Luis F. Torres

Cybersecurity Expert (Co-Founder Rivelti Group)

- C|EH, ECSA, GCIH, GPEN, OSWP, LPT, Linux+, OSCP

Agenda

- Los Retos y Riesgos de los Negocios en Ciberseguridad
- Algunos Tipos de Ciber Ataques
- Cronología de un Ciber Ataque
- Tiempo Promedio de Detección de un Ciber Ataque
- Evolución de los Ciber Atacantes
- Las Amenazas de Hoy
- Tecnologías de Hoy Día
- Nuevos entornos y sus Ciber Amenazas
- Nuevas Ciber Amenazas
- Acciones a Tomar / Recomendaciones

Los Retos y Riesgos del Negocio

Cybersecurity

Migración a la Nube:

- **Nuevo** foco de los atacantes
- Nuevas y más amenazas
- **Configuraciones básicas**

Transformación Digital:

- Más areas que proteger
- Nuevos ambientes
- **Ataques más sofisticados**

APTs (Advance Persistent Threat) más sofisticados:

- Procesos dirigidos
- Más sofisticados
- Múltiples etapas
- Nuevos objetivos (Backups)
- Comportamientos que mutan

Exigencias de certificaciones o regulatorias:

- Check mark
- Objetivos limitados

Mercado altamente fragmentado:

- Web Security
- App Security
- End Point Security
- Cloud Security
- Threat Intelligence

Alto consumo en:

- Análisis
- Validaciones
- Integraciones
- Gestión
- Mantenimiento

Los Retos y Riesgos del Negocio

Cybersecurity

Escacez de personal

- Rotación
- Promoción
- Migración
- **Agotamiento**

Presupuesto limitado:

- Casos de Negocio
- Justificaciones
- Control del Gasto
- ROI

Picture or Movie:

- Gestión estática de las vulnerabilidades
- Falta de priorización en tiempo real

Falsa postura de ciberseguridad

- No hay pruebas de reacción
- No hay simulaciones de ataque
- Lack de best practices

Cuantificación del riesgo:

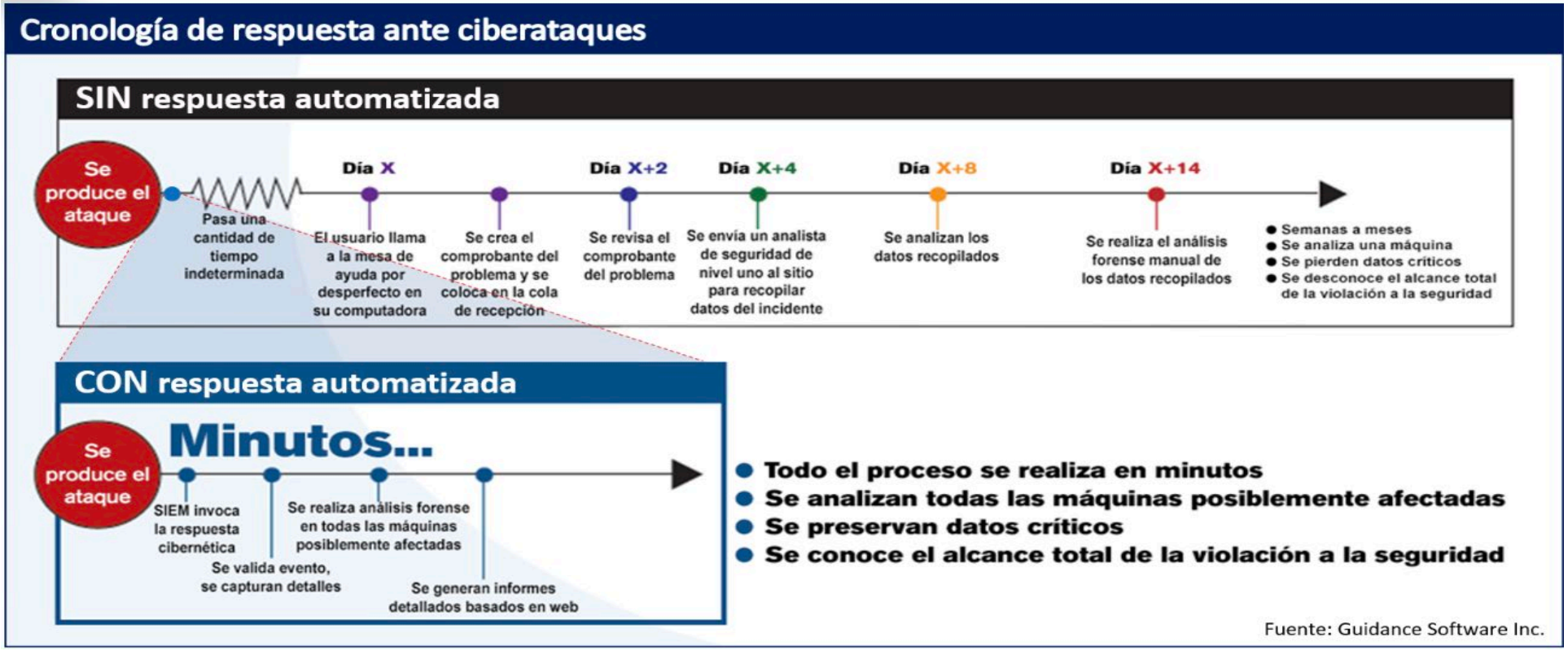
- No hay Certeza del riesgo
- Dificultad en la valoración de impacto

