#STICPUNTACANA

LOS ÉXITOS SON REPETIBLES

Desarrollo de un plan de madurez ante incidentes, más allá de la respuesta heróica

Jess Garcia
Founder & CEO of One eSecurity

(one) eSecurity

CCN-CERT centro criptológico nacional
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)
DNI REPÚBLICA DOMINICANA
OEA Más derechos para más gente
BID
Barceló Bávaro Grand Resort

Who am I

Jess Garcia
@j3ssgarcia

- Fundador y CEO de One eSecurity
  25 años de experiencia
- Compañía global de DFIR
  15 años
- Líder del proyecto DS4N6
  www.ds4n6.io
- Senior Instructor en SANS Institute
  20 años

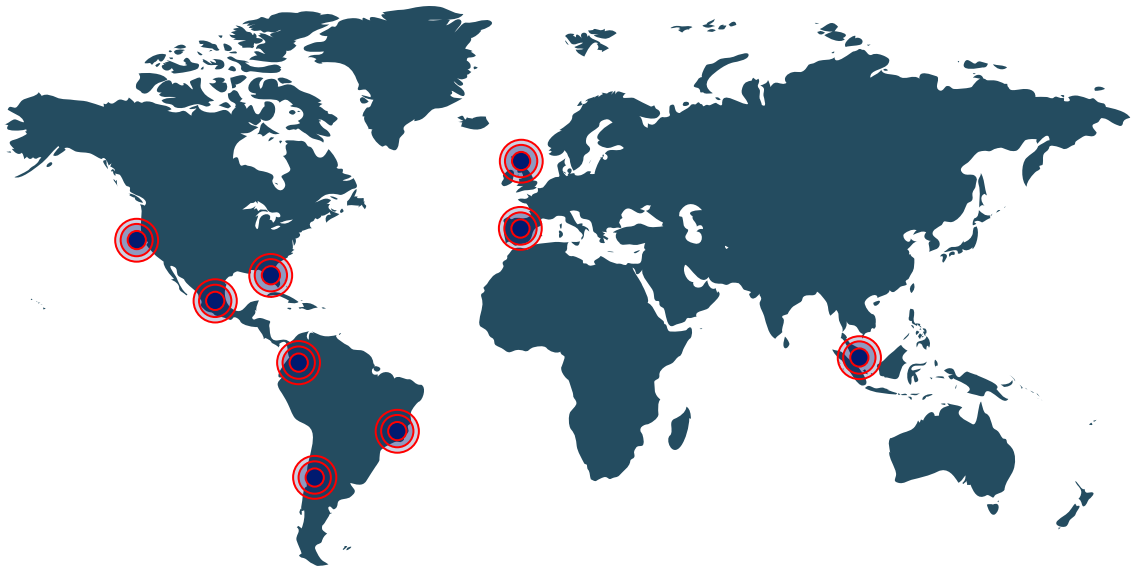
Who we are

One eSecurity es un especialista **líder del mercado en Servicios y Tecnología de Análisis Forense Digital y Respuesta a Incidentes** (DFIR) desde 2007.

- **Flexibilidad y Adaptabilidad**
- **Proveemos cualquier servicio del universo DFIR**
- **Visión y Foco Forense en cualquier proyecto**
- **Equipo de élite altamente especializado**
- **Clientes: G. Fortune 500 y Organismos Internacionales**

Who we are

Estamos siempre preparados para apoyar a nuestros clients sin importer el lugar o la hora



En las trincheras desde 2007

+15 años

Incidentes Globales

Hemos liderado incontables incidentes a nivel global
Múltiples incidentes en paralelo durante meses

Equipo de élite

Consultores DFIR con +40 GIAC Certifications
+50 expertos en Ciberseguridad
Equipo de Desarrolladores dedicado

Servicios Globales 24x7

Equipo Global: 24x7 follow-the-sun
Capacidad de despliegue muy rápida: SLAs < 1h

Tecnología

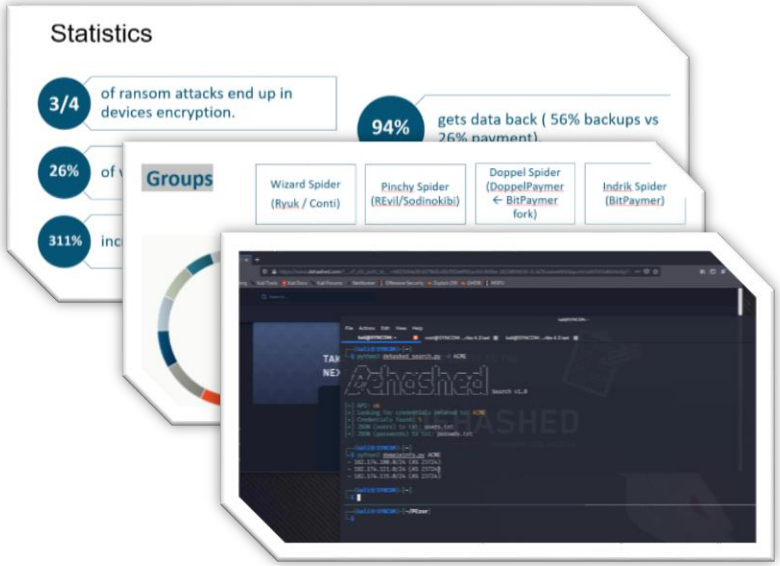
Tecnología DFIR propia: SKY, FOREST, TRINITY
Tecnología disruptive DS/AI: ds4n6

Presencia internacional

España, Reino Unico, Estados Unidos, México, Brasil, Colombia, Chile y Singapur

Anteriormente

Ransomware:
Lecciones desde las trincheras



Desde las trincheras:
Sobreviviendo a una intrusión avanzada de Ransomware

one-esecurity.com/ens21

one-esecurity.com/sticco22

Tendencias 2022

TOP 8 de amenazas durante 2022

1. Ransomware
2. Malware
3. Amenazas de ingeniería social
4. Amenazas contra los datos
5. Amenazas contra la disponibilidad Denegaciór de servicio
6. Amenazas contra la disponibilidad: Amenazas de Internet
7. Desinformación -misinformación
8. Ataques a la cadena de suministro

