El ciberexpolio **hotelero**

pandasecurity.com

panda

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?

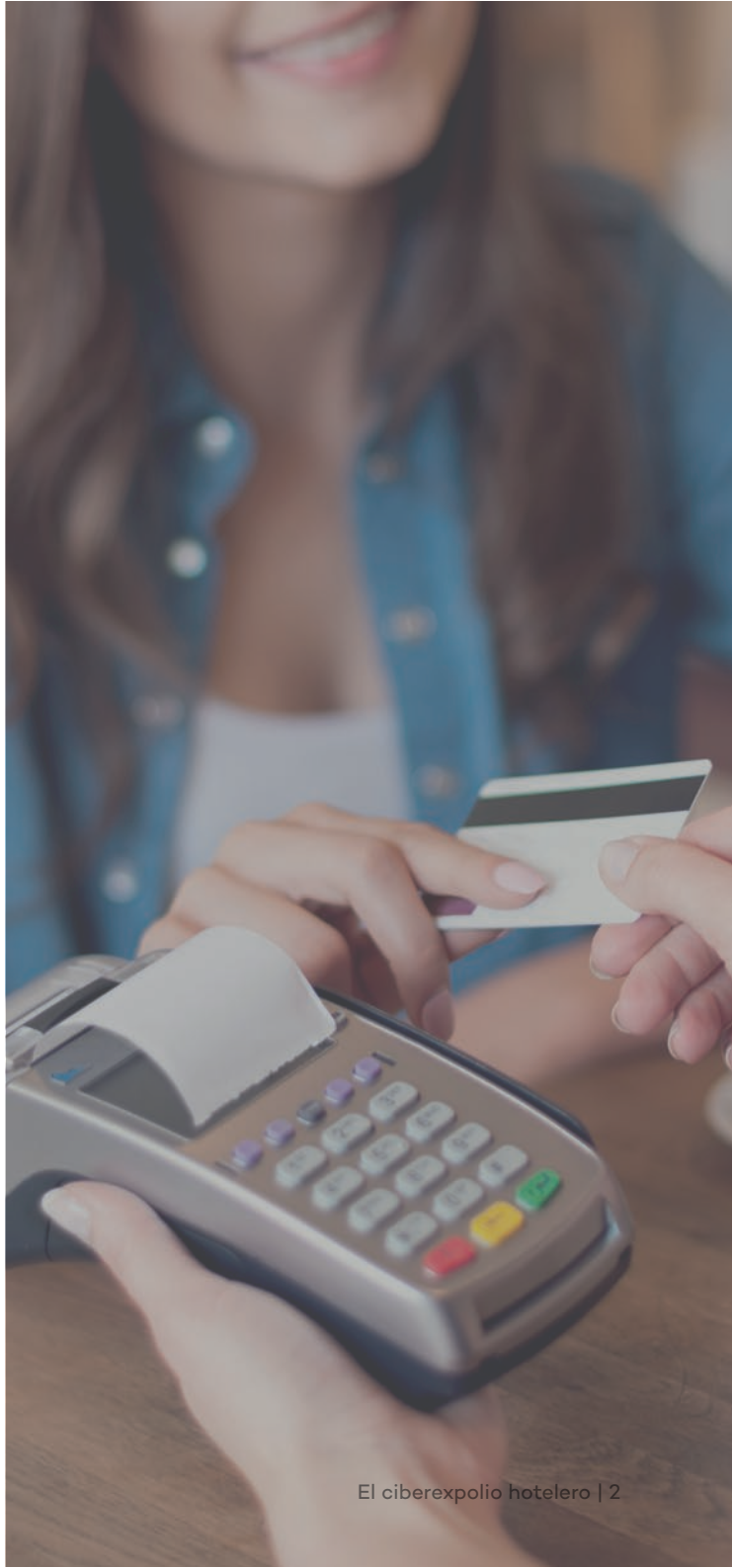
Cuando un ciberdelincuente piensa en un hotel, piensa en una empresa con un volumen de negocio muy suculento.

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

2015 ha marcado, sin duda, un antes y un después en este sector.

Al menos, en lo que se refiere a intrusiones y robo de información de sus clientes. Todas las compañías, sin importar su tamaño, **han sido objetivo de diferentes bandas de ciberdelincuentes**.

