

Versión Actualizada
Noviembre 2018

El ciberexpolio **hotelero**



El ciberexpolio hotelero

Si algo podemos asegurar, después de tantos años analizando ciberataques, es que la principal motivación de los delincuentes es el dinero.

De ahí que la mayoría de las amenazas que se engendran sean troyanos, que su número no deje de aumentar, y que el robo de información se haya convertido en su objetivo.

Es por eso que **durante los dos últimos años se han popularizado tanto los ataques tipo Cryptolocker**, que utilizan ransomware para cifrar la información y obligar a la víctima a pagar un rescate para poder recuperarla.

También hemos sido testigos de cómo las empresas se ven obligadas a enfrentarse a nuevos tipos de ataques. Teniendo que lidiar con el malware “clásico” y, además, con amenazas avanzadas pensadas y diseñadas específicamente para cada víctima.

¿Por qué hoteles?

Cuando un ciberdelincuente piensa en un hotel, piensa en una empresa con un volumen de negocio muy suculento.

Una empresa que cuenta con millones de habitaciones, que son utilizadas por millones de clientes. Que genera negocio por sí misma pero que, a su vez, ofrece una tajada extra: **las tarjetas de crédito de todos sus clientes.**

Cada vez que un cliente pernocta debe utilizar su tarjeta de crédito, si no es para pagar su habitación, es como garantía de depósito de los gastos que pueda generar durante su estancia.

Muchas cadenas cuentan además con tiendas, restaurantes y otros servicios que aceptan a su vez el pago con tarjetas de crédito, lo que convierte cada uno de sus hoteles en una red compleja con múltiples puntos débiles susceptibles de ser comprometidos.

Un sector que factura billones de dólares, que gestiona el descanso de millones de huéspedes cada día, y que almacena una cantidad ingente de datos muy sensibles y comprometedores.

Un sector, el hotelero, que se ha convertido en blanco muy suculento.



Un historial comprometido

Ya en los últimos meses de 2017 hablábamos de que **los hoteles españoles sufrían a diario numerosos intentos de ataque** y que muchos de ellos no eran conscientes ni de estos peligros, ni de la importancia de contar con una tecnología y sistemas necesarios para detectar estas amenazas.

Que la ciberseguridad debe incluirse en la agenda de cualquier establecimiento y cadena hotelera es un mantra que ha cobrado fuerza a partir del mes de mayo, con la **aplicación de la normativa europea de protección de datos GDPR**.

Porque al margen de la posible multa, la consecuencia más inmediata de una brecha de seguridad (que pasa a tener que ser reportada en 72h) es una caída de las ventas, y por supuesto un grave daño a la imagen de la marca.

Y es que los ataques informáticos al sector turístico en 2018 han seguido la estela del pasado año, con un **crecimiento exponencial que lo sitúa como uno de los principales objetivos a día de hoy de los hackers**. De hecho este año 2018 se ha posicionado en el ranking de las industrias más ciberatacadas, junto al sector sanitarios, el educativo y el energético; precisamente por contener grandes cantidades del principal activo para los ciberdelincuentes a día de hoy: **los datos**.

Hoteles, agencias de viaje y prácticamente cualquier negocio que se desarrolla en el sector turístico dispone de grandes bases de datos sensibles de usuarios y clientes que necesitan ser auditadas para no llegar a sufrir el peor escenario posible para una empresa: **la fuga de información**. Para evitarlas, las estrategias que combinan prevención, planificación, sensibilización y concienciación siguen siendo las más eficientes.



White Lodging

Un buen ejemplo es el de White Lodging, una empresa que ofrece servicios a diferentes hoteles (Hilton, Marriott, Hyatt, Sheraton, Westin,...).

Fue víctima de un ataque en 2013, aunque no se hizo público hasta un año después. **En este asalto fueron comprometidas tarjetas de crédito y débito de los clientes que utilizaron algunos de los servicios de White Lodging en al menos 14 hoteles.**

En 2015, esta misma empresa volvió a sufrir un nuevo ataque que afectó a 10 hoteles, algunos de los cuales, eran los mismos que en el ataque anterior. De nuevo, volvieron a robar los datos de las tarjetas de crédito, incluyendo el nombre completo del cliente, su número de tarjeta, el código de seguridad y la fecha de caducidad. White Lodging dijo que se trataba de un ataque diferente.



24 hoteles afectados

Mandarin Oriental

La famosa cadena de hoteles de lujo, fue víctima de un ataque en marzo de 2015.

