RESUMEN EJECUTIVO: TRES COSAS QUE DEBE SABER ACERCA DE LA SUPLANTACIÓN DE IDENTIDAD

Comprender al suplantador de identidad, la suplantación de identidad y los hechos

RESUMEN

La suplantación de identidad aún es una amenaza real y ha evolucionado hasta convertirse en formas peligrosas, como spear-phishing y whaling. En el pasado, la suplantación de identidad se veía principalmente como un problema de los consumidores, pero actualmente los ataques de suplantación de identidad tienen un impacto directo financiero y en la reputación de las empresas. Los ataques dirigidos se inician comúnmente a través de campañas sofisticadas de suplantación de identidad para recolectar credenciales o entregar cargas como ransomware. A menudo, las empresas ignoran o minimizan la suplantación de identidad, ya que dan por sentado que su filtro de correo no deseado detectará la suplantación de identidad o que los empleados pueden darse cuenta con facilidad; ninguno de estos casos es cierto. En este documento se analizan los desafíos que las empresas enfrentan al mantenerse por delante de la suplantación de identidad.

Para combatir la suplantación de identidad, hay tres cosas que debe comprender: el suplantador de identidad, la suplantación de identidad y los hechos.

El suplantador de identidad: El álter ego más grande y malicioso del pirata informático

Muchas empresas tratan a los suplantadores de identidad como "solo un emisor más de correo no deseado" y, en cierto modo, los correos electrónicos de suplantación de identidad lucen y actúan como correo no deseado. Llegan sin ser solicitados y suelen pedir algo al destinatario, como efectuar una compra, realizar una acción o ingresar información. Pero la similitud termina ahí.

Mientras que los emisores de correo no deseado envían este tipo de correo que con frecuencia es abiertamente correo no deseado, los suplantadores de identidad se ocultan bajo la apariencia de un socio o amigo confiable. Mientras que el emisor de correo no deseado busca captar la atención, el suplantador de identidad la evita, al hacerse pasar por una fuente confiable y al utilizar su sistema de correo electrónico corporativo y a sus empleados en su contra.

Aunque ni el emisor de correo no deseado ni el suplantador de identidad son bienvenidos en su sistema de correo electrónico corporativo, el suplantador de identidad es mucho más amenazador. Aunque un poco de correo no deseado podría ser molesto pero aceptable, la suplantación de identidad es totalmente inaceptable. Un solo caso exitoso de suplantación de identidad de correo no deseado dirigido a su empresa podría exponer a su red corporativa, sus datos corporativos, sus empleados y sus clientes a la imaginación criminal o maliciosa de cada hacker y delincuente en Internet. Incluso si se remienda el error casi de inmediato, el suplantador de identidad o (más probablemente) sus asociados maliciosos podrían tener el tiempo suficiente para activar un ataque de ransomware o recolectar una base de datos completa de números de tarjetas de crédito de cliente y destruir su reputación.

La suplantación de identidad: Actualizaciones falsas y fraude fiscal

Los tres tipos más comunes de correos electrónicos fraudulentos son la suplantación de identidad, las actualizaciones falsas y el fraude fiscal.

Suplantación de identidad

La suplantación de identidad intenta atrapar víctimas incautas al aprovechar su confianza en las marcas reconocidas y fuentes confiables. Como su equivalente consumidor, los correos electrónicos de suplantación de identidad de empresas también parecen provenir de fuentes confiables, como la administración de la empresa, su departamento del área de TI o un socio comercial. Le informan al destinatario que se necesita la información actualizada inmediatamente para mantener una cuenta abierta o mantener el acceso a la red. Generalmente incluyen un vínculo a un sitio web "falsificado" o falso. Con solo seguir las indicaciones, el empleado

La investigación de SonicWall demuestra que las campañas de suplantación de identidad son el vector preferido para los ataques de ransomware.

proporciona al suplantador de identidad involuntariamente datos financieros confidenciales o información de acceso a la red. Con su red corporativa comprometida, es posible que no tenga otra opción que recuperar y volver a emitir todas las identificaciones seguras, verificar todos los dispositivos en busca de software malicioso y realizar un seguimiento de toda la actividad de la cuenta en busca de evidencia de actividad no autorizada.

