Panda Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

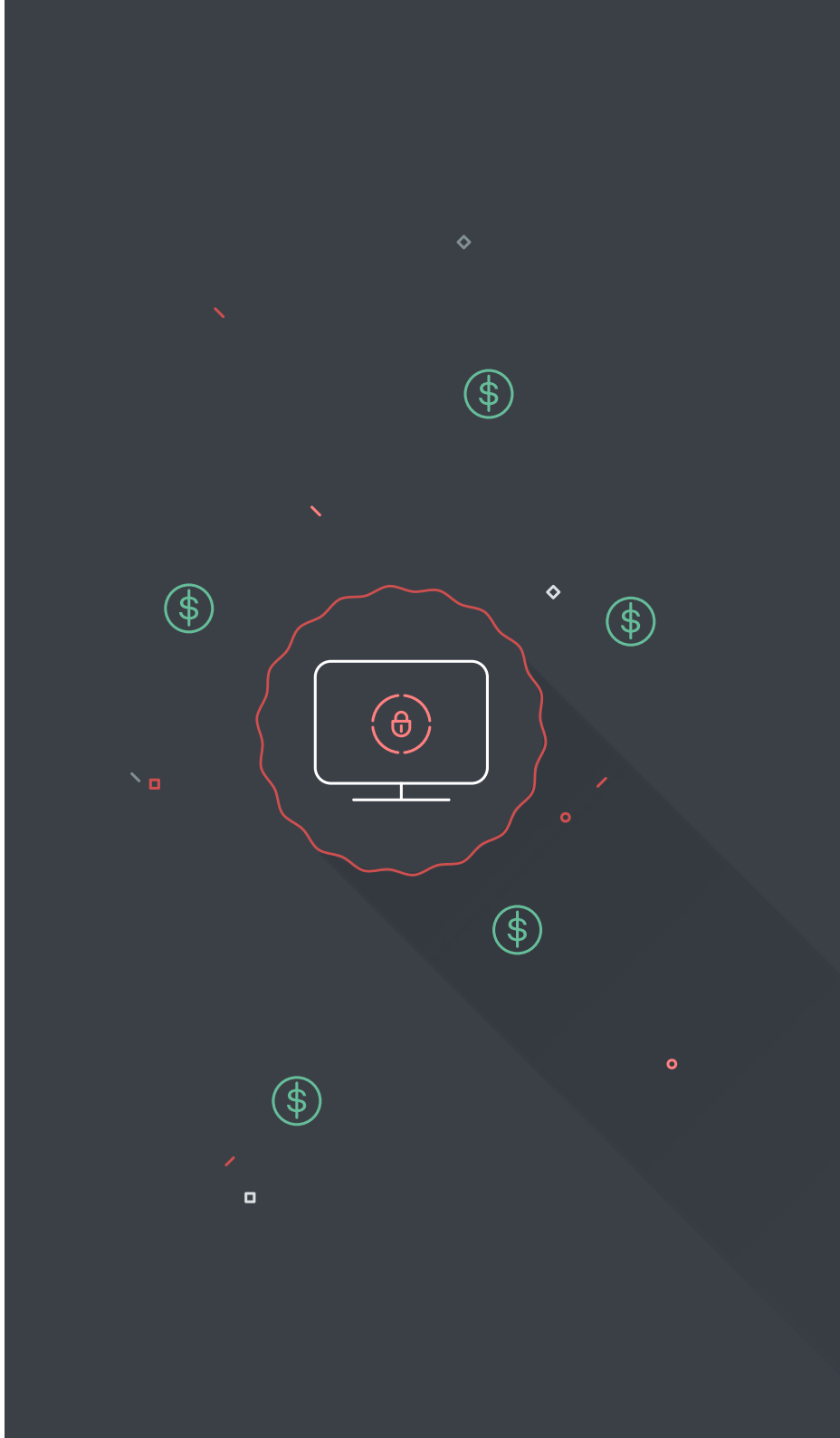
SIN SECUESTRO, NO HAY RE$CATE

panda

pandasecurity.com/business/adaptive-defense/

Índice de Contenidos

1. Introducción. 3
2. El paradigma de la transformación digital. 4
3. Ataques patrocinados por Estados. 5
4. Empresas, en el punto de mira. 6
5. El Precio de los Ataques. 8



