HORNETSECURITY

INFOPAPER

CIBERCRIMINALES EN LA TEMPORADA PRENAVIDEÑA – 5 CONSEJOS PARA PROTEGER MEJOR TU NEGOCIO

El año está llegando a su fin: hace más frío, oscurece más pronto y los primeros compradores ya están pensando qué regalar a sus seres queridos por Navidad. Los proveedores de tiendas online y los comercios locales están preparando ya todo para el negocio anual y de alta rotación antes de las Navidades.

El pistoletazo de salida comienza con los descuentos del último fin de semana de noviembre y el **"Black Friday" y "Cyber Monday".** Idealmente, este período también es bueno para que las empresas promuevan ofertas adecuadas para sus clientes, con el fin de atraer a más compradores. Pero este período no sólo es rentable para las empresas, los ciberdelincuentes también quieren cobrar y reclamar su bono navideño.

¿Qué tipos de ciberataques son los más utilizados por los ciberdelincuentes? ¿qué hace que los ataques sean tan peligrosos? Y, ¿cómo está cambiando la pandemia del coronavirus el negocio prenavideño? Explicamos todo esto y más en el siguiente **Infopaper y te damos 5 consejos sobre cómo proteger mejor tu negocio.**

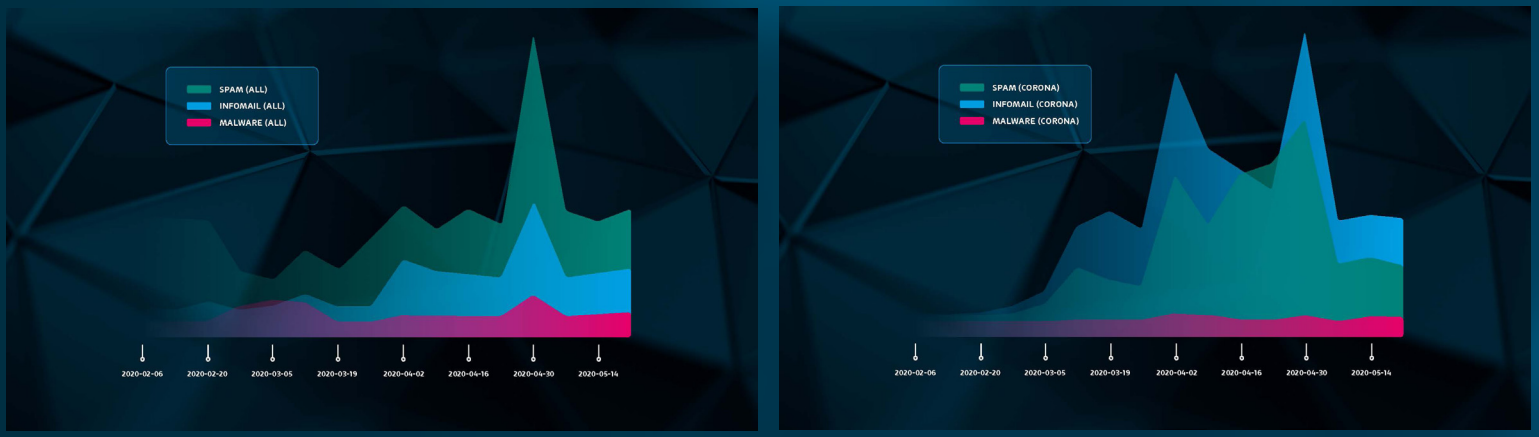
Contenido

Precaución: Cibercriminales con espíritu navideño... ¿o no?

Las organizaciones de ciberdelincuentes utilizan para sus ataques acontecimientos actuales y mediáticos.

Esto es un hecho que ha quedado claro para todo el mundo, especialmente desde la llegada del coronavirus: el aumento de los ataques de hackers a instalaciones médicas, laboratorios de investigación, así como los ataques de phishing con referencia a pruebas falsas de coronavirus o campañas de descuento de mascarillas ya adornaron los titulares. El **Security Lab de Hornetsecurity ha registrado un aumento de ciberataques por correo electrónico desde febrero de 2020**, como se muestra en el gráfico que aparece a continuación:

ABB. 1: Aumento del spam, infomail y malware antes y durante Corona

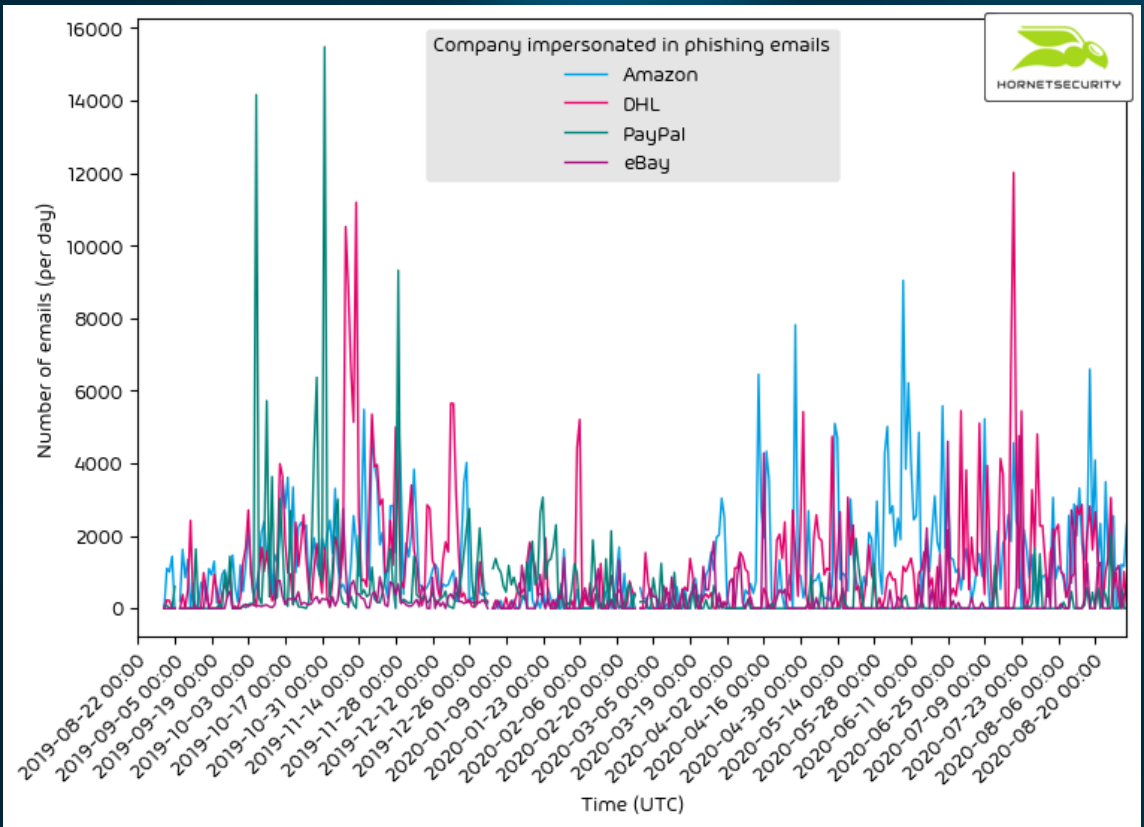


Aunque la pandemia del coronavirus está lejos de haber terminado, ya se vislumbra en el horizonte otro evento que ha sido utilizado una y otra vez en los últimos años como desencadenante de ciberataques: el negocio prenavideño alrededor del **"Black Friday" y el "Cyber Monday".**