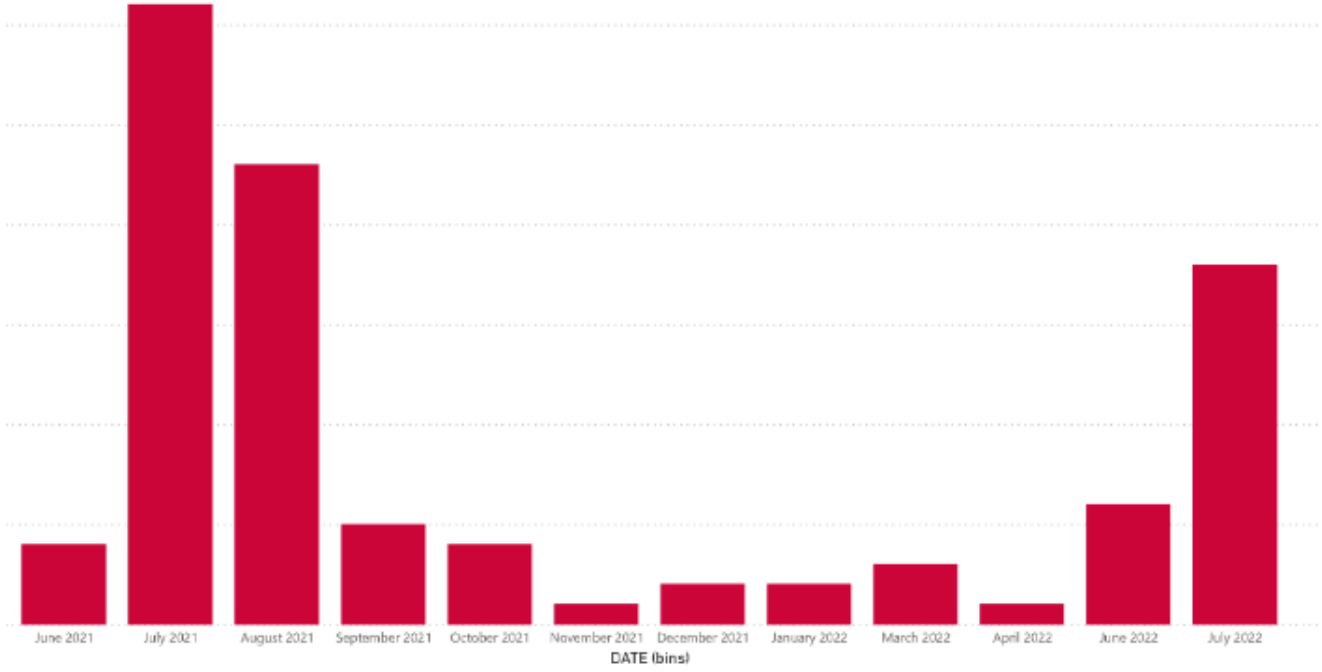
DURANTE 2022 RANSOMWARE SIGUE SIENDO LA PRINCIPAL AMENAZA

Referencia: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Tendencias 2022: RANSOMWARE

Tendencias en Ransomware durante 2022:

- Lockbit, Conti y ALPHV lideran las listas
- El phishing es el vector inicial más común
- Las técnicas de extorsión evolucionan aún más
- Las filtraciones ofrecen una visión única de la organización
- Rápida militarización de las vulnerabilidades
- El impacto de la aplicación de la ley a escala mundial
- Prohibición de pagos



Referencia: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Cifras: RANSOMWARE

33% Incremento en el número de incidentes de Ransomware

41% Ataques que utilizan phishing como vector inicial de acceso

21% Porcentaje de ataques de Ransomware

9,9 dias Tiempo de media de un ataque de Ransomware (desde el ataque inicial hasta la reanudación de la actividad normal)

1º El sector Industrial ocupa el TOP1 en ataques con un 23,2 %

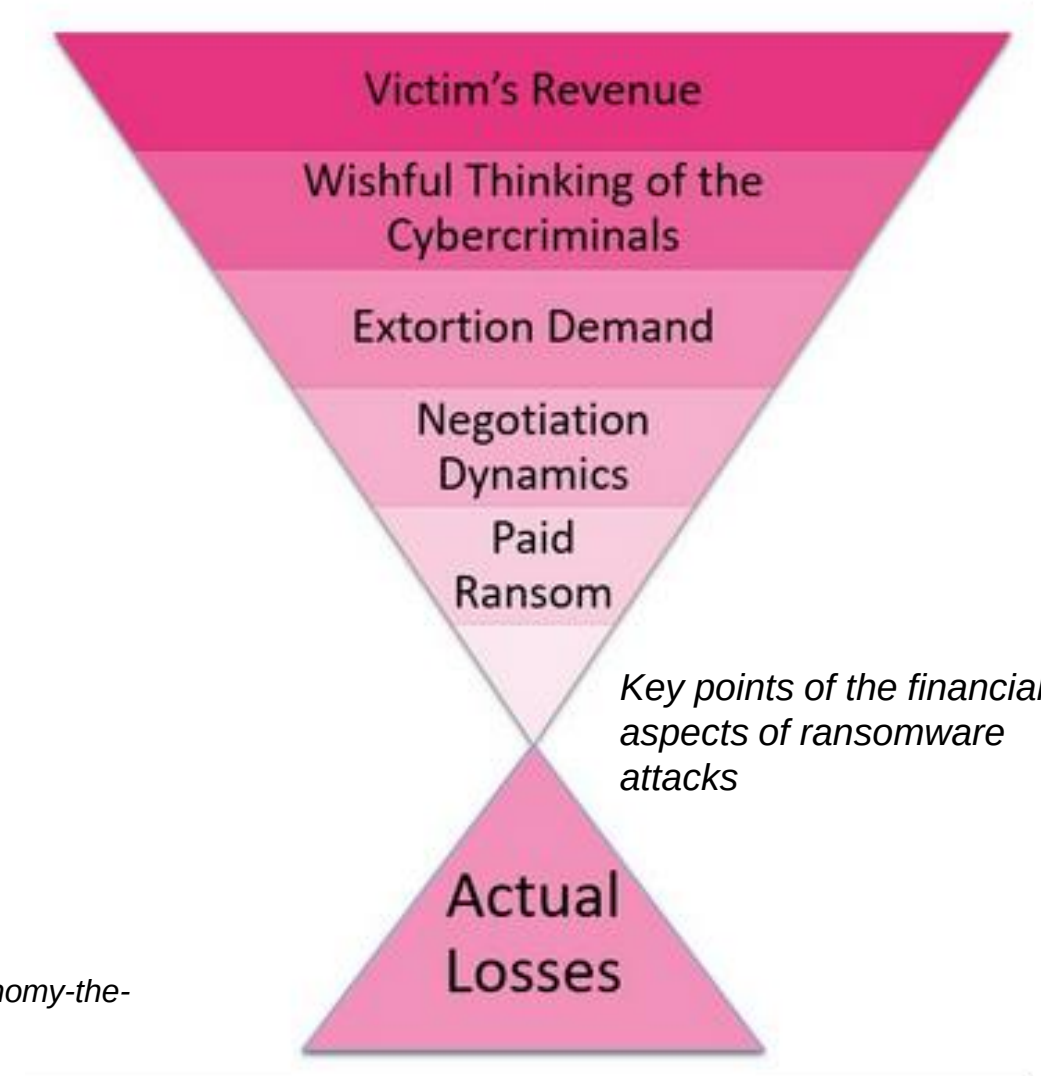
Referencia : IBM X-Force Threat Intelligence Index 2022: Resumen ejecutivo https://www.ibm.com/downloads/cas/3VANOMEA
Behind the Curtains of the Ransomware Economy – The Victims and the Cybercriminals
https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

Cifras: RANSOMWARE

***7** La media de coste total es 7 veces mayor que el pago por el rescate.

2,8 % Demanda media de rescate se sitúa en torno al 2,82% de los ingresos anuales de la víctima.

0,48 Ratio entre la demanda media de extorsión y el pago medio de extorsión.



