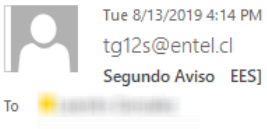
Campaña activa de Mekotio busca captar clientes de Chile

En el día de ayer llego a un colaborador del Laboratorio de ESET un curioso aviso de que mantenía una deuda con una compañía de servicios de telefonía de Chile, lo que por supuesto hizo que desestimara el mensaje, ya que nunca fue cliente de dicha empresa y no dudo a priori de un robo de identidad a su nombre.

Pero lo interesante del caso es que se descubre una campaña activa del Troyano Bancario Mekotio asociada a este correo electrónico que demuestra que sigue siendo una amenaza activa y principalmente en Chile.

Todo empieza con la recepción del aviso informando de la deuda



Estimado **cliente**,
Creemos que ha ocurrido algún imprevisto con el **pago de su cuenta**, pues identificamos en nuestro sistema que hay valores en abierto relacionado a su RUT.

Para más detalles: [**Descargar Su Factura**]

ATENCIÓN: Para una mejor visualización, abra en un ordenador (Windows).

Si bien el enlace de descarga de la factura no corresponde con ningún sitio oficial de la compañía, este tipo de campañas de ingeniería social, buscan en el envío masivo de correos captar usuarios distraídos o apurados en resolver el problema que no verifiquen donde hacen click.

Lo particular que esta campaña busca atacar clientes que sus dispositivos estén conectados en Chile.

Tal como se vio en la investigación sobre la amenaza de Mekotio, la computadora quedo infectada, y en capacidades de empezar a capturar credenciales bancarias principalmente.

Lo particular de este tipo de amenazas es la utilización de varias capas para el ataque con la finalidad de saltear los posibles sistemas de detección de los usuarios, como se puede observar desde la redireccion al momento de acceder al archivo a descargar, para luego ser un autojecutable MSI, donde se instalan un exe que no es malicioso en si mismo, sino que llama a una librería DLL (con un nombre conocido por el sistema) a la cual se le inyecto el código malicioso.

Como protegerse

Campaña de phishing o ingeniería social, para no ser víctimas de este tipo de engaño o similar, es importante además que los usuarios estén atentos a este tipo de mensajes y que antes de hacer clic revisen la URL que contiene el mensaje.