En esta ocasión **un malware infectó los terminales de punto de venta** de algunos hoteles del grupo en Europa y América.

Un malware especialmente diseñado y dirigido al sistema de estas máquinas que le permitía robar la información de las tarjetas de crédito según iban siendo utilizadas.




Miles de tarjetas de crédito comprometidas

Trump Hotels

También fue víctima de un ataque en siete de sus establecimientos.

Tal y como ellos mismos reconocieron, entre mayo de 2014 y junio de 2015 **fueron infectados ordenadores y terminales de punto de venta de sus restaurantes, sus tiendas de regalos, y demás comercios**. Los atacantes se hicieron con los datos de las tarjetas de crédito usadas por sus clientes.

 **Decenas de ordenadores y TPVs infectados**

Hard Rock Las Vegas

Vio comprometidos los terminales de punto de venta de sus restaurantes, bares y tiendas, pero no los pertenecientes al propio hotel o a su casino.

Durante 7 meses, desde el 13 de septiembre de 2014 al 2 abril de 2015, **los delincuentes accedieron a un total de 173.000 tarjetas de crédito diferentes** que fueron utilizadas en ese periodo.

Pero no ha sido este el único hotel/casino afectado por estos ataques. FireKeepers Casino Hotel de Battle Creek, es otra de las víctimas conocidas durante 2015.

 **173.000 tarjetas de crédito robadas**

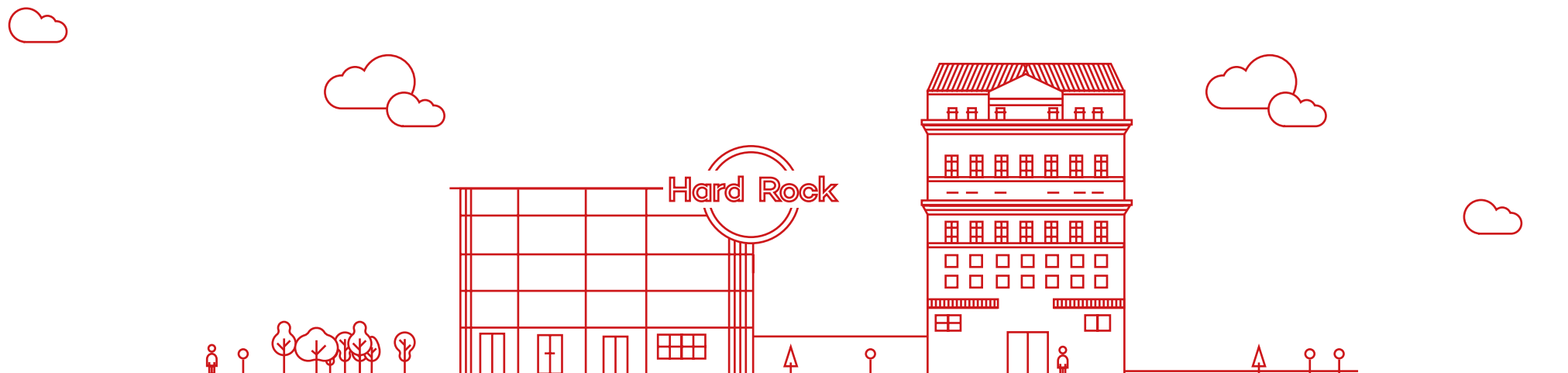
Hilton Worldwide

En noviembre de 2015 publicó una nota de prensa reconociendo que habían sido atacados.

No especificaron el número de establecimientos afectados pero declararon que, **entre la información robada de los terminales de punto de venta, se encontraban los números de tarjeta de crédito, el nombre completo, la fecha de caducidad y los códigos de seguridad**.

Por suerte, los códigos PIN y otro tipo de información personal, permanecieron a salvo.

 **Acceso a información confidencial**



Starwood

También en noviembre de 2015, la cadena hotelera Starwood anunció haber sido víctima de un ataque.

A través de un malware que infectó sus terminales de punto de venta, habían robado información de tarjetas de crédito de varios clientes en 54 de sus hoteles.

La cadena hizo público un documento con el listado de hoteles afectados que ha ido actualizando, la cifra asciende ya a un total de 105 hoteles (Sheraton, St. Regis, Westin, W, entre otros). **El caso Starwood se convirtió en el mayor ataque contra el sector hotelero, hasta el momento.**

 **105 hoteles afectados**

Hyatt

El récord de Starwood fue bastante efímero. Pocos días antes de finalizar 2015, la cadena hotelera Hyatt confirmaba que había sufrido un ataque mediante una nota de prensa.