Key points of the financial aspects of ransomware attacks

Referencia : https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

Cifras: RANSOMWARE

Industry	Attacker	Date	Loss Breakdown	Estimated Insurance Payment
Prepackaged Software	NotPetya	June 2017	Lost income: $68M Remediation and response: $24M Other losses: $50M	$30M
Pharmaceutical Preparations	NotPetya	June 2017	Lost income: $410M Remediation and response: $320M	$275M
Financial Services	Revil	December 2019	Extortion: $2.3M Other losses: $23.7M	$26M
Information Technology Services	Ryuk	October 2020	Lost income: $9M Remediation: $49.5M	$35M
US County	DoppelPaymer	September 2020	Extortion: $500K Remediation and response: $404K	Unknown
Insurance Agents, Brokers, and Service	CryptoLocker	March 2021	Extortion: $40M Other losses: $60M	$100M

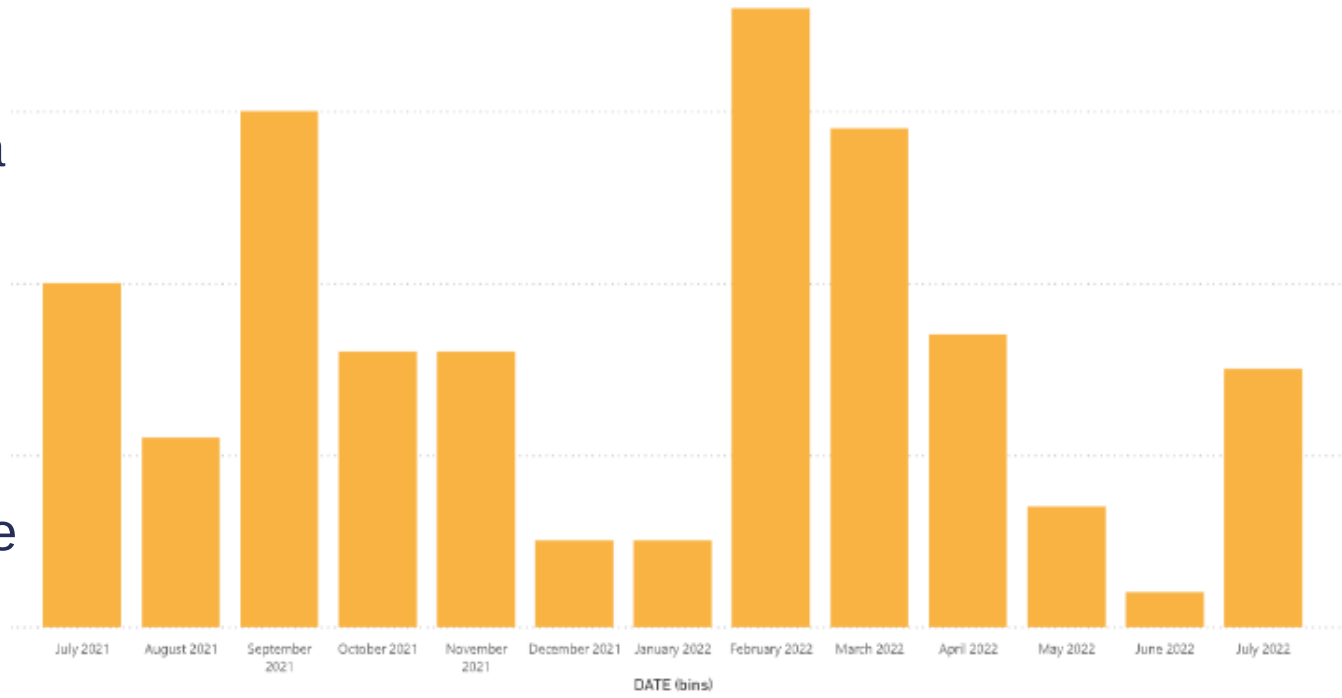
El impacto de los ataques de Ransomware no se limita al coste de la extorsión, sino que en muchos casos el coste de la extorsión es sólo marginal en comparación con otras pérdidas sufridas por la víctima.

Referencia: https://research.checkpoint.com/2022/behind-the-curtains-of-the-ransomware-economy-the-victims-and-the-cybercriminals/

Tendencias 2022: MALWARE

Tendencias en Malware durante 2022:

- Tras la caída de COVID-19, la detección de malware vuelve a aumentar
- El malware dirigido al IoT casi se duplica
- Ataques a la cadena de suministro dirigidos a marcos de trabajo de código abierto
- El alejamiento de las macros de MS Office
- Distribución de malware para móviles: de la infección generalizada a los ataques selectivos
- El malware en el contexto de Ucrania
- Destrucción coordinada del malware móvil FluBot

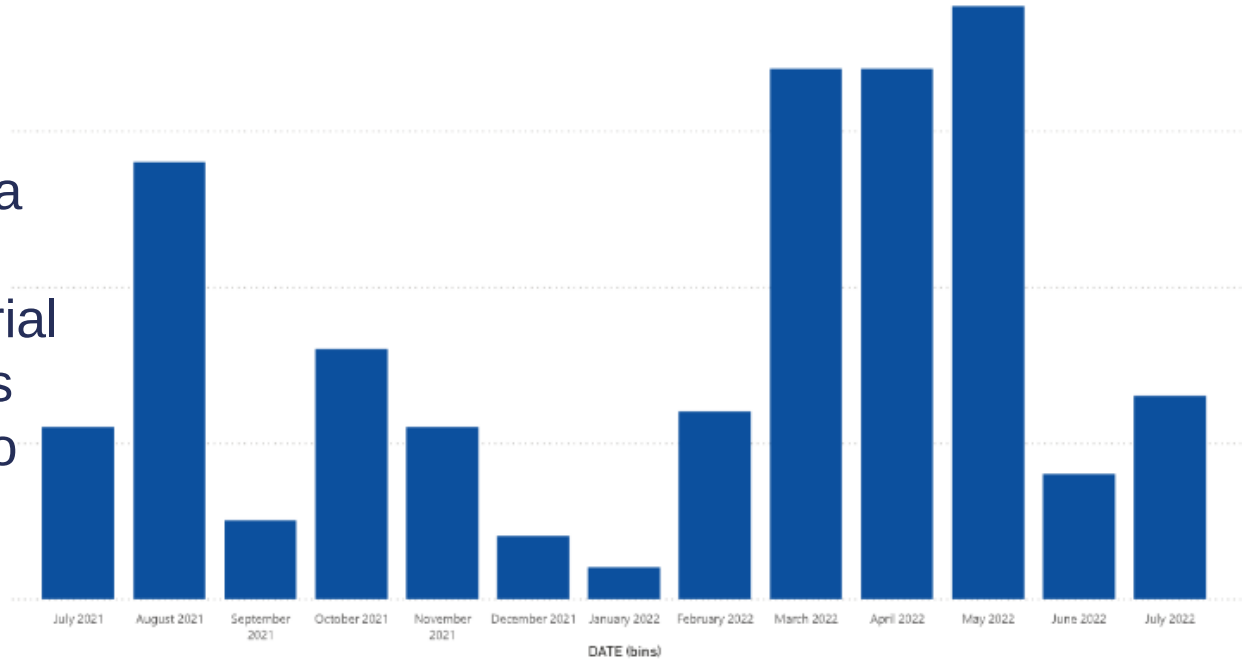


Referencia: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Tendencias 2022: SOCIAL ENGINEERING

Tendencias en Social Engineering durante 2022:

- Kits y servicios
- Campaña de spear-phishing de The Dukes
- Ataques con temática de la guerra de Ucrania
- Phishing desde cuentas conocidas
- Compromiso del correo electrónico empresarial
- Códigos de respuesta rápida (QR) maliciosos
- Suplantación de identidad por consentimiento
- Automatización
- Smishing a través de FluBot
- Aumento de los ataques a criptomonedas
- Vishing mediante la estafa de las cuentas seguras
- Ataques de ingeniería social de larga duración



