VIGI PRENSA: 2015

Durante estos dos últimos años, las pequeñas y medianas empresas se han visto afectadas por los ataques de ciberinfiltración a las comunicaciones establecidas con sus proveedores o clientes, donde se emplea como medio el correo electrónico para acordar transacciones comerciales.

Este tipo de ataque se conoce como email spoofing, que consiste en inducir en error a la víctima, al hacerle creer que el mensaje de correo electrónico proviene de un proveedor o cliente, cuando en realidad, es originado en la computadora del ciberdelincuente.

Alcance Internacional

El éxito de los ataques de email spoofing se deriva de la ingeniería social practicada al contexto social de la víctima. Por esta razón, es importante establecer en la empresa un protocolo de atención a eventos de esta índole. Por lo anterior, la Organización de los Estados Américanos pone a disposición en su portal Web la guía IRM #10 que trata sobre "Cómo manejar un incidente de ingeniería social".

Ref.https://www.sites.oas.org

CENTRO CIBERNÉTICO POLICIAL 1

VIGI PRENSA: 2015

POLICÍA NACIONAL – Dirección de Investigación Criminal e INTERPOL 15 de julio de 2015

CENTRO CIBERNÉTICO POLICIAL

B@CIP – 001 | Boletín de Análisis en CIBERSEGURIDAD PyME

Características

En Colombia esta técnica ha sido usada por el cibercrimen para inducir al cambio de las condiciones de pago de cuentas, por parte de las empresas víctimas.

Por ejemplo, en un correo solicitan cambiar el número de cuenta bancaria y anticipar el pago de una obligación pendiente; mediante el uso de plataformas de email spoofing, el criminal puede simular que el origen del mensaje es de la cuenta de correo habitualmente usada por el verdadero proveedor para realizar transacciones comerciales.

En este sentido, la víctima cree en realidad hablar con su proveedor, accede al cambio de cuenta y termina consignando el valor de la obligación en la nueva cuenta bancaria ahora bajo control del cibercriminal.

Este fraude por EMAIL SPOOFING finaliza, cuando el proveedor notifica del incumplimiento de la obligación a la empresa víctima que apenas se percata que ha sido objeto de esta novedosa pero ilegal maniobra informática.

Diversos medios de comunicación han reseñado que las víctimas en Colombia, podrían haber sido defraudadas por un monto cercano a 8.000 mil millones de pesos.

Enlace de la noticia: http://www.eltiempo.-com/archivo/documento/CMS-13011974

Imagen tomada de: http://www.fse.gov.co/images/img6.jpg

Formas de ataque

En otra modalidad de email spoofing, los delincuentes simulando cuentas de correo, habitualmente usadas por gerentes comerciales de empresas clientes, solicitan a los proveedores que en esta oportunidad serían las víctimas, la entrega de productos en el menor tiempo posible. Las empresas víctimas ante la oportunidad de negocio, termi-

VIGI PRENSA: 2015

POLICÍA NACIONAL – Dirección de Investigación Criminal e INTERPOL 15 de julio de 2015

CENTRO CIBERNÉTICO POLICIAL

B@CIP – 001 | Boletín de Análisis en CIBERSEGURIDAD PyME

nan accediendo a las pretensiones del cliente (cibercriminal) quien exige condiciones logísticas de entrega, que le facilitan acceder a los productos y luego desaparecer sin dejar mayor rastro.

Obviamente no consignan por anticipado, por el contrario, cuando la empresa envía la factura a la dirección real del cliente, se percata de que este nunca solicitó los productos cerrando el ciclo del fraude por suplantación de correo electrónico.

Recomendaciones

1. Disponer de un listado actualizado de los correos electrónicos y datos de contacto de los proveedores y clientes.

2. Antes de realizar transacciones bancarias, siempre es importante confirmar el titular y la legítimidad de la cuenta respecto al proveedor o el cliente a quien va dirigido el pago.

3. Preservar los correos electrónicos objeto del ataque para entregarlos a las autoridades correspondientes.

4. Bloquear los correos electrónicos desconocidos, evitando abrir documentos o archivos adjuntos sospechosos ya que estos pueden contener programas maliciosos.

5. Implementar en la empresa un modelo de atención a incidentes informáticos para este tipo de ataques.

Imagen tomada de: http://www.fse.gov.co/images/img2.jpg

Fuente: Centro Cibernético Policial Nacional/Ministerio de Defensa Nacional-MDN. http://www.ccp.gov.co/sites/default/files/bacip_001_7.pdf