GUIA PARA LA EXTRACCIÓN DE IOC (INDICADORES DE COMPROMISO) DE PHISHING

CONTENIDO

GUIA PARA LA EXTRACCIÓN DE IOC (INDICADORES DE COMPROMISO) DE CORREOS DE PHISHING

1 OBJETIVO:

Determinar si un correo electrónico es phishing y como extraer los indicadores de compromiso para compartir a través de la plataforma MISP.

2 MEDIDAS DE SEGURIDAD PARA REALIZAR EL ANÁLISIS

Los procedimientos aquí descritos deben realizarse en una máquina virtual aislada a nivel de red o una máquina independiente, ya que implica analizar archivos y url potencialmente dañinas.

3 PROCEDIMIENTO PARA VERIFICAR SI EL CORREO ES PHISHING

3.1 Verificar el remitente

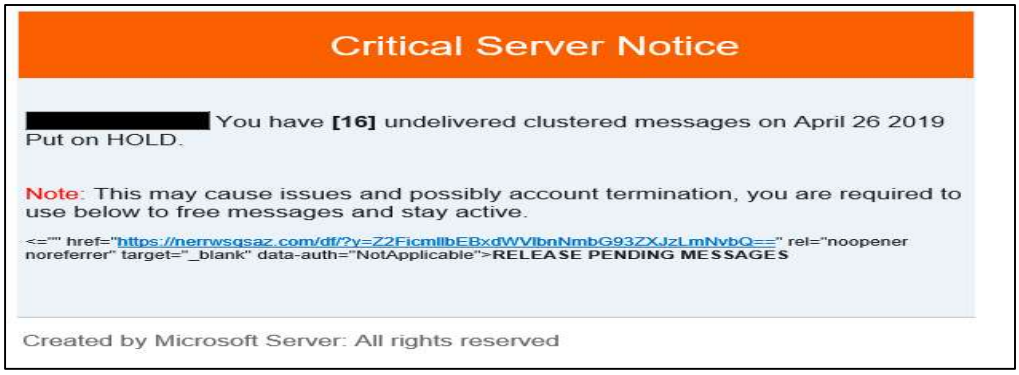
el buzón del remitente debe coincidir con el dominio de la entidad que dice estar enviando el correo. Por ejemplo los correos de XM siempre llegarán desde “xm.com.co”. Uno de los indicadores son cadenas extensas para ocultar el remitente real (plesk.movem)

3.2 *Asunto del correo:*

en ocasiones el asunto del correo muestra que es un reenvío, muestra las palabras “fwd”, de forward o “Rv” de reenvío, “Re” de respuesta. Muchas veces el asunto viene con frases que pueden generar un sentimiento de alarma por parte del destinatario.

3.3 Cuerpo del correo:

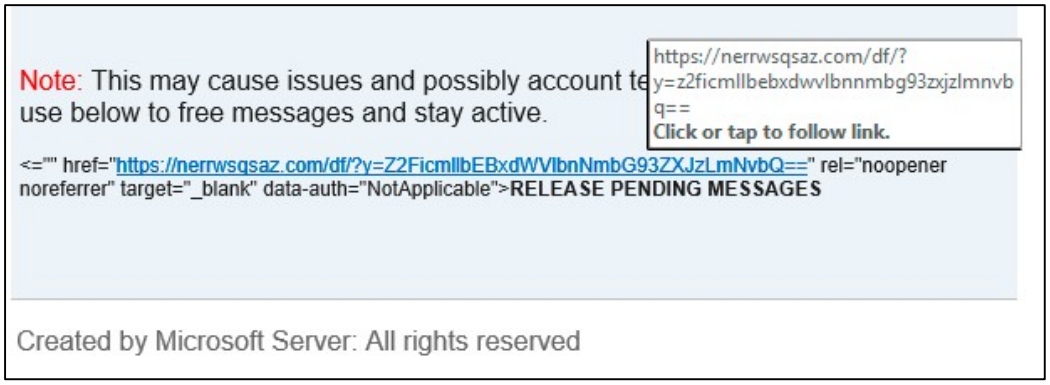
En ocasiones tiene errores ortográficos o corresponden a traducciones de otro idioma.



3.4 Link:

El correo solicita hacer clic en el link que relacionan, se debe colocar el mouse encima, sin dar clic, y verificar la url a la cual lo llevará, normalmente es una URL maliciosa que no tiene nada que ver con la entidad que envía el correo[1].

Se debe tener en cuenta que estas urls en ocasiones suelen parecer a simple vista igual a la original, haciendo uso de técnicas como agregar tildes, cambio de "i" por una "l", por lo cual siempre se debe copiar e inspeccionar esta url en portales como virus total.



3.5 **Tema del correo***:*

En la mayoría de los casos son "impactante", recurren a las emociones de quien recibe haciendo alusión a un premio, castigo, robo, multa, sanciones, urgencia entre otros.

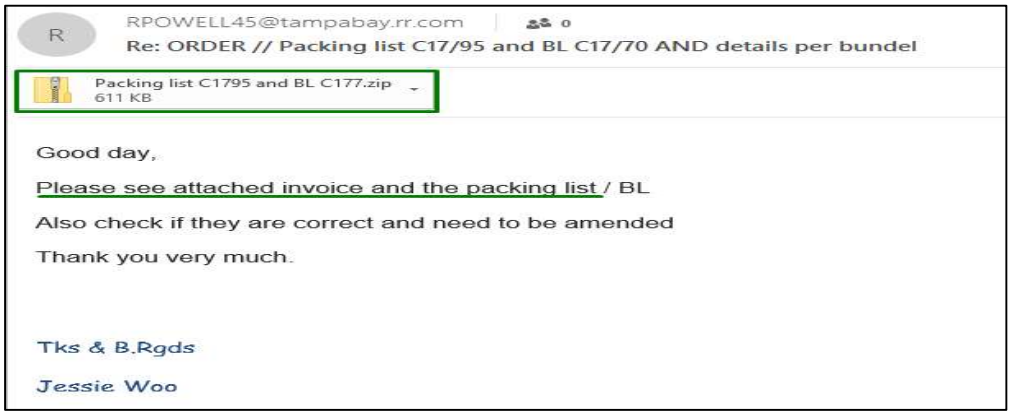
3.6 Saludo genérico:

Normalmente en el cuerpo del correo llegan con saludo genérico como "apreciado usuario", "apreciado cliente", "apreciado ciudadano", entre otros.

3.7 **Archivos adjuntos***:*

En caso de dudar de la procedencia con los pasos anteriores por ningún motivo abra el archivo adjunto.

[1] https://www.welivesecurity.com/la-es/2015/01/20/como-se-esconde-phishing-urls-falsas/

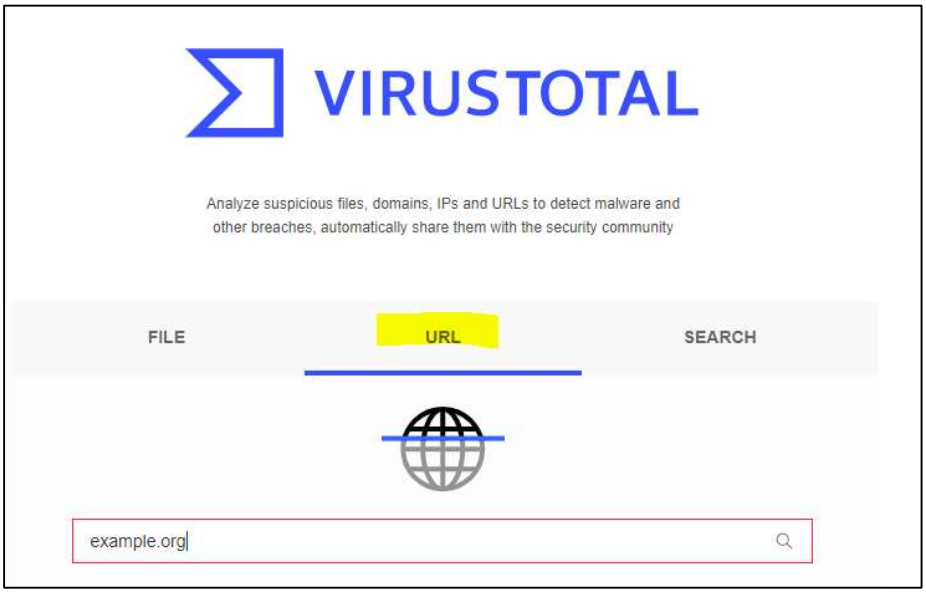


4 PROCEDIMIENTO PARA EXTRAER LOS INDICADORES DE COMPROMISO

Si el análisis anterior, muestra que el correo es un phishing, entonces se procede a la extracción de los IOCs para ser cargados en la plataforma MISP del CSIRT 0 del sector eléctrico, de acuerdo a la guía "**Reporte de eventos en MISP**".

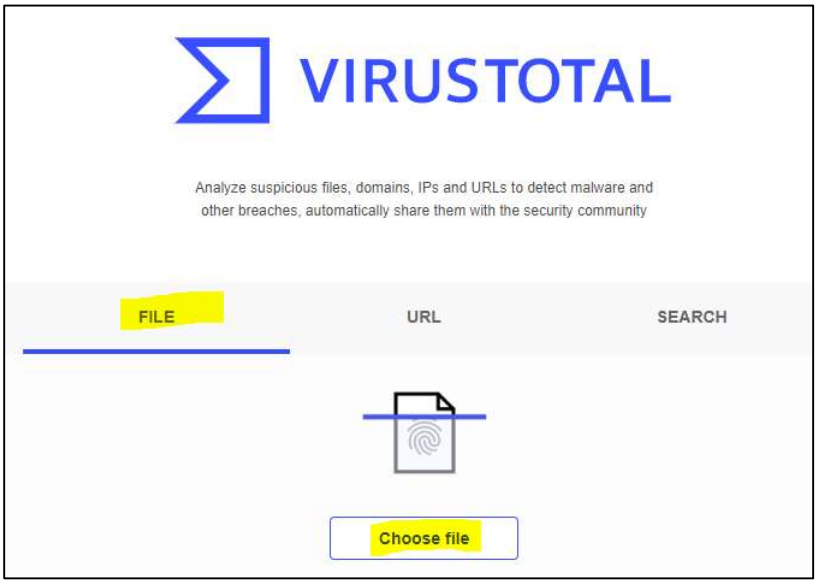
4.1 **Dominios, URLs e IPs***:*

Identificar todos los enlaces de URL y dominios que se encuentren en el correo identificado como phishing y validarlos en un sitio que permita su análisis como https://www.virustotal.com/:



4.2 **Archivos adjuntos***:*

Descargar los archivos adjuntos teniendo precaución de no ejecutarlos y proceder a analizarlos en un sitio de análisis de malware como https://www.virustotal.com/:

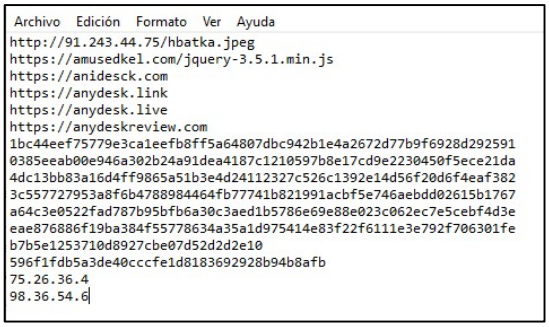


4.3 **Emails o direcciones de correo***:*

Adicionalmente, relacionar el correo electrónico del cual se originó la comunicación para que también pueda ser parametrizada en le evento que se reporte en la plataforma MISP.

5 PROCEDIMIENTO PARA CARGAR LOS IOCs EN MISP

Una vez se tengan los Indicadores de compromiso plenamiente identificados, estos deben ser copiados en un archivo ".txt", de la siguiente manera:



Esto con el fin de facilitar la carga en la plataforma MISP, de acuerdo al punto 3 de la "Guia **para el reporte de eventos en MISP":**