SIEM como servicio o Next Gen SOC:

- SOAR
- **Personal Experto**
- Procesos
- **Controles**
- Integraciones
- **Interoperabilidad**
- Certificaciones

Algunos Tipos de Ciber Ataque

Cronología de un Ciber Ataque



Tiempo Promedio de Detección de un Ciber Ataque

Secciones Miércoles, 2 agosto 2023 ISSN 2745-2794 **Semana** Suscribirse Crear cuenta Iniciar sesión

Últimas noticias | Semana TV | Semana Play | Economía | Impresa | Nación | Política | Galerías | Especiales | Más

Home > Tecnología > Artículo

CIBERSEGURIDAD

Una empresa puede tardar hasta 7 meses en detectar un ataque cibernético

Una empresa puede tardar hasta siete meses en detectar un ataque cibernético, dado que las organizaciones están utilizando técnicas obsoletas para identificar a los atacantes, según un análisis de la empresa de ciberseguridad Lumu Technologies.

EL PAÍS

NEGOCIOS

EMPRENDEDORES · INVERSIÓN · FINANCIACIÓN · VIVIENDA · ÚLTIMAS NOTICIAS

DELITOS INFORMÁTICOS >

E Código rojo, nos han hackeado: así son los ciberataques empresariales

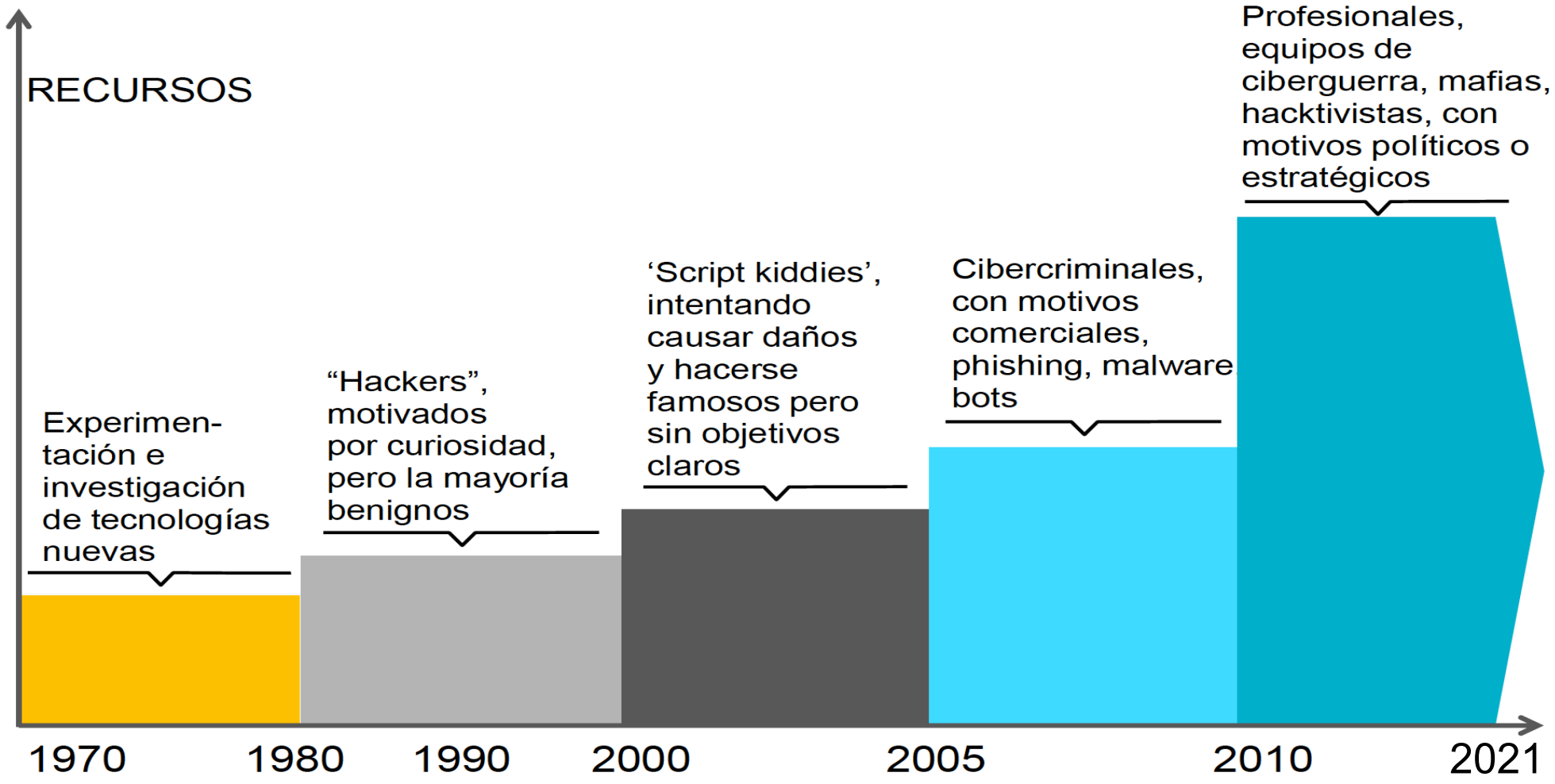
La delincuencia informática crece en todo el mundo y las pymes son el eslabón más débil por su menor capacidad de inversión

