LA MEJOR PROTECCIÓN CONTRA EL SPEAR PHISHING

SPEAR PHISHING: UNA ESTAFA DIFÍCIL DE DETECTAR

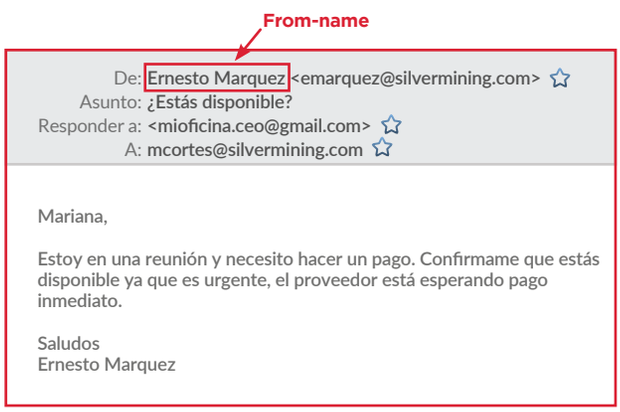
Spear phishing, también llamado usurpación de identidad, es una técnica utilizada por los hackers para perpetrar estafas que se conocen como Business Email Compromise **(BEC) o fraudes CEO.** Estas amenazas propagadas por medio del correo electrónico están creciendo rápidamente, y a diferencia de los ataques phishing, que son dirigidos de manera aleatoria a muchas personas a la vez, el Spear Phishing se enfoca en grupos o individuos específicos.

Estos ataques preocupan de sobremanera a los directores de IT porque son muy difíciles de detectar y, cuando logran tener éxito, son capaces de provocar daños muy costosos.

Zerospam ha desarrollado características muy avanzadas y una opción de vanguardia llamada Targeted Threat Mitigation, que bloquea los ataques Spear Phishing. Estos métodos brindan el mejor nivel de protección que existe contra estas amenazas.

Claves para identificar correos de Spear Phishing

- Correos enviados a un grupo limitado o individuo específico por un remitente dentro de la organización.
- Esos remitentes son personas que tienen la autoridad de iniciar giros de dinero o compartir datos sensibles.
- Los mensajes son hechos de tal manera que aparentan ser correos internos.
- Los correos usurpan la identidad de personas en posiciones de autoridad **(CEO, CFO, Gerente, etc.).**



1 -MITIGACIÓN DE AMENAZAS DIRIGIDAS (TTM por sus siglas en inglés) DE ZEROSPAM - UN ADELANTO

Después de haber analizado a fondo el problema, **Zerospam** ha creado la opción de **seguridad TTM**; disponible sin costo adicional. Esta opción bloquea los correos electrónicos entrantes basándose en la parte más incriminadora de un correo Spear Phishing: la identidad de la persona que el hacker intenta usurpar. Cuando se activa, la opción permite definir una lista de "remitentes usurpados" a partir de los nombres de las personas que los cibercriminales podrían tratar de usurpar. Siendo que las amenazas de Spear Phishing son hechas para pasar por correos internos, nuestra opción especializada pondrá en cuarentena los correos electrónicos enviados desde la red externa de su organización que utiliza el From-Name de uno de los nombres en la lista.

Ejemplo:

Partiendo del supuesto de que los hackers podrían tratar de usurpar la identidad de Jorge Morales o de María Hernández, cualquier correo de esos From-Names recibido desde fuera de la red de la organización, será puesto en cuarentena.

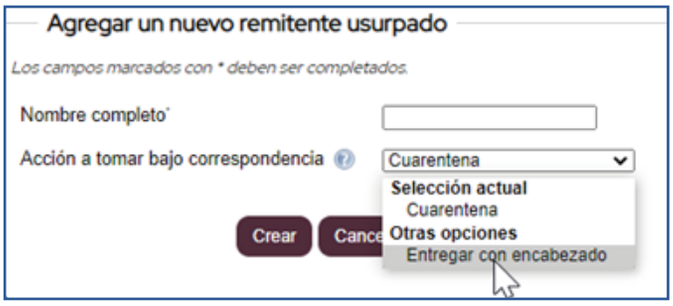
INTCOMEX CLOUD

zerospam

Información adicional

- Cuando se agrega un nuevo "remitente usurpado", también se puede elegir la opción de implementar **reglas de transporte** en el servidor del cliente para tomar acción cuando se detecten correos de Spear Phishing. Por ejemplo, entregar el correo con una etiqueta de peligro. Esto se puede hacer utilizando el encabezado Zerospam una vez el correo ha sido filtrado.

- Antes de agregar un nuevo nombre en la lista de "remitentes usurpados", las direcciones de correo personal que podrían ser utilizadas para enviar mensajes legítimos (como gmail o hotmail) deberán ser incluidas en la lista blanca, de lo contrario, los correos de estas direcciones serán bloqueados.

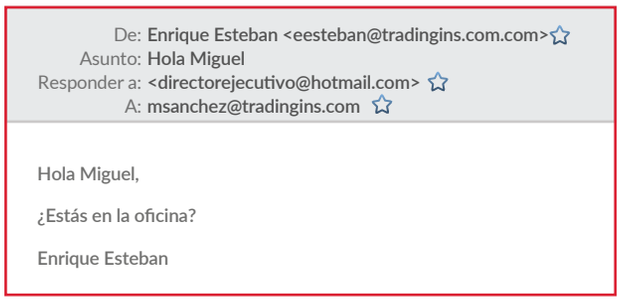


2 - PROTECCIÓN INCORPORADA CONTRA EL SPEAR PHISHING

Zerospam también ofrece protección contra Spear Phishing que reconoce y bloquea este tipo de correos. No se requiere configuración especial; los clientes están protegidos por defecto.

Ejemplo Paso 1 de un correo Spear Phishing :

Durante la preparación de su ingeniería social, el spammer sabe que debe usurpar a Enrique Esteban y enviar su requerimiento a Miguel Sánchez. Si Miguel contesta al correo recibido, el spammer podrá seguir al próximo nivel y enviar sus instrucciones por correo. Ya que Miguel ha sostenido una conversación con Enrique, será menos probable que sospeche.



En 2017, después de que un correo Spear Phishing lograra engañar a un grupo de empleados para que hicieran giros de dinero a cuentas bancarias en el extranjero controladas por un hacker, Google y Facebook perdieron US$ 100 millones cada uno. Los spammers no solamente atacan a las grandes compañías; las víctimas van desde microempresas hasta gigantes corporativos.

La protección incorporada Zerospam contra el Spear Phishing utiliza características avanzadas que se basan en:

- La correspondencia entre la dirección de correo electrónico del content-from (parte visible del FROM), del envelope-from (la dirección real de envío) y la dirección de respuesta reply-to.
- La reputación y validez del dominio remitente.
- Diferencias entre los dominios FROM y TO.
- Diagnóstico derivado de los algoritmos de aprendizaje automático (machine learning).

Note que el reply-to es una dirección Hotmail. La mayoría de los usuarios no lo hubieran notado.

La opción Targeted Threat Mitigation y la protección incorporada contra el Spear Phishing trabajan de manera independiente. Cuando se utilizan en conjunto, ofrecen la protección más completa contra el Spear Phishing que existe.