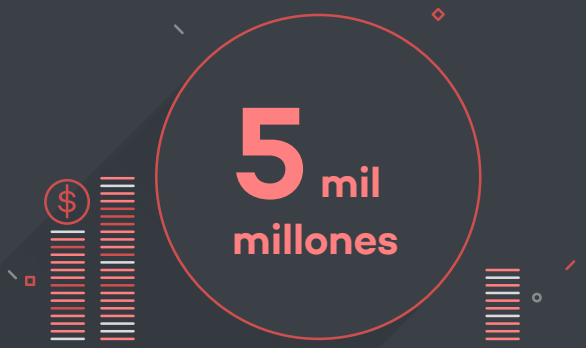
panda

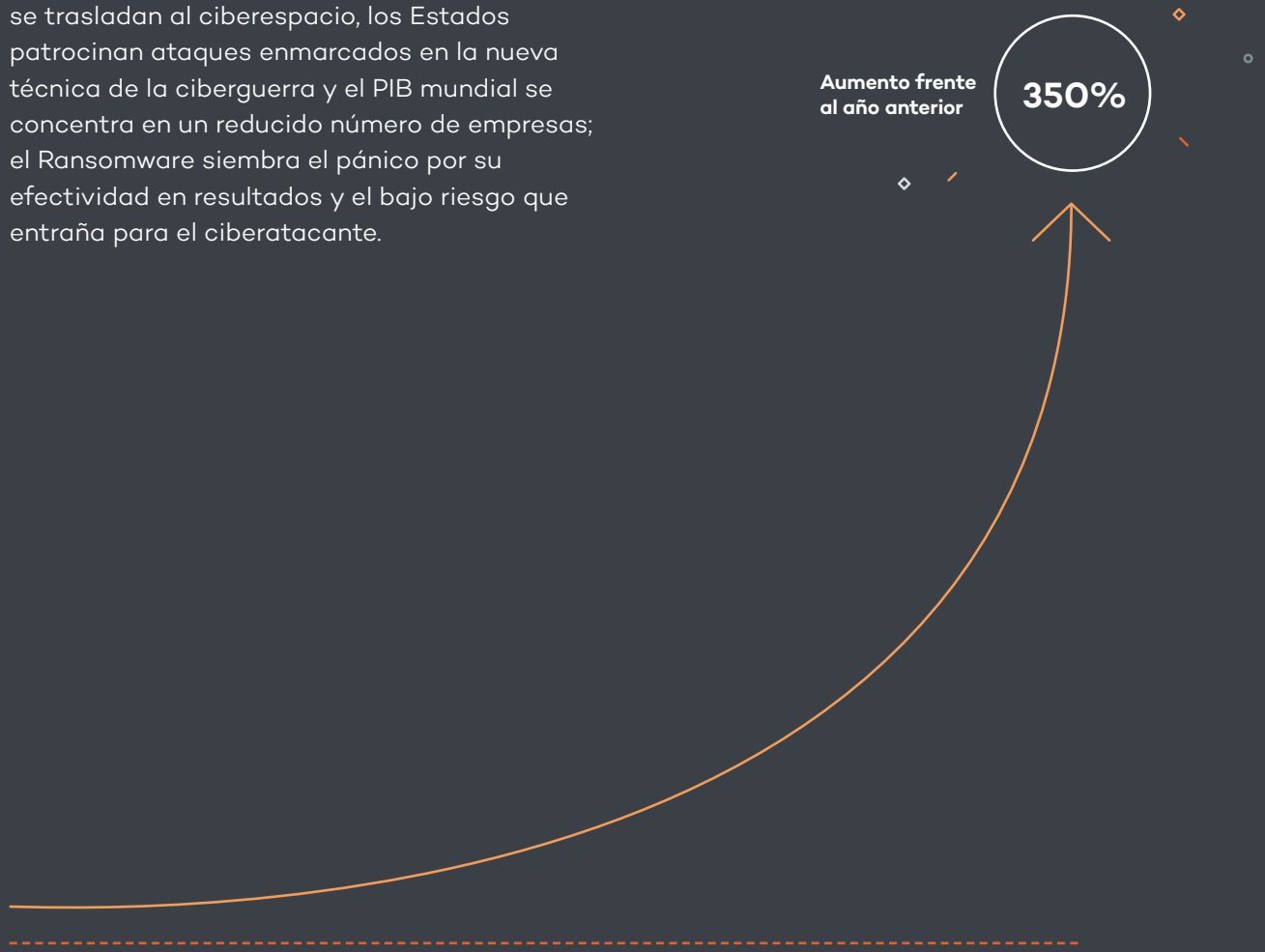
1. Introducción

El Ransomware sigue siendo una de las armas más lucrativas que tienen los cibercriminales. Esta modalidad de cibercrimen encripta archivos de los ordenadores y los bloquea hasta que se recibe el rescate requerido, generalmente en forma de bitcoin, una **criptomoneda virtual** ilocalizable.

Durante el 2017, este troyano provocó costes en torno a los **cinco mil millones de dólares**, lo que lo ha convertido en el tipo de ciberataque con más impacto y sofisticación, con un **aumento de 350% frente al año anterior**.