Las empresas tardan 56 días de media en identificar un ciberataque

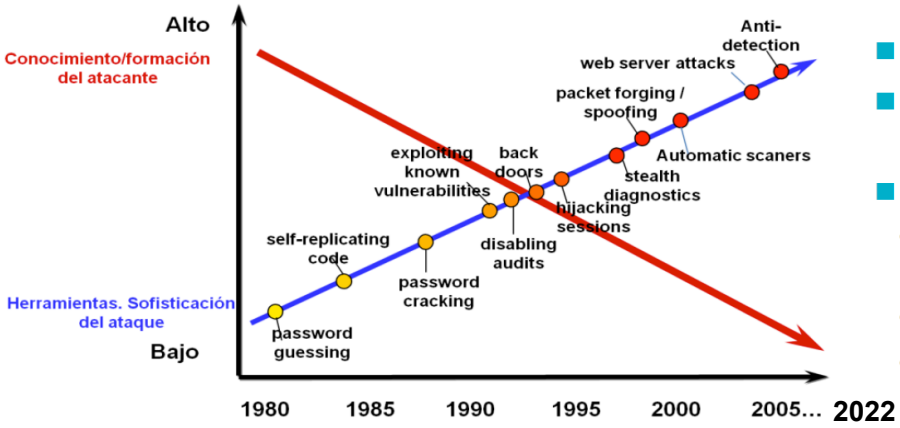
Seguridad 02 MAR 2020

El plazo que transcurre entre que se inicia un ciberataque y su identificación es de 56 días. Puede parecer mucho tiempo pero la media en 2018 era de 78 días, lo que evidencia que las organizaciones han mejorado sus sistemas de detección.

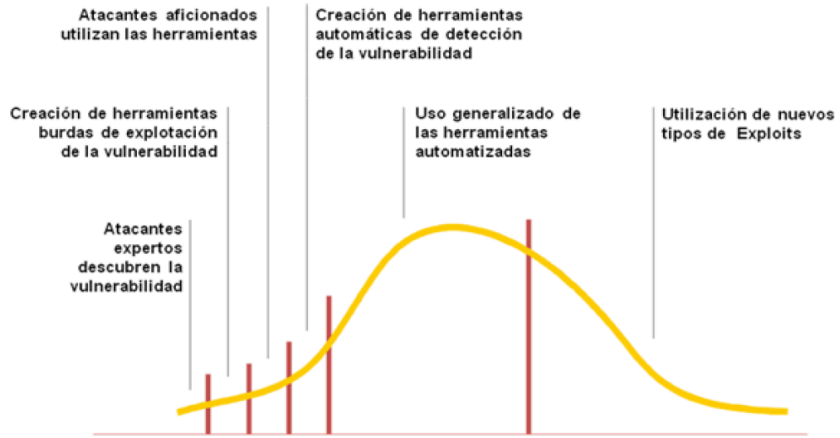
Evolución de los Ciber Atacantes



Las Amenazas de Hoy



- Guerra asimétrica
- Irrupción de ciberactivistas y ciberterroristas.
- Nuevos tipos de amenazas:
  - Amenazas Persistentes Avanzadas (APT, APA).
  - Subversive Multi-Vector Threats (SMT).
  - Advanced Evasion Techniques (AETs).



La identificación de estas amenazas es clave para poder protegerse de las mismas, así como lo es el intento de predicción de futuras amenazas todavía desconocidas

