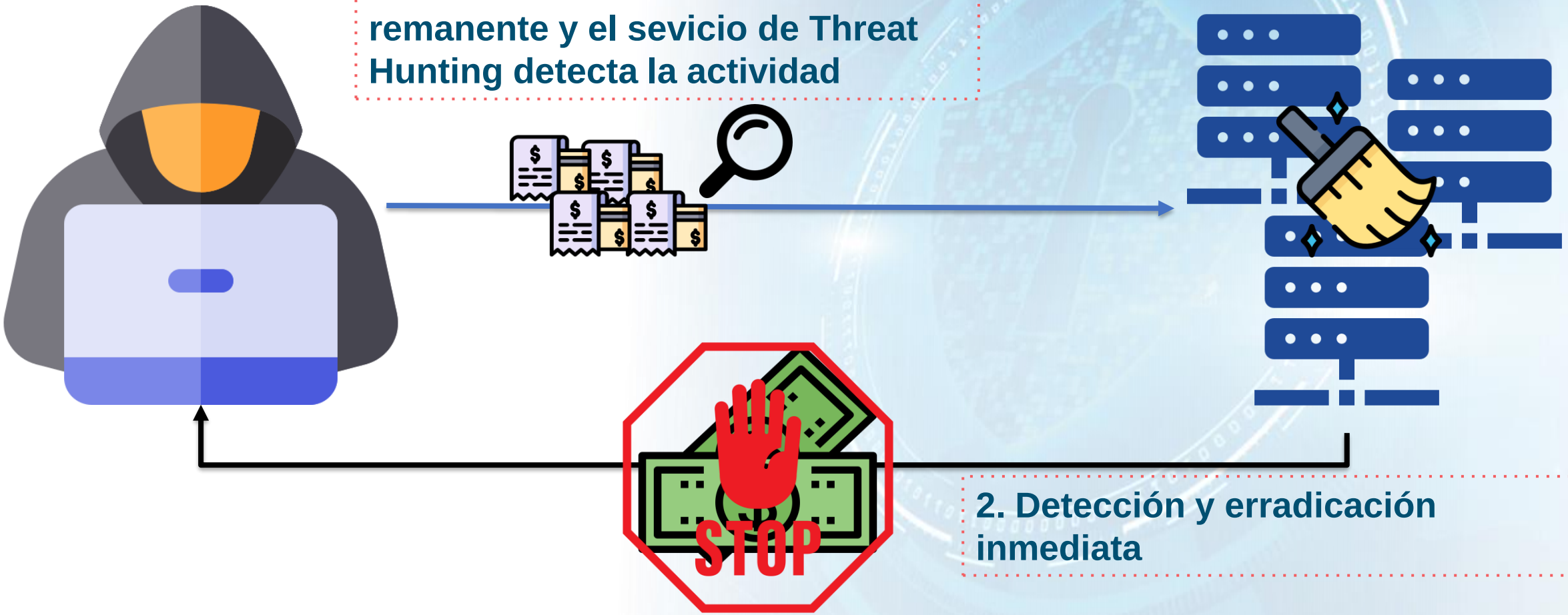
2. Cifrado de transacciones fraudulentas con proceso legítimo



4. Se obtienen altas cantidades de dinero

Caso 3: ¿Qué ocurrió?

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



2. Detección y erradicación inmediata

Caso 3: Medidas generales

- **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 4: Ransomware Ataque APT

Caso 4: ¿Qué ocurrió?

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

Caso 4: ¿Qué ocurrió?

Alcance del ataque

Estados Unidos

Riesgo de propagación mundial

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

Caso 4: ¿Qué ocurrió?