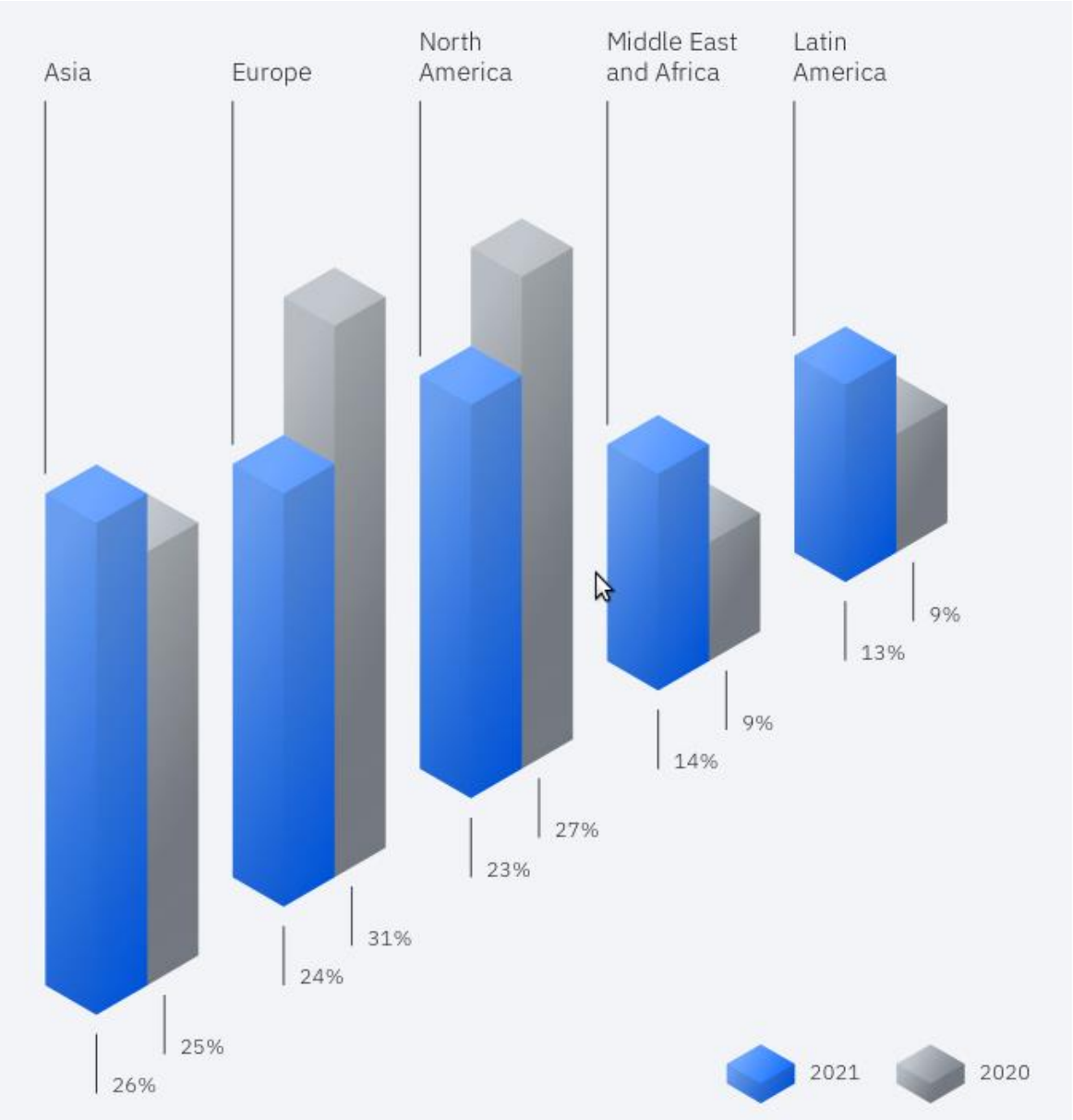
Referencia: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Cifras por regiones

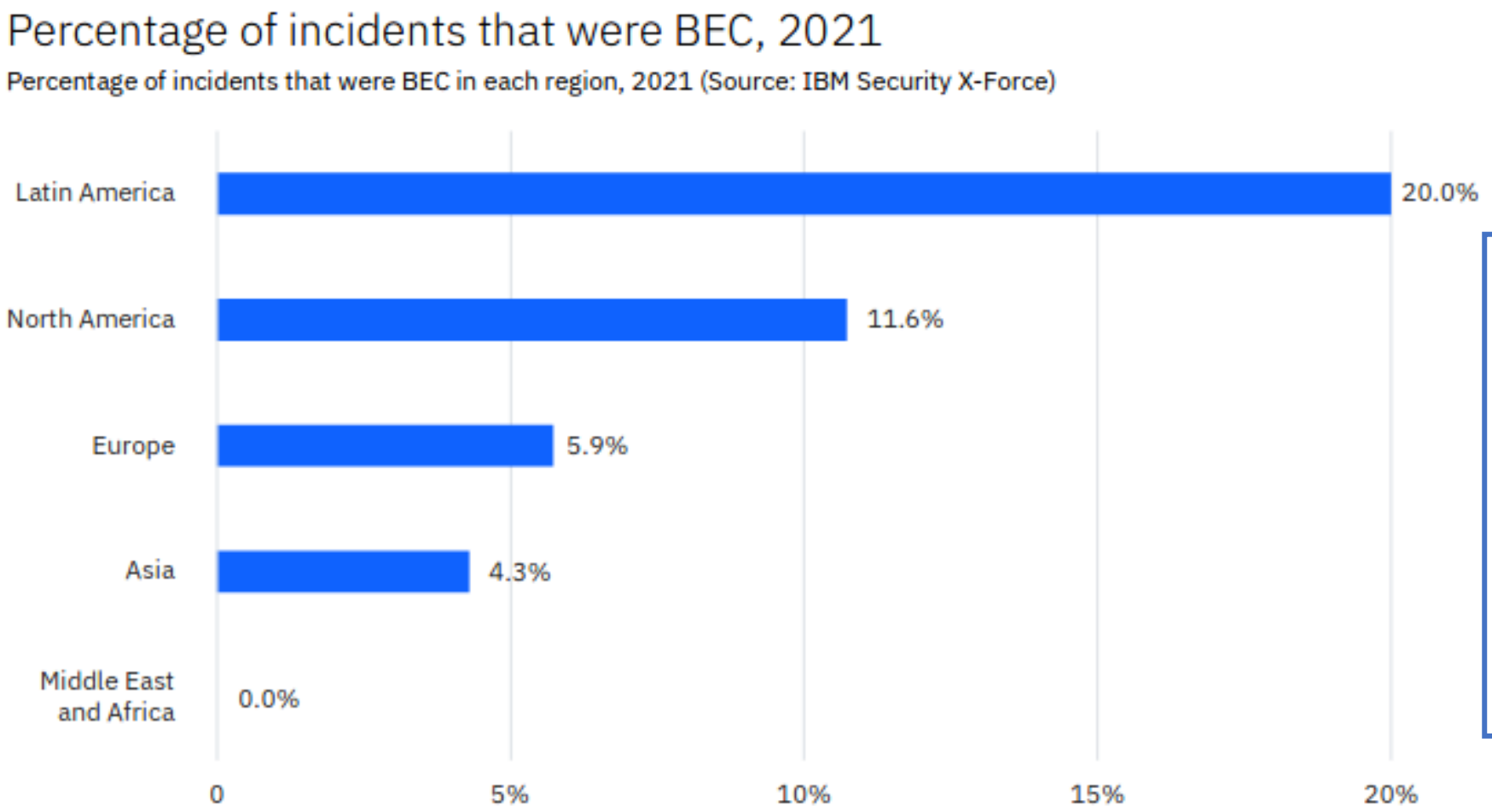
TOP 1 de regiones que han sufrido más ataques