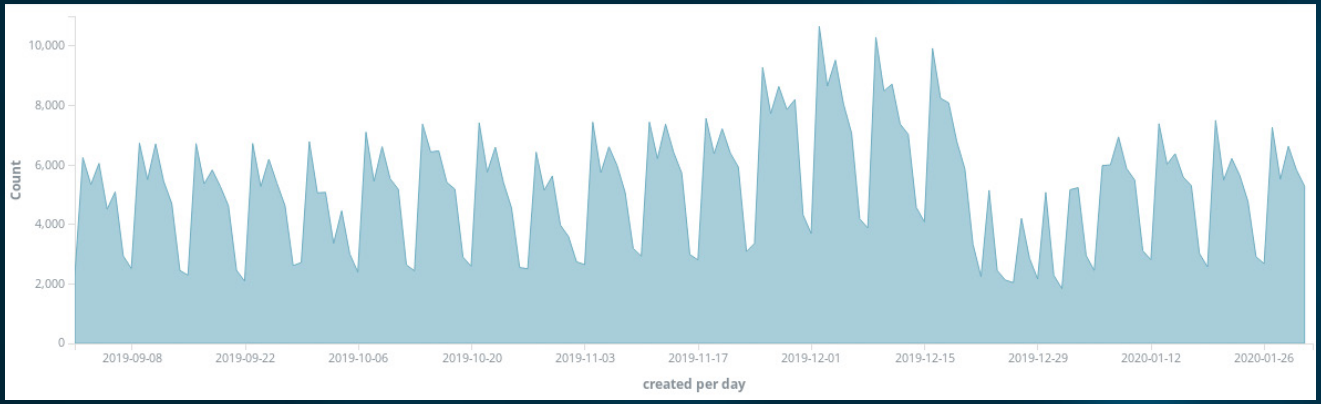
¿Pero, cómo se comporta la demanda de los consumidores en tiempos de coronavirus? ¿Siguen siendo el "Black Friday" y el "Cyber Monday" tan importantes para hacer negocios? La respuesta es sí. A mediados de año, Google ya comenzó una encuesta mundial entre sus usuarios, para saber cómo la pandemia del coronavirus está cambiando el comportamiento de compra. El **75% de los usuarios encuestados, planean aumentar sus compras navideñas online este año**. Mientras que en los últimos años algunos consumidores todavía preferían comprar localmente en tiendas, todo está cambiando cada vez más hacía la compra a través de Internet. Como resultado, los proveedores de tiendas en Internet esperan que la demanda aumente este año, pero también esperan una mayor presión competitiva. Especialmente si el comercio minorista estacionario también muestra su valor en los negocios online y se centra en el precio en particular. Como consecuencia de la reducción de la jornada laboral y del aumento del desempleo en todo el mundo, los proveedores de servicios online están entrando en la guerra de precios y los consumidores van a la caza de gangas.

Todo esto se traduce en más posibilidades de que los ciberdelincuentes ataquen.

El año pasado, el Security Lab de Hornetsecurity observó **un aumento en las campañas de phishing desde noviembre hasta mediados de diciembre.** Los s correos electrónicos falso a menudo atraen con ofertas tentadoras durante el período prenavideño y los días de alto consumo como el "Black Friday" y el "Cyber Monday".



El gigante online Amazon, con su reconocida marca, tiene que pagar por las actividades criminales de hackers una y otra vez. **A partir de finales de noviembre, un número creciente de correos electrónicos de phishing fueron enviados en nombre de Amazon.** Esto se muestra en el siguiente gráfico del año pasado, generado por los expertos del Security Lab de Hornetsecurity:



Pero no sólo se espera que los ataques de phishing aumenten en estos días, en concreto el negocio minorista online debe prepararse para un aumento de los ataques DDoS. Con una avalancha de solicitudes de servidores, los hackers están forzando a los sistemas de los proveedores a ponerse de rodillas, lo que significa que se pierden muchas oportunidades de venta.

Pero eso no es todo: desde hace dos años, **Emotet ha regresado con felicitaciones navideñas al final del año**. Por lo tanto, es probable que un mayor número de ciberataques de ransomware a empresas se pueda esperar también este diciembre.

A continuación, te daremos una visión completa de la situación de amenaza resultante de los ataques DDoS, phishing y ransomware. Por último, podrás encontrar cinco consejos útiles que te ayudarán a protegerte contra la creciente profesionalización de este tipo de ataques.

„Servidor caído". Cómo los ataques DDoS ponen de rodillas al comercio online

En el mundo del comercio online los ciberataques representan una de las mayores amenazas y en concreto: los ataques DDoS. Este tipo de ciberataques pueden causar un enorme daño económico a las empresas afectadas y, no menos importante, tener un enorme impacto en su imagen.

Un ataque DDoS es una abreviatura de "Distributed Denial of Service" o los ataques de denegación de servicio. A diferencia del ataque DoS, se utilizan varios sistemas previamente secuestrados para actuar contra el sistema objetivo. **El ataque consiste en enviar un número excesivo de solicitudes a un servidor, de modo que el sistema objetivo se sobrecarga y no puede responder a más solicitudes.** Los sistemas objetivo son, por ejemplo, un servidor de correo o un servidor web de una empresa. Especialmente en el período previo a las navidades, tal falla, aunque sea por poco tiempo, tiene consecuencias fatales. Todos los servicios que dependen del servidor ya no están disponibles o sólo lo están parcialmente. La base de clientes se desborda a la competencia y el proveedor de la tienda de Internet pasa la temporada de Navidad con trabajos de reparación.

