Panda Security

panda

pandasecurity.com/business

Estado España Digital

85%
Población conectada

40.000M€
Ecommerce

+27%
2019 vs 2018

Ciberseguridad en cifras

+120.000
Incidentes seguridad vs 2018

1/3
Usuarios afectados

43%
Pymes

60%
Pyme NO se recupera

35.000€
Coste por ataque

Considera ciberseguidad
0,05%
como algo estratégico

Nuevo reto: la ciberseguridad en un entorno cambiante

¿Qué está ocurriendo actualmente?

Teletrabajo

2019- 7,9% máximo histórico

03/2020- ¿x3? ¿x4?

panda

Uso de internet desde Marzo 2020

+40%
Tráfico IP

+50%
Llamadas

+25%
Datos móviles

Ciberataques detectados desde Marzo 2020

+200.000
Oleadas de ataque

70%
Correos malware

30%
Web falsas

Malware & Ransomware CoronaVirus

Gracias al servicio 100% attestation service hemos conseguido identificar y bloquear los siguiente ejecutables maliciosos relativos a estas campañas:

Nombre del archivo	SHA 256
CORONA VIRUS AFFECTED CREW AND VESSEL.xlsm	ab533d6ca0c2be8860a0f7fbfc7820ffd 595edc63e540ff4c5991808da6a257d
	17161e0ab3907f637c2202a384de67fca 49171c79b1b24db7c78a4680637e3d5
	315e297ac510f3f2a60176f9c12fcf9 2681bbad758135767ba805cdea830b9ee
CoronaVirusSafetyMeasures_pdf.exe	c9c0180eba2a712f1aba1303b90cbf12c11 17451ce13b68715931abc437b10cd
	29367502e16bf1e2b788705014d0142 d8bcb7fcc6a47d56fb82d7e333454e923
LIST OF CORONA VIRUS VICTIM.exe	3f40d4a0d0fe1eea58fa1c71308431b5c2c e6e381cacc7291e501f4eed57bfd2
POEA HEALTH ADVISORY re-2020 Novel Corona Virus.pdf.exe	3e6166a6961bc7c23d316ea9bca87d82 87a4044865c3e73064054e805ef5ca1a
POEA Advisories re-2020 Novel Corona Virus.2.pdf.exe	b78a3d21325d3db7470fbf1a6d254e23d34 9531fca4d7f458b33ca93c91e61cd

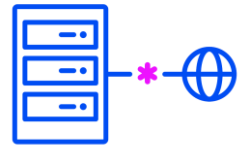
Dominios relativos a campañas CoronaVirus

- acccorona [.] com
- alphacoronavirusvaccine [.] com
- anticoronaproducts [.] com
- beatingcorona [.] com
- beatingcoronavirus [.] com
- bestcorona [.] com
- betacoronavirusvaccine [.] com
- buycoronavirusfacemasks [.] com
- byebyecoronavirus [.] com
- cdc-coronavirus [.] com
- combatcorona [.] com
- contra-coronavirus [.] com
- corona-blindado [.] com
- corona-crisis [.] com
- corona-emergencia [.] com
- corona explicada [.] com
- corona-iran [.] com
- corona-ratgeber [.] com
- coronadatabase [.] com
- coronadeathpool [.] com
- coronadetect [.] com
- coronadetection [.] com

¿Están protegidos del ransomware las empresas?

¿Cómo se propaga el Ransomware?

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



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

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

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

panda

Ficheros de firmas y heurísticas

Tecnologías antivirus

- Firmas específicas
- Detección genérica y heurística

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

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 detector ataques conocidos.

Capa 2 / Detecciones contextuales

Nos permiten detector ataques malwareless y fileless.

Capa 3 / Tecnología antiexploit

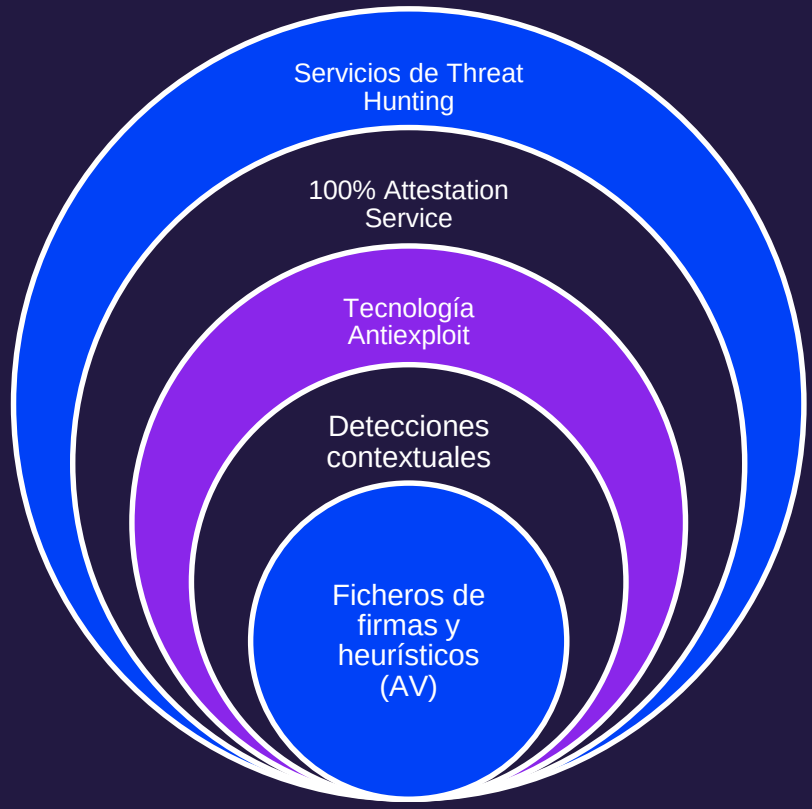
Nos permiten detector ataques fileless que explotan vulnerabilidades