En un momento en el que los hábitos de vida se trasladan al ciberespacio, los Estados patrocinan ataques enmarcados en la nueva técnica de la ciberguerra y el PIB mundial se concentra en un reducido número de empresas; el Ransomware siembra el pánico por su efectividad en resultados y el bajo riesgo que entraña para el ciberatacante.

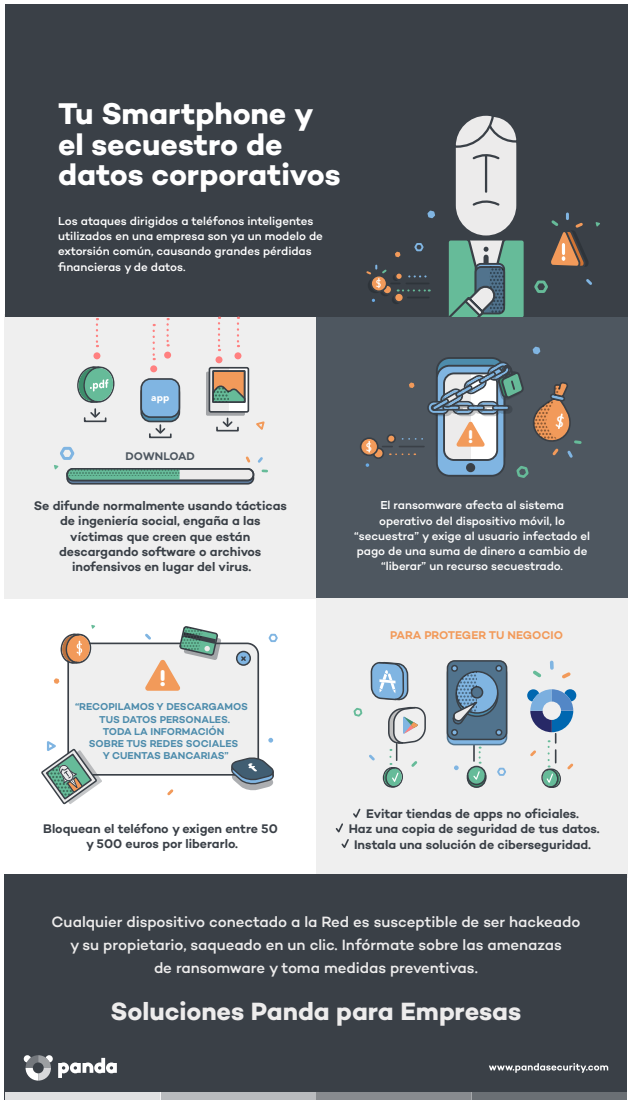




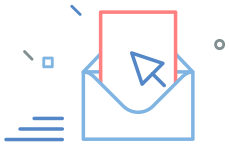
2. El paradigma de la transformación digital