Actualizaciones falsas

Otra forma de ataque de correo electrónico es la actualización falsa. Entre los tipos más comunes de actualización falsa está la actualización de software. Se trata de un correo electrónico fraudulento que informa a sus empleados sobre la disponibilidad de nuevas versiones de software y los envía a sitios web falsificados. Una vez allí, se les solicita que verifiquen la información de la cuenta para recibir la actualización y luego descargar involuntariamente el código malicioso. El código malicioso, una vez descargado, puede atacar de diferentes maneras. Puede evitar los protocolos de seguridad para obtener información empresarial, dañar los discos duros más allá de la recuperación, robar direcciones de correo electrónico para enviar mensajes maliciosos masivos, o infectar a otros usuarios a través de sesiones de chat. La clave para que un empleado detecte una actualización falsa es tener una política claramente definida y comunicada sobre "cómo actualizar el sistema", de modo que los mensajes de correo electrónico con actualizaciones falsas nunca sean confiables desde el principio.

Fraude fiscal

Los mensajes de correo electrónico de fraude fiscal aprovechan el hecho de que ningún proceso ni persona es perfecto. Todos los días, en los departamentos de contabilidad de todo el mundo, el personal de contabilidad procesa millones de dólares en pagos comerciales legítimos. Cuando se atrasa alguna cuenta, a veces un proveedor envía un aviso por correo electrónico que, a su vez, solicita a una persona de contabilidad que procese el pago según lo indicado. Algunas veces, para acelerar el pago, el departamento de contabilidad puede utilizar una tarjeta de crédito corporativa para pagar la factura en línea. Al imitar cuidadosamente la apariencia y el estilo de un proveedor o socio confiable, los suplantadores de identidad utilizan mensajes de correo electrónico de fraude fiscal para obtener información sobre tarjetas de crédito, pagos ilegales o ambos. En casos extremos, los suplantadores de identidad cambian sus procesos de facturación electrónica al redirigir todos los pagos al suplantador de identidad en lugar de a un proveedor en particular.

Los hechos: Las soluciones contra correo no deseado y antivirus por sí solas no detienen la suplantación de identidad.

Las empresas están plenamente conscientes de que las amenazas por correo electrónico, como el correo no deseado y los virus, pueden paralizar la productividad, aumentar la responsabilidad y ocasionar que los costos del área de TI aumenten rápidamente. En consecuencia, han invertido millones de dólares en protecciones contra correo no deseado y antivirus.

1. **Mito:** La mejor manera de evitar la suplantación de identidad es detener los correos electrónicos de suplantación de identidad de la misma manera en que detiene el correo no deseado: con su filtro de correo no deseado.

   Hecho: Los correos electrónicos de suplantación de identidad fueron creados específicamente para imitar los correos electrónicos legítimos. Son correos electrónicos bien escritos con orientación comercial de una fuente aparentemente confiable, exactamente aquello que los filtros contra correo no deseado deben permitir que ingrese a su empresa. Algunos correos electrónicos de suplantación de identidad llevan a cabo este engaño tan bien que evitan constantemente a los filtros contra correo no deseado. Aunque es tentador equiparar a los dos, la suplantación de identidad no es correo no deseado. La suplantación de identidad requiere análisis, identificación y manipulación específicos, a fin de evitar que tenga un impacto negativo en su empresa.

2. **Mito: El uso de un servicio de bloqueo de direcciones URL bloqueará los correos electrónicos de suplantación de identidad.**

   Hecho: Un servicio de bloqueo de direcciones URL es una lista de sitios web conocidos de suplantación de identidad. Los vínculos en un mensaje de correo electrónico se prueban en comparación con esta lista y, si hay alguna coincidencia, el mensaje de correo electrónico es un correo electrónico de suplantación de identidad. Este método es bueno, pero lento. Los suplantadores de identidad pueden iniciar ataques y recopilar la información deseada en solo algunas horas, con frecuencia antes de que la dirección URL se informe, verifique e incluya en la lista de bloqueo de direcciones URL. Se requiere un análisis del contenido para ayudar a identificarlo como un posible correo electrónico de suplantación de identidad. Los filtros de correo no deseado están capacitados para descubrir correo no deseado, es decir, un mensaje de correo electrónico que parezca inadecuado; se requiere un filtro de correo no deseado que busque un mensaje de correo electrónico que parezca adecuado, pero que tenga algunos trucos sutiles, como enmascaramiento de direcciones URL o remitente falsificado.

