



Amenazas digitales al sector financiero y sus clientes corporativos: retos y soluciones

Jess García

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

Founder and CEO of One eSecurity

Senior SANS Instructor

www.ds4n6.io - Project leader

The SANS logo, consisting of the word "SANS" in a large, white, serif font, positioned in the bottom right corner of the slide.

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

Índice

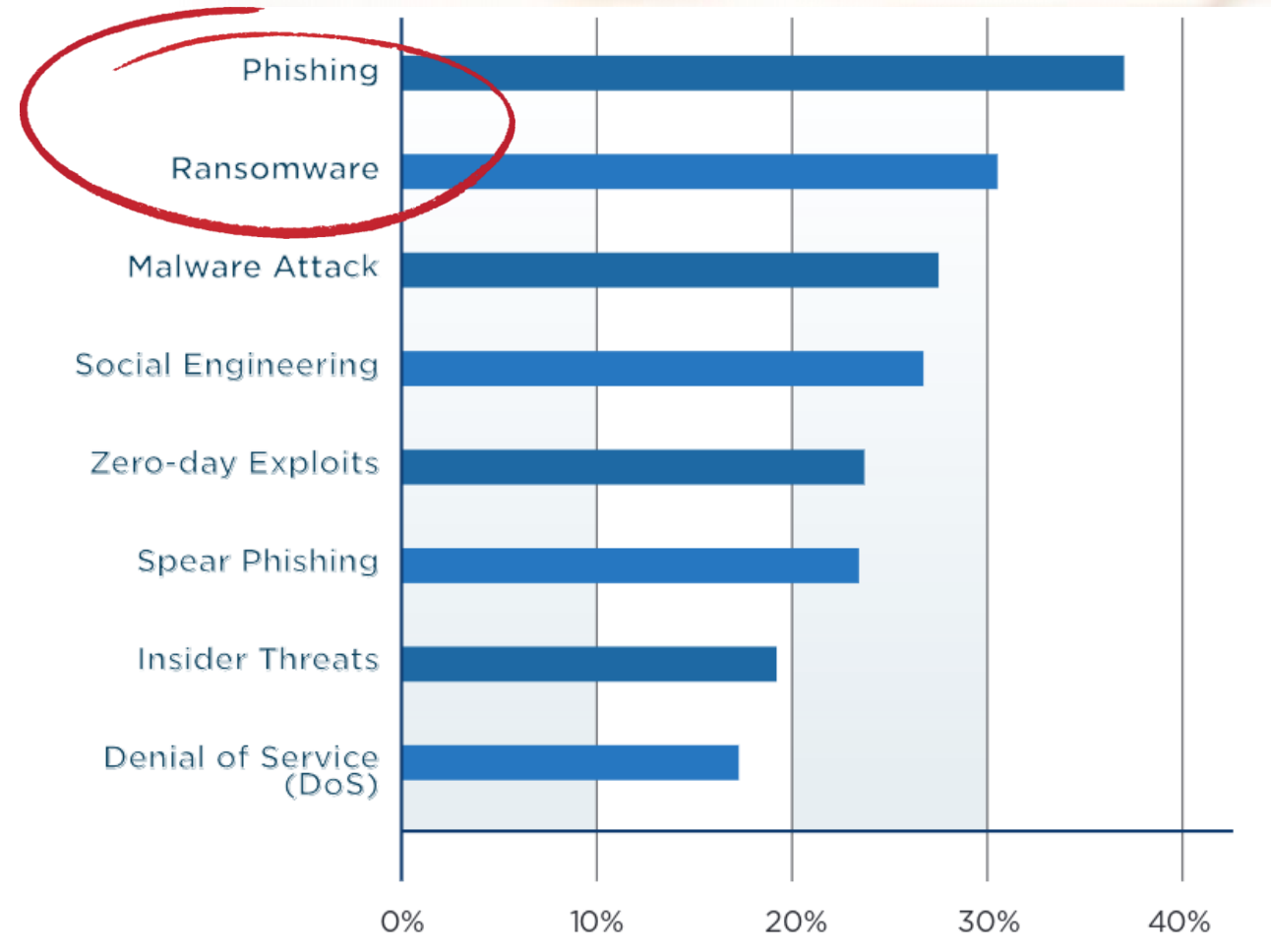


- Actores operando en LATAM
- Casos reales
- Roadmap to Detection & Response Maturity

