Readiness · Hunting · Detection · Response

ENISE 2022

whoami - whoisone

ONE SERVICES

>250 DFIR Services
>120 SANS Trainings
>100 TH & Cycon

ONE SERVICES

>85.000 DFIR Hours
>7.000 SANS Hours
>25.000 TH & Cycon Hours

CASES MANAGED

> 200
Complex Investigation EIR/DFIR Cases since 2007

COUNTRIES SERVICED

>20 Countries
DFIR Services

Antes de la batalla: ¿Qué es un Retainer?

- Servicio de respuesta a incidentes externalizado
  - Emergency Incident Response (EIR)

- Expertos on Call - Follow the Sun. Tiempo de respuesta garantizado

- Formato de bolsa de horas.
- Si no incidente-> Readiness, IR Plans, Ejercicios

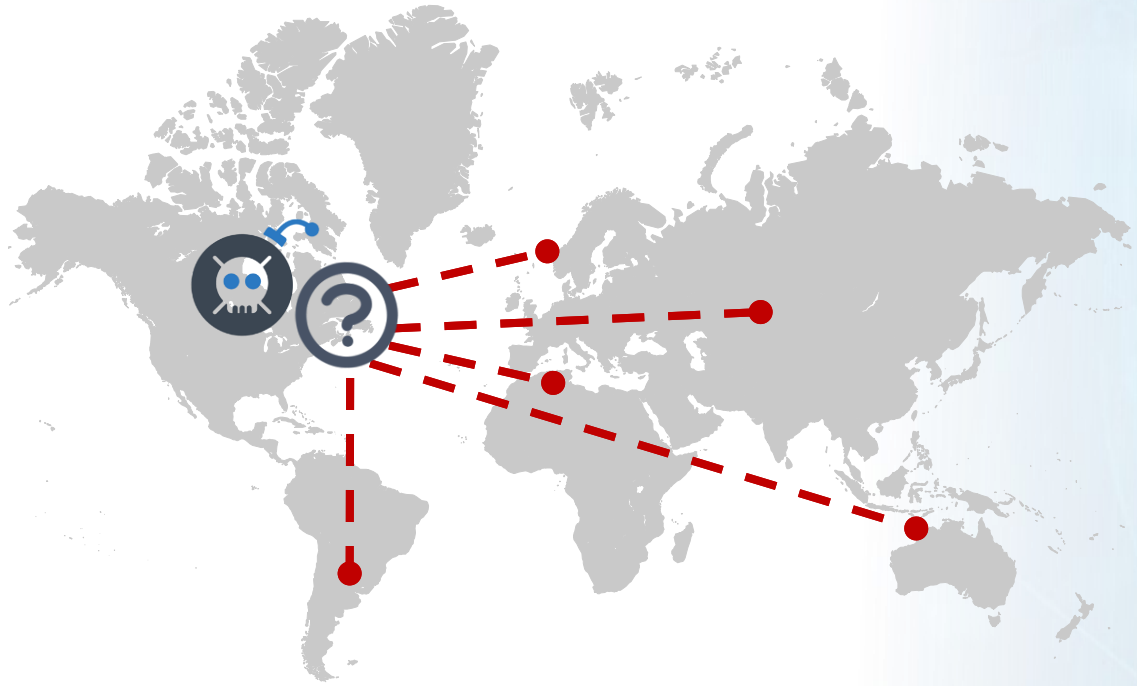
- Relación ya establecida:

  - Conocimiento de la infraestructura y del equipo
  - Accesos ya disponibles a la plataforma. Tanto de cliente como propias.
  - Plataformas de Análisis Forense y entorno Colaborativo ya establecidos.

- ¿Por qué fue esto importante?

Dia 0 : Contexto

Empresa global.
5000 servidores. 350 controladores de dominio. 12000 endpoints.
Riesgo inminente de despliegue de ransomware



Alerta del SOC

Herramientas de Pre-Ransomware encontradas

5 máquinas infectadas

Posible propagación a otras regiones

Dia 0: Activación Retainer

Despliegue de fuerzas.

15+ Personas

- Incident Managers
- Incident Responders
- Investigadores
- Analistas de CTI
- Threat Hunting Team
- Ciber Operaciones 24x7

