Prevención y detección temprana de *ransomware*

Prof. Dr. Pedro García Teodoro

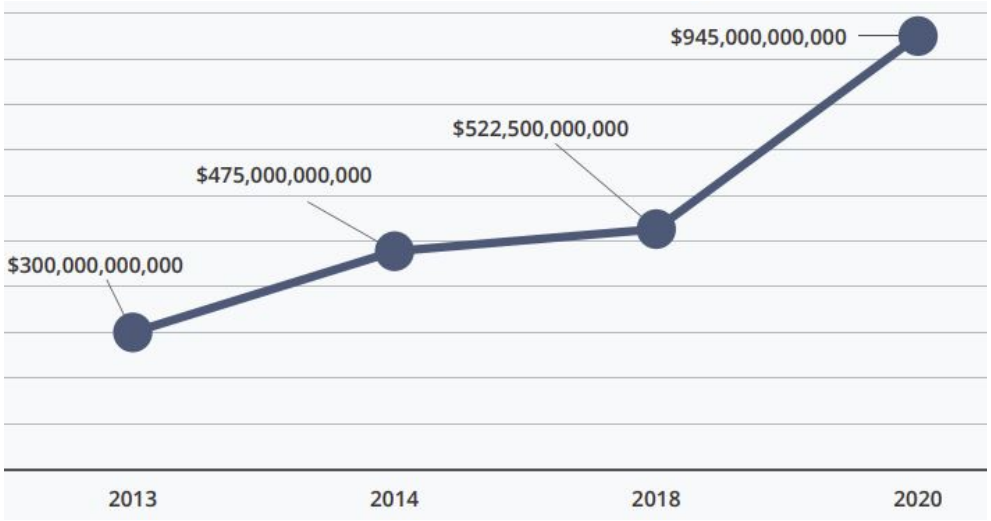
Catedrático de *Ingeniería Telemática*
Coordinador de *Engineering & Security Group (NESG – https://nesg.ugr.es)*
Secretario de la *Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC – https://www.renic.es)*
Director de la *ETS Ing. Informática y de Telecomunicación (ETSIIT – https://etsiit.ugr.es)*
-Universidad de Granada-

Índice

- Ciberseguridad en cifras
- Fundamentos del *ransomware*
- Modelos de ataque y defensa
- R-Locker
- Tendencias y retos

Alcance

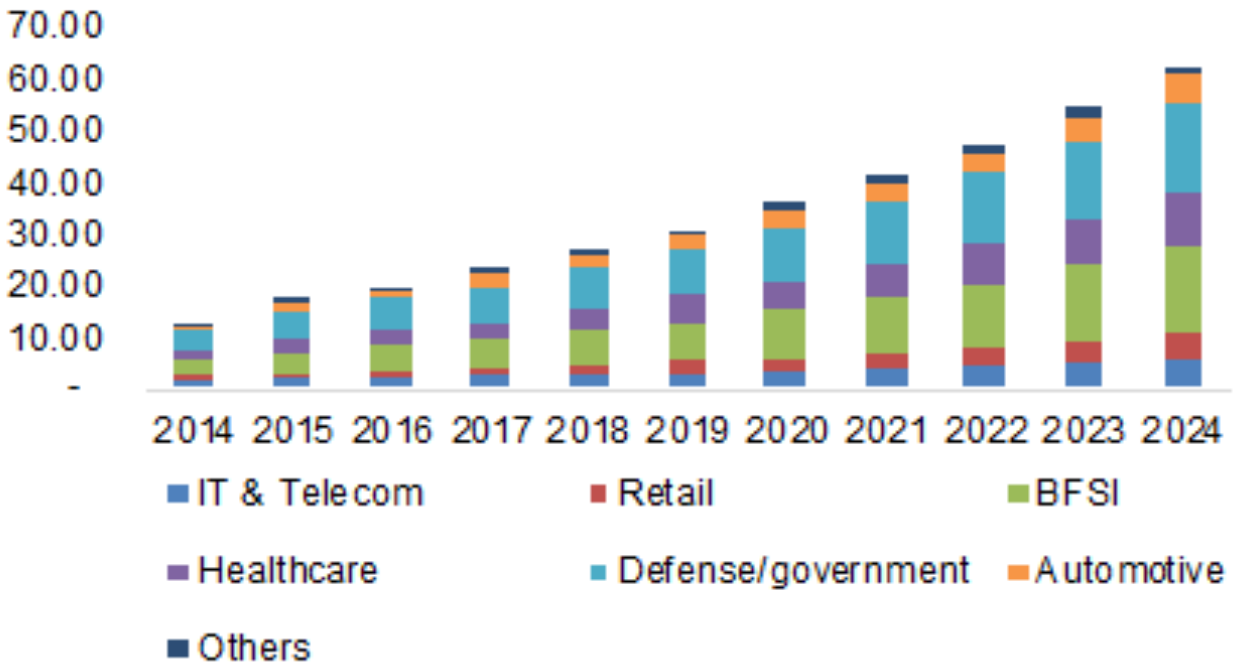
- En torno al 80% de las organizaciones han sufrido al menos un ataque con éxito
- Coste del cibercrimen:



© CompariTech, 2022

Inversión

- Inversión en ciberseguridad ($b):



© Grand View Research

Demanda de perfiles *(i)*

- Demanda de profesionales en ciberseguridad:

Consider this –between 2020 and 2025, there will be a growth of 7 million jobs in security and privacy worldwide[1] but only 4.2 million trained candidates

7,000,000

new cybersecurity jobs worldwide but only 4.2 million trained candidates

That's a gap of almost 2.8 million unfilled jobs[2]

The number of cybersecurity jobs is expected to more than double between now and 2025