Las víctimas de los ataques DDoS ya han sido pequeñas tiendas, pero incluso grandes empresas online conocidas como Amazon y Grupo Otto no son inmunes a tales ataques. **Los ataques DDoS suponen un mayor riesgo, especialmente durante eventos especiales.** La BSI* pudo determinar en su informe de estado que tales ataques se lanzan cada vez más durante el período prenavideño y en el"Black Friday" y el "Cyber Monday".

BSI* = Oficina Federal de Seguridad Informática de Alemania

El negocio profesional de los ciberataques DDoS

Además de la creciente profesionalización de los ataques de phishing, también se desarrollan continuamente los ataques DDoS. Entre ellos figuran, por ejemplo, los ataques técnicamente sofisticados que utilizan estrategias cada vez más desarrolladas en lugar de las de gran ancho de banda.

El año pasado, la BSI registró un aumento de los informes de ataques controlados activamente en los que los atacantes reaccionaron a la defensa de seguridad del servidor objetivo, intensificando así considerablemente el ataque. **En el segundo semestre de 2019, los analistas también observaron el uso de los llamados „carpet bombing".** En esta estrategia de ciberataque, los atacantes eluden las medidas de protección clásicas en la frontera de la red, de modo que están por debajo de los umbrales de detección (en Gbit/s) y, por lo tanto, no son reconocidos por el sistema. Para ello, los piratas informáticos dirigen su ataque contra un gran número de direcciones IP dentro de la red.

Así pues, las empresas se enfrentan a estrategias nuevas y profesionalizadas de ataques DDoS, en las que incluso las soluciones de protección clásicas llegan a sus límites. Se requieren contramedidas dinámicas para evitar estos ataques avanzados.

Vale la pena: Cómo los hackers se benefician con los ataques de ransomware

El ransomware, también conocido como programa de secuestro y chantaje, es un programa malicioso que asegura que los archivos se bloqueen para el usuario y sólo se liberen de nuevo pagando un rescate. **La principal puerta de entrada es la comunicación por correo electrónico,** tan relevante para los negocios. Un programa de ransomware suele ser recargado por otro malware oculto detrás de los archivos adjuntos o URLS. Si el usuario abre el archivo o enlace malicioso, se supera el primer obstáculo y el ransomware llega al ordenador. Tan pronto como el malware se activa, comienza el cifrado de los archivos. Se pueden cifrar archivos individuales de un sistema o incluso varios sistemas de una red de empresa. Para recuperar el acceso a los archivos, la víctima tiene que pagar un rescate. Pero no hay garantía de que los archivos sean realmente devueltos después del pago.

El daño a las empresas en un ataque exitoso de ransomware es enorme. En 2018, por ejemplo, los atacantes pudieron incautar 8 mil millones de dólares sólo en los EE. UU. En el año 2019, esta cifra aumentó a casi 24 mil millones de dólares. El daño causado a las compañías afectadas es usualmente mucho mayor que el dinero del rescate pagado. Esto resulta en considerables costes adicionales para la limpieza y la restauración de los sistemas. Para muchas empresas, un ataque de ransomware exitoso también implica una pérdida de reputación.

En particular, en el período prenavideño de alta rotación, es de esperar un aumento en el número de ciberataques de ransomware. Con el fin de mantener el negocio en funcionamiento, hay una mayor posibilidad de que las empresas paguen un rescate - este hecho es explotado sin piedad por los ciberdelincuentes.

Nuevas estrategias para los ciberataques de ransomware

El mero cifrado de archivos parece estar lejos de ser suficiente para los ciberdelincuentes. **Desde 2019, se ha observado una nueva estrategia entre las bandas de ciberdelincuentes.**

Por ejemplo, los actores detrás del laberinto ransomware amenazaron con publicar los archivos robados si el pago del rescate de la empresa afectada no se materializaba. Esta estafa da a los ataques de ransomware una nueva dimensión de peligro. La empresa afectada se encuentra así bajo una presión aún mayor para proteger los datos sensibles de ser publicados.

Los proveedores de tiendas online, por ejemplo, no sólo almacenan datos personales de sus clientes, como el nombre y la dirección, sino también a menudo información delicada sobre los pagos, que es muy vulnerable. Si se publicaran esos datos, se produciría una enorme pérdida de reputación y ventas.

Precaución: ataques de phishing, misión navideña

Como se mencionó al principio, los correos electrónicos de phishing son un tipo de ataque común y simple, pero aun así muy efectivo. Los atacantes utilizan el phishing para obtener acceso a datos sensibles y personales.