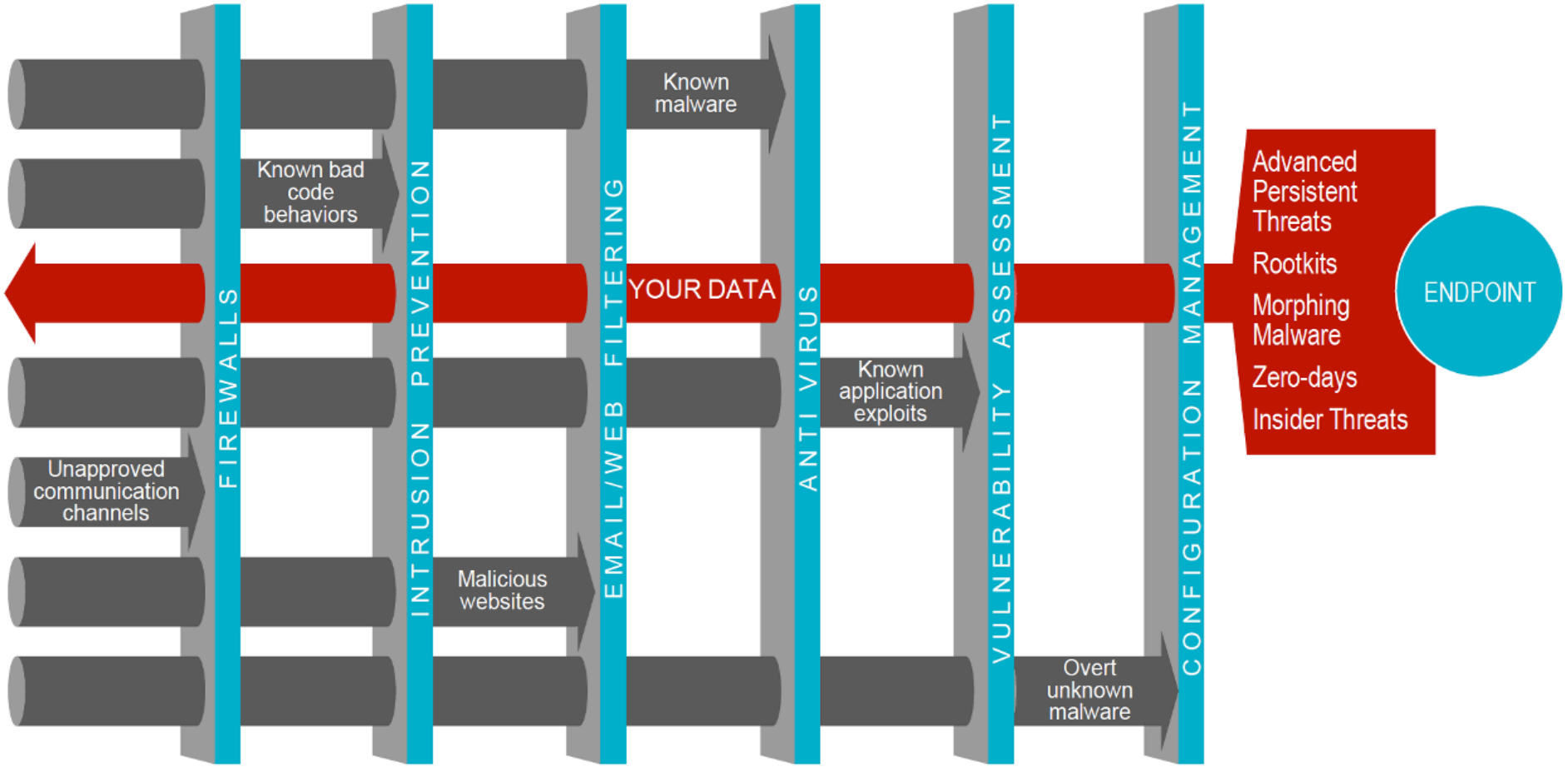
Tecnologías de Hoy Día

En la seguridad la clave de gestionar las amenazas es tener una visibilidad del entorno global del riesgo

Prácticas Seguridad Tradicionales → Mecanismos Protección Actuales → Nuevas Tecnologías Avanzadas