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 detector máquinas comprometidas, ataques en fase temprana y actividades sospechosas

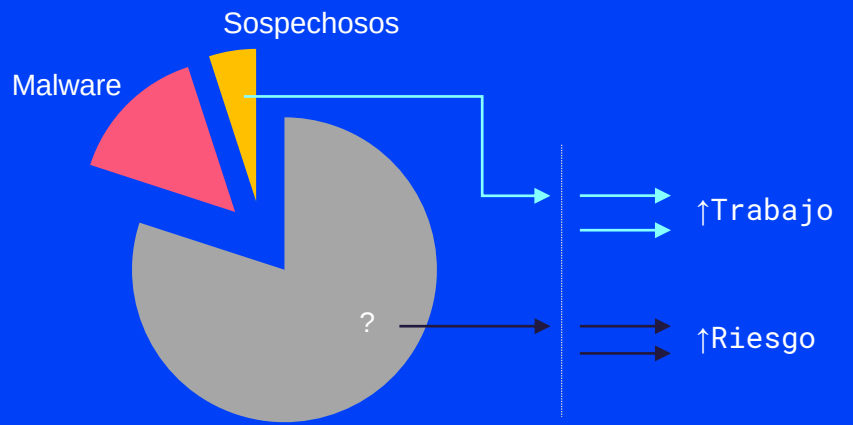


100% Attestation Service

- Complementa a las capas previas
- Imprescindible para organizaciones ya infectadas y para detener ataques en red interna
- 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

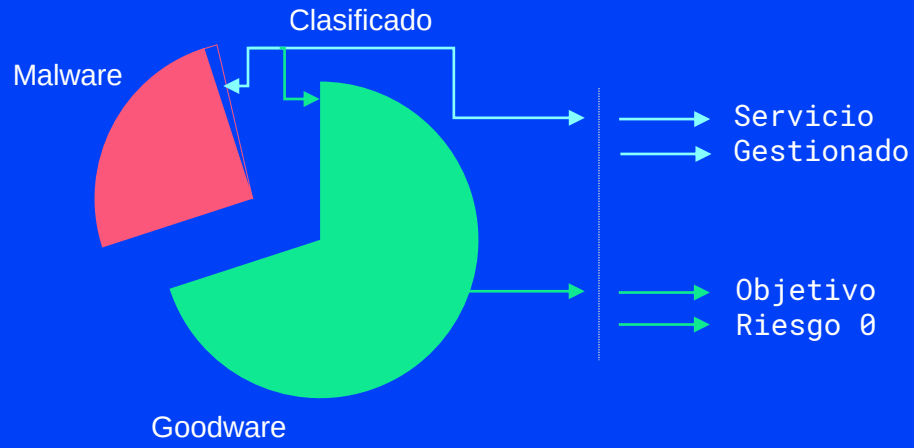
Conocen el malware pero desconocen lo demás
-> Riesgo



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.



panda

Servicios de Threat Hunting

- Los hackers lanzan **ciberataques extremadamente sofisticados**
- **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 incluido en nuestro EDR (Adaptive Defense)

panda

Ventajas Competitivas

Ventajas Competitivas

Más de 5 años con nuestro EDR en el mercado

Nos permite tener la ***Inteligencia Colectiva*** con conocimiento de aplicaciones legítimas y maliciosas, que es continuamente alimentada con nuevo conocimiento procedente de los millones de endpoints protegidos.

Sistema basado en Inteligencia Artificial en la nube

En la que se ejecutan diversos algoritmos de clasificación, desde los más sencillos, como algoritmos de similaridad y árboles de decisión, hasta los más complejos, como redes neuronales y modelos de deep learning.

El 99,98% de las aplicaciones son clasificadas automáticamente y el 0,02% restante por un equipo de expertos de nuestro laboratorio.

Completa Visibilidad

La completa visibilidad que nos da Adaptive Defense nos permite tener un proceso de mejora continúa de las detecciones contextuales que se adaptan a las nuevas amenazas.

Sin sospechosos, ni elementos en investigación

2 grandes ventajas:

- Los equipos de seguridad no tienen que analizar las alertas en profundidad. Eso podría significar: más personal o dejar alertas sin verificación, por lo tanto, el riesgo de seguridad no está bajo control.
- Si tiene que verificarlos, significa que MTTD y MTTR (Tiempo medio para detectar / Tiempo medio para responder) serán peores que los nuestros. Retrasar los minutos de decisión podría significar ser masivamente afectados por un atacante o una violación de datos.

panda

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.

panda

¿Fiabilidad?

Certificaciones oficiales

Europea

COMMON CRITERIA “EAL2”
por el Information Technology Security Evaluation

Nacionales

Clasificación “ENS” Alto
por el Esquema Nacional de Seguridad

Producto de Seguridad IT Cualificado
por el Centro Criptológico Español

panda

Gracias

pandasecurity.com/business