Con más de 285.000 nuevas amenazas detectadas al día por PandaLabs, la denominada transformación digital implica nuevos e importantes retos. La ciberdelincuencia está hoy más activa que nunca. Los ataques informáticos y el fraude económico a través de la tecnología alcanzan un grado de sofisticación hasta ahora inimaginable en un medio que facilita el anonimato y que se aprovecha de la "ingeniería social", las redes donde la barrera de la confianza elimina muchas cautelas habituales y deja al descubierto nuestra intimidad.

Y en estos nuevos hábitos, adquirimos también nuevas plataformas como **Android**, el sistema operativo más utilizado en el mundo y que lo convierte en el principal vector de ataque para infección y propagación de **Ransomware** como Charger, capaz de secuestrar los datos de cualquier Smartphone.



En la misma línea, se espera que para 2020 haya un total de 50.000 millones de dispositivos conectados a Internet, generando 40 trillones de GB cada 10 minutos. En el **Internet de las Cosas (IoT)** la seguridad se convierte en un aspecto crítico. Tener acceso a un mayor número de dispositivos conectados en nuestra mano permite a los hackers usar nuevos métodos; ¿infectar a otros para librarte de pagar el rescate? Es el morboso método de propagación de Popcorn Time.

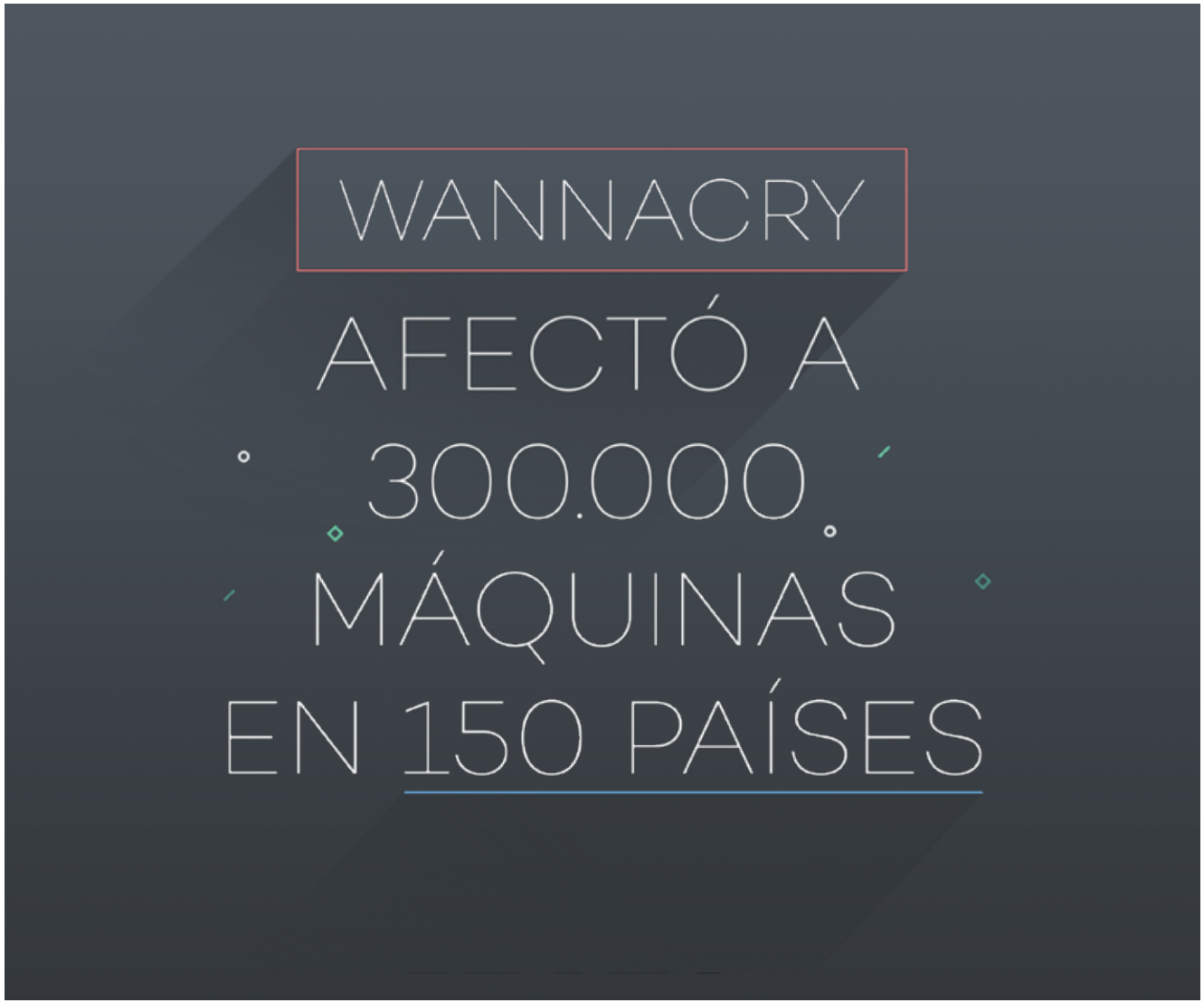


Esta proliferación de dispositivos móviles da pie a nuevas técnicas de ataque emprendidas por los hackers, realizadas en espacios de tecnología avanzada como sucedió en un hotel en Austria que, tras ser atacado por ciberdelincuentes, éstos bloquearon las puertas de las habitaciones e inutilizaron el software de programación de las tarjetas de entrada a las habitaciones.

3. Ataques patrocinados por Estados