ASIA 26%

Referencia: IBM Security X-Force
https://www.ibm.com/downloads/cas/ADLMYLAZ



Cifras por regiones



TOP 1 de incidentes BEC por región

LATAM 20%

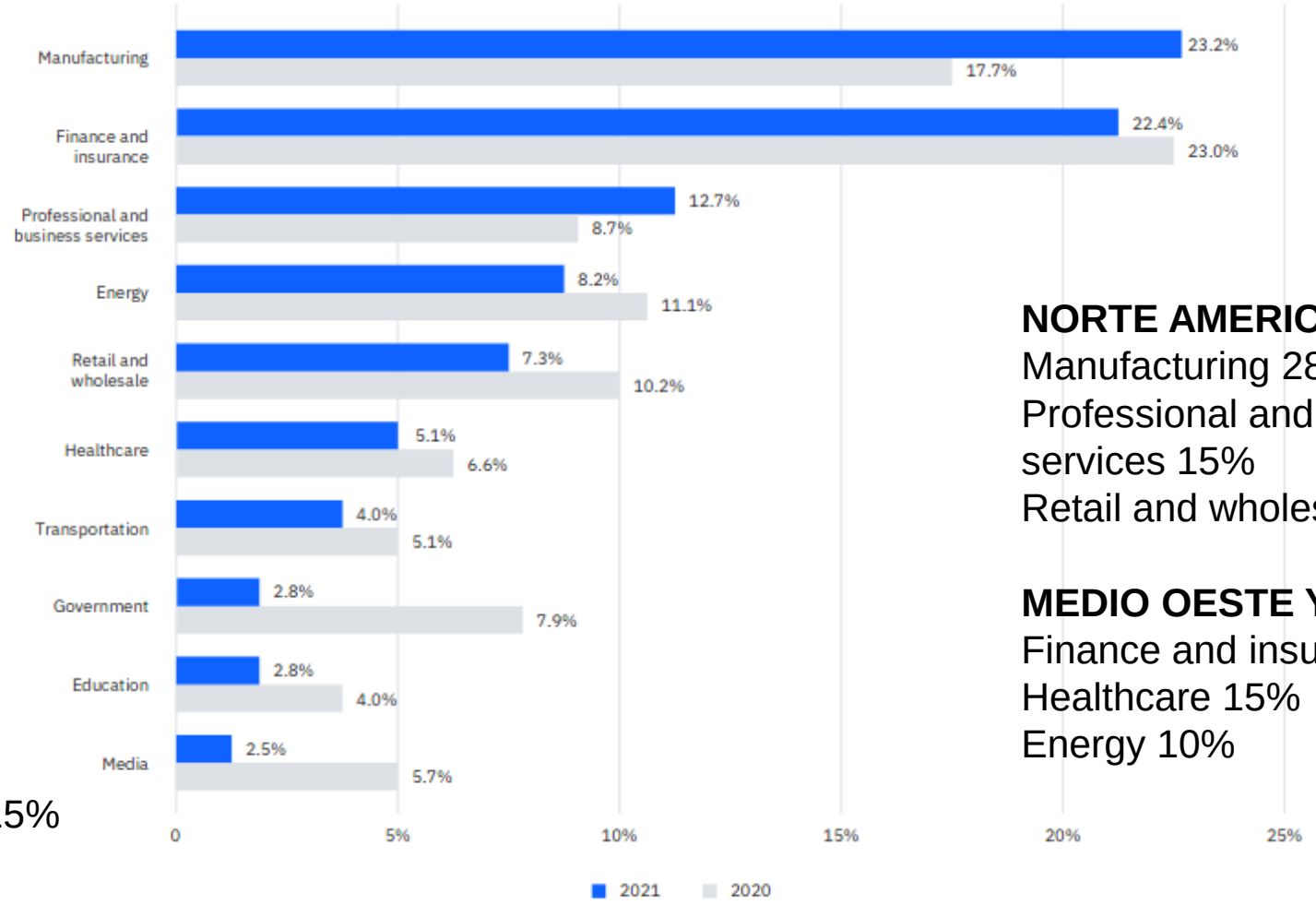
Referencia: IBM Security X-Force *https://www.ibm.com/downloads/cas/ADLMYLAZ*

Cifras: Principales sectores atacados

LATAM
Manufacturing 22%
Retail and wholesale 20%
Finance and insurance 15%

ASIA
Finance and insurance 30%
Manufacturing 29%
Professional and business services 13%

EUROPA
Manufacturing 25%
Finance and insurance 18%
Professional and business services 15%



NORTE AMERICA
Manufacturing 28%
Professional and business services 15%
Retail and wholesale 11%

MEDIO OESTE Y AFRICA
Finance and insurance 48%
Healthcare 15%
Energy 10%

Referencia: IBM Security X-Force https://www.ibm.com/downloads/cas/ADLMYLAZ

¿Quién es el enemigo?

Tendencias 2022: Actores

- Aumento de la explotación de vulnerabilidades de día 0 y otras vulnerabilidades críticas
- Los actores de las amenazas respaldadas por el Estado se centran cada vez más en los compromisos de la cadena de suministro
- Aumento de la sofisticación y el alcance de la desinformación
- **La adopción generalizada de la nube y del IoT ofrece oportunidades de ataque a los ciberdelincuentes**
- Los ciberdelincuentes siguen perturbando el sector industrial
- El conflicto entre Rusia y Ucrania ha afectado al ecosistema de la ciberdelincuencia
- Aumento de los hackers de alquiler
- Ransomware hacktivista