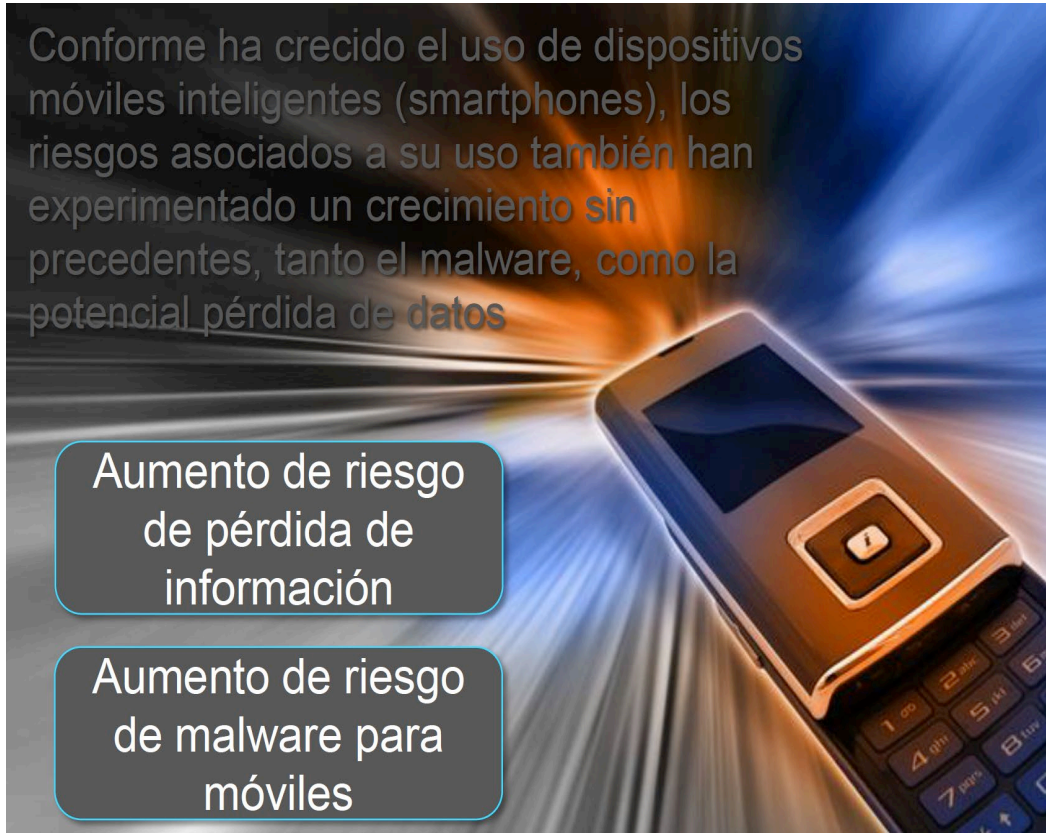
AV/AM Control de Acceso Gestión de Vulnerabilidades	Análisis Malware Análisis Forense	DRA/DRM Dynamic Risk Assessment/Management
	IDS/IPS Intrusion detection/ prevention system	DLP/IRM Data Leak Prevention Info. Rights Management
	SIEM Security Information and Event Management	Otros CiberInteligencia, DataDiode, Simulación Avanzada