Actores operando en LATAM en los últimos años

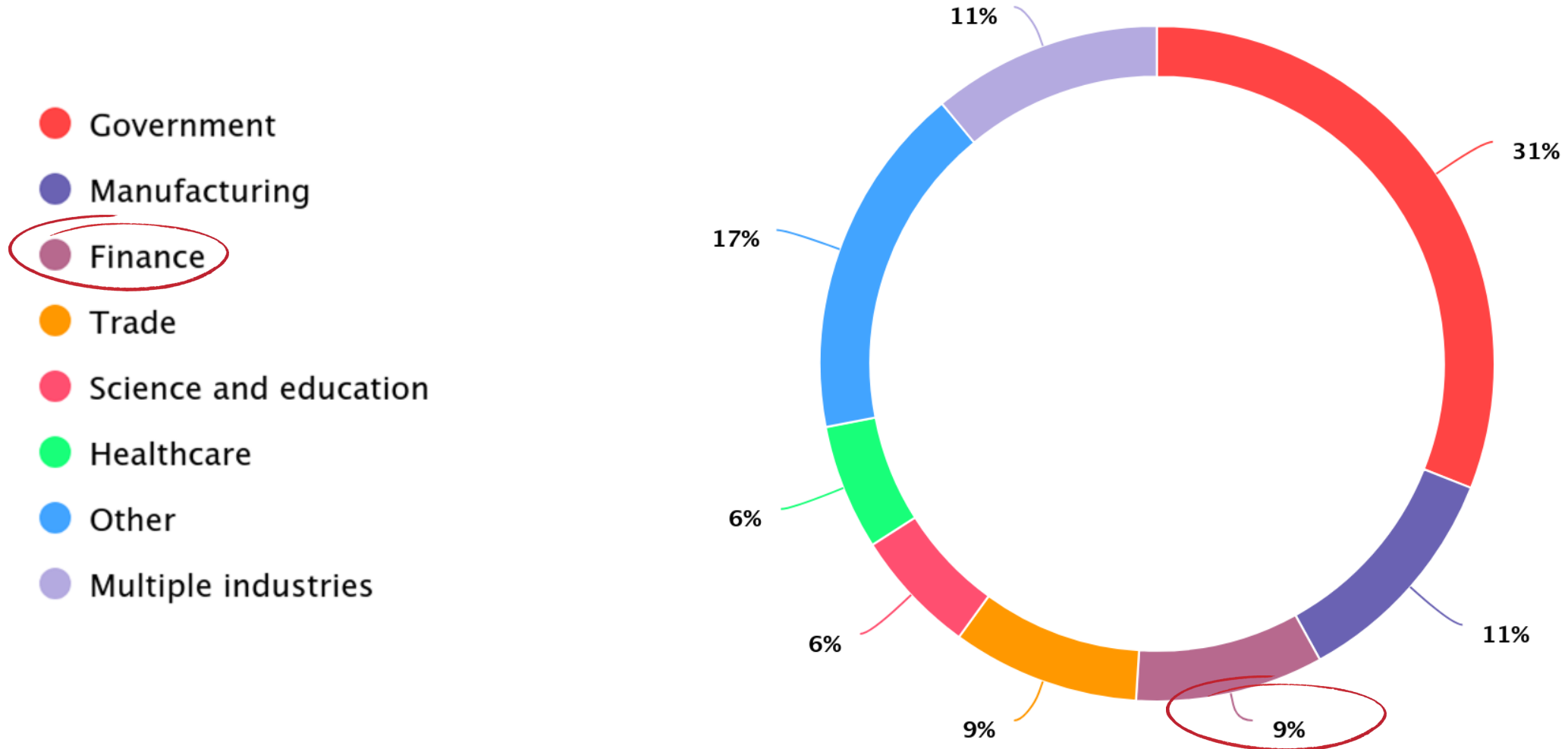
TOP Ataques LATAM 2023

- 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

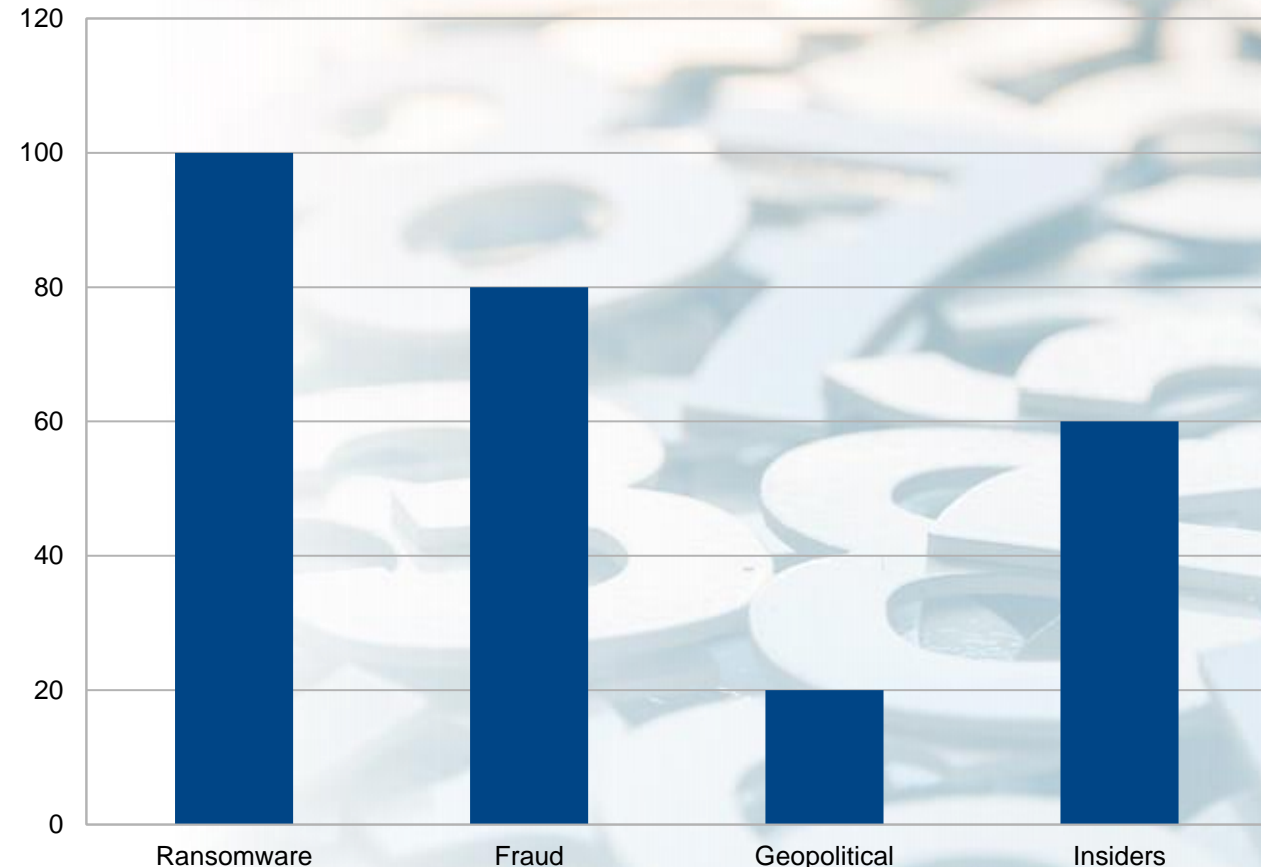
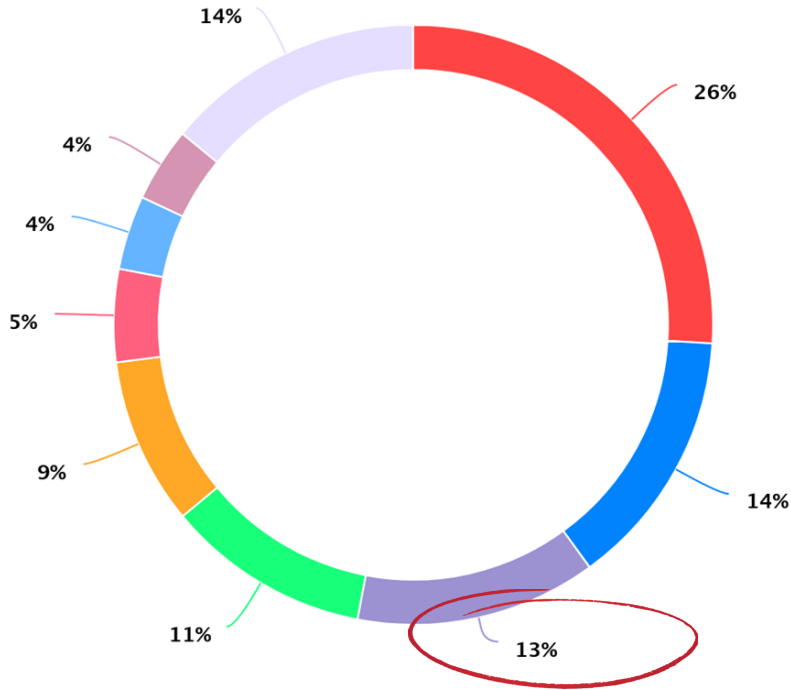