3. **Mito: Si falla la tecnología de detección de suplantación de identidad, los empleados pueden reconocer los correos electrónicos de suplantación de identidad.**

   Hecho: No puede depender de las habilidades de sus empleados para distinguir contenido legítimo de su gemelo de suplantación de identidad. Según un informe, se abre el 30 % de los correos electrónicos de suplantación de identidad y se hace clic en el 12 % de los adjuntos en correos electrónicos de suplantación de identidad[1].

Conclusión

La suplantación de identidad no es nueva y las empresas han luchado contra el suplantador de identidad desde el inicio del comercio electrónico. Pero a medida que las prácticas comerciales evolucionan para seguir el ritmo de la tecnología emergente, los suplantadores de identidad también se adaptan a las nuevas oportunidades que ofrece la tecnología, como los ataques de ransomware. Sin embargo, al entender la suplantación de identidad como un tipo diferente y más sofisticado de amenaza por correo electrónico, y al buscar soluciones diseñadas específicamente para detener los correos electrónicos de suplantación de identidad, puede protegerse a usted mismo y a su empresa.

Obtenga más información sobre las mejores prácticas para detener los ataques de suplantación de identidad. Lea nuestro resumen de soluciones: Cuatro pasos para una solución eficaz contra la suplantación de identidad.

[1] *Verizon Data Breach Investigation Report 2016 (Informe de investigación sobre filtración de datos de Verizon de 2016)*

© 2017 SonicWall Inc. TODOS LOS DERECHOS RESERVADOS.

SonicWall es una marca comercial o marca comercial registrada de SonicWall Inc. o sus afiliados en EE. UU. u otros países. Todas las demás marcas comerciales y marcas comerciales registradas son propiedad de sus respectivos dueños.

La información presentada en este documento se proporciona en relación con los productos de los afiliados de SonicWall Inc. No se otorga ninguna licencia, expresa o implícita, por impedimento legal o de otro modo, a ningún derecho de propiedad intelectual o en relación con la venta de los productos SonicWall. EXCEPTO LO ESTABLECIDO EN LOS TÉRMINOS Y CONDICIONES ESPECIFICADOS EN EL ACUERDO DE LICENCIA PARA ESTE PRODUCTO, SONICWALL, O SUS AFILIADOS, NO GARANTIZA RESPONSABILIDAD ALGUNA Y RENUNCIA A CUALQUIER GARANTÍA EXPRESA, IMPLÍCITA O REGLAMENTARIA RELACIONADA CON SUS PRODUCTOS, INCLUIDAS, ENTRE OTRAS, LA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, ADECUACIÓN PARA ALGÚN FIN EN PARTICULAR O NO INFRACCIÓN. EN NINGÚN CASO SONICWALL, O SUS AFILIADOS, SE HARÁ RESPONSABLE POR DAÑOS DIRECTOS, INDIRECTOS, DE CARÁCTER CONSECUENTE, PUNITIVOS, ESPECIALES NI INCIDENTALES (INCLUIDOS, ENTRE OTROS, DAÑOS POR PÉRDIDA DE GANANCIAS, INTERRUPCIÓN DEL NEGOCIO O PÉRDIDA DE LA INFORMACIÓN) QUE SURGIERAN POR EL USO O LA INCAPACIDAD DE USAR ESTE DOCUMENTO, INCLUSO SI SONICWALL, O SUS AFILIADOS, LE HUBIERA ADVERTIDO SOBRE LA POSIBILIDAD DE TALES DAÑOS. SonicWall, o sus afiliados, no efectúa declaraciones ni otorga garantías con respecto a la precisión o la integridad de los contenidos de este documento y se reserva el derecho de realizar modificaciones en las especificaciones y descripciones del producto en cualquier momento sin previo aviso. SonicWall Inc. o sus afiliados no se comprometen a actualizar la información que figura en este documento.

Acerca de nosotros

SonicWall ha luchado contra la delincuencia cibernética durante más de 25 años, defendiendo a las pequeñas y medianas empresas en todo el mundo. Nuestra combinación de productos y socios ha permitido ofrecer una solución de defensa cibernética en tiempo real adaptada a las necesidades específicas de más de 500.000 empresas en más de 150 países de todo el mundo, para que pueda hacer más negocios con menos temor.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Visite nuestro sitio web para obtener más información.
www.sonicwall.com.