Día 1

El despliegue de Ransomware es **inminente**

Medidas agresivas para evitar el cifrado masivo

Misiones

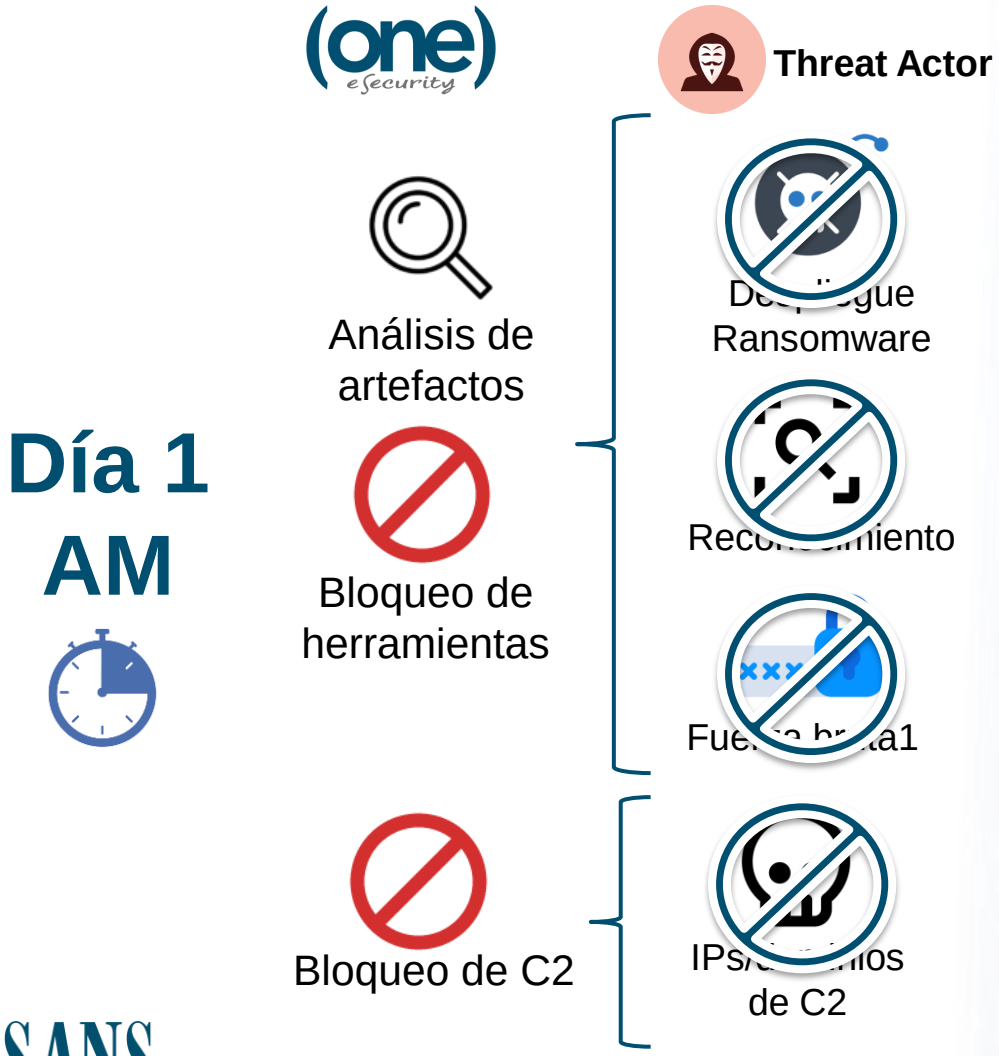
Contención

- Proteger backups
- Aislar de redes
- Desconectar DCs
- SOC alerta máxima
- Apoyo C-level
- Impacto al negocio

Frenar al actor (*tarpitting*)

- Deshabilitar cuentas comprometidas
- Cambio de credenciales masivo
- Bloquear IPs/dominios maliciosos
- Desplegar de Firewalls/Proxies
- Limitar opciones de entrada
- Actualizar AV

Caso 4: ¿Qué ocurrió?



Caso 4: ¿Qué ocurrió?

Día 1 - PM

Se identifica al actor:

CONTI

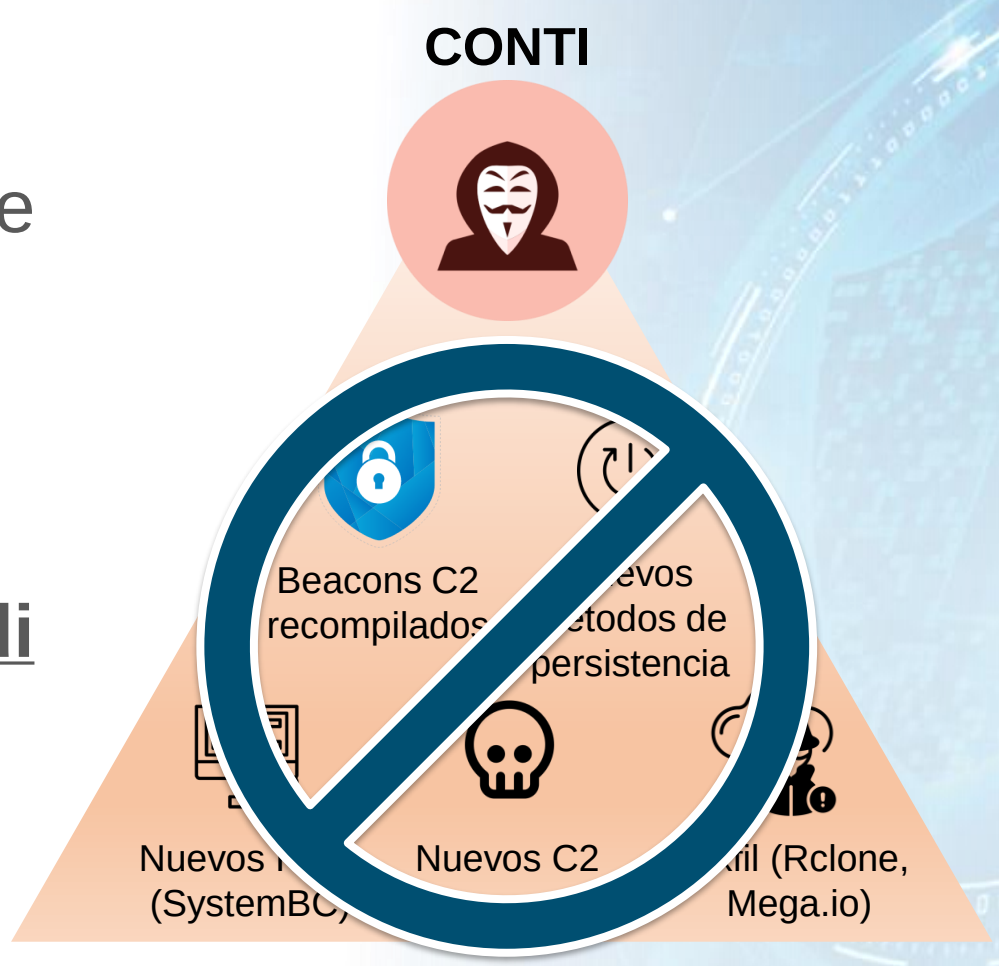
- Actor ruso
- **TOP Threat Actor**
- Ransomware as a Service **(RaaS)**
- Especializado en doble extorsión **(Robo de datos + Ransomware)**

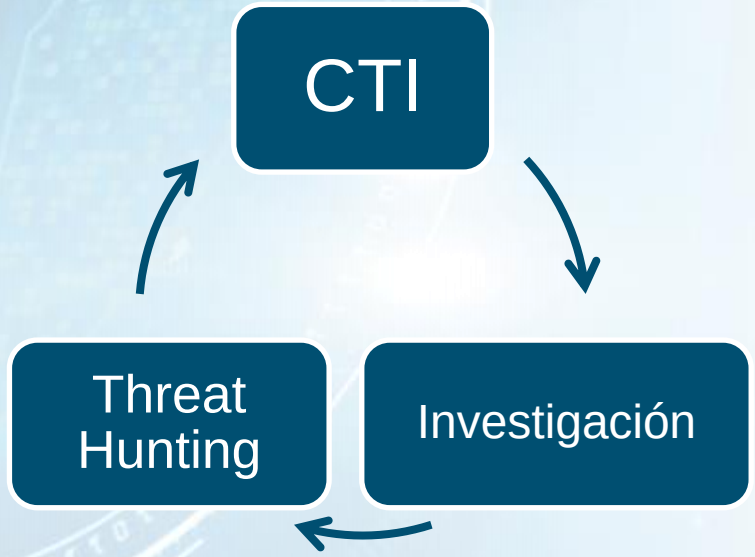
Caso 4: ¿Qué ocurrió?