Referencia: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Actores

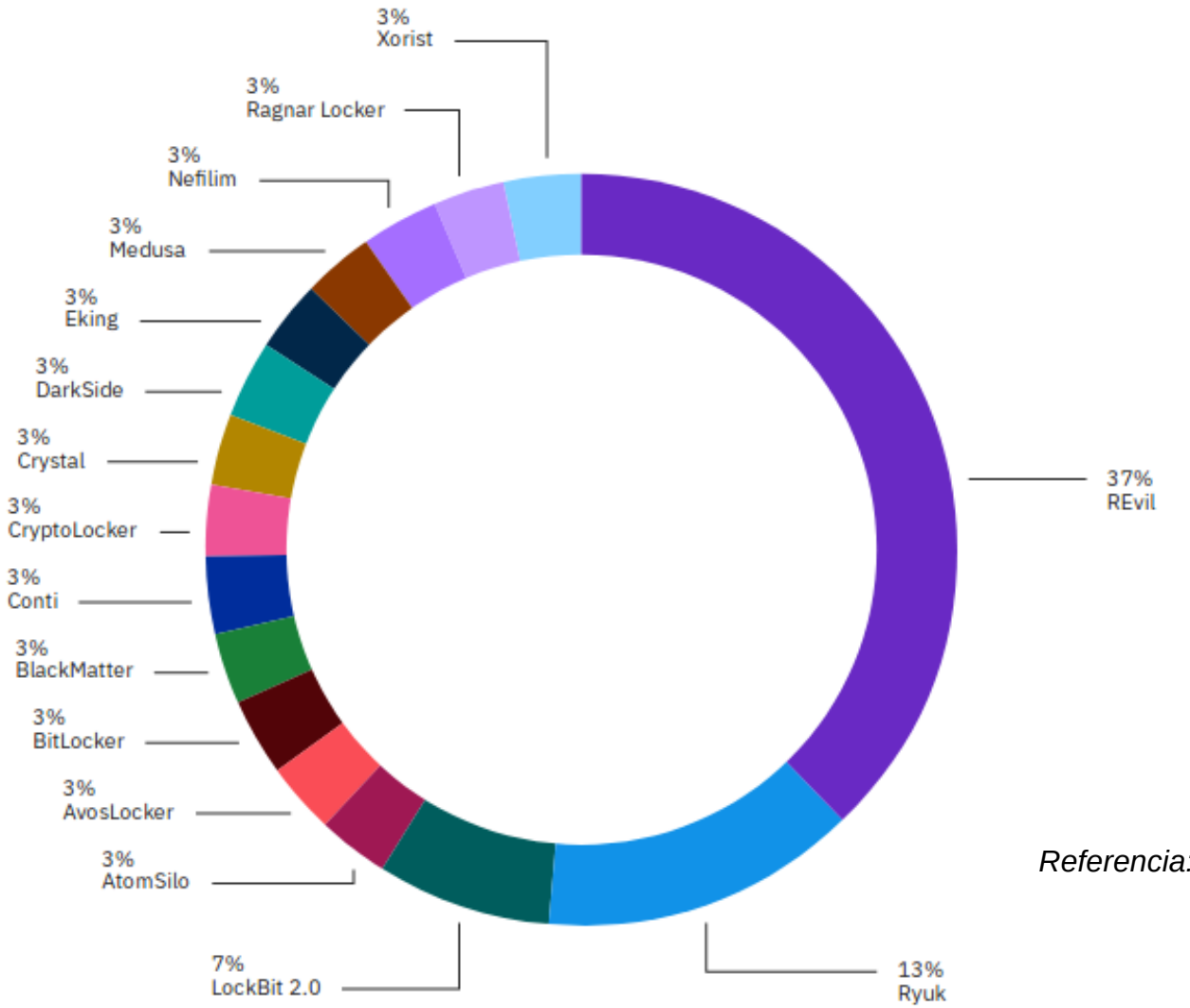
21 Nuevos adversarios

45% Aumento de las campañas de intrusión interactiva

170 + Total de adversarios rastreados

Referencia: CrowdStrike 2022 Global Threat Report *https://go.crowdstrike.com/global-threat-report-2022.html*

Actores

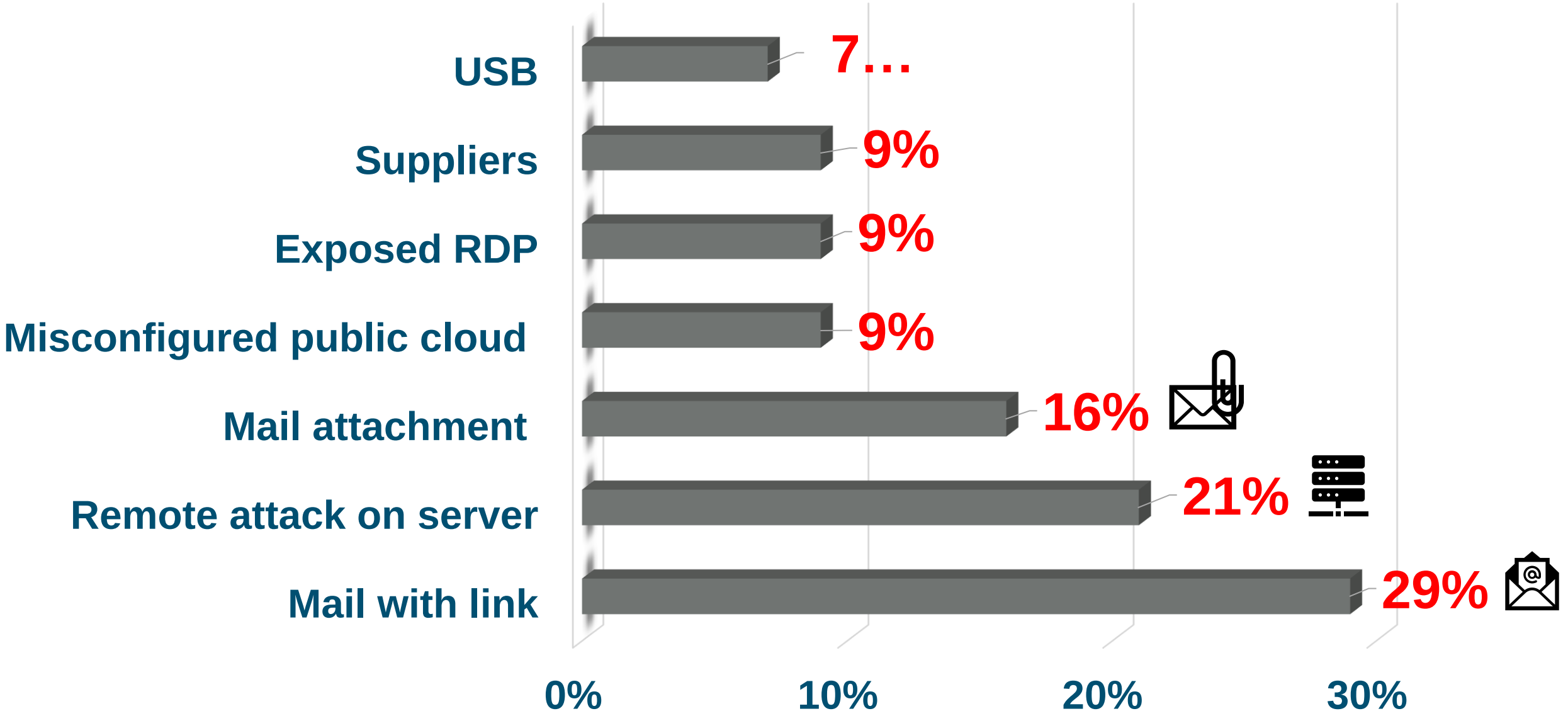


TOP 3 ACTORES

REVil (Pinchy Spider)	37%
Ryuk (Wizard Spider)	13%
LockBit 2.0 (Lockbit)	7%

Referencia: IBM Security X-Force *https://www.ibm.com/downloads/cas/ADLMYLAZ*

Actores: Vectores de entrada



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	

Ransomware	
Prepararse	Detectar
Responder	

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

Cifras que sustentan los factores de éxito

13% Aumento de costes por brechas de seguridad de 2020 a 2022

1mill Media de ahorro en dólares para organizaciones que han implantado arquitectura Zero Trust

3 mill Dolares de ahorro por empleo de IA y automatización de la seguridad

29 Días menos de media en respuesta para organizaciones con tecnología de detección y respuesta ampliada

2 mill Dolares de ahorro para organizaciones con equipo de EIR

XDR Ventaja significativa con tecnologías de detección y respuesta ampliada

Referencia: The Cost of a Data Breach Report 2022 *https://www.ibm.com/uk-en/security/data-breach*

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:
  - Brasil / Londres / NY / Sídney
- SOC basado en EEUU
- **SIN Retainer: En el momento del incidente no se contaba con ningún servicio de One eSecurity.**

Cyber Consulting

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

- **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
- Desarollo de planes/playbooks de IR
- Mapeo de detección (MITRE)
- Mejora de capacidades

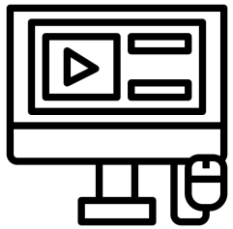
Malware

- Threat Landscapes basados en inteligencia
- Playbooks propios de Ransomware
- Manuales de decisiones de alto nivel
  - ¿Apagar sistemas?
  - ¿Pagar o no pagar?
  - ¿Hacer público?