2025

The gap is expanding: Cybersecurity jobs more than double by 2025

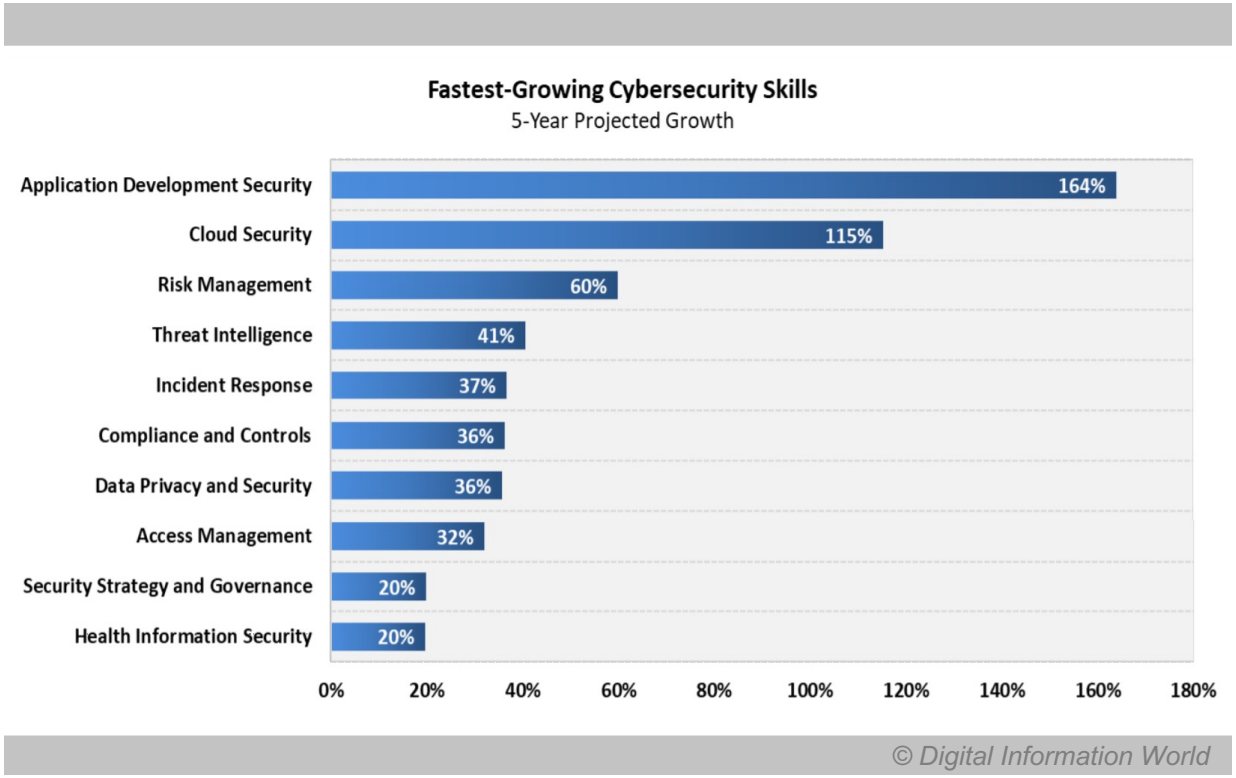
71%

And costing money:
71% of employers have incurred damages because of cyber talent deficit.[3]

© New Horizons Ireland

Demanda de perfiles *(ii)*

- Perfiles en ciberseguridad:



Formación en ciberseguridad

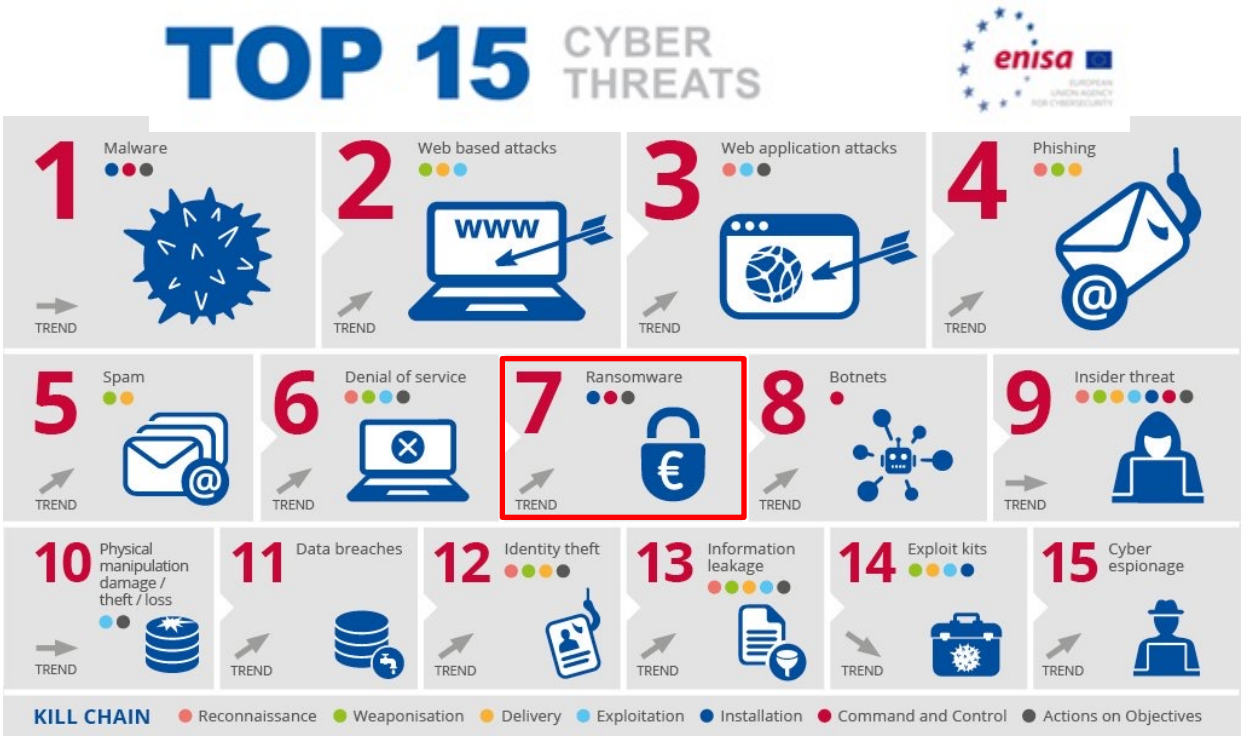
- Cybersecurity curricula (ACM/IEEE 2017):

© CC2020, ACM

Índice

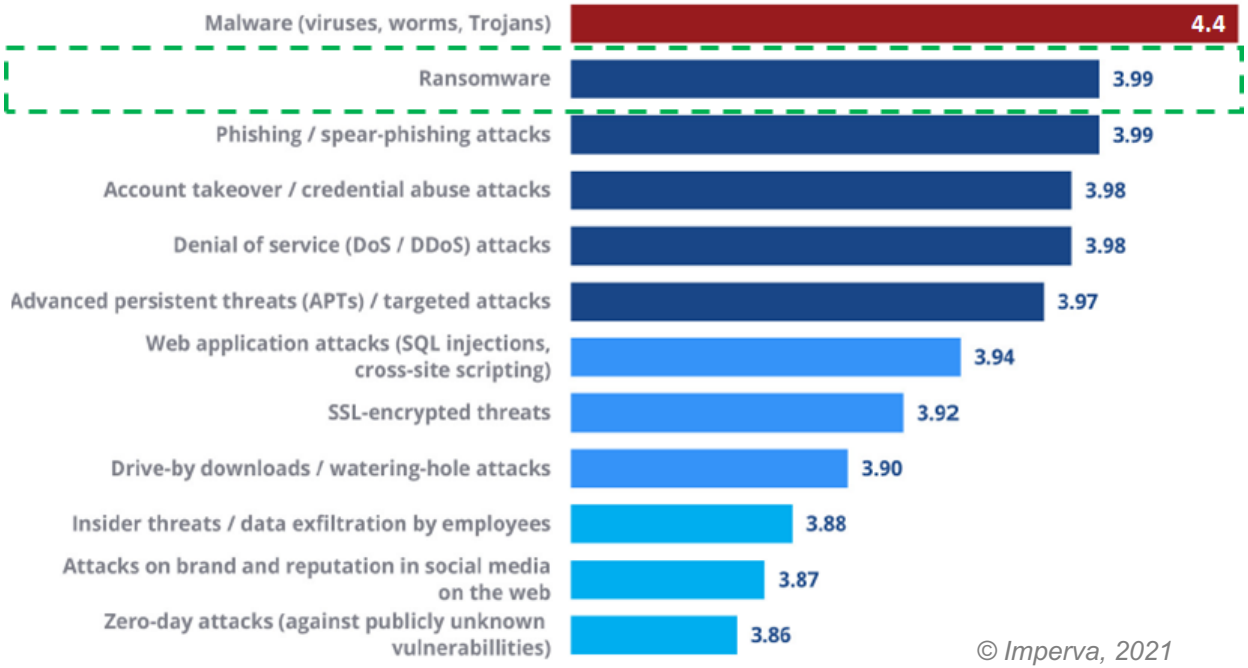
Amenazas *(i)*

- Amenazas de seguridad principales:



Amenazas *(ii)*

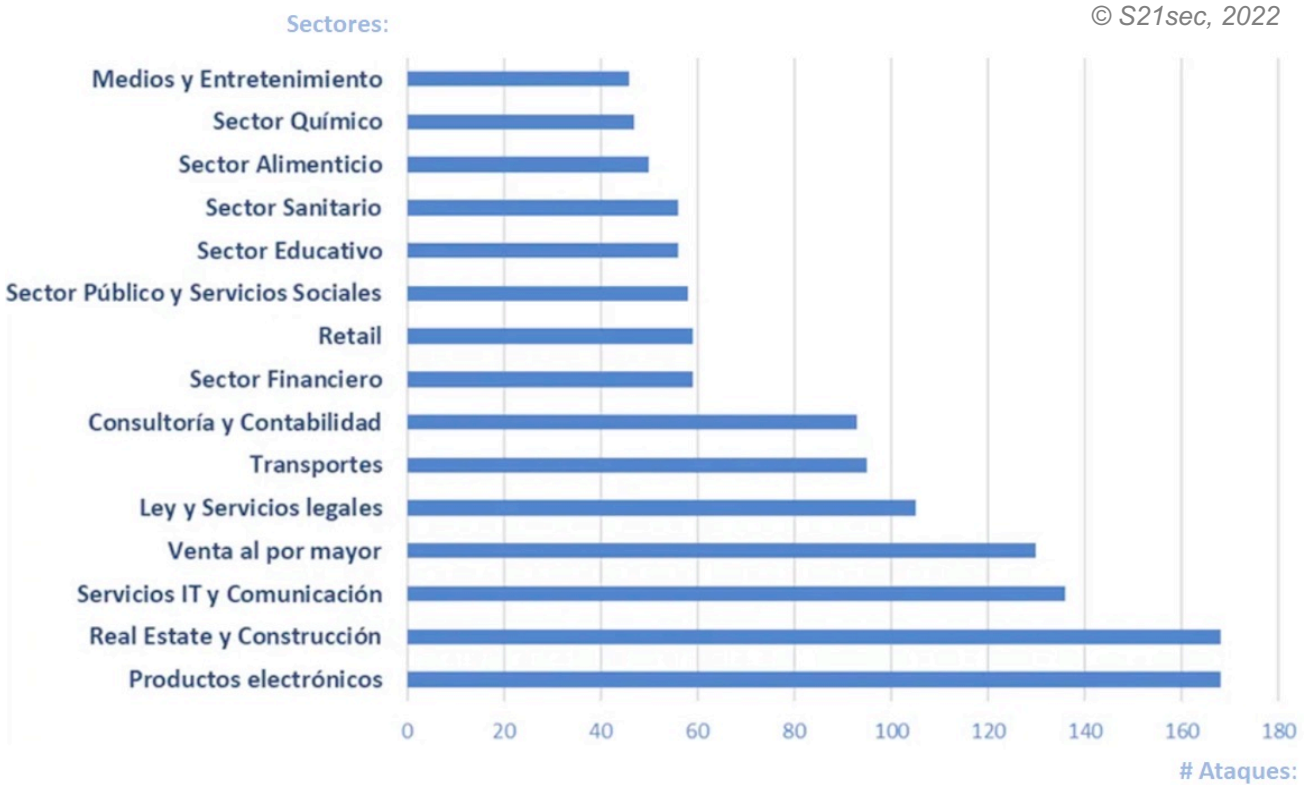
- Percepción de amenazas (1-5):



© Imperva, 2021

Amenazas *(iii)*

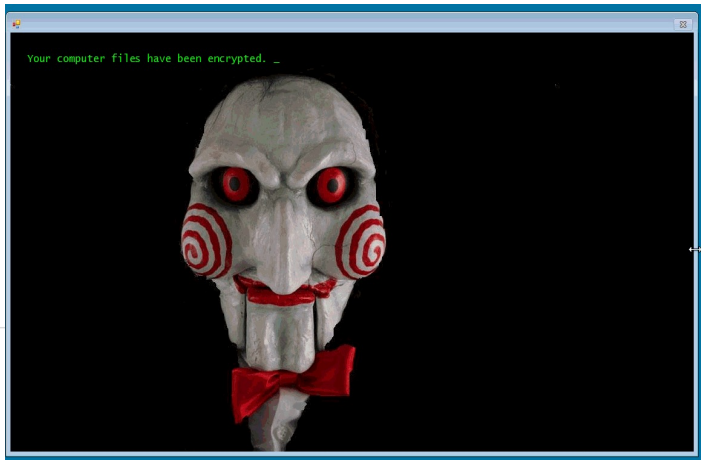
- Afectación:



© S21sec, 2022

Amenazas *(iv)*

- Afectación *(cont.)*:



Sanidad

Un "grave" ciberataque paraliza los servicios de al menos tres grandes hospitales de Barcelona

Los centros Moisès Broggi de Sant Joan Despí, el Dos de Maig de Barcelona y el Creu Roja de L'Hospitalet sufren afectaciones por un ataque de tipo 'ransomware' que secuestra datos para pedir un rescate económico

elDiario.es

Hazte socio/a Inicia sesión

Castilla-La Mancha

Política Social Agroalimentaria Universidades Nuestros blogs Provincias Nuestro boletín

El programa malicioso Ryuk, causante del ciberataque en la Universidad de Castilla-La Mancha, el mismo que hizo caer al SEPE

La Institución académica confía en recuperar los datos y los servicios digitales de la UCLM "en próximos días" tras el ataque "premeditado contra la infraestructura crítica de la universidad"

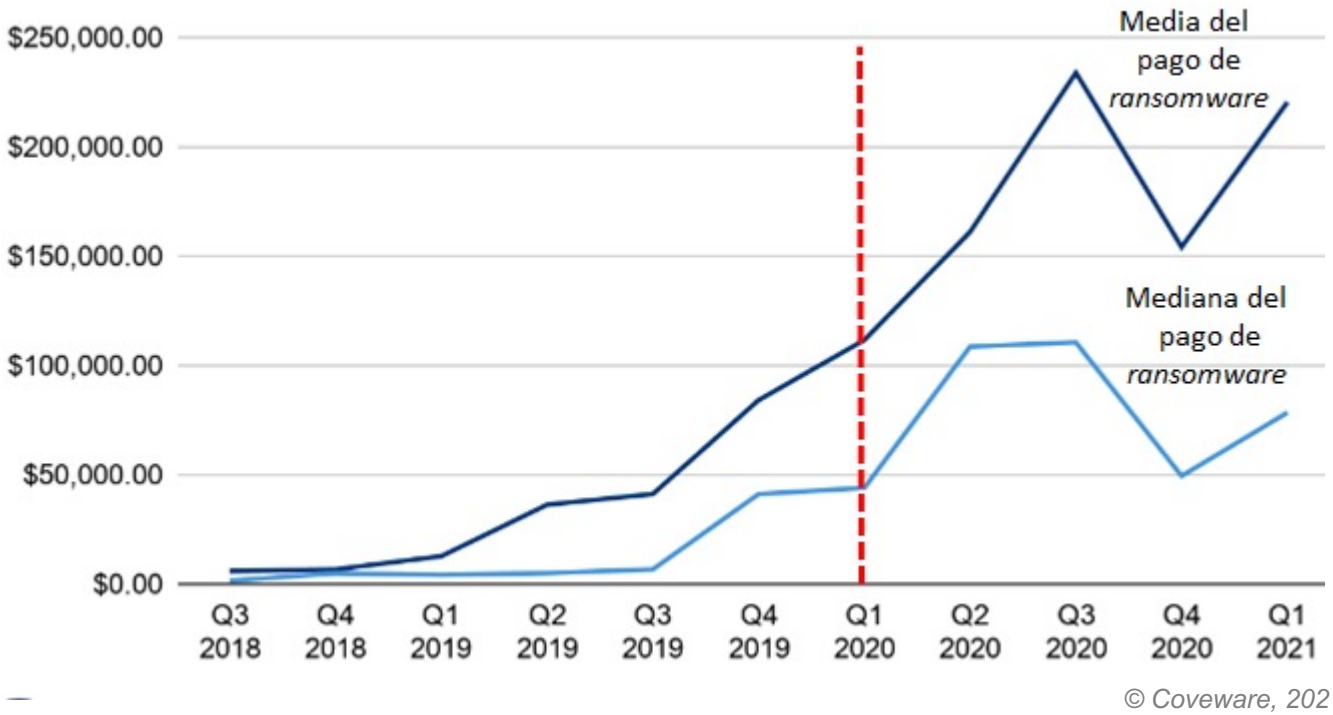
2021

Tipologías

- Tipos de *ransomware*: *locker* vs *crypto*

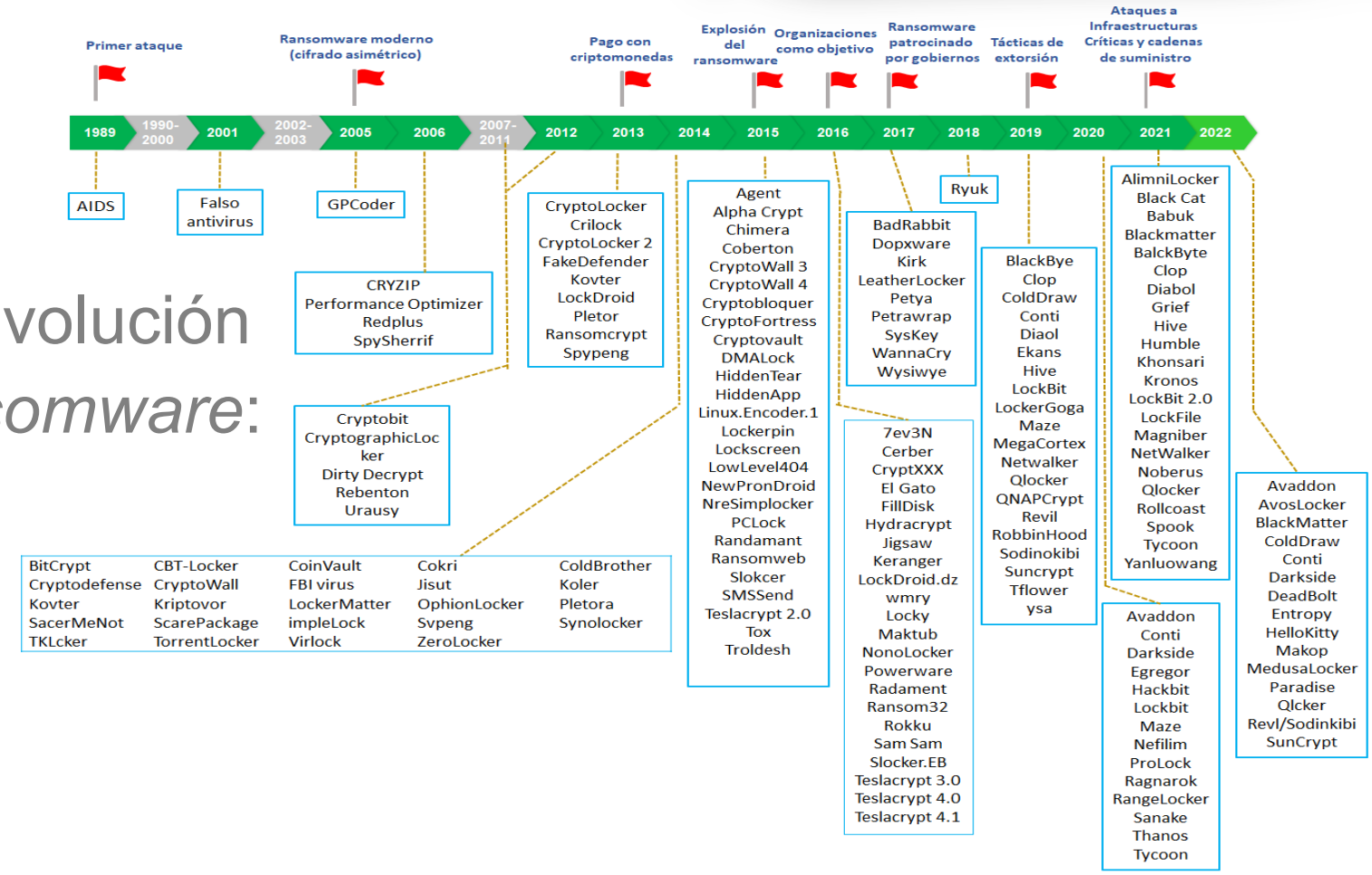
Impacto

- Coste rescate:



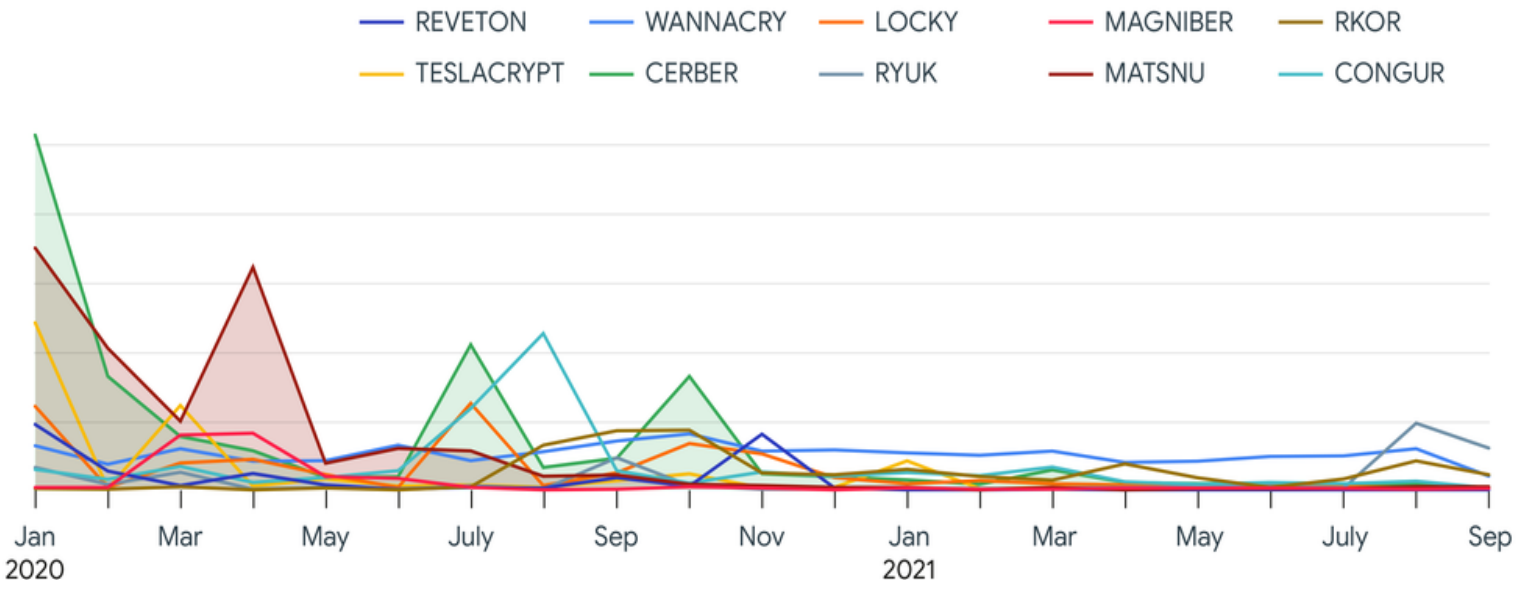
Evolución *(i)*

- Evolución *ransomware*:



Evolución *(ii)*

- Familias más activas:

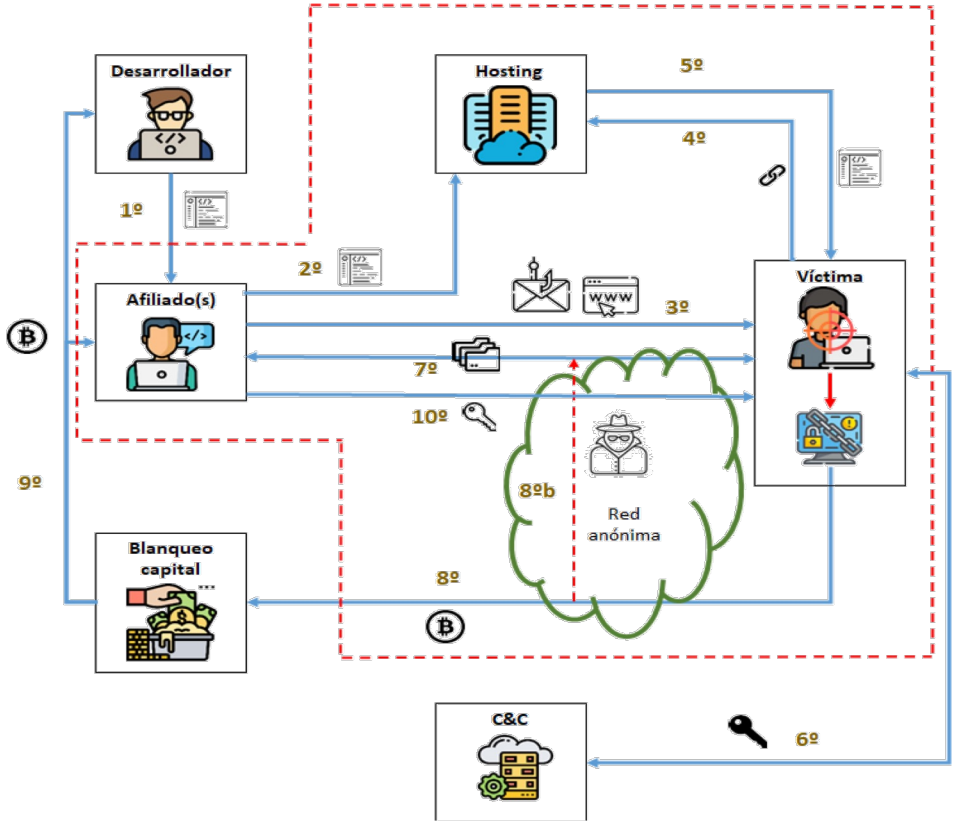


© VirusTotal, 2022

RaaS

- *Ransomware-as-a-Service*:

Modelo de negocio

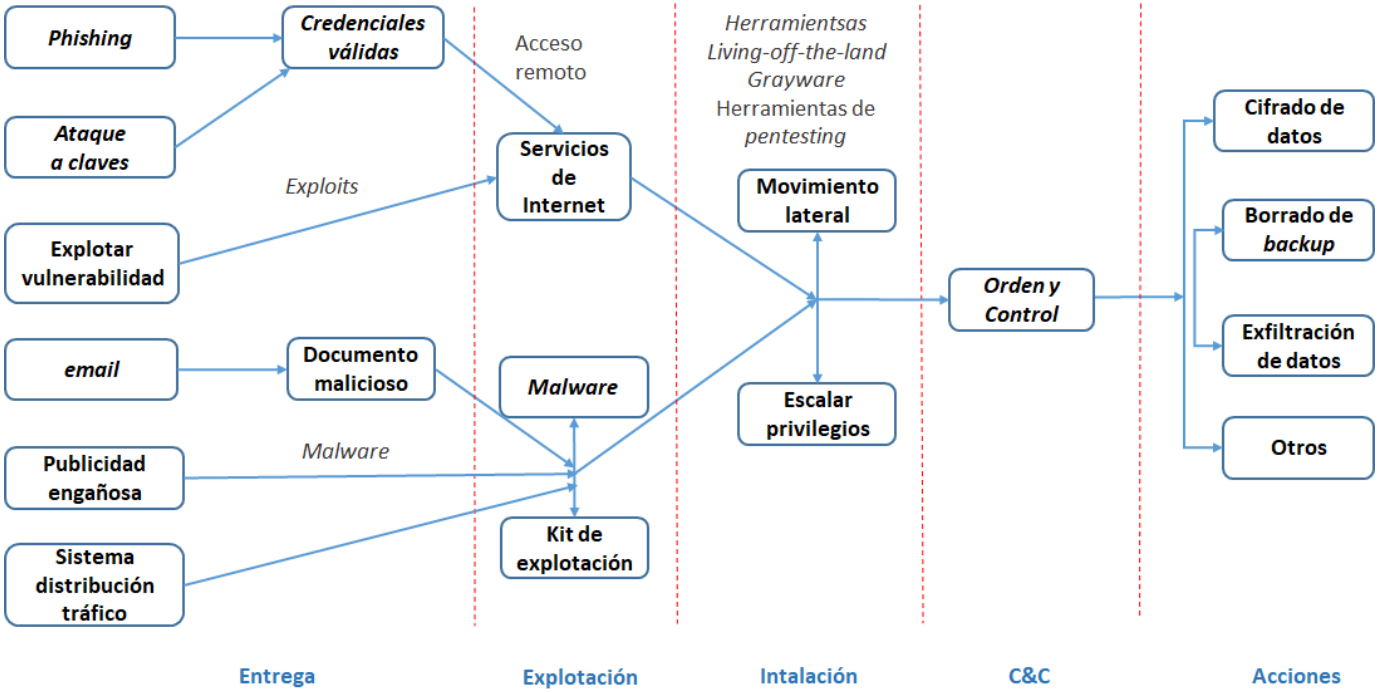


Índice

- Ciberseguridad en cifras
- Fundamentos del *ransomware*
- Modelos de ataque y defensa
- R-Locker
- Tendencias y retos