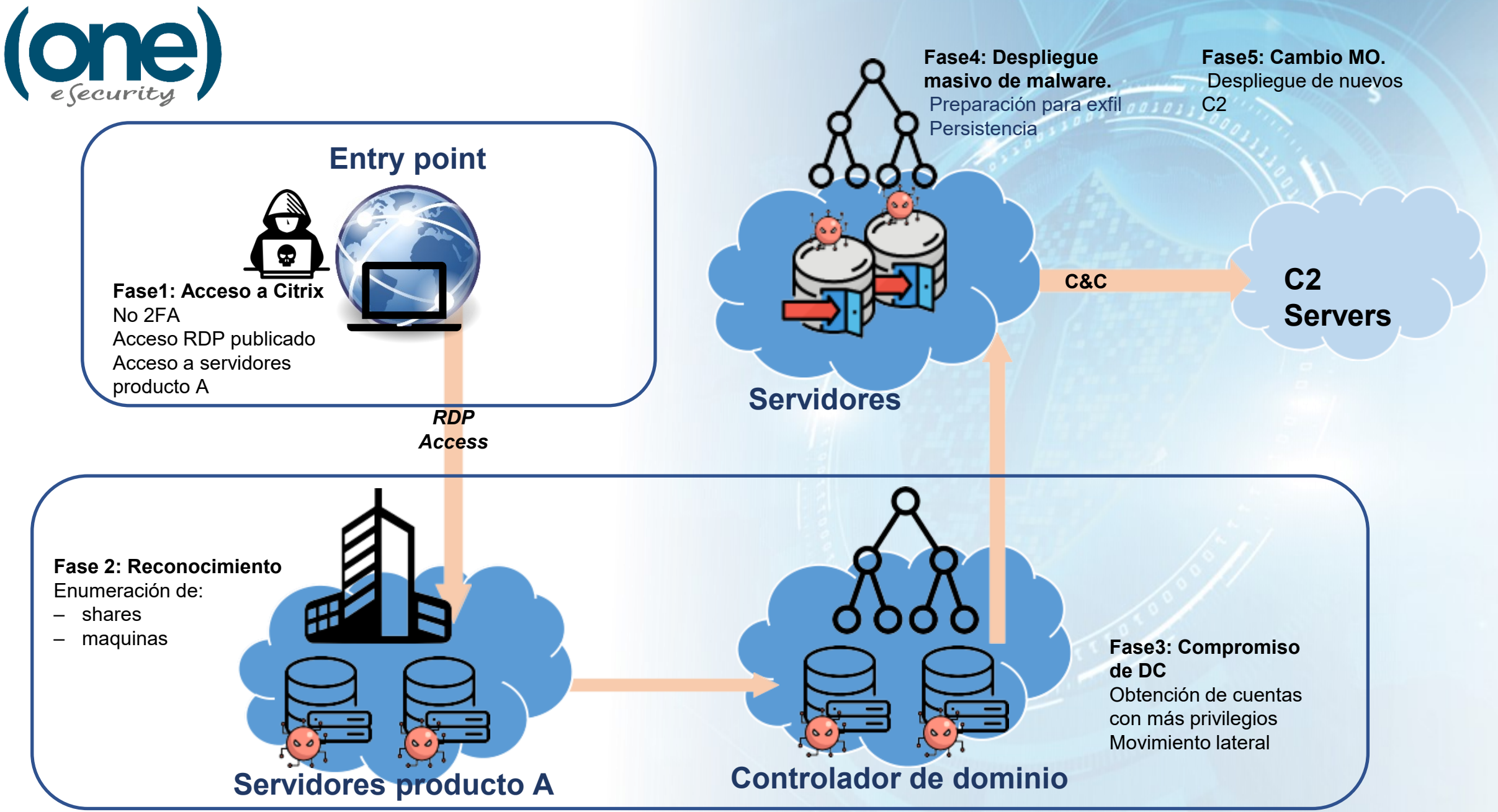
- Despliegue masivo de agentes
- Monitorización /protección DC
- Actualización masiva de AV
- Ingeniería

20+ personas

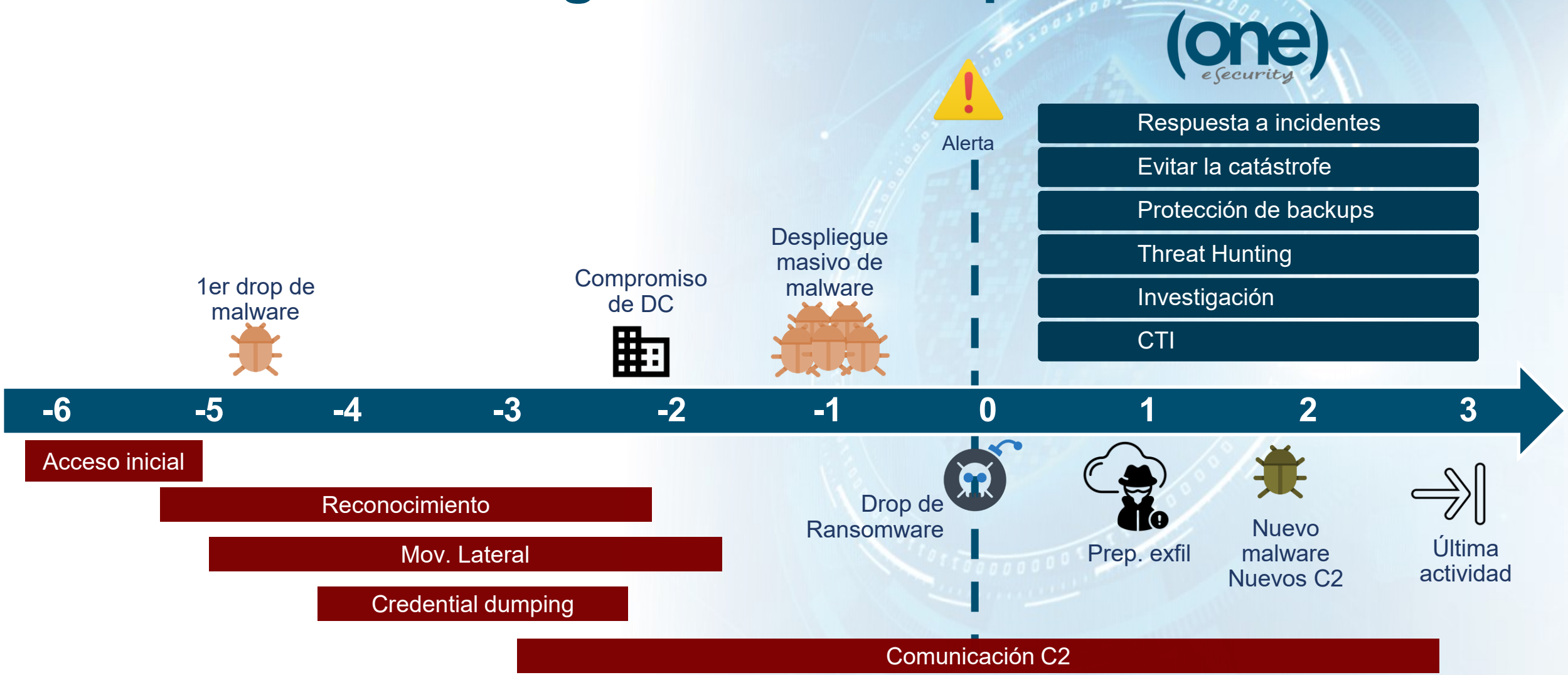
- CISO & C-level
- Equipo de ciberseguridad
- Responsable de IT
- SOC
- Relaciones Públicas
- Legal