Protección Tradicional: Defensa en Profundidad

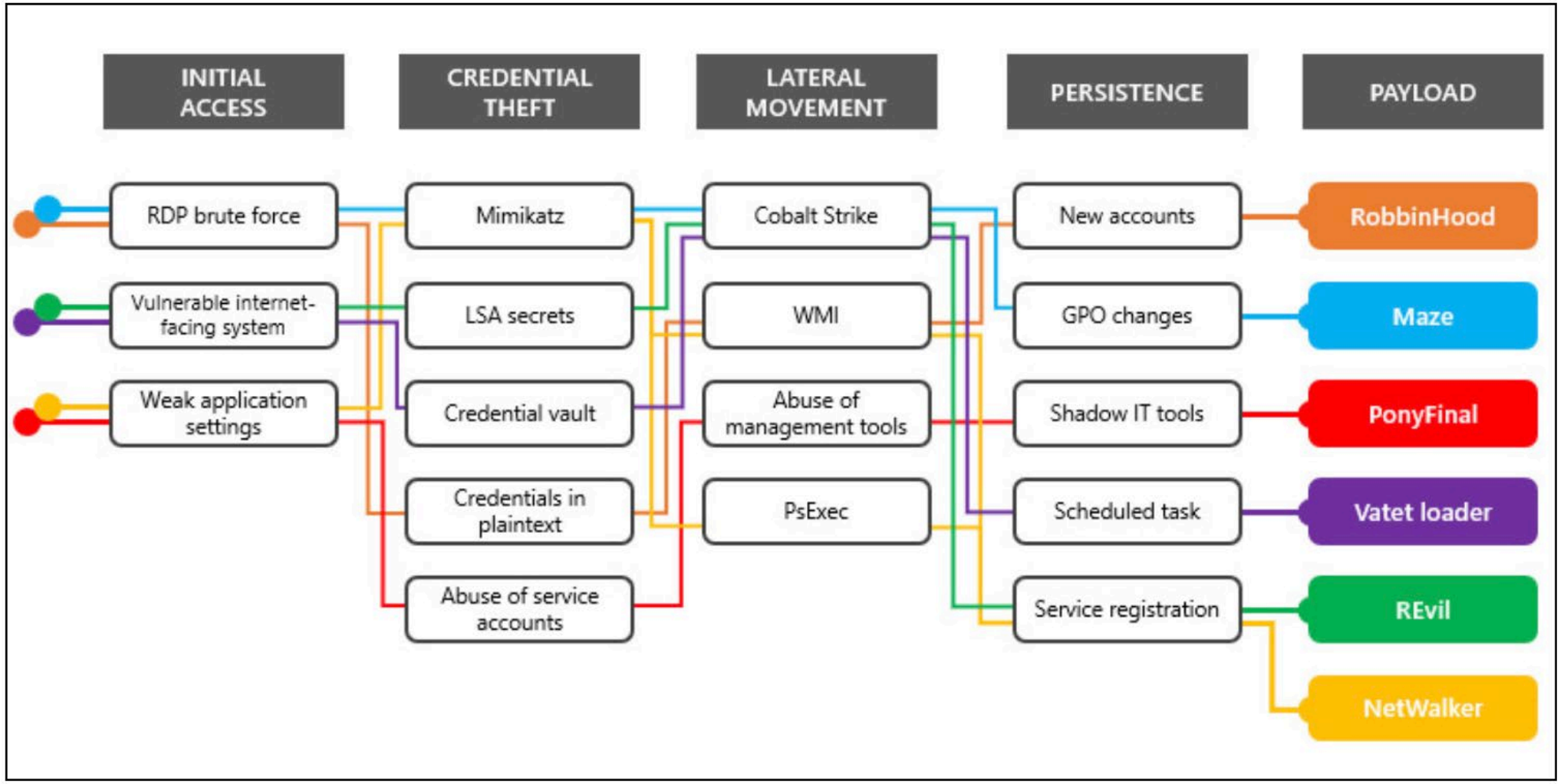


Nuevos entornos y las Ciber Amenazas

- **Movilidad**
- **Virtualización**
- **Externalización y colaboración**
- **Cloud computing**
- **Incremento consumo IT / Redes Sociales**
- **Industrialización de hackers**
  - Crimeware as a Service (CaaS): HaaS, FaaS, DDoSaS, …