Readiness Hunting Detection Response

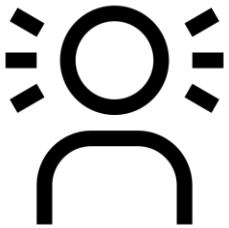
Cyber Exercises

Concientizar/evaluar	
Eval. capacidades	Medir conocimiento
Medir preparación	Identificar brechas
Crear conciencia	



- **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

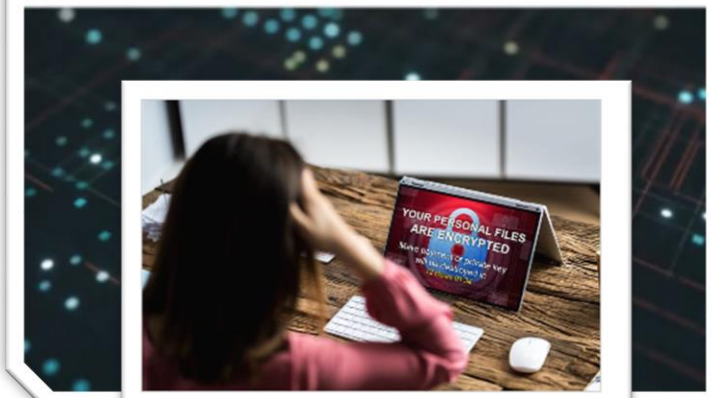
- Ejercicios ad-hoc / customizados
- Repositorio de ejercicios
- Workshops con expertos de One eSecurity
- Formato híbrido
  - CybEx/Workshop

Readiness Hunting Detection Response

¿Con qué nos enfrentamos?

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

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

TECHNOLOGY

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

5-Minute Listen

Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers

The payment clea
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 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 clea
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

Asegurarse	
Suscripción	Cálculo de impacto
Coberturas y servicios	1ª respuesta

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 EDR

Herramientas de Pre-Ransomware encontradas

5 máquinas infectadas

Posible propagación a otras regiones

Estrategia global

Impacto al negocio

Paro de actividades

Robo de datos

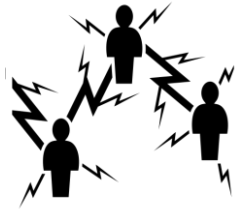
Extorsión

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

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**

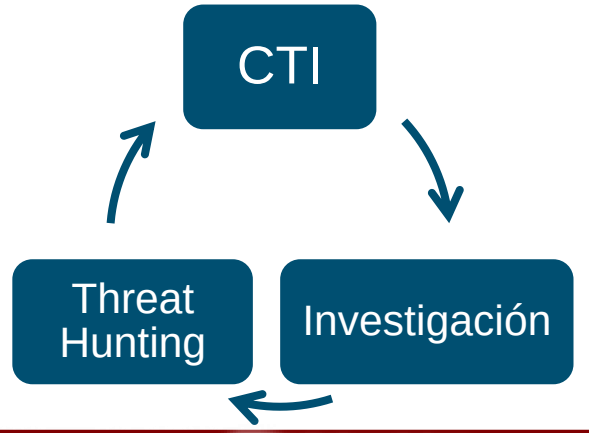
- **Contar con apoyo** en la gestión táctica/estratégica
- **Asegurar apoyo** de la organización (dirección, TI, SOC, etc.)
- **Operaciones 24x7**

  (Ambas partes)
- Equipo de IR **global**

Responder	
Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar

- **Capacidad** de análisis masivo

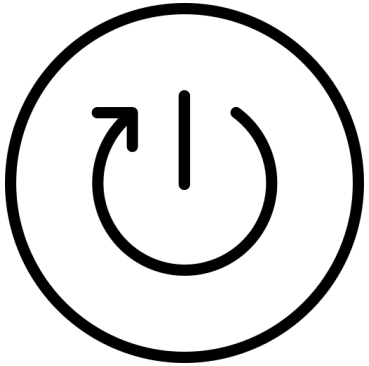
  Hunting de 4000+ máquinas
- **Utilizar Ciberinteligencia** para contención/remediación:



Readiness | Hunting | Detection | **Response**

Emergency Incident Response

Responder	
Reacción rápida	Identificar
Contener	Erradicar
Minimizar downtime	Restaurar y mejorar



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

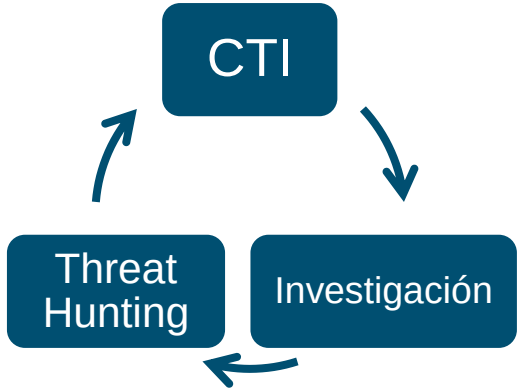
Readiness | Hunting | Detection | **Response**

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

Multivendor

Escalable

Threat Intelligence

Automation

Endpoints / Network

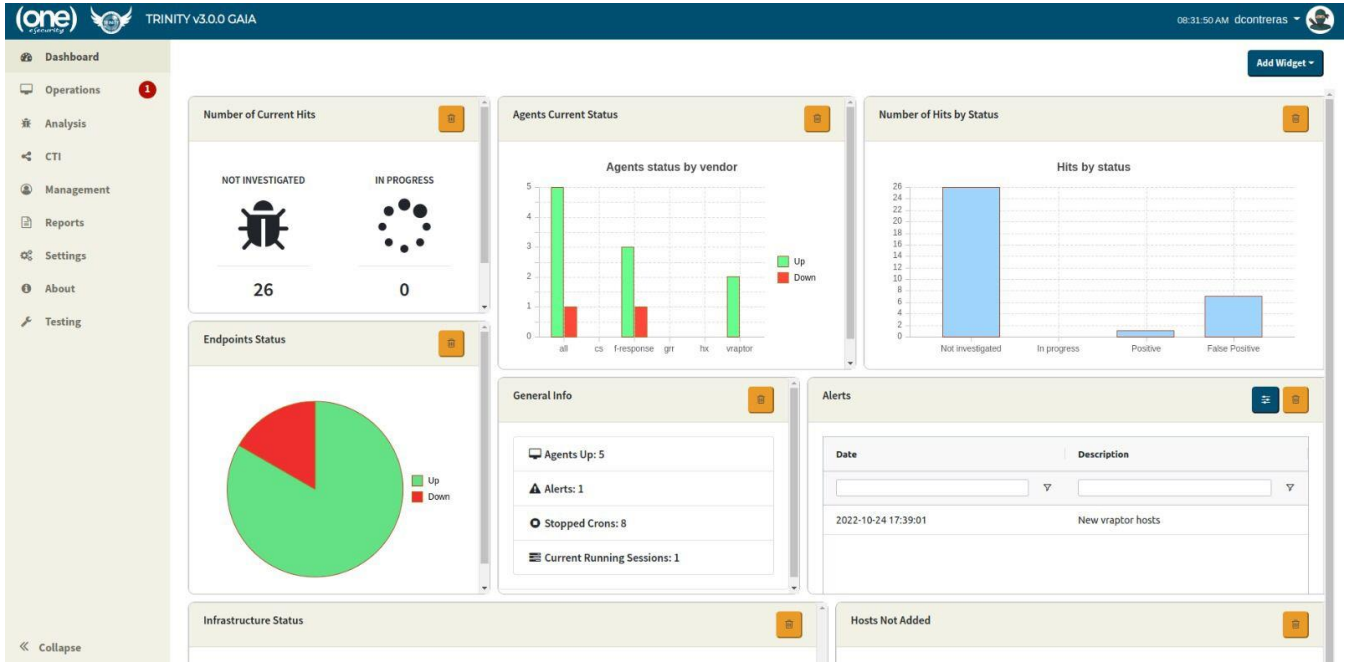
Powered with AI

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.