Aunque no sólo estas compañías están en peligro, ya que aquellas que ofrecen servicios a este tipo de negocio, también pasan a formar parte de sus objetivos.

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

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.

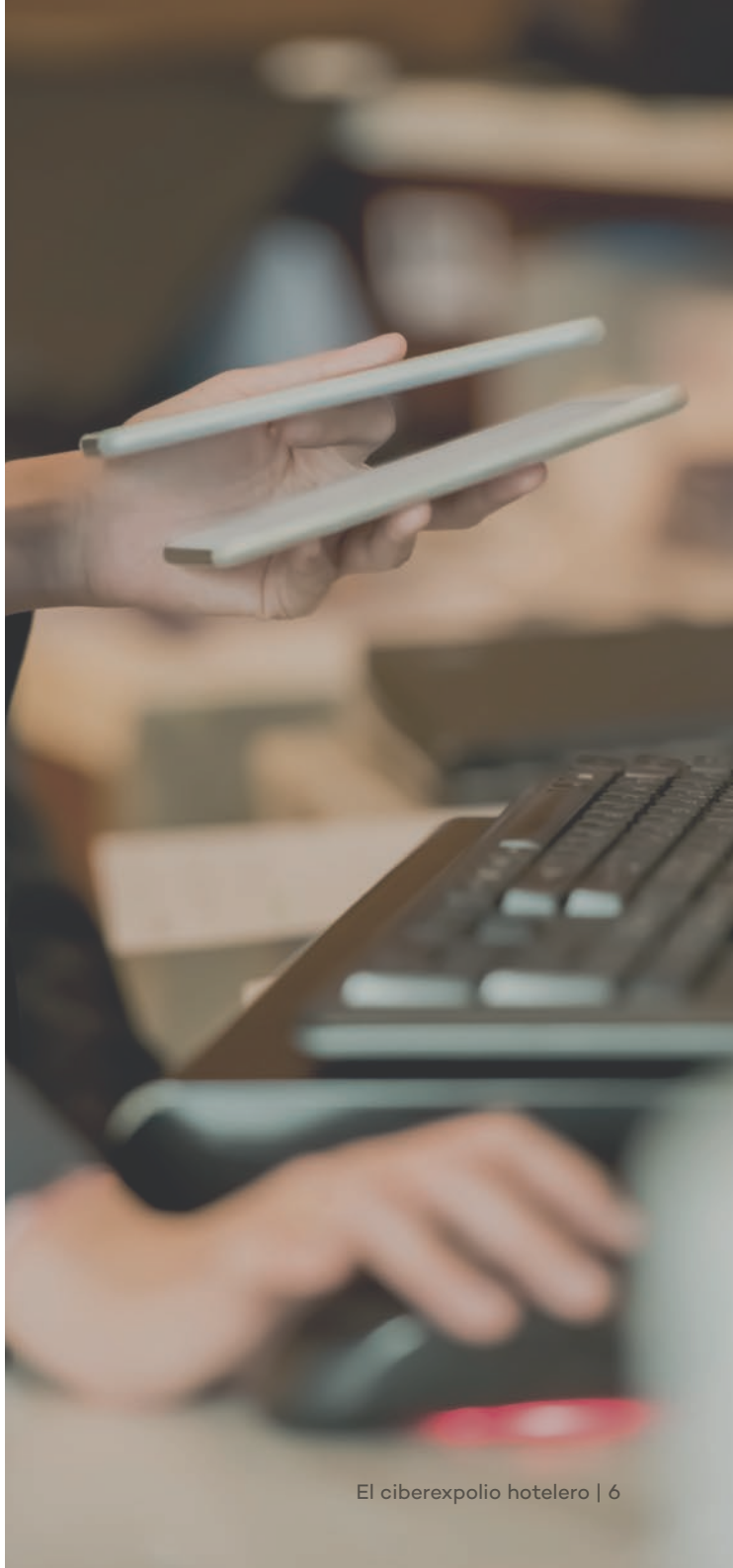
Indudablemente se trata de una situación preocupante que, además del importante impacto económico, causa un gran daño a la imagen de todo el sector y siembra el miedo entre sus clientes.