Entre julio y septiembre de 2015, sus terminales de punto de venta -una vez más- habían sido infectados para poder robar los datos de las tarjetas de crédito de sus clientes.

En total, **se vieron afectados 249 hoteles repartidos en 54 países**, convirtiéndose así en el mayor ataque de la historia al que se ha enfrentado una cadena hotelera.

 **249 hoteles afectados**

Rosen Hotels & Resorts

La última víctima, por el momento, se trata de la cadena Rosen Hotels & Resorts.

Aunque no se han dado cifras sobre el robo, sí han confirmado que **sus terminales de punto de venta han estado infectados con malware desde septiembre de 2014 hasta febrero de 2016.**

El malware ha tenido acceso a la información de las tarjetas de crédito utilizadas por clientes en sus establecimientos a lo largo del casi año y medio en el que han estado infectados sin saberlo.

 **1,5 años infectados sin percatarse**

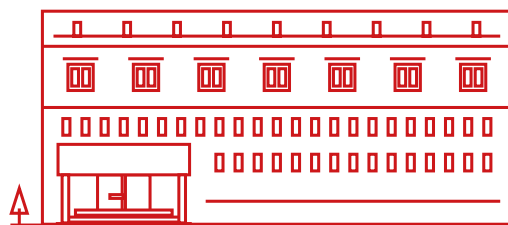


Sabre Holdings

Este [caso](#) es el más grave ocurrido en los últimos tiempos. Sabre, uno de los principales proveedores de soluciones tecnológicas para la industria de los viajes, cuenta con un sistema a través del cual da servicio a más de 32.000 hoteles y establecimientos de alojamiento. El sistema estuvo comprometido desde el 10 de agosto de 2016 al 9 de marzo de 2017. Un total de 7 meses en el que afectó a las tres líneas de negocio del grupo, comprendiendo agencia de viajes, alquiler de coches y operadores turísticos, entre otros.

De este incidente se han derivado diferentes noticias de ataques a hoteles, aunque en esta ocasión no habían atacado los sistemas de los hoteles, sino que se han visto afectados por el ataque a Sabre. Cadenas hoteleras afectadas por este ataque que se han registrado: Four Season Hotels & Resorts, Trump Hotels, Kimpton Hotels & Restaurants, Red Lion Hotels Corporation, Hard Rock Hotels y Loews Hotels.

 **32.0000 hoteles afectados**

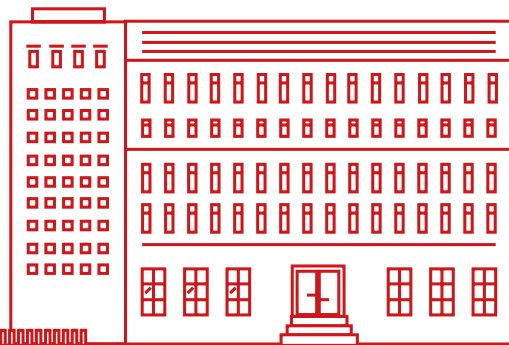


IGH (Intercontinental Hotels Group)

Otro ataque de envergadura al sector se produjo en diciembre de 2016, siendo el grupo IGH su víctima. [Este caso](#), no relacionado con el Sabre, puso a las tarjetas de crédito de los consumidores en su diana. El ciberataque consistió en la instalación de malware en TPV's de más de 1.000 de los establecimientos del Grupo en todo el mundo.

El experto periodista [Brian Krebs](#), a raíz del el último informe anual de Investigación de Violaciones de Datos (DBIR por sus siglas en inglés) de Verizon, afirma que los ataques de programas maliciosos en terminales de punto de venta utilizados en la recepción y restaurantes de los hoteles están “absolutamente disparados” en el sector servicios. Los alojamientos fueron la principal industria con intrusiones en los puntos de venta según los datos de este año, con un 87% de infracciones dentro de ese patrón.