Readiness | **Hunting** | **Detection** | Response

Digital Forensics

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

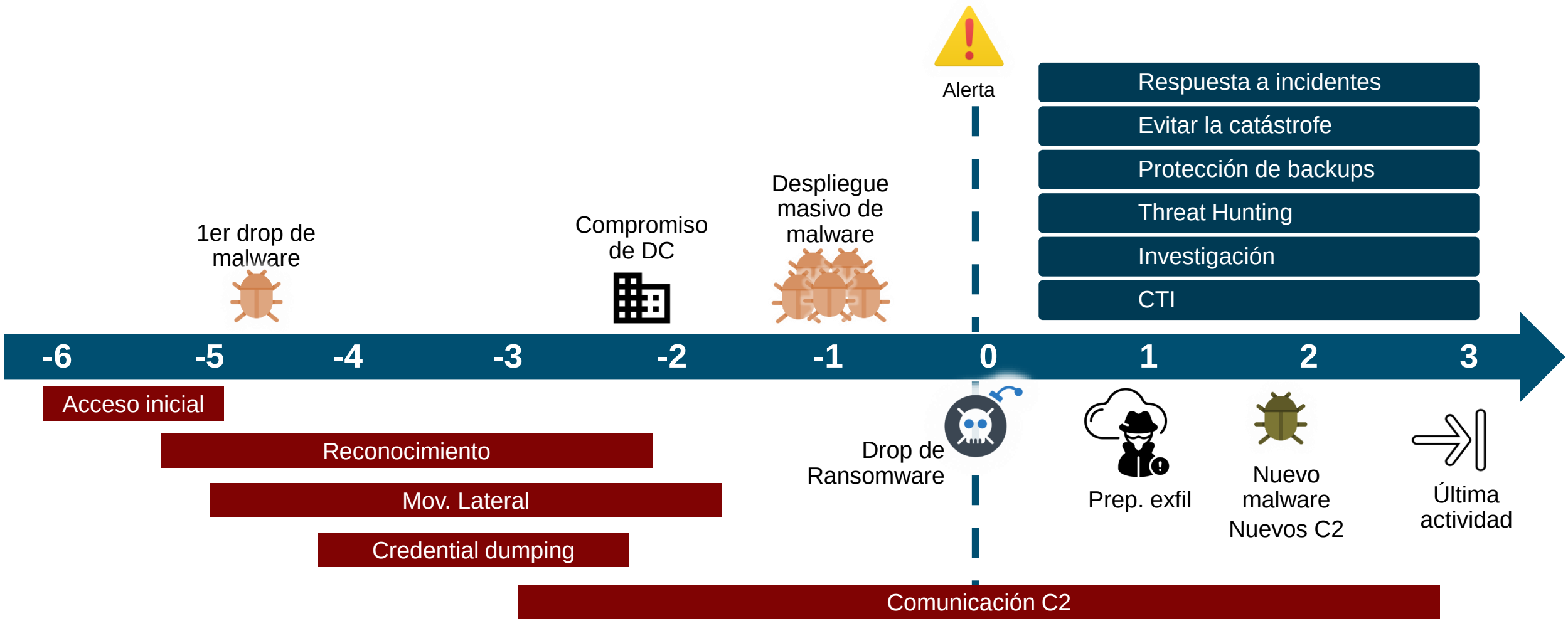
- **Analizar** a fondo
- **Obtener evidencia** de actividad
- **Contestar** preguntas investigativas

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

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

Readiness | Hunting | Detection | **Response**

Timeline global



Factores de éxito

Cyber Consulting
Evaluar y mejorar

Cyber Exercises
Concientizar/evaluar

Digital Forensics
Investigar

Emergency Incident Response
Responder

Offensive
Garantizar eficacia medidas

Threat Hunting: Compromise Assessment
Detectar amenazas

Threat Hunting: MTH
Detectar amenazas de manera contínua y proactiva

Retainer

Readiness — Hunting — Detection — Response

Diferenciadores

Cyber Threat Intelligence

- **Experiencia propia liderando y respondiendo a incidentes**
- A través de los años y alrededor del mundo

Data Science/ Artificial Intelligence

- Comunidad de analistas forenses, data scientists y desarrolladores
- **Evolucionar e innovar** los métodos tradicionales de DFIR

Next Generation Forensic Lab: SKY PRO

- Plataforma para automatizar tareas de DF/IR/CTI
- Integradora de herramientas
- **Automatización de tareas complejas de análisis forense**

Cyber Operations 24x7

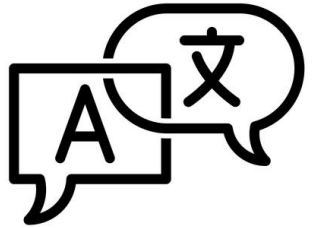
- Equipo de operaciones
- **Mantiene los servicios funcionando contínuamente**
- Follow-the-sun

¿Porqué nuestros clientes nos eligen?

Somos Especialistas

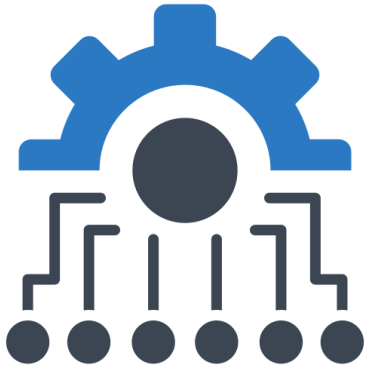
Respuesta rápida

Flexibles



Multilingües

Vendor-neutral



One-stop DFIR service company

Retainer:

- Servicios contínuos / EIR
- Cualqueir otro servicio de nuestro catálogo

Nadie está a salvo de un ciberataque

"KEEP CALM AND GET A ONE RETAINER"

Estrategia global

Respuesta a incidentes
Preparacion > 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

Y si hubiera habido un Retainer…

Ciclo de **TH continuo 24x7 con infraestructura propia** de One eSecurity: Trinity y SKY PRO con identificación rápida y eficaz.

Cyber Exercises para la preparación adecuada de un equipo de '**First Response**'.

Evaluación temprana para una correcta configuración de sistemas y herramientas de seguridad gracias a MTH que identifica **puntos de mejora** gracias a análisis de DFIR.

Plan de continuidad listo para aportar soluciones a procesos críticos durante un incidente gracias a Cyber Consulting.

Garantía SLAs menor a 1h para la primera respuesta.

MUCHAS GRACIAS

Jess Garcia
@j3ssgarcia

(one) eSecurity

www one-esecurity.com

One_eSecurity

one-esecurity

one-esecurity.com/sticrd23

#STICPUNTACANA