Día 2

El actor sabe que está siendo contenido

<u>Cambia su modus operandi</u>





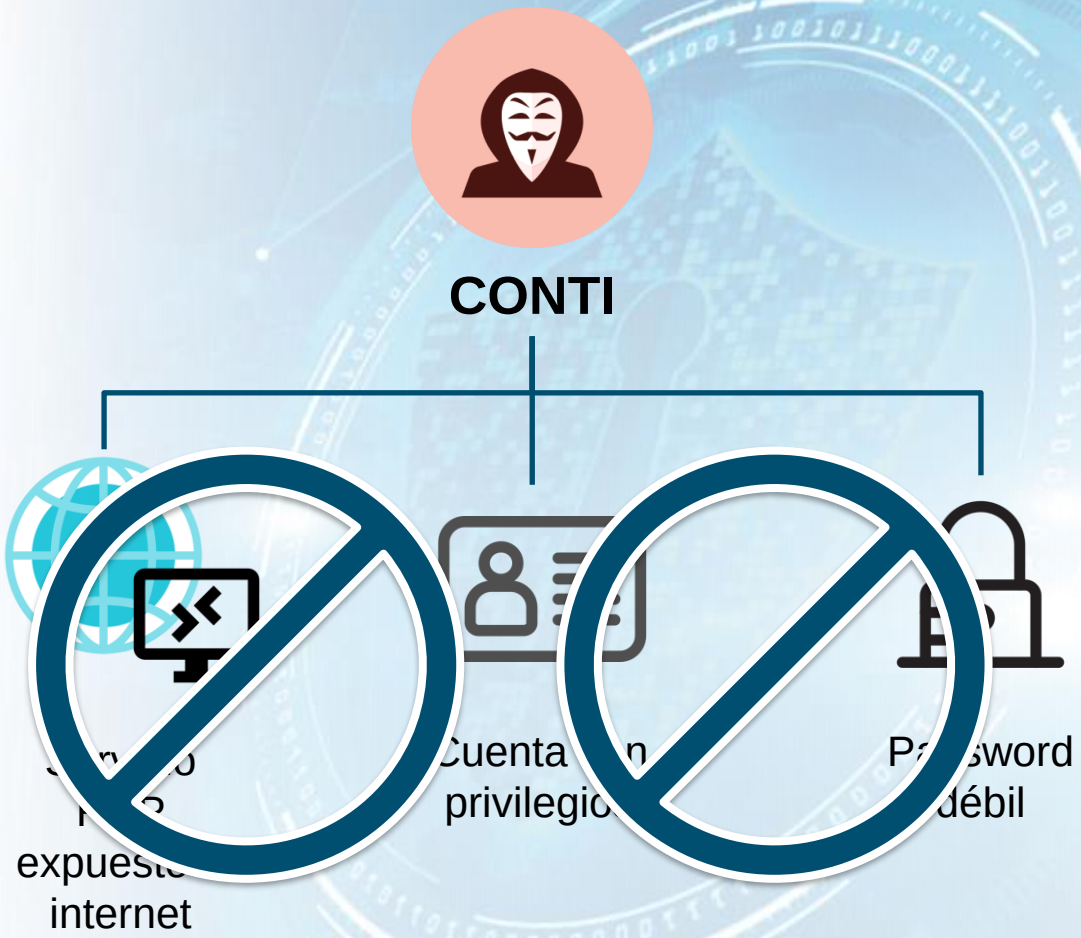
Caso 4: ¿Qué ocurrió?

Día 3

Se confirma el **punto de entrada**

Se continúa el **bloqueo de IOCs**

Último día de actividad del actor



Caso 4: ¿Qué ocurrió?

Siguientes 4 semanas

DCs comprometidos

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

Caso 4: Medidas generales

- Securización de acceso. remotos/VPN expuestos/vulnerables
- Segmentación de redes.
- Gestión robusta de credenciales.
- Optimización de capacidades de monitorización.
- Security awareness.
- Empleo de Ciberinteligencia.
- Servicio de **Threat Hunting**.

Factores de éxito: Camino a la madurez

Roadmap to Detection & Response Maturity

Detection & Response Maturity

Depth

Incident Response RETAINER

Technology	People &Talent	Monitoring	DFIR Assessment + Cyber Threat Intelligence	Cyber Exercises	Proactive Detection & Response	Purple Team
SIEM	Talent Recruitment	SOC	Threat Landscape (TL)	Workshops	Compromise Assessment (CA)	Adversary Emulation (AE)
EDR	Training & Knowledge Management: 1. Fundamentals 2. Advanced	Correlation	Incident Response Plan (IRP)	Cyber Exercises: 1. Tabletop 2. Top-bottom tabletop 3. Real interaction 4. Real offensive 5. Detectable activity 6. Real attacks	Threat Hunting (TH): 1. Intelligence based 2. Hypothesis based 3. Anomaly based	Deception
XDR	Knowledge Updates & Challenges	Use Cases	Data Source Analysis (DSA)		Managed Detection & Response (MDR)	
SOAR	Talent Retention Strategy	Cyber Threat Intelligence (CTI)	Playbooks			
		Artificial Intelligence (AI)	IRMM Gap Analysis			

¡Gracias!

Jess Garcia

@j3ssgarcia

jess.garcia@one-esecurity.com

one-esecurity.com

One_eSecurity

One eSecurity

www.one-esecurity.com/events_training/2024/mexico_22mar24.html

www.sans.org

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