

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

CONTENIDO

1	OBJETIVO:.....	2
2	MEDIDAS DE SEGURIDAD PARA REALIZAR EL ANÁLISIS	2
3	PROCEDIMIENTO PARA VERIFICAR SI EL CORREO ES PHISHING	2
3.1	Verificar el remitente	2
3.2	<i>Asunto del correo:</i>	2
3.3	Cuerpo del correo:	2
3.4	Link:	3
3.5	Tema del correo:	3
3.6	Saludo genérico:.....	3
3.7	Archivos adjuntos:.....	3
4	PROCEDIMIENTO PARA EXTRAER LOS INDICADORES DE COMPROMISO	4
4.1	Dominios, URLs e IPs:	4
4.2	Archivos adjuntos:.....	5
4.3	Emails o direcciones de correo:	5
5	PROCEDIMIENTO PARA CARGAR LOS IOCs EN MISP.....	5

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)



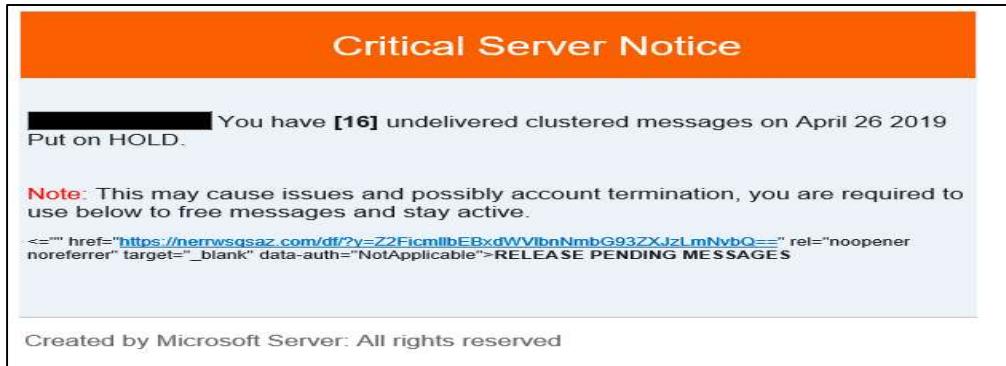
3.2 Asunto del correo:

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:

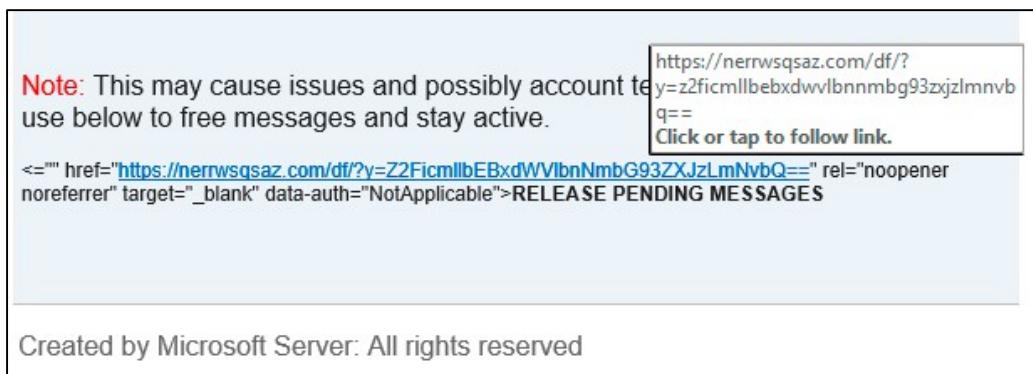
En ocasiones tiene errores ortográficos o corresponden a traducciones de otro idioma.



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 correo¹.

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 “í” por una “I”, 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/>

RPOWELL45@tampabay.rr.com | 0
Re: ORDER // Packing list C17/95 and BL C17/70 AND details per bundle

 Packing list C1795 and BL C177.zip - 611 KB

Good day,
Please see attached invoice and the packing list / BL
Also check if they are correct and need to be amended
Thank you very much.

Tks & B.Rgds
Jessie Woo

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**”.

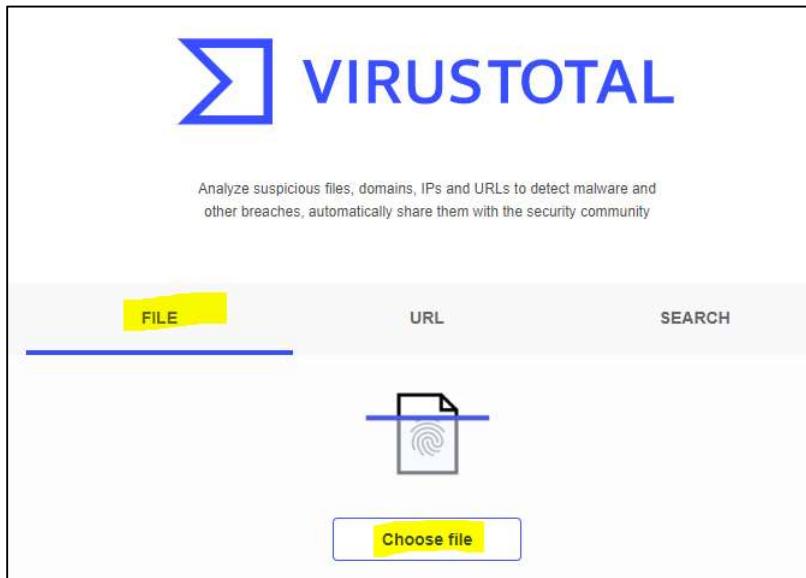
4.1 Dominios, URLs e IPs:

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 el evento que se reporte en la plataforma MISP.

5 PROCEDIMIENTO PARA CARGAR LOS IOCs EN MISP

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

```
Archivo Edición Formato Ver Ayuda
http://91.243.44.75/hbatka.jpeg
https://amusedkel.com/jquery-3.5.1.min.js
https://anidesck.com
https://anydesk.link
https://anydesk.live
https://anydeskreview.com
1bc44eef75779e3caeefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
0385eab00e946a302b2491dea4187c1210597b8e17cd9e2230450f5ece21da
4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
a64c3e0522fad787b95fb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e
eae876886f19ba384f55778634a35a1d975414e83f22f6111e3e792f706301fe
b7b5e1253710d8927cbe07d52d2d2e10
596f1fdb5a3de40cccf1d8183692928b94b8afb
75.26.36.4
98.36.54.6
```

Esto con el fin de facilitar la carga en la plataforma MISP, de acuerdo al punto 3 de la “Guía para el reporte de eventos en MISP”: