

Panda Security

Alberto Tejero- Director General Iberia

¿Están protegidos
del ransomware las
empresas?

Los ataques de Ransomware se han disparado un 500% en 2019 desde el año pasado en este mismo periodo.

Un grupo de ciberdelincuentes filtra los archivos robados durante un ataque a la multinacional portuguesa EDP, a la que exigió 10 millones de euros como rescate

Alberto R. Aguilar 6 May 2020 07:16h. - Actualizado: 6 May 2020 07:16h.



El mayor grupo de hospitales privados de Europa y dueño de Quirónsalud sufre un ataque global con ransomware

Alberto R. Aguilar 8 May 2020 07:46h. - Actualizado: 8 May 2020 07:46h.



Adeslas sufre un ataque de ransomware sobre sus sistemas informáticos

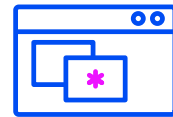
Por Redacción - 11 septiembre, 2020

¿Qué está ocurriendo?

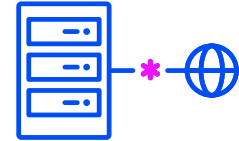
¿Cómo se propaga el Ransomware?



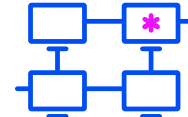
- En muchas ocasiones a través de correos electrónicos (phishing)



- Vulnerabilidades del software. Recordemos el caso del Wannacry y Petya



- Servidores expuestos a Internet no parcheados. Intentar entrar por RDP, exploits, etc



- Se infiltran en las redes de empresas más pequeñas (de marketing o de recursos humanos, por ejemplo) que son generalmente proveedores del objetivo final

Ficheros de firmas y heurísticas

Tecnologías antivirus

- Firmas específicas
- Detección genérica y heurística
- Bloqueo de URLs de Ransomware

Cryptolocker: 10 steps to avoid the ransomware virus

Global cybercrime agencies say users already infected with the Cryptolocker ransomware have a two-week window to remove it
[Cryptolocker virus network thwarted by global operation](#)



The Windows Club

Home News Windows Downloads Security IE Office Phone General Deals Forum About

CryptoLocker Tripwire: Free Cryptolocker Prevention Tool

A THREE TIME GARTNER MAGIC QUADRANT LEADER

Conclusión / Insuficientes

- Nuevas variantes de malware muy sofisticadas siguen infectando los sistemas de las empresas con niveles de protección menor.
- Gran cantidad de consejos y herramientas disponibles en Internet para intentar detener la avalancha de infecciones.

Panda Adaptive Defense

Panda Adaptive Defense 360

La solución al ransomware y otras amenazas avanzadas y Zero-day

Protección por capas

Capa 1 / Ficheros de firmas y tecnologías heurísticas

Tecnología eficiente y optimizada para detectar ataques conocidos.

Capa 2 / Detecciones contextuales

Nos permiten detectar ataques malwareless y fileless.

Capa 3 / Tecnología antiexploit

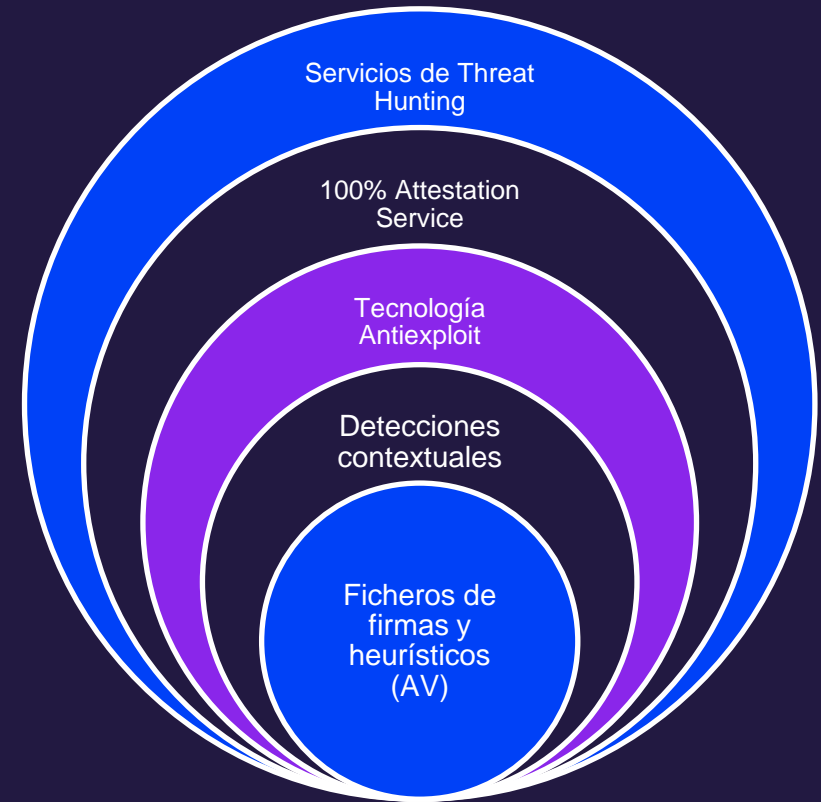
Nos permiten detectar ataques fileless que explotan vulnerabilidades

Capa 4 / 100% Attestation Service

Necesaria para brechas de capas previas, detener ataques en equipos ya infectados y para ataques en red interna por movimientos laterales

Capa 5 / Servicios de Threat Hunting

Nos permiten detectar máquinas comprometidas, ataques en fase temprana y actividades sospechosas



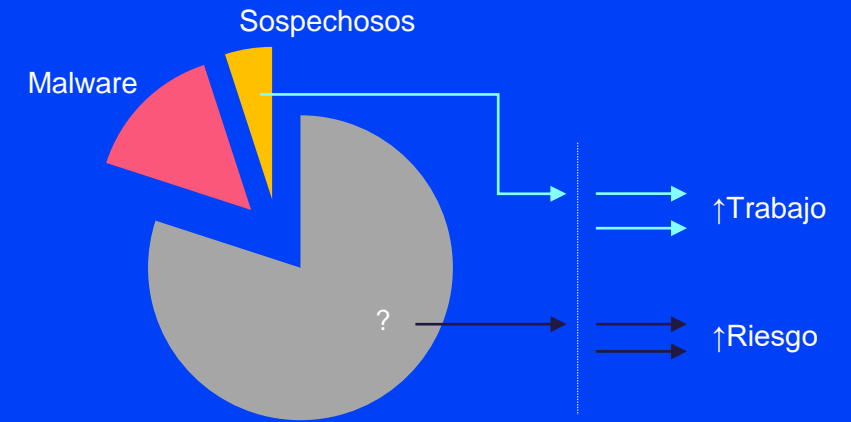
100% Attestation Service

- Complementa a las capas previas
- Imprescindible para organizaciones ya infectadas y para detener ataques en red interna por movimientos laterals
- Muy importante también para proteger equipos/servidores en organizaciones con equipos desprotegidos o con otras soluciones a las que se les escapa malware



Antivirus tradicionales y otros EDRs

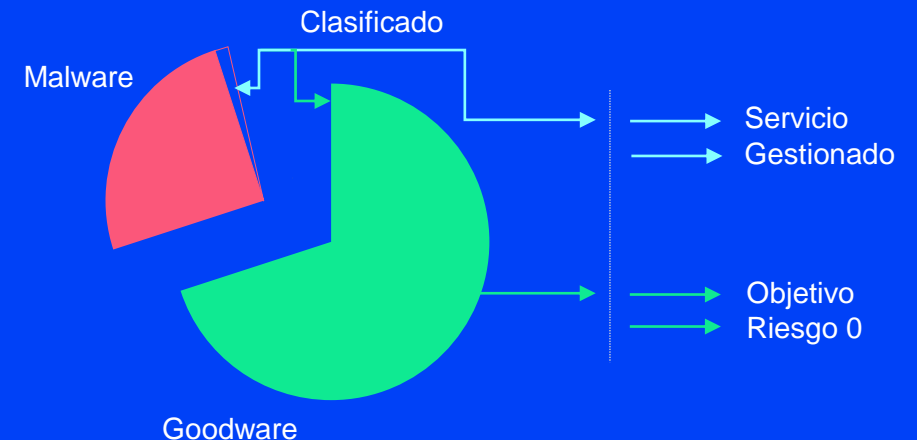
Conocen el malware pero desconocen lo demás
-> Riesgo



Adaptive Defense

Monitorización de todos los procesos en ejecución para permitir únicamente la ejecución de los clasificados como confiables por Panda.

Servicio gestionado. Máxima protección sin delegar la decisión en el cliente.



Servicios de Threat Hunting

- Los hackers lanzan **ciberataques extremadamente sofisticados**. Ninguna medida de seguridad te garantiza el 100% de seguridad.
- **Una amenaza puede permanecer durante meses sin ser descubierta** si no hay un proceso proactivo de búsqueda de amenazas.
- **Los hackers dejan trazas** que nos permite detectar ataques “desconocidos” que utilizan técnicas LOTL (Living-off-the-Land Techniques)



¿Qué ofrece Panda?

- Servicio Threat Hunting cross (THIS) incluido en nuestro EDR (Adaptive Defense)

Única solución en el mercado
que clasifica el 100% de los
procesos que se ejecutan en
los equipos.

Permitiendo ejecutar únicamente lo
clasificado como confiable.

¿Están
protegidos
nuestros
clientes?

0,00%
Infecciones

NINGÚN cliente de Adaptive
Defense ha sido infectado.

¿Qué opina el mercado?

Reconocimientos



Certificaciones oficiales



COMMON CRITERIA “EAL2”
por el Information Technology Security Evaluation



Clasificación “ENS” Alto
por el Esquema Nacional de Seguridad



Producto de Seguridad IT Cualificado
por el Centro Criptológico Español

Gracias