Nuevas Ciber Amenazas

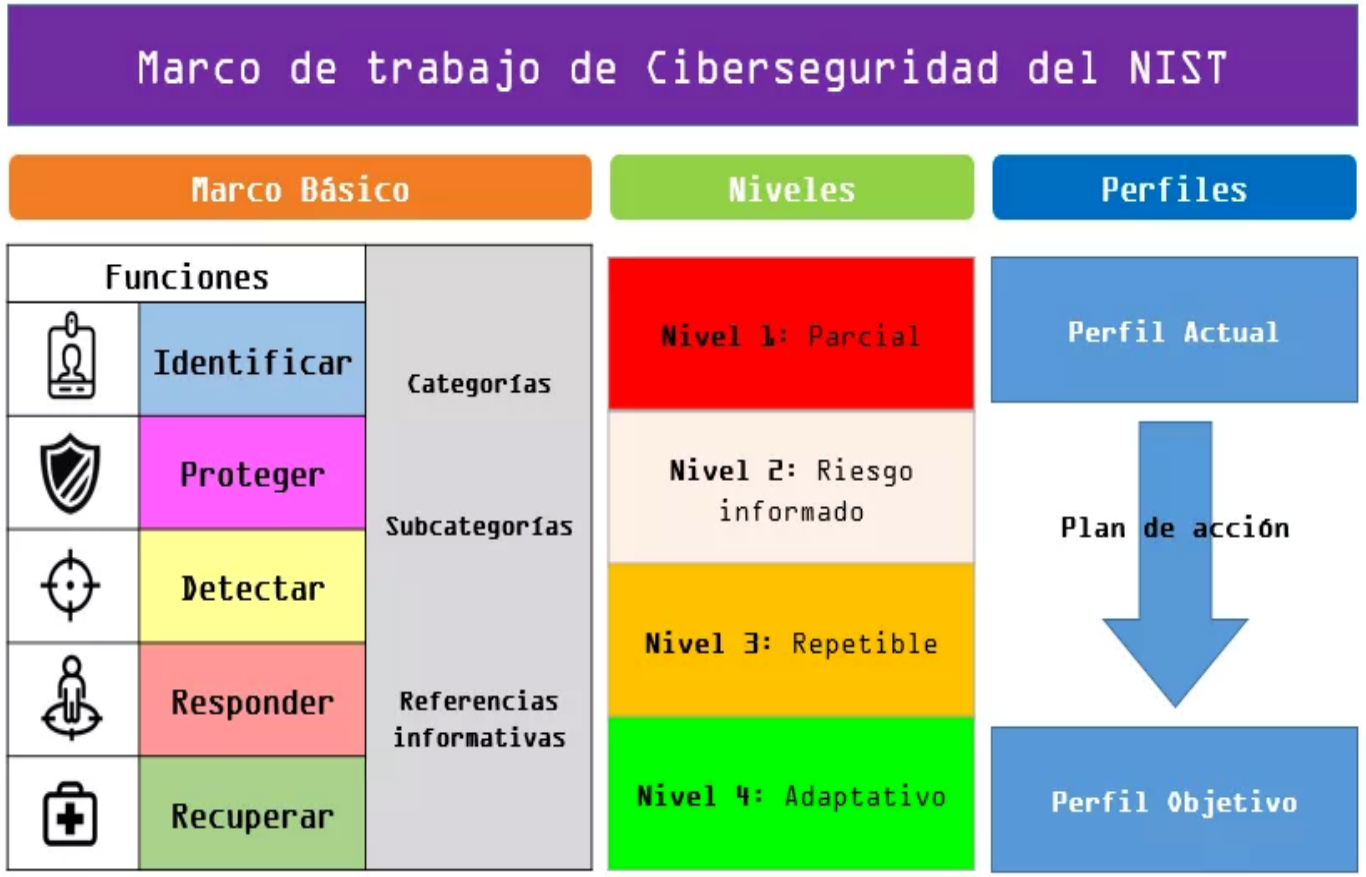


Source: Microsoft

Al menos diez (10) variantes de ransonware han sido descubiertas de Enero 2023 a la fecha.
Cada una con mayor sofisticación y agresividad que la anterior.

¿ Que acciones tomar ?
¡Recomendaciones!

- ✓ **Adoptar un marco metodológico de seguridad de la información (ISO 27001, PCI, NIST Cyber Security Framework).**
- ✓ **Tener una estrategia clara y definida de Respuesta a Incidentes y Recuperación de Desastres.**
- ✓ **Mecanismos de Detección oportuna de vectores de ataques (Vulnerability Management, Continuous Penetration Testing). Simulación de Ataques (Red&Blue Team, Purple Team)**
- ✓ **Poseer mecanismos de control en todas las capas (Firewall NGN/UTM perimetrales, AV/AS perímetro, DLP endpoint y red, NAC ethernet y wifi, EDR/XDR MDR, SASE, MDM).**
- ✓ **Monitoreo Continuo (SIEM, Cyber Intelligence, Threat Intelligence, Log Analytics).**
- ✓ **Estrategía de respaldo onsite/offsite.**
- ✓ **Aprendizaje y mejora continua.**



¿ Preguntas ?

Gracias