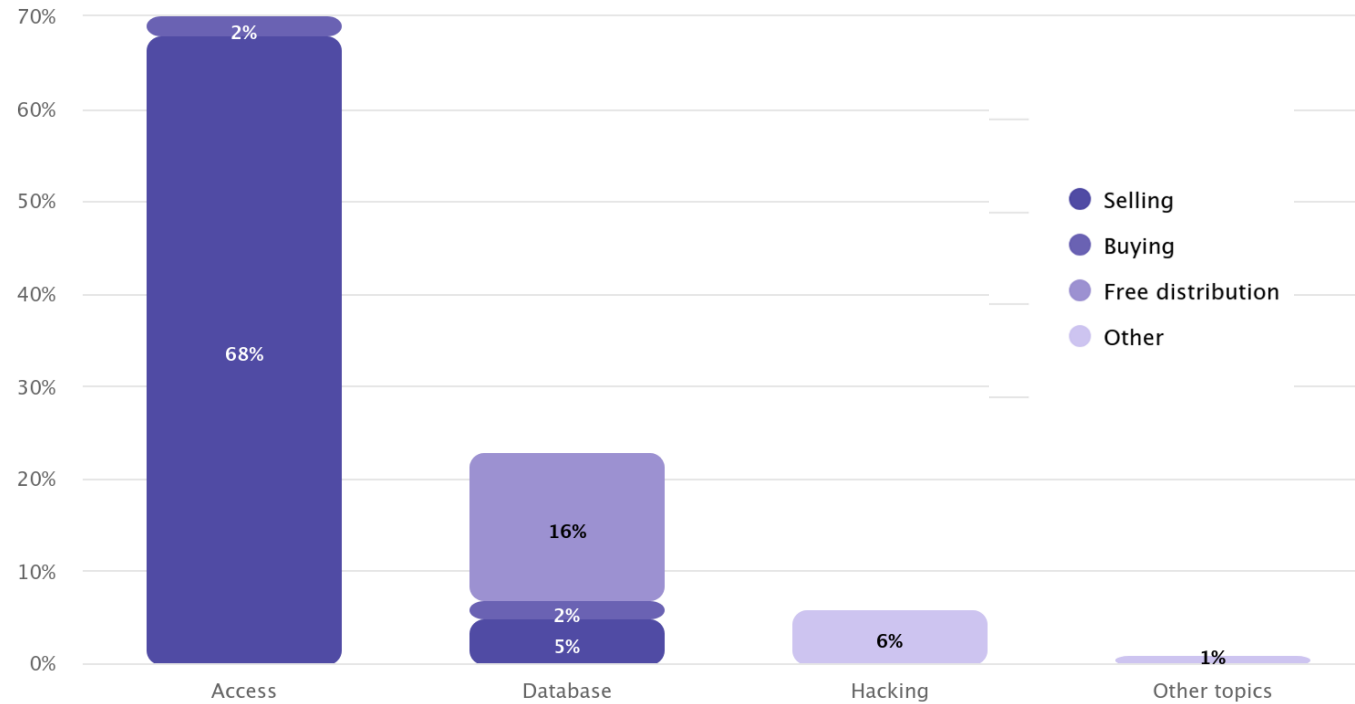
Gráfico de elaboración propia

Datos robados en LATAM 2023

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



- Brazil
- Argentina
- Mexico
- Chile
- Peru
- Ecuador
- Colombia
- Costa Rica
- Other



Threat actors en Mexico actualmente

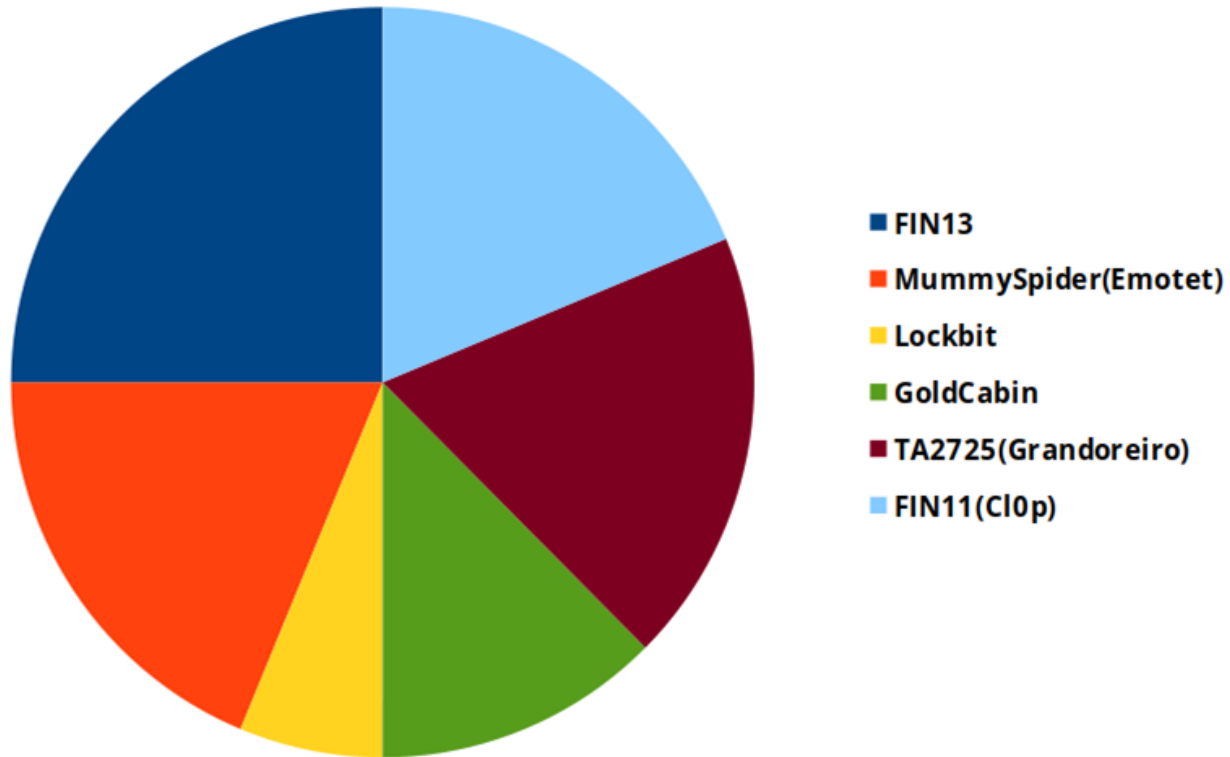


Gráfico de elaboración propia

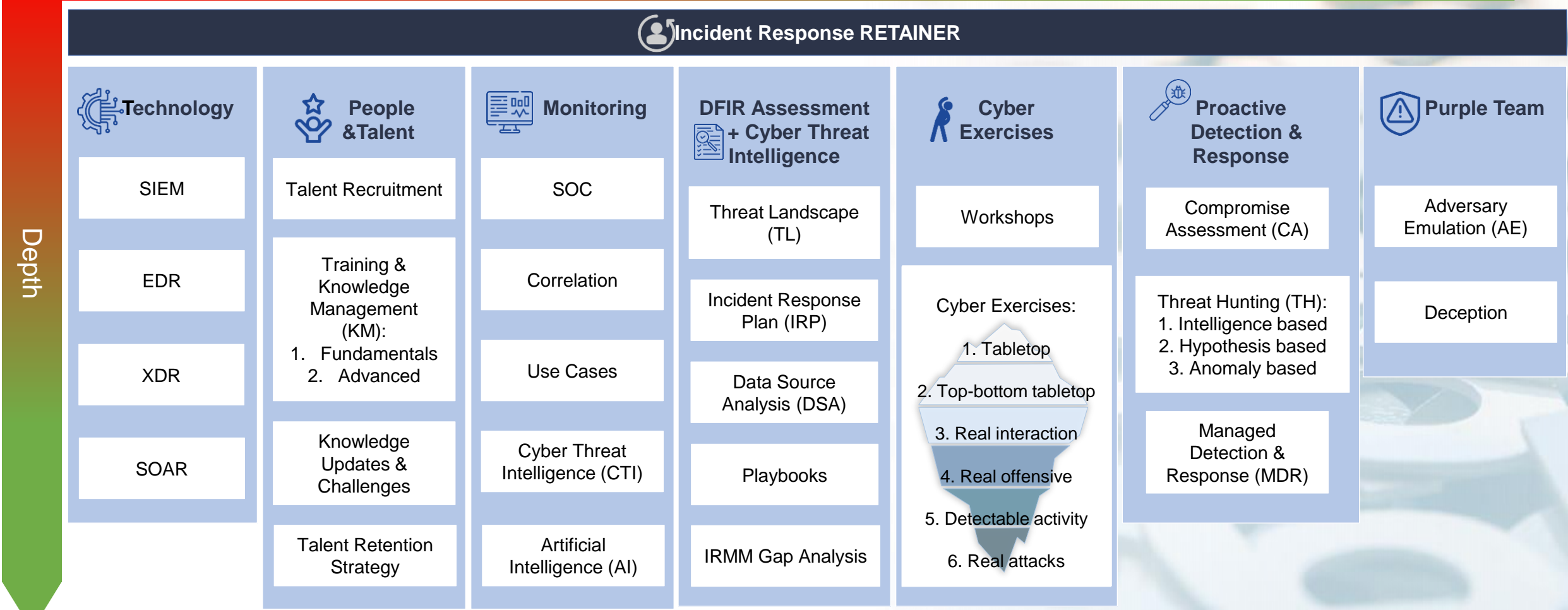
- Grupo FIN13 ataca México robando información sensible.
- MummySpider, usando Emotet acaba lanzando desde robos a Ransomwares.
- Lockbit, uno de los grupos de Ransomware con más ingresos del mundo.
- GoldCabin relacionado con los famosos Bumblebee, icedID o Qbot.
- Grandoreiro, uno de los Bankers más utilizados en LATAM.
- FIN11 con el ransomware CI0p como herramienta principal

Antes de comenzar con
casos reales...