Dia 1: Respuesta Multihilo Tarpitting

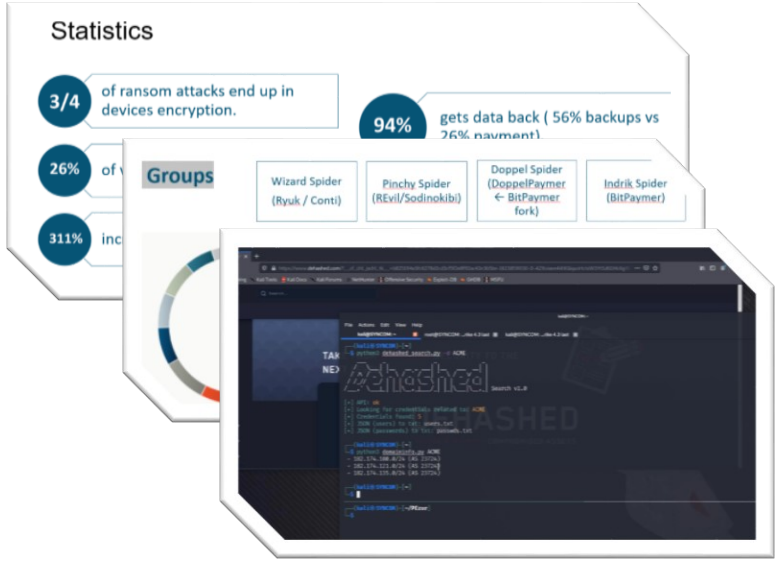
- Threat hunting
- Contención en AD
- CTI
- Coordinación SOC
- Backup Isolation
- Investigación
- Despliegue herramientas
- Coordinación con telecomunicaciones y arquitectura.
- Reversing
- Comunicación con Negocio
- Operaciones plataforma forense


Entry point
Fase1: Acceso a Citrix
No 2FA
Acceso RDP publicado
Acceso a servidores producto A
RDP Access
Fase4: Despliegue masivo de malware.
Preparación para exfil
Persistencia
Fase5: Cambio MO.
Despliegue de nuevos C2
Servidores
C&C
C2 Servers
Fase 2: Reconocimiento
Enumeración de:
– shares
– maquinas
Servidores producto A
Controlador de dominio
Fase3: Compromiso de DC
Obtención de cuentas con más privilegios
Movimiento lateral

Metodología: Línea Temporal



Ransomware:
Lecciones desde las trincheras



Desde las trincheras:
Sobreviviendo a una intrusión avanzada de Ransomware

one-esecurity.com/ens21

one-esecurity.com/sticco22

Cómo podemos ayudar:

Our services

- Emergency Incident Response (EIR)
- Digital Forensics (DFIR)
- Threat Hunting (TH)
- Managed Detection & Response (MDR)
- Compromise Assessment
- Cyber Consulting (CyCon)
- Cyber Exercises (CybEx)
- Cyber Insurance (CybIns)

Our Differential Value

- Cyber Threat Intelligence (CTI)
- Data Science and Artificial Intelligence (DS/AI)
- Next Generation Forensic Lab: SKY
- Cyber Operations (CybOps) 24x7

one-esecurity.com

Antonio Diaz
@thedfirofficer

Thanks!

one eSecurity

www one-esecurity.com

One_eSecurity

One eSecurity