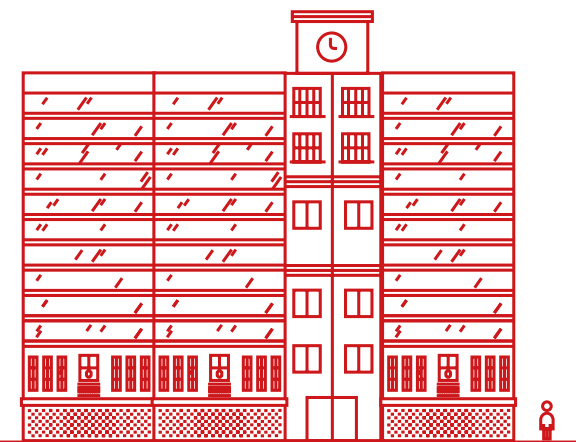
 **Malware en TPV's de más de 1.000 establecimientos**



Romantik Seehotel Jaegerwirt

En [el mes de enero](#), los huéspedes de este lujoso establecimiento de Austria se quedaron “secuestrados” fuera de la habitación por un ataque de ransomware que afectó el sistema de llaves electrónicas, impidiendo el acceso a la estancia.

 **Habitaciones secuestradas por ransomware**



Principales ataques 2018:

Orbitz:

La plataforma digital de reserva de viajes Orbitz, subsidiaria de Expedia, anunció en el mes de marzo que había sufrido un robo de datos que podría haber afectado a **880.000 tarjetas de crédito de usuarios** que hicieron compras en algunas de sus páginas web entre 2016 y 2017. De acuerdo con la empresa de viajes, la web actual no tiene nada que ver en el incidente y las afectadas fueron su plataforma para consumidores, entre enero y mitad de junio de 2016, y su plataforma para socios, entre enero de 2016 y mitad de diciembre de 2017. La información a la que supuestamente había accedido el ciberdelincuente abarcaba nombres completos, direcciones, fechas de cumpleaños, género, números de teléfono y datos de la tarjeta de crédito.

!  **880.000 tarjetas de crédito de usuarios Afectadas**

FastBooking:

Cientos de hoteles se vieron afectados por la filtración de datos del proveedor de software de reservas hoteleras. Los datos personales y los datos de las tarjetas de pago de los huéspedes de cientos de hoteles fueron robados en el mes de junio por un atacante desconocido.

Los datos fueron tomados de FastBooking, una empresa con sede en París que vende software de reservas hoteleras a más de 4.000 hoteles en 100 países, como afirma en su sitio web. El atacante utilizó una vulnerabilidad en una aplicación alojada en su servidor para instalar una herramienta maliciosa (malware). Esta herramienta permitía al intruso el acceso remoto al servidor, que utilizaba para extraer los datos. El incidente salió a la luz cuando los empleados de FastBooking descubrieron esta herramienta maliciosa en su servidor.

!  **Cientos de hoteles Afectados**

Huazhu Hotels Group Ltd:

Una de las cadenas hoteleras más grandes de China sufrió una violación masiva de datos que afectó a **130 millones de personas**. La víctima fue la cadena hotelera Huazhu Hotels Group Ltd, que opera 13 marcas de hoteles, incluyendo Hanting Inns and Hotels, Hi Inn y Starway Hotel. La empresa gestiona 5.162 hoteles en 1.119 ciudades chinas.

Entre la información comprometida se encontraban en el número de teléfono, la dirección de correo electrónico y número de tarjeta de identificación china; incluyendo direcciones postales y cumpleaños; e información de reserva, incluyendo hora de registro, hora de salida y número de habitación. El vendedor solicitó 8 bitcoin (alrededor de 57.000 dólares) para todo el conjunto de datos. Los investigadores lo han atribuido a que Huazhu ha subido copias de su base de datos a una cuenta de GitHub.

!  **130 Millones de personas Afectadas**

Marriott international:

[Los registros de hasta 500 millones](#) de clientes del grupo hotelero Marriott International pueden haberse visto implicados en una brecha de datos. De hecho, ha sido considerada la segunda brecha de datos más grande de la historia.

La cadena de hoteles ha dicho que la base de datos de su división de Starwood ha sido comprometida por un tercero no autorizado, y que el atacante ha podido acceder a los datos de clientes registrados en su red desde 2014.

La empresa va a notificar a los clientes cuyos datos están en la base de datos, y que ya ha notificado a las autoridades relevantes.