Roadmap to Detection & Response Maturity

Detection & Response Maturity

Incident Response RETAINER



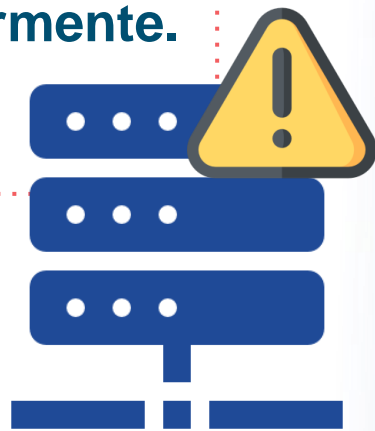
Casos reales en LATAM

Caso 1: Fraude Transacciones fraudulentas como legítimas

Caso 1: ¿Qué ocurrió?

1. Servidor web comprometido anteriormente.

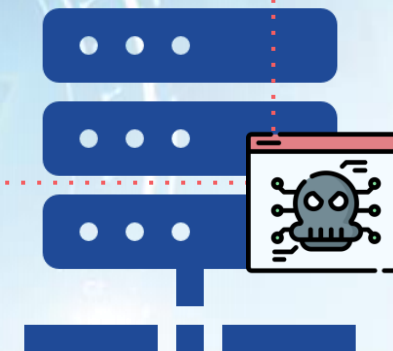
Mala erradicación



2. Servidor web continua siendo vulnerable
File upload

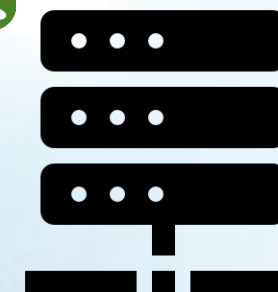
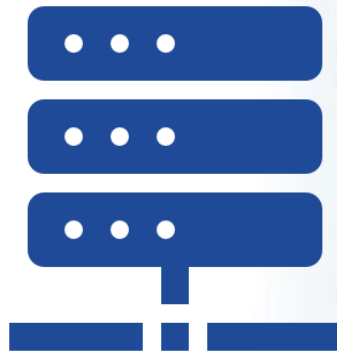
3. Meses después el atacante vuelve a aprovechar la misma vulnerabilidad

Despliegue de herramientas
Webshells y backdoors para persistencia



Caso 1: ¿Qué ocurrió?

1. Ciberatacante consigue credenciales
Archivo txt



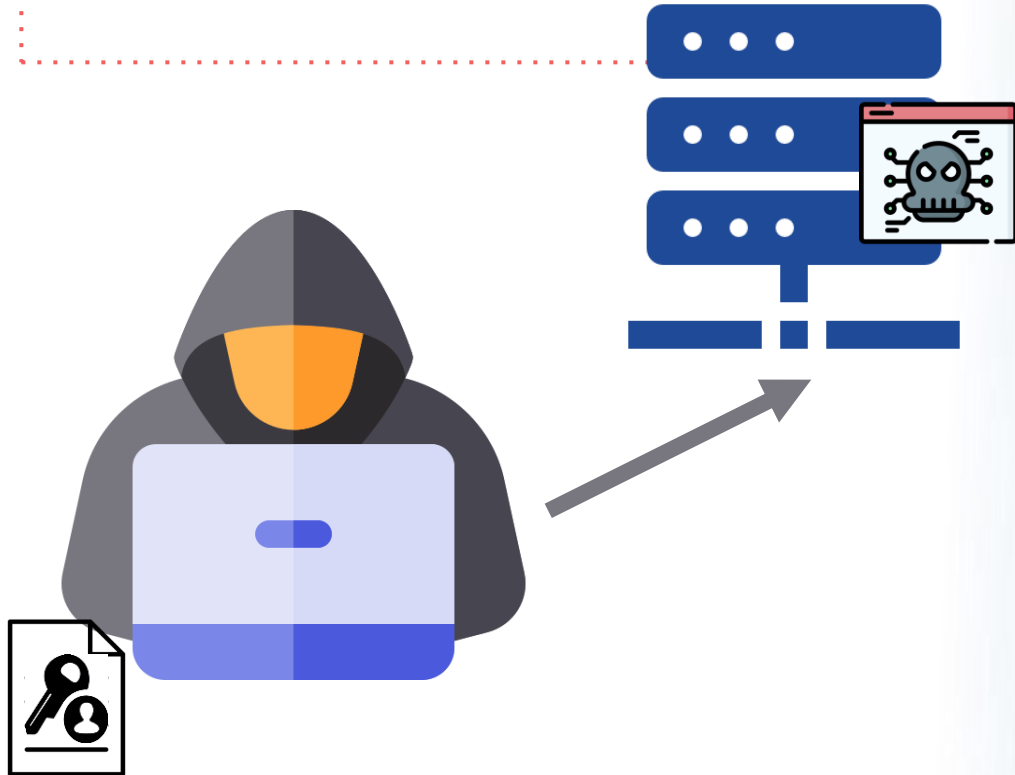
2. Realiza reconocimiento y movimiento lateral durante 8 meses

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

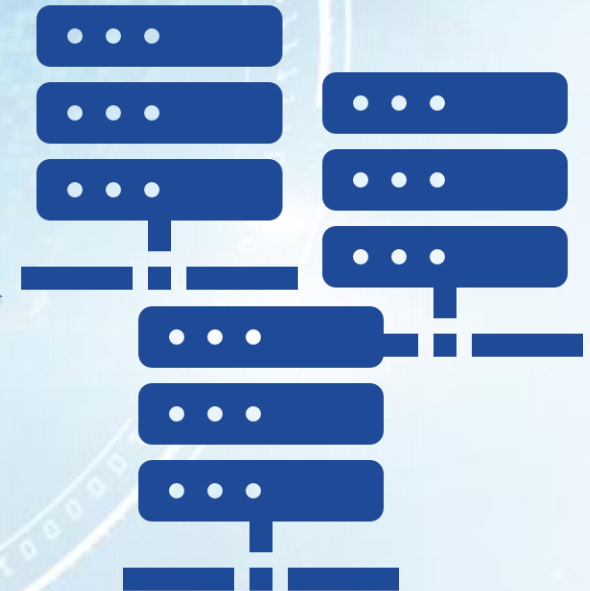
Caso 1: ¿Qué ocurrió?

1. Modificación de archivos de transacciones legítimas



3. Ejecución de transacciones con cambios en el destinatario

2. Cifrado de transacciones fraudulentas con proceso legítimo

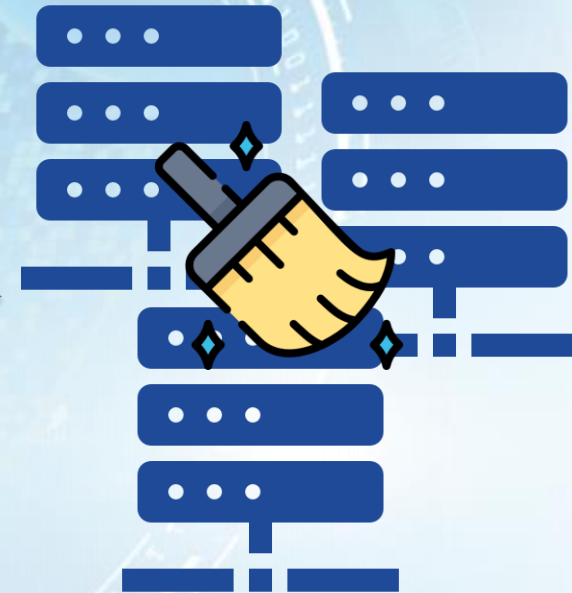


4. Se obtienen altas cantidades de dinero



Caso 1: ¿Qué ocurrió?