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.

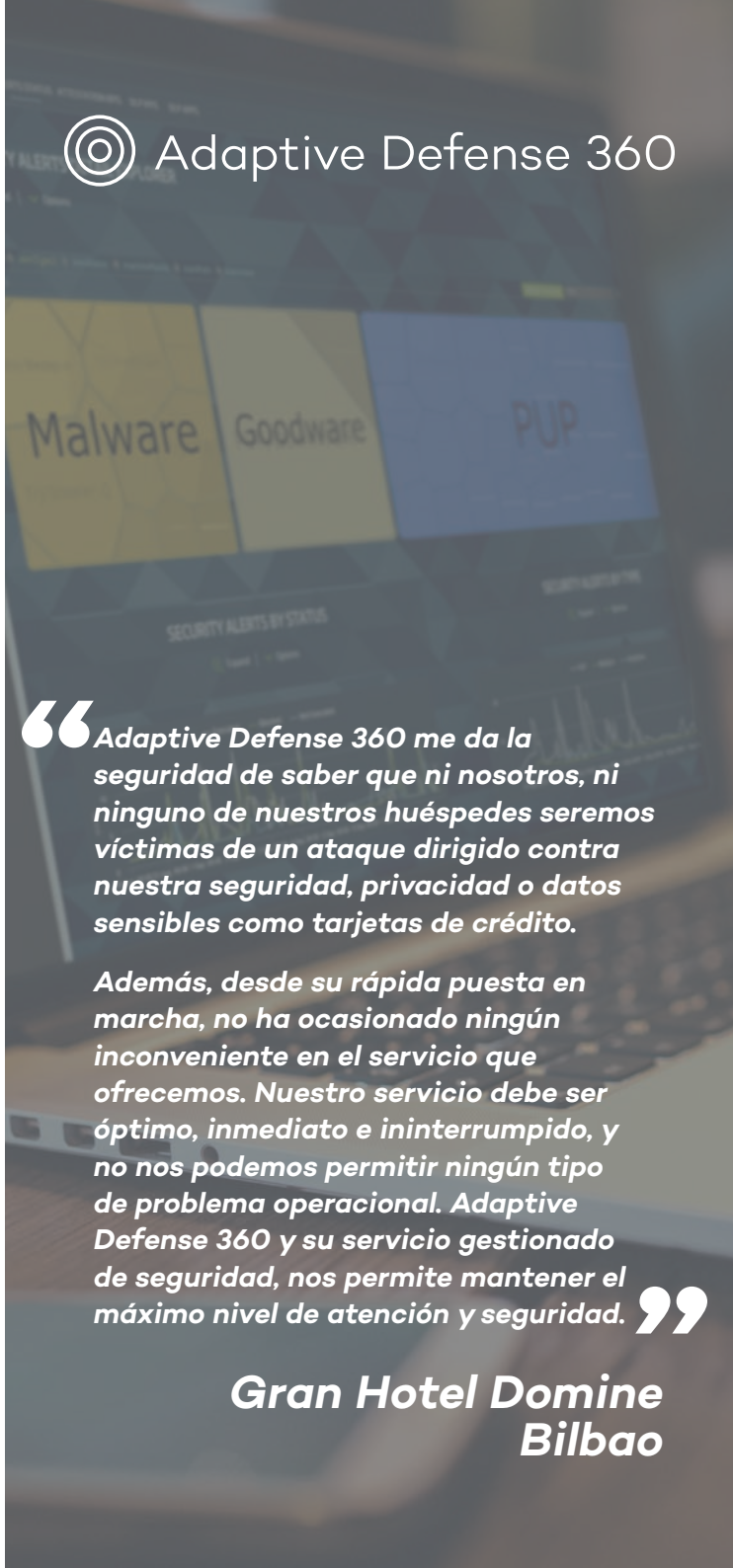
Averigua quién y cómo accede a tus datos y controla la fuga de información, la que intente realizar un malware o la que realicen tus empleados.

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 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

panda

Más información en:

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

Contacta:

900 90 70 80

panda

Adaptive Defense 360

Visibilidad sin Límites, Control Absoluto

pandasecurity.com

panda