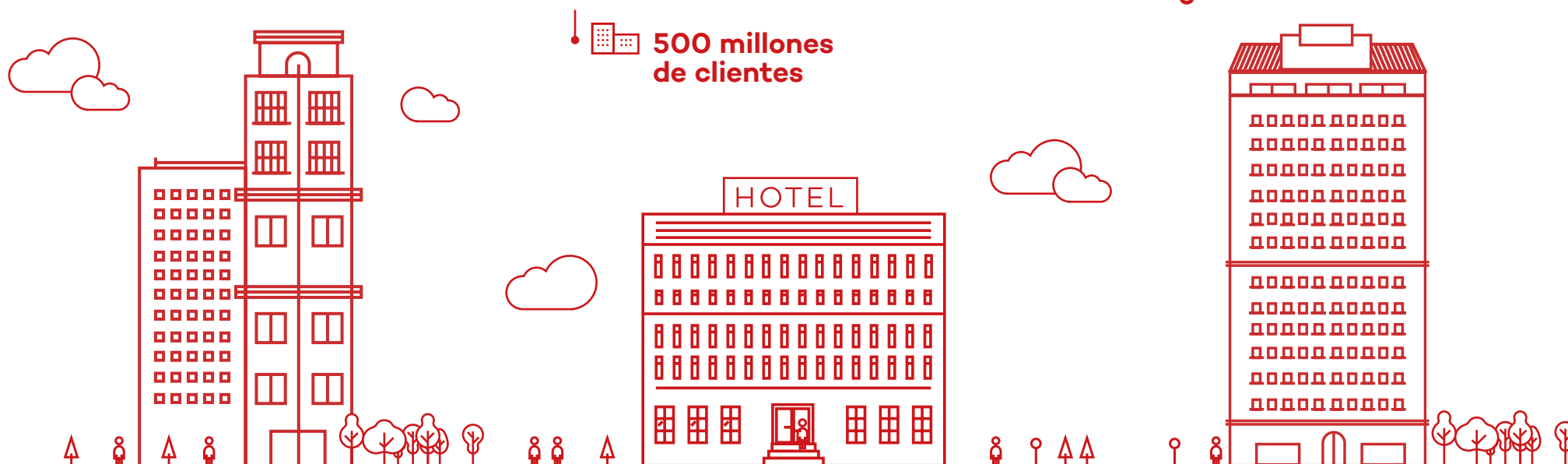
Según Marriott la empresa recibió una alerta de una herramienta interna, y tras una investigación descubrió que “un tercero no autorizado había copiado y cifrado información”.

Para alrededor de 327 millones de huéspedes, la información incluía “una combinación” de su nombre, dirección física, número de teléfono,

email, número de pasaporte, información de cuenta, fecha de nacimiento, género, e información de llegada y salida.

Ha confirmado también que algunos registros incluían información de tarjetas de pago cifrada, pero que no podía descartar la posibilidad de que se hubieran robado las claves de cifrado también.

↓  **2ª Brecha de datos más grande de la historia**



No es una moda pasajera

Queda claro que los ataques sufridos por este sector no son algo casual o pasajero, sino que hay detrás un verdadero interés económico y un interés en pasar desapercibido.

El sector hotelero se ha convertido en un objetivo capital de bandas organizadas de ciberdelincuentes con malware específicamente diseñado para robar información de las tarjetas utilizadas en los terminales de punto de venta.

Indudablemente se trata de una situación preocupante que, además del importante impacto económico, causa un gran daño a la imagen de todo el sector y siembra el miedo entre sus clientes.

El principal motivo por el que los hoteles son tan vulnerables ante los robos de datos es la recepción y transmisión de los datos de tarjetas de los clientes a través de medios como email, teléfono, fax, website, etc. El almacenamiento de todos estos datos en múltiples plataformas hace que garantizar la seguridad de los datos de los clientes sea una tarea muy difícil para un hotel. A esta situación, hay que sumarle la entrada en vigor del nuevo Reglamento General de Protección de Datos (GDPR) que exige a las empresas a cumplir con la nueva Directiva de protección de datos de la UE a finales del primer

trimestre de 2018. Ahora las empresas deberán hacer públicas las violaciones de seguridad que sufran y notificarlo en un plazo de 72 horas, lo que hará crecer el presupuesto destinado a la seguridad de redes en las corporaciones ante la obligatoriedad de informar sobre estos incidentes, así como el número de casos ante la obligatoriedad de reportar estas brechas, como ya sucede en Estados Unidos.