Para ello, los cibercriminales se aprovechan de una debilidad difícil de controlar: el ser humano. Suelen apelar emociones como la utilidad, el miedo, el sentido de la urgencia o el respeto a la autoridad, y así intentan manipular a sus víctimas.

Al hacerlo, se orientan cada vez más hacia acontecimientos actuales como las campañas con ofertas del "Black Friday".

Aquí se necesita un ojo particularmente atento al procesar los correos electrónicos, especialmente en el negocio prenavideño de este año, donde se esperan más campañas con ofertas especiales.

Profesionalización de los correos electrónicos de phishing

El timo nigeriano ha sobrevivido mucho tiempo a su utilidad: **los ataques de phishing se están profesionalizando cada vez más y, por lo tanto, son difíciles de distinguir de los originales.** Rara vez se encuentran deficiencias gramaticales y ortográficas; en cambio, los correos electrónicos de phishing suelen estar escritos en un lenguaje gramaticalmente correcto.
Ni siquiera el uso de protocolos HTTPS facilita el desenmascaramiento de los ataques de phishing: en su informe de estado de IT Security 2020, la BSI explica que los ciberdelincuentes utilizan cada vez más los enlaces HTTPS en los mensajes de phishing. Mientras que en noviembre de 2019 la cuota todavía era del 44%, en diciembre se produjo un aumento del 20% con las ofertas prenavideñas. La primera mitad de 2020 también vio un aumento en el uso de protocolos HTTPS en un promedio del 75% de los correos electrónicos de phishing.

¿Qué debo tener en cuenta como empresa?

Básicamente, la seguridad de la infraestructura interna de la empresa debe mantenerse durante todo el año. Ciertamente esto no es siempre una alta prioridad, porque la seguridad informática no es parte del negocio principal de la mayoría de las empresas.

En este caso es precisamente cuando **los servicios de gestión completa son la respuesta.** En vista de la situación de amenaza descrita anteriormente, recomendamos las siguientes cinco medidas de protección:

- **Protección contra el spam y el malware:** Una barrera de seguridad inicial se crea cuando la comunicación por correo electrónico está protegida de los ataques de spam y malware.
- **Protección contra el phishing:** También se debe prestar especial atención a los ataques de phishing, en concreto hay que fijarse en los enlaces incorporados en los mensajes. La exploración de URL se utiliza para examinar los enlaces en los correos electrónicos y abrirlos en un entorno seguro. En cuanto el sistema clasifica el enlace como sospechoso, el usuario recibe una notificación.
- **Protección contra los ataques DDoS:** Las soluciones de seguridad apropiadas deberían ser capaces de bloquear el impulso de las solicitudes en una etapa temprana. En lo que respecta al uso de „carpet bombing", se debe implementar un sistema de seguridad en caso de emergencia, que pueda intervenir sin interrupción en caso de fallo del servidor.
- **Protección contra ataques de ransomware:** los filtros antivirus clásicos llegan a sus límites con sofisticadas tácticas de ciberataque. Las soluciones de seguridad apropiadas deberían utilizar al menos un "Sanbox" para abrir los archivos adjuntos sospechosos en un entorno seguro y con el correspondiente retraso de tiempo. No es raro que las funciones maliciosas de los programas de ransomware se activen posteriormente. Algunos proveedores, como Hornetsecurity, también ofrecen mecanismos de detección inteligentes que pueden desenmascarar los ataques dirigidos a personas especialmente vulnerables y reaccionar a determinadas pautas de contenido que indican una intención maliciosa.

Como operador responsable de una tienda online, también debes preocuparte de proteger a tus clientes:

- ☑ Proporcionar información sobre las campañas de phishing actuales.
- ☑ Establecer una línea telefónica para cualquier caso sospechoso que tus clientes puedan denunciar.
- ☑ Ofrecer a tus clientes información sobre cómo distinguir tus mensajes de los mensajes de phishing.

Como proveedor de seguridad de correo electrónico basado en la nube, Hornetsecurity tiene en su cartera servicios integrales de seguridad de correo electrónico. Con Advanced Threat Protection puedes asegurar tu tráfico de correo electrónico contra el phishing, el ransomware y los ataques dirigidos. ¿Utilizas Microsoft 365? En segundos, 365 Total Protection Suite se integra perfectamente con Microsoft 365 y proporciona 21 características para protegerte de forma integral contra los ciberataques a través del correo electrónico.

www.hornetsecurity.com