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



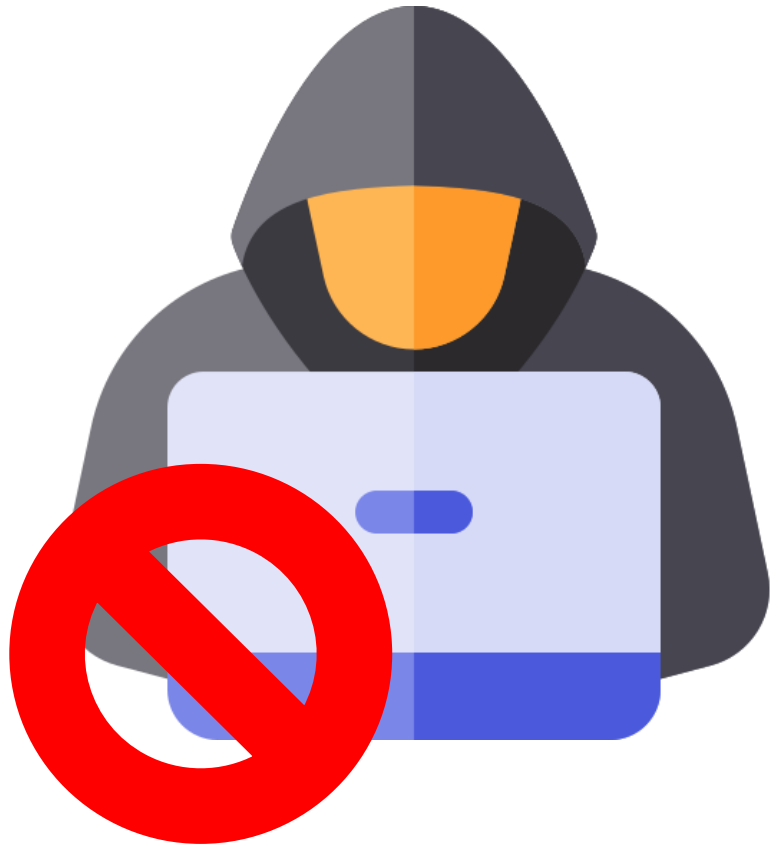
2. Detección y erradicación inmediata



¿Qué pudo haberse hecho?

¿Ustedes, qué opinan?

Caso 1: 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 2: Suplantación de identidad

Caso 2: ¿Qué ocurrió?



Caso 2: ¿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.



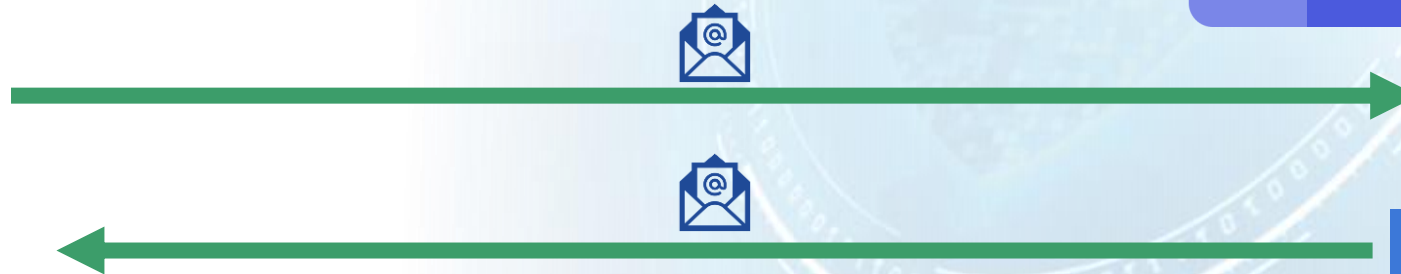
Empleado



Ciberatacante



Colaborador



Caso 2: ¿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 2: ¿Qué ocurrió?

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



Empleado



Ciberatacante



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



¿Qué pudo haberse hecho?

¿Ustedes, qué opinan?

Caso 2: Medidas generales



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 3: Ataque a la cadena de suministro

Caso 3: ¿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 3: ¿Qué ocurrió?

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

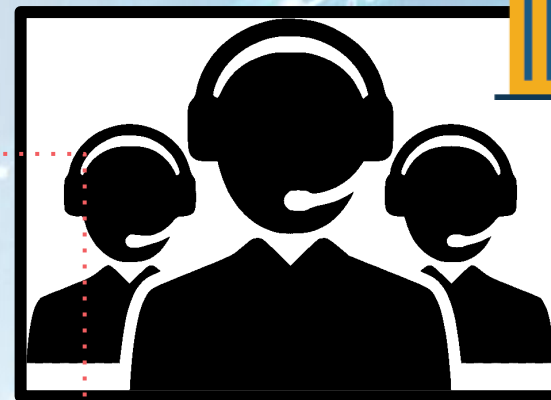


2. Realiza movimientos laterales y ataques de password
Obtiene credenciales de varios empleados del Call Center

Caso 3: ¿Qué ocurrió?



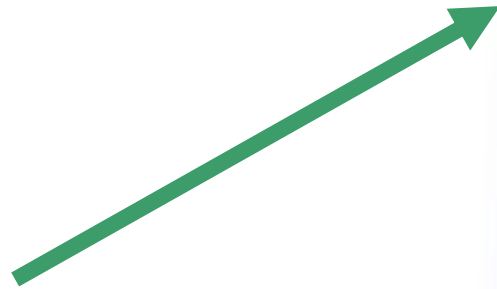
1. Atacante modifica condiciones de clientes de la empresa



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

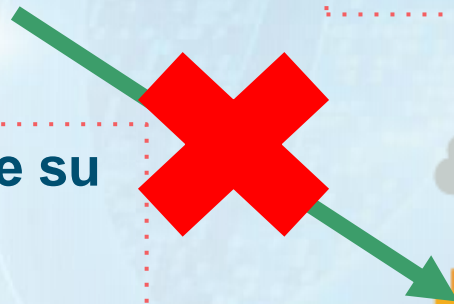


Caso 3: ¿Qué ocurrió?

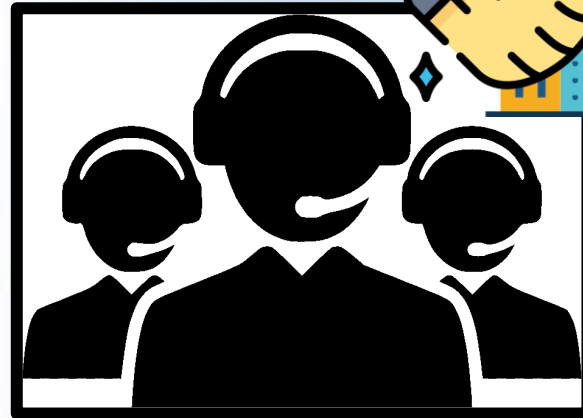
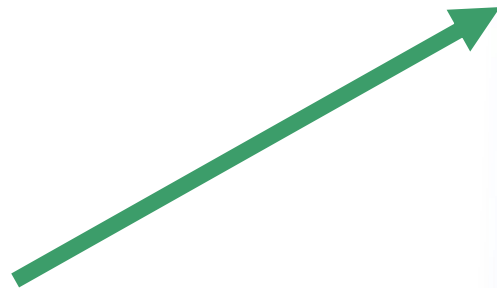


2. La empresa se aísla de su Call Center y éste no puede dar servicio a su cliente

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



Caso 3: ¿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.