Hay sospechas de que detrás de los 2 grandes ataques de la historia (WannaCry y Goldeneye/NotPetya) podría haber gobiernos (Corea del Norte en el caso del WannaCry y Rusia en el de Goldeneye/NotPetya). Ambos ataques son de ransomware y tienen gran capacidad de replicarse, como pudimos comprobar con el caso de Bad Rabbit, que muestra muchas similitudes con el Ransomware Notpetya.

Al ser un Ransomware con funcionalidad de gusano de red, el ordenador infectado por WannaCry acababa con sus documentos secuestrados, además de que esto contribuyó a una rápida expansión por más de **300.000 ordenadores aprovechándose de una antigua vulnerabilidad de Microsoft Windows** para infectar y propagarse hasta el núcleo de organizaciones y negocios.



4.Empresas, en el punto de mira

El Ransomware es un mal que afecta a cada vez un mayor número de compañías, y que solo sale a relucir cuando alguna de estas piezas se viraliza, como ocurrió el año pasado con WannaCry.

Hoy en día, el 18% de la capitalización bursátil de las empresas cotizadas de Estados unidos, es la suma de 5 empresas: Apple, Google, Amazon, Microsoft y Facebook.

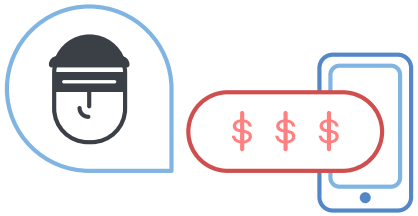
Teniendo en cuenta que el fin del Ransomware es el lucro económico y que apropiarse de esta riqueza no puede hacerse con medios físicos, pero sí hay medios para conseguir la transferencia de esa riqueza de unas manos a otras a través de nuevas armas, los delincuentes no dudan en usar sus artimañas para hacerse con ella a través de:

Ciber-robo

- El ciber-robo, como del que fue víctima Equifax, protagonizando la mayor pérdida de datos personales sensibles de la historia y que pudo llevarse a cabo por una vulnerabilidad explotada previamente por Ransomware, abriendo la puerta a los ciberatacantes.

Extorsión

- La Extorsión, como práctica para obtener algo, especialmente dinero, a través de la fuerza o de amenazas. Tenemos tres claros ejemplos, los ciberataques de WannaCry, NotPetya o BadRabbit.