Hay que estar alerta

Malware que infecta terminales de venta para robar los datos de las tarjetas de crédito, ataques dirigidos contra los sistemas de gestión de las cadenas hoteleras para obtener su información más confidencial, la vulnerabilidad creciente de los empresarios y sus clientes y el daño reputacional, son realidades tangibles a las que se enfrentan las cadenas hoteleras diariamente.

Tomar medidas al respecto ya no es una opción. **Los hoteles se han visto obligados a reforzar la seguridad de sus redes, dispositivos y sistemas** para evitar ser víctimas de este tipo de amenazas.

Pero tampoco vale cualquier sistema de protección porque no todos ofrecen el mismo nivel de seguridad, ni todos son válidos para cualquier ecosistema o tejido empresarial.



La Solución

Una protección contra amenazas avanzadas y ataques dirigidos, e incluso, que sea capaz de detectar comportamientos extraños. Un sistema que pueda asegurar la confidencialidad de los datos, la privacidad de la información, el patrimonio y reputación empresarial.

Esto es Adaptive Defense 360, **el único sistema de ciberseguridad avanzado que combina protección de próxima generación y la última tecnología de detección y remediación con la capacidad de clasificar todos los procesos en ejecución.**

Adaptive Defense 360 clasifica absolutamente todos los procesos activos en todos los endpoint, garantizando la protección contra el malware conocido y contra amenazas avanzadas del tipo Zero-Day, Advanced Persistent Threats y Ataques Dirigidos.

Gracias a la clasificación del 100% de los procesos en ejecución, es capaz de detectar malware y comportamientos extraños o no comunes de los que el resto de sistemas de protección del mercado no se percatan.

Como sabemos exactamente todo lo que pasa con cada uno de los procesos y de los archivos, podemos realizar un estudio pormenorizado del flujo de la información y representar gráficamente todo el progreso desde cómo ha intentado entrar el malware, por dónde, desde dónde viene, qué pretendía hacer o quién y cómo intenta llevarse información.


Averigua quién y cómo accede a tus datos y controla la fuga de información, la que intente realizar un malware o la que realicen tus empleados.

Descubre y soluciona las vulnerabilidades de los sistemas y de los programas instalados y previene la utilización de los no deseables (barras de navegación, adwares, add-ons,...).

Adaptive Defense 360: visibilidad sin límites, control absoluto.

Más info:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/


 Adaptive Defense 360


“Adaptive Defense 360 me da la seguridad de saber que ni nosotros, ni ninguno de nuestros huéspedes seremos víctimas de un ataque dirigido contra nuestra seguridad, privacidad o datos sensibles como tarjetas de crédito.

Además, desde su rápida puesta en marcha, no ha ocasionado ningún inconveniente en el servicio que ofrecemos. Nuestro servicio debe ser óptimo, inmediato e ininterrumpido, y no nos podemos permitir ningún tipo de problema operacional. Adaptive Defense 360 y su servicio gestionado de seguridad, nos permite mantener el máximo nivel de atención y seguridad.”


**Gran Hotel Domine
Bilbao**


Contacta con nosotros para más información


 **ARGENTINA**
+54 11 6632 6632
argentina@pandasecurity.com


 **COSTA RICA**
+506 2523-4300
ventas@cr.pandasecurity.com

 **PANAMÁ**
+507 833 7263
ventas.panama@pandasecurity.com


 **BOLIVIA**
+59 12 21 20 300
bolivia@pandasecurity.com

 **ECUADOR**
+593 02 6012384
ecuador@pandasecurity.com

 **PARAGUAY**
+595 21 6075 94
paraguay@pandasecurity.com


 **BRASIL**
+55 11 3054-1722
brazil@pandasecurity.com

 **EL SALVADOR**
+503 22087435
ventas.elsalvador@pandasecurity.com


 **PERÚ**
+51 1 204 55 00
peru@pandasecurity.com

 **CHILE**
+56 2 6394774
chile@pandasecurity.com

 **GUATEMALA**
+502 66400100
ventas.guatemala@pandasecurity.com

 **URUGUAY**
+598 2 402 0673
ventas@uy.pandasecurity.com

 **COLOMBIA**
+57 1 2560344
colombia@pandasecurity.com

 **MÉXICO**
+52 55 8000 2381
mexico@pandasecurity.com

 **VENEZUELA**
+58 212-7612535
venezuela@pandasecurity.com



© Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

Más información en:

pandasecurity.com/enterprise/solutions/adaptive-defense-360/

Contacta:

900 90 70 80



Para más información contacta con tu

Distribuidor habitual