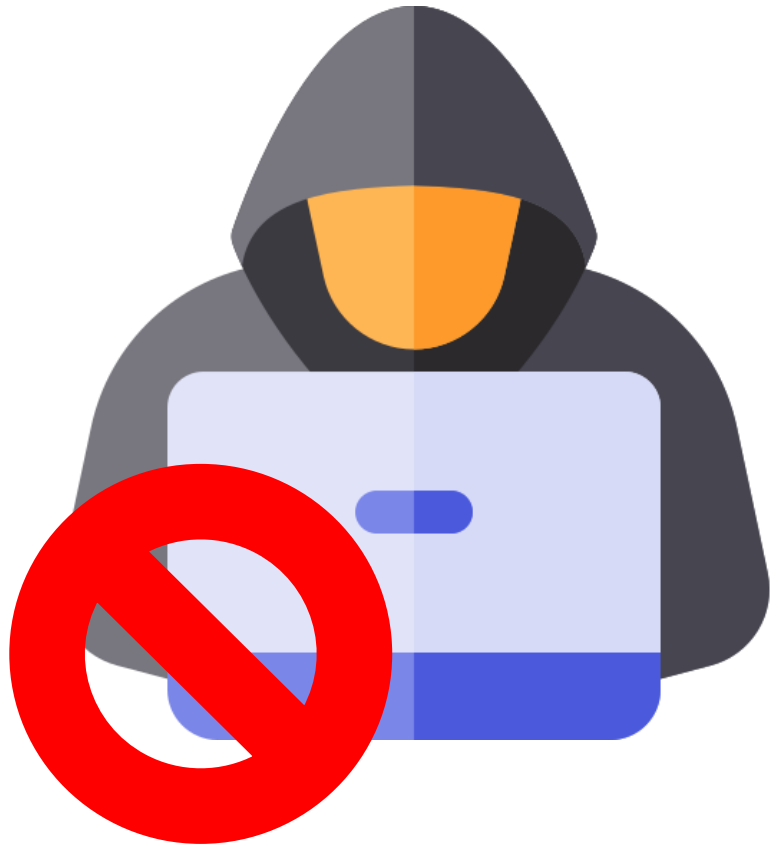




¿Qué pudo haberse hecho?

¿Ustedes, qué opinan?

Caso 3: Medidas generales



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.

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



Alerta del SOC



Caso 4: ¿Qué ocurrió?

Alcance del ataque

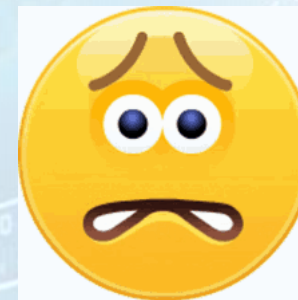


Estados Unidos

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



Riesgo de propagación mundial



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 (*tarpping*)

 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)



Manual
filtrado de
CONTI

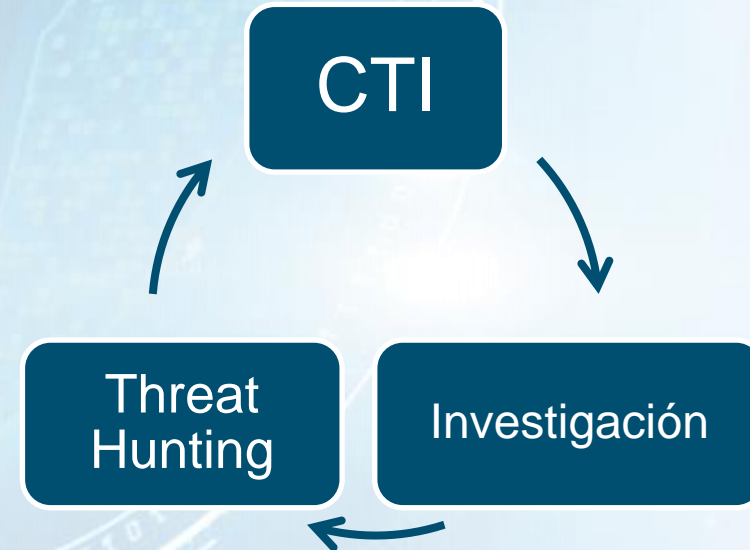
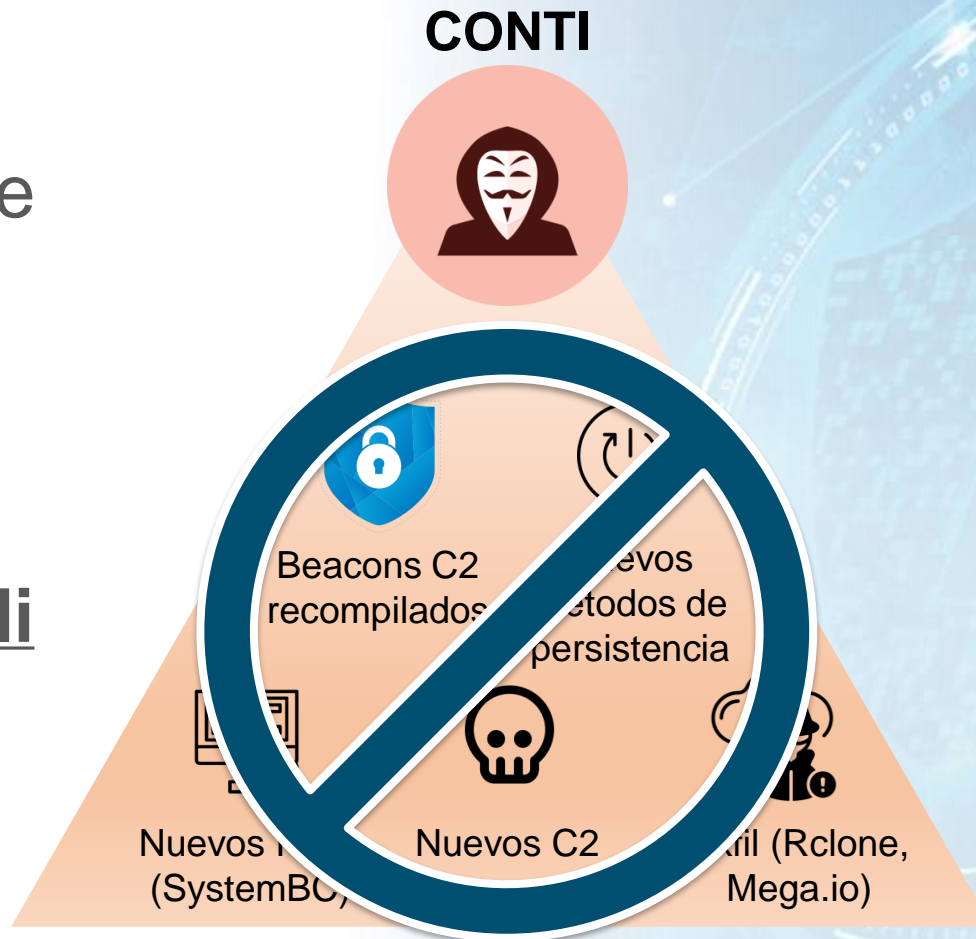


Caso 4: ¿Qué ocurrió?