Sabotaje

- O el Sabotaje de instalaciones civiles o militares. Por ejemplo en agosto de 2012, con la infección por parte de Shamoon de más de 30.000 puestos de la empresa estatal de petróleo y gas de Arabia Saudita llamada Aramco, paralizaron su actividad de exportación durante 2 semanas. El mismo software se utilizó años después para llevar a cabo unos ciberataques incluyendo un nuevo módulo que sí contenía Ransomware.

Además de los mencionados delitos, en los últimos meses hemos visto distintas tipologías para insertar Ransomware en las redes corporativas, como el uso y el abuso de herramientas legítimas de Windows como PowerShell, para infectar equipos con **Cerber**. Ese mismo fue el objetivo de **Crysis/Dharma**, un caso en el que el servidor ejecutaba el Protocolo de Escritorio Remoto (RDP) y los atacantes empleaban un ataque de fuerza bruta hasta adivinar las credenciales y tomar el acceso remoto. La tendencia de instalar malware a través del RDP llega a un punto de sofisticación tal que el propio Ransomware posee una interfaz propia y que permite al delincuente seleccionar las carpetas cuyo contenido se cifrará, los ordenadores de la red, auto- borrado, la dirección de email a la que deben dirigirse las víctimas,etc; como vimos con el Ransomware **WYSIWYE**, descubierto por PandaLabs.

También hay familias de Ransomware que añaden funcionalidades para ser más dañinos; trucos como trabajar sin conexión o distribuirse más rápidamente son los implementados por el temido **Locky**.

Con estos datos, cada vez parece más lógico pensar que las potenciales víctimas deberían contar con **pólizas de seguro** que puedan cubrir, al menos en parte, el coste de uno de estos ciberataques. Se trata de un sector en pleno desarrollo y, de hecho, la mayoría de los ciberseguros para paliar el Ransomware se contratan prácticamente a medida, analizando antes los principales riesgos a los que se enfrenta una empresa.

5. El Precio de los Ataques

Hemos visto como la democratización de los ciberataques ha sido facilitada por variables como la profesionalización de los atacantes, la evolución tecnológica, o la facilidad de acceso a los datos.

		Desde	Hasta
Herramienta de Ataque	Malware	$50	$200
	Ransomware	$1	$400
	Software	$100	$700
	Pagos y Log-ins	$1	$25
Datos	Información Personal	$3	$150
	Registros de BBDD	$25	
Servicios	Hacking	$100	$300
	Usuarios	$20	$150
	Malware	$1	$25
	Spam	$20	$400
	Documentos Falsos	$15	$25

Fuente: Recorded Future.

Aunque algo que, sin duda, ha ayudado a popularizar este tipo de amenazas, es la rentabilidad que suponen sus acciones. Ciber-armas que se venden a precios muy económicos, y con las que el atacante puede conseguir una suculenta recompensa.

Asegurarse de que las cuentas de usuario de los empleados utilizan contraseñas robustas y sin permisos de Administrados.

No abrir correos de usuarios desconocidos o que lo haya solicitado: mejor eliminarlos directamente y no contestarlos en ningún caso.

Desconfiar de los enlaces acortados y ficheros adjuntos, aunque sean de contactos conocidos.

Crear copias de seguridad regulares que eviten la pérdida de datos.

Los ataques de Ransomware están en auge, y así seguirán mientras las víctimas sigan pagando los rescates. Aunque siempre podemos tomar medidas concretas para evitar estos ataques:

Planificar y ejecutar un plan de auditoría (llevado a cabo por equipos internos de auditoría o terceros especializados), tanto de los sistemas como de las políticas de la organización, de manera que podamos detectar posibles vulnerabilidades.

Emplear recursos para mejorar la formación y concienciación del personal en materia de seguridad informática y en particular de este tipo de amenazas.

La importancia de la seguridad multicapa: ante amenazas actuales como el ransomware, una protección básica no es suficiente. Para asegurar la máxima protección es recomendable utilizar herramientas multiplataforma complejas y robustas como [Panda Adaptive Defense 360](#).

Panda Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

Más información en:

pandasecurity.com/business/adaptive-defense/

Hablemos:

900 90 70 80

panda