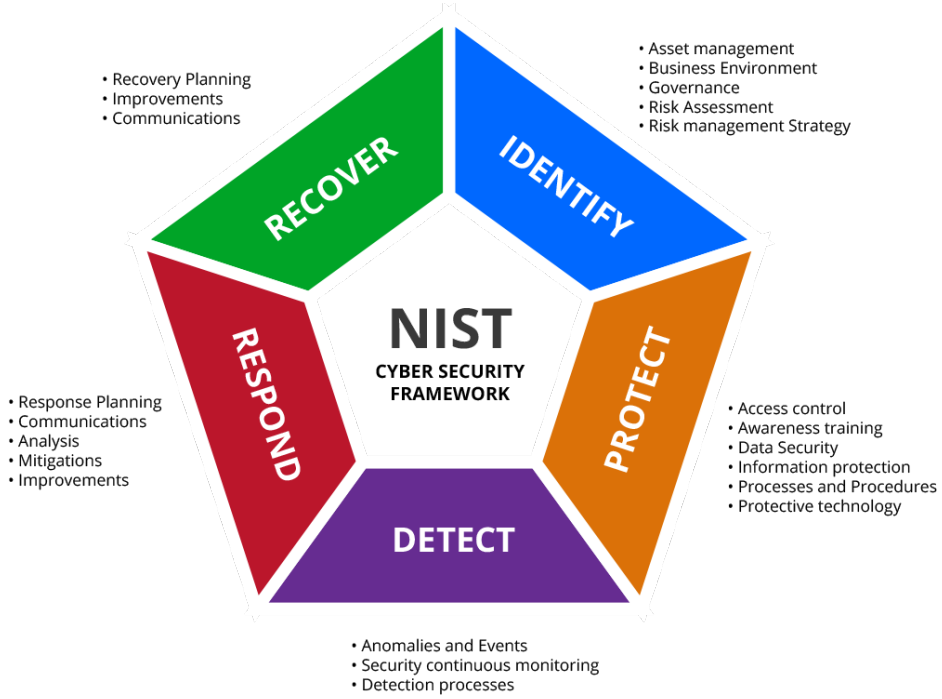
Ciclo de vida

- Ciclo de vida del *ransomware*:



Defensa

- *NIST Cyber Security Framework*:

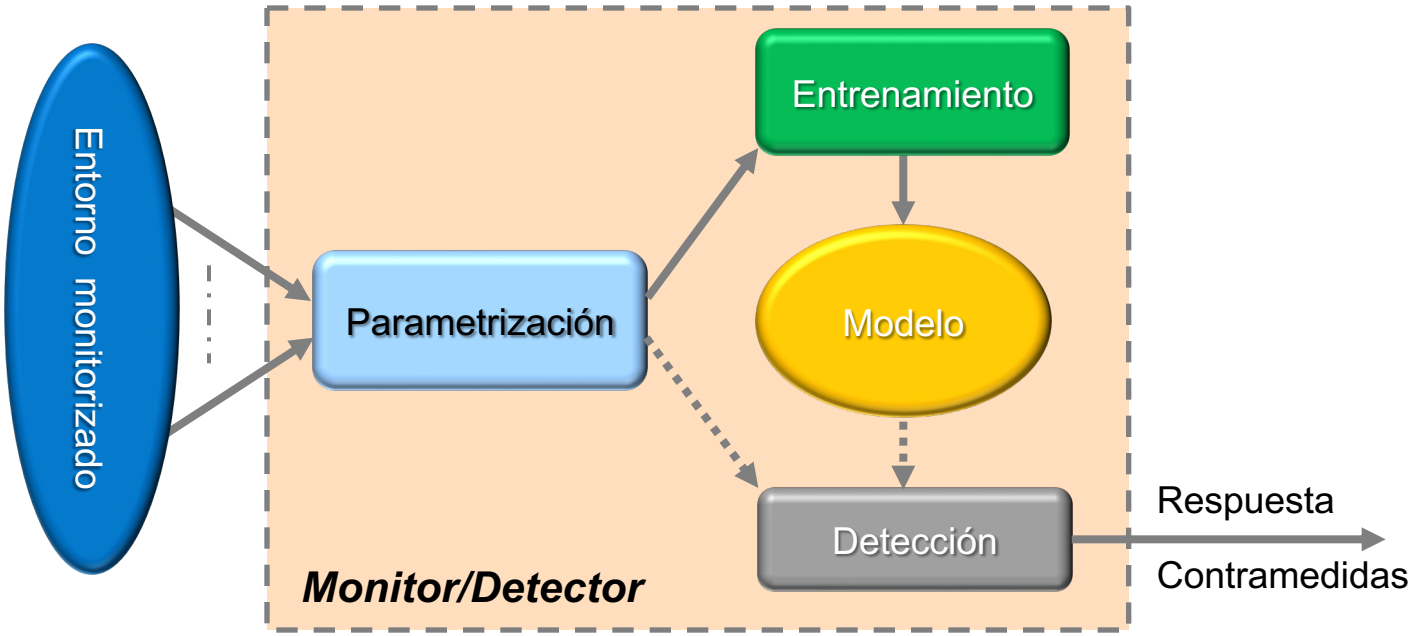


Prevención

- Medidas preventivas:
  - Concienciación de usuarios
  - Uso de software legítimo
  - Actualización de software y *firmware*
  - Segmentación de redes
  - Control de accesos (permisos, recursos)
  - Políticas BYOD
  - *Backups* periódicos
  - Herramientas monitorización anti-*malware*…

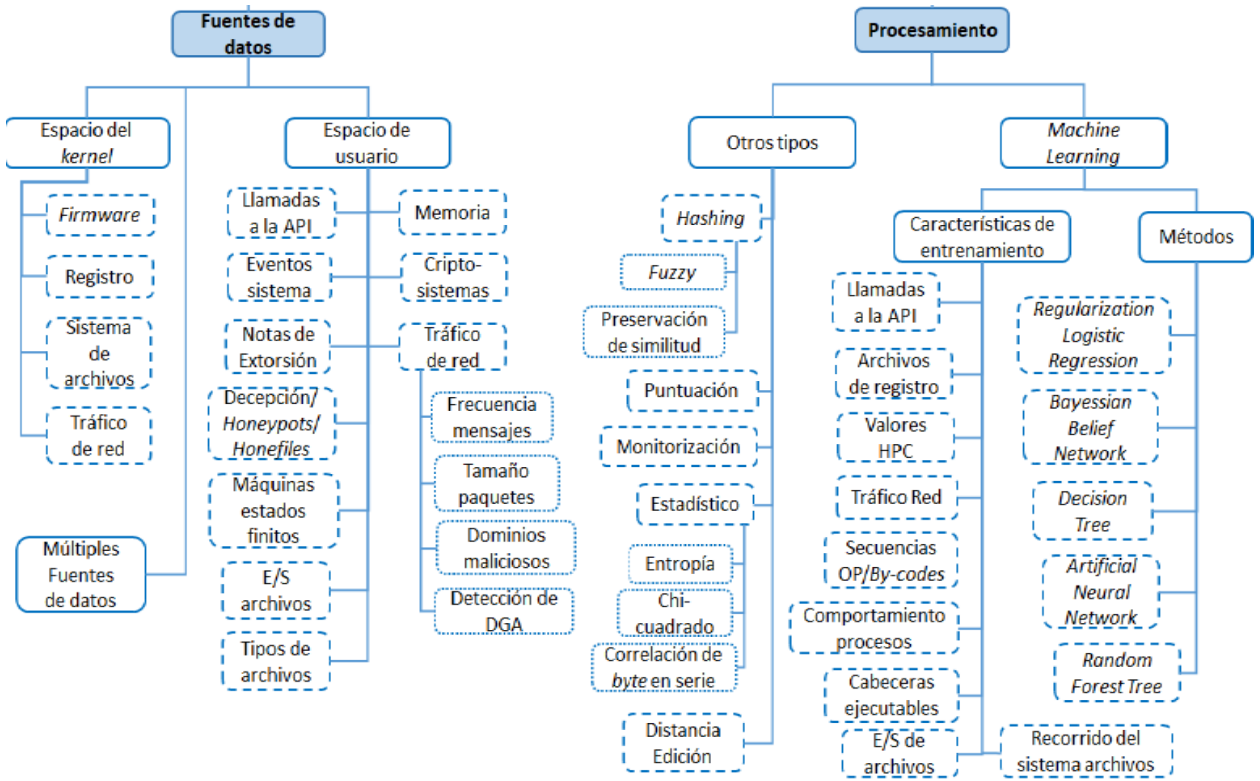
Detección *(i)*

- Monitorización del entorno:



Detección *(ii)*

- Monitorización del entorno *(cont.)*:



Respuesta

- Respuesta/contramedidas:
  - Detención/eliminación *ransomware*
  - Notificación al usuario
  - Obtención de claves… Pago rescate?
  - Plan de contingencia y recuperación
  - Datos distribuidos
  - Observación/cuarentena

Herramientas

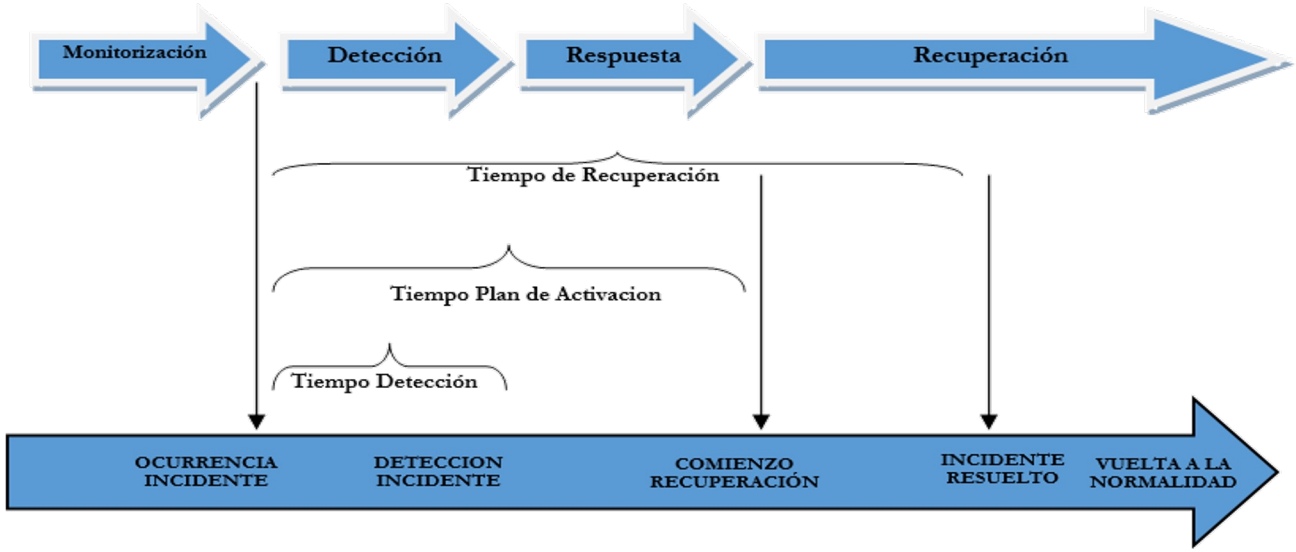
	Detección																Recuperación							
	Fuente		*Machine Learning*					Procesamiento					Acciones					Fuentes				Proc		Acción	
Nombre	*Kernel*	Usuario	RLR	DT	RF	ANN	BBN	H	S	M	E	ED	Su	K	B	L	Nu	Bk	Es	Ch	API	K	DD	Re	D
Connection Monitor		N								√	√						√								
CryptoDrop	SF							√	√	√	√			√	√		√								
Data Aware Defense	SF									√	√				√										
EldeRun	SF R	CA	√							√															
Honeypot		HT								√				√		√	√								
RAPPER	CA				√				√			√				√									
Redemption	SF								√	√	√			√			√	√	√						
R-Killer	SF	N				√				√				√			√								
R-Locker		HT								√				√											
Pay-Break																					√	√			√
SSD-Insider	A			√												√	√		√	√			√	√	
USNP(*)		CS								√				√		√	√								
Unveil	SF	No								√	√			√		√									
2entFOX	R/SF	API CS Ev					√				√														

Abreviaciones: B: Bloquear; Bk: Copia de seguridad; Ch: Caché; CS: Cripto-sistema; D: Descifrado; DD: Detección retrasada; E: Estadístico; ED: Distancia; Es: Interceptación de E/S; Ev: Eventos; H: Firmas; HT: Trampa; K: Obtener claves; Ke: Kernel; L: Aislamiento; M: Monitorización; K: Matar; N: Red; No: Nota extorsión; Nu: Notificar usuario; R: Registro; Re: Restauración; S: Puntuación; SF: Sistema de archivos; Su: Vigilancia; Us: Usuario. // (*) USNP: USahllNotPass

Índice

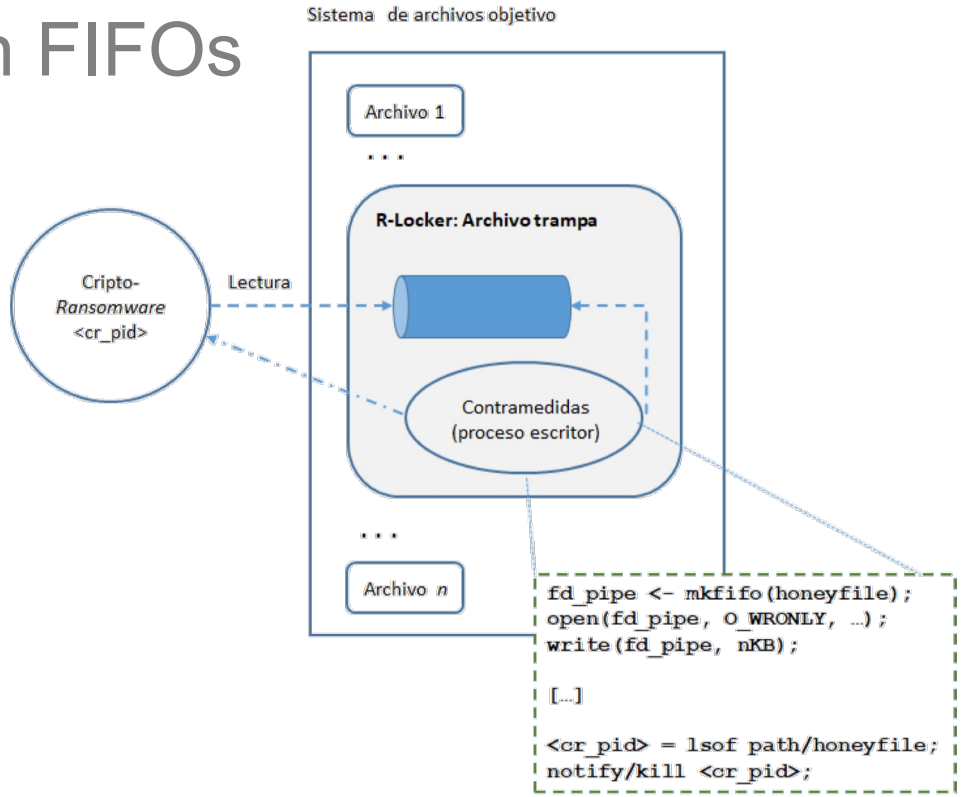
Recuperación incidentes

- Minimización *Time-To-Ransom*:



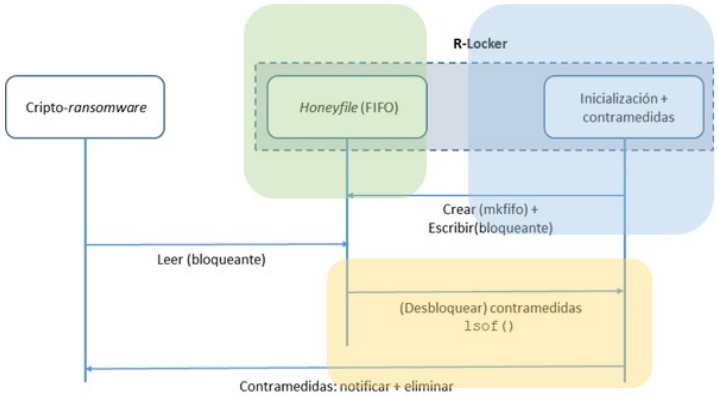
R-Locker *(i)*

- Despliegue de *honeyfiles* en el *filesystem*, soportados en FIFOs
- Anatomía:



R-Locker *(ii)*

- Algoritmo sobre Linux:



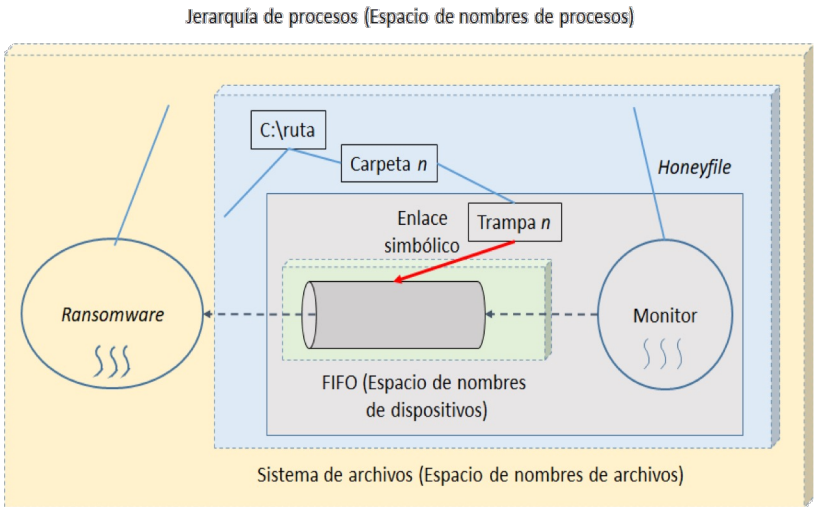

```
Entrada: nula
Salida: nula
1  ruta_trampa                    // Enlace simbólico al honeyfile
2  lista_extensiones_trampa ← {.pdf .jpg .doc ...}
3  Honeyfile                      // Nombre del FIFO
4  Función PoblarTrampas(ruta_trampa):
5      lista_carpetas ← Generar la lista de carpetas
6      para cada carpeta en lista_carpetas hacer
7          si no existe ruta_trampa entonces
8              Crear_Enlace (Honeyfile, ruta_trampa.extension_trampa);
9      Función InstanciarHoneyfile(rutaFIFO):
10         Crear_Fifo(Honeyfile,...)          // Crear el FIFO
11     Función Principal:
12         InstanciarHoneyfile(Honeyfile)
13         PoblarTrampas(Honeyfile)
14         dF = Abrir_Archivo (Honeyfile, O_WRONLY) // Abrimos
               el FIFO de escritura
15         para (;;) hacer
16             Escribir (dF, 4 KB + 1) // El proceso queda
                   bloqueado hasta que llegue un lector
               // Cuando se desbloque el proceso...localizar su
                   ID a través de su inodo
17             cr_pid ← Proceso accediendo al Honeyfile
               // Terminar proceso lector
18             Terminar_Proceso (cr_pid, señal_finalizar)
19             ... notificar usuario
```

R-Locker *(iii)*

- R-Locker sobre Windows:
  - Espacio de dispositivos ≠ espacio de nombres

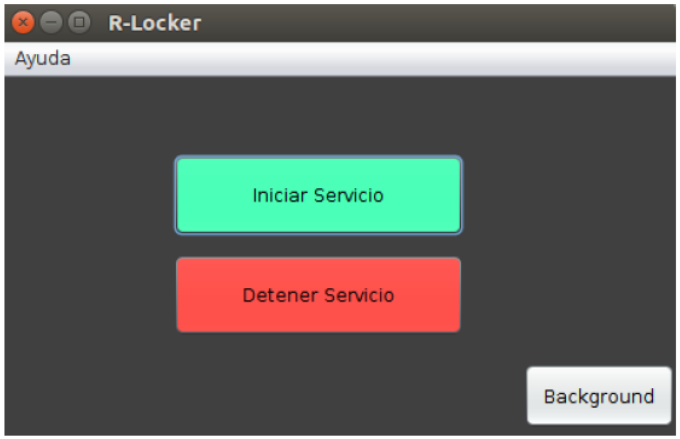
Enlaces simbólicos

  - Solución multihebrada
  - Listas blancas/negras



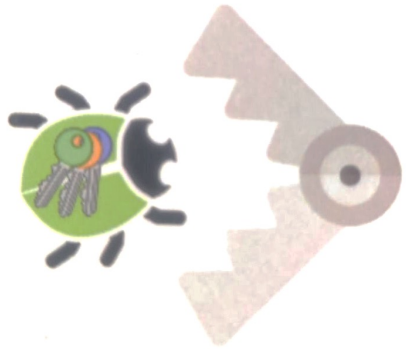
R-Locker *(iv)*

- Resultados:
  - *https://github.com/JA-Gomez-Hernandez/R-Locker*
  - 100% detección (Cerber, Jigsaw, Bash-Ransomware, Wannacry, Linux.Encoder.1, Genérico… *repo: TheZoo/VirusTotal/VirusShare/…*)



R-Locker *(v)*

- Características:
  - Alta efectividad
  - Bajo consumo
  - No privilegios
  - Sencillez
  - Transparencia



- *… ¿Uso en Android?...* No FIFO, No enlaces

Monitorización reactiva con *inotify* -FileOberserver()-

Índice

- Ciberseguridad en cifras
- Fundamentos del *ransomware*
- Modelos de ataque y defensa
- R-Locker
- Tendencias y retos

Tendencias y retos

- *Ransomware* continúa siendo pandemia
- Nuevas familias y metodologías
- Necesidad de alerta temprana
- Algoritmos *lightweight:* móviles, IoT,…
- IA y colaboración
- Normativa y legislación en la persecución del *ransomware*

NESG
Network Engineering & Security Group

(+34) 958242305
pgteodor@ugr.es
https://nesg.ugr.es

Pedro García Teodoro
Full Professor-Group Head

Dpto. Teoría de la Señal, Telemática y Comunicaciones
ETS Ingenierías Informática y de Telecomunicación

UNIVERSIDAD DE GRANADA