Día 2

El actor sabe que está siendo contenido

Cambia su modus operandi



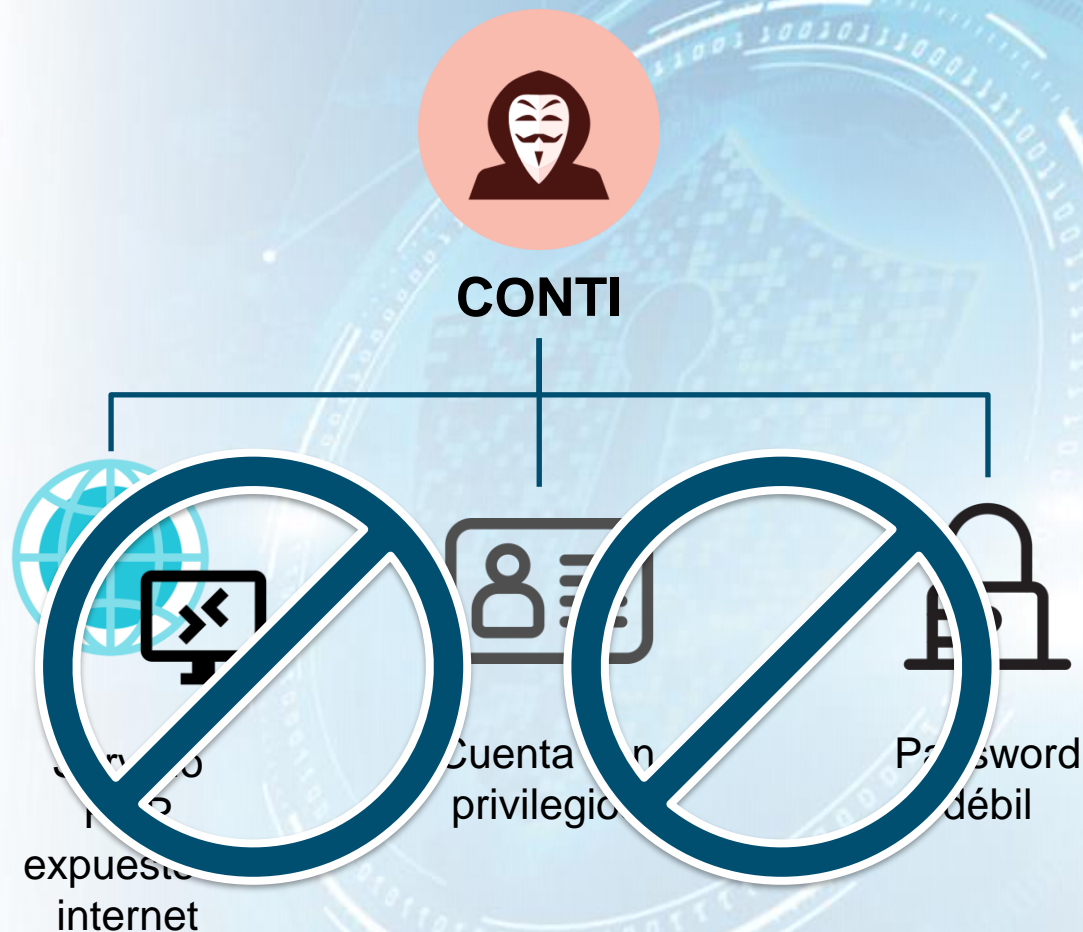
Caso 4: ¿Qué ocurrió?

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!



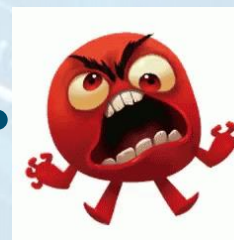
Ciclo de TH continuo
24x7



Continúa la limpieza y la
recuperación



Mejoras de seguridad



Hacerle la vida
imposible al atacante



¿Qué pudo haberse hecho?

¿Ustedes, qué opinan?

Caso 4: Medidas generales



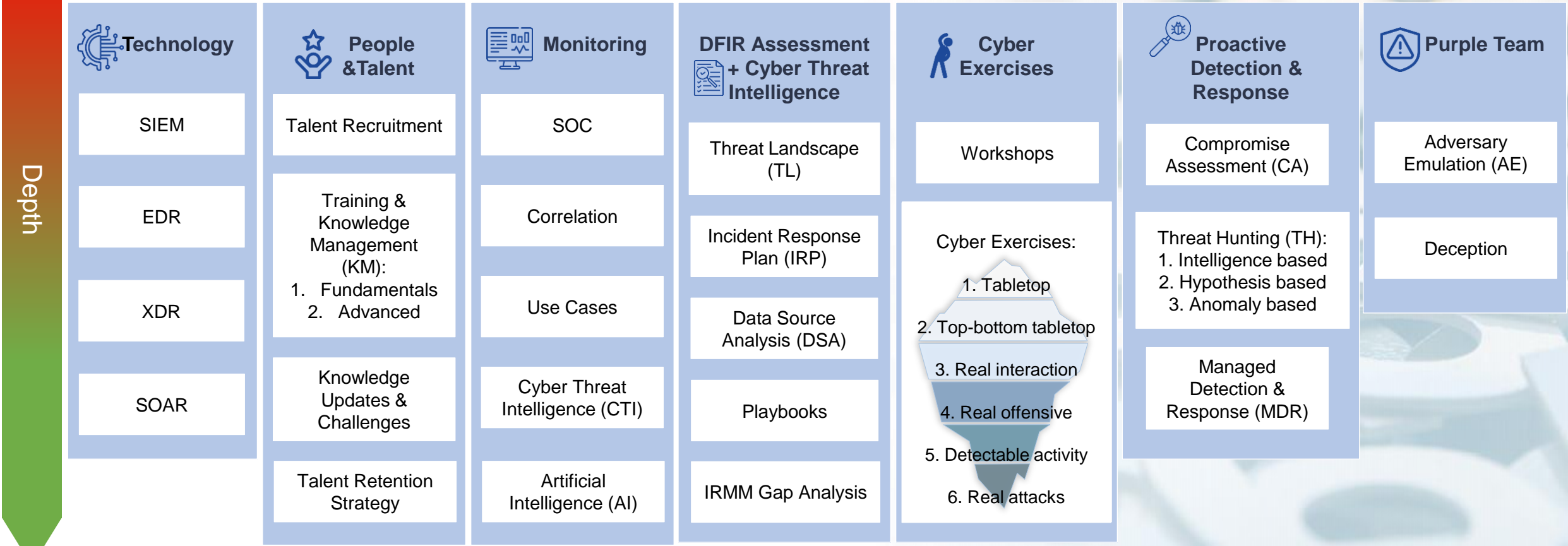
- Securización de accesos remotos/VPN expuestos/vulnerables
- Segmentación de redes
- Gestión robusta de credenciales
- Optimización de capacidades de monitorización
- Security awareness
- Empleo de Ciberinteligencia
- Servicio de Threat Hunting

Factores de éxito: Camino a la madurez

Roadmap to Detection & Response Maturity

Detection & Response Maturity

Incident Response RETAINER





¡Gracias!

Jess Garcia


@j3ssgarcia

jess.garcia@one-eseurity.com


SANS

www.sans.org



 one-eseurity.com

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

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



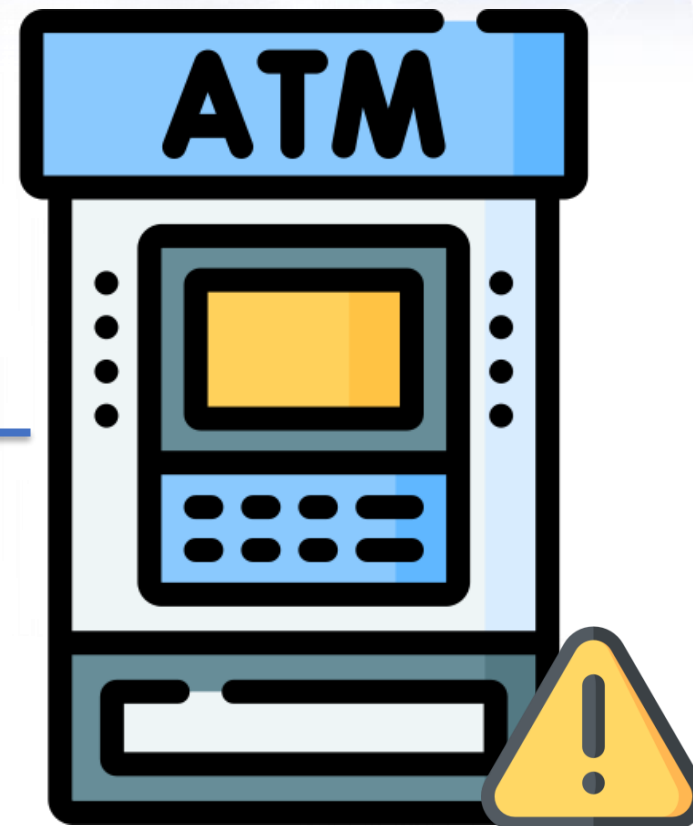
www.one-eseurity.com/events_training/2024/mexico_20mar24.html

(BONUS) Jackpotting Robo en cajeros

Caso 3: ¿Qué ocurrió?



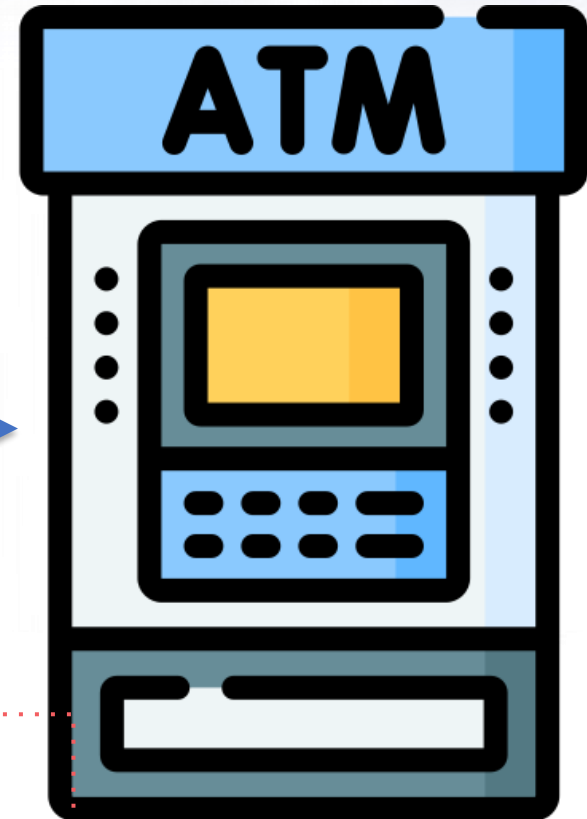
1. Se detecta extracción de altas cantidades de dinero que provienen de cajeros



2. Cajeros vulnerables
Ataque blackbox

Caso 3: ¿Qué ocurrió?

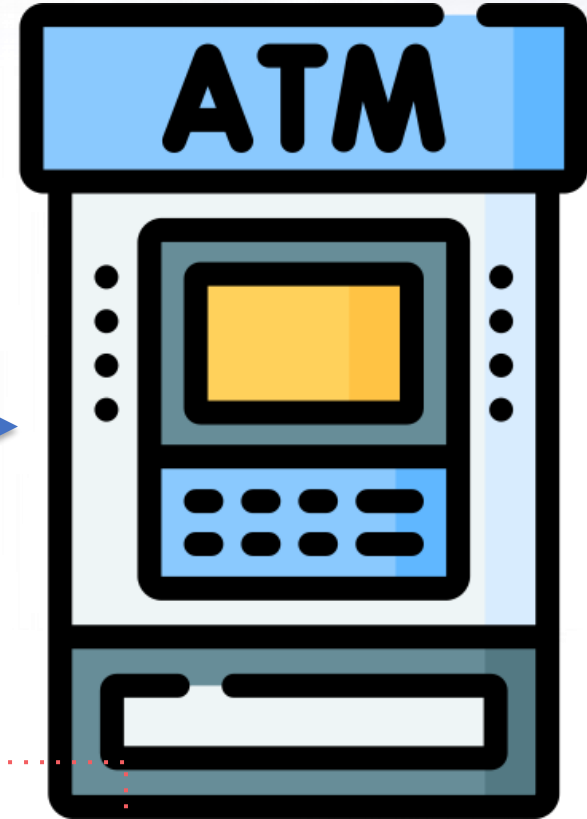
1. Autores desmonta en varias ocasiones un mismo ATM para conectar un dispositivo Blackbox que proporciona acceso directo al SW del ATM.



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

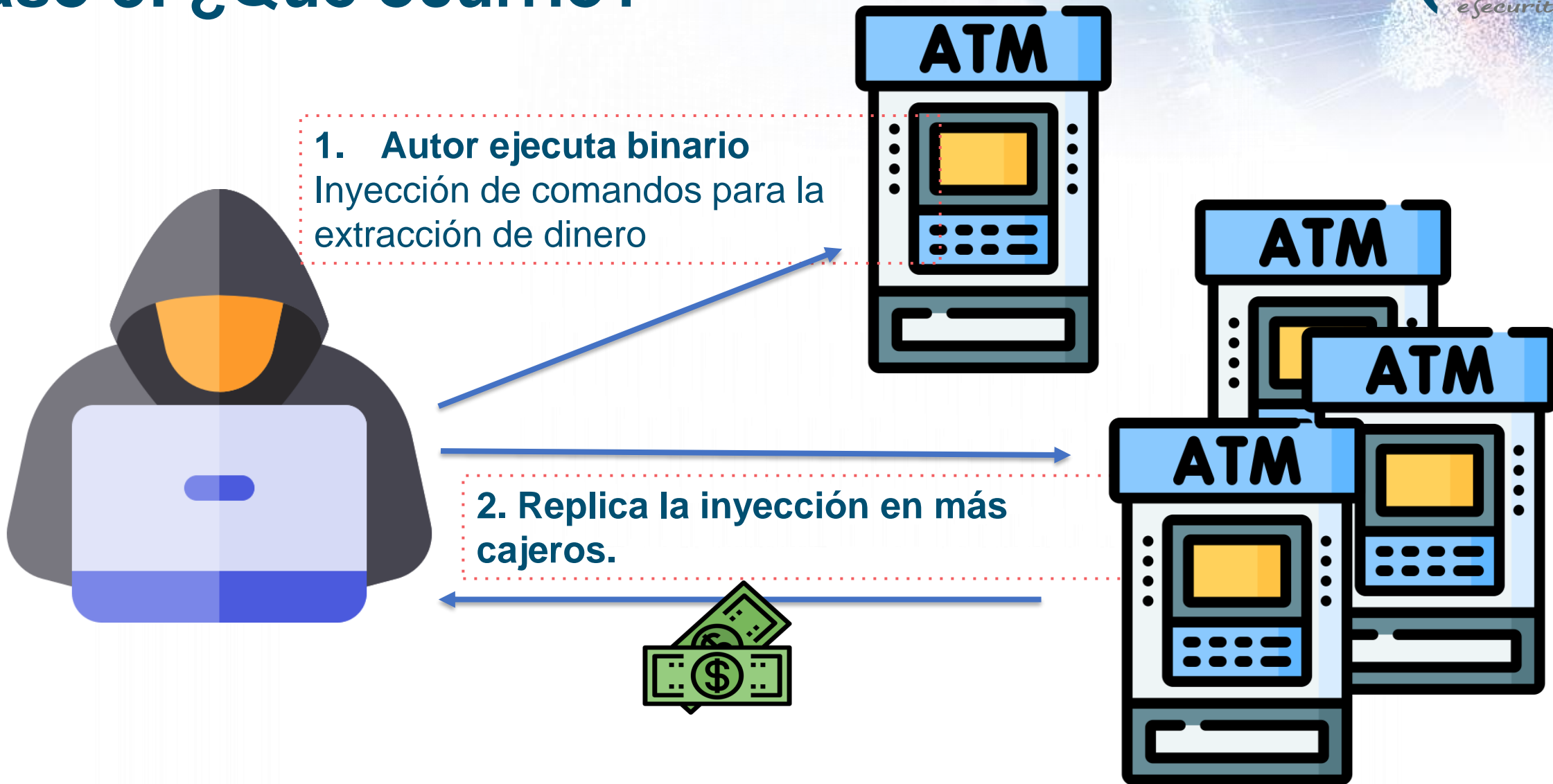
Caso 3: ¿Qué ocurrió?

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 3: ¿Qué ocurrió?



Caso 3: ¿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.



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