RESPUESTA DEL GOBIERNO

(184) PREGUNTA ESCRITA CONGRESO

184/24370 **02/10/2020** **60292**

AUTOR/A: SÁNCHEZ DEL REAL, Víctor Manuel (GVOX); RUEDA PERELLÓ, Patricia (GVOX); ESTEBAN CALONJE, Cristina Alicia (GVOX); ALCARAZ MARTOS, Francisco José (GVOX); FERNÁNDEZ-LOMANA GUTIÉRREZ, Rafael (GVOX); GESTOSO DE MIGUEL, Luis (GVOX)

RESPUESTA:

En relación a la pregunta de referencia, se informa que la campaña de suplantación comenzó el día 19 de agosto de 2020, repitiéndose en una segunda oleada el día 26 de agosto de 2020. Desde esa fecha se ha ido repitiendo de forma periódica, variando en cada caso los parámetros de ejecución, la infraestructura utilizada y la web donde se aloja el enlace malicioso.

Son campañas que inicialmente montan una infraestructura de suplantación de un organismo público, con el fin de dar veracidad a las mismas, para posteriormente lanzar un correo electrónico masivo a un gran número de cuentas de correo electrónico, obtenidas por medios ilícitos, buscando mediante la técnica de phishing que algún ciudadano o empresa caiga en el engaño y le proporcione información, normalmente bancaria.

En este tipo de campañas, el atacante y la víctima son ajenos a la infraestructura del Ministerio de Trabajo y Economía Social (MITES), tanto en la parte lógica del ataque como en la infraestructura informática utilizada. Está situación lleva a que el MITES tenga muy limitadas sus actuaciones y no pueda tomar medidas sobre el atacante o tener conocimiento del número de víctimas que han sido afectadas.

En el caso de ciberataques es muy complicado establecer su atribución, ya que los atacantes son capaces de esconder muy bien sus pasos y borrar toda huella en muy corto espacio de tiempo. La campaña sigue activa variando las plataformas utilizadas para lanzar los ataques.

Entre las medidas de subsanación ejecutadas se encuentran las siguientes:

- Envío de notificaciones de alerta a las diferentes Unidades de seguridad de los organismos dependientes del Ministerio.

- Se confirma que el sistema de seguridad del Ministerio ha bloqueado todos correos entrantes de estas características en nuestra infraestructura.

- Se mantiene la alerta de monitorización implantada el día 19 de agosto.

Por otro lado, cabe indicar que el Ministerio del Interior tiene constancia de los hechos referenciados tras recibir comunicaciones de diferentes ciudadanos alertando de la situación. En todos los casos se han solicitado los correos originales a los ciudadanos para proceder a su análisis y actuaciones según protocolo establecido ante ataques phishing, incluyendo la notificación a Instituto Nacional de Ciberseguridad (INCIBE-CERT) y, en su caso a las Fuerzas y Cuerpos de Seguridad del Estado. Adicionalmente, se han emitido alertas a través de Redes Sociales para alertar a la ciudadanía

(https://twitter.com/DGTes/status/1239879269498728449).

Por otra parte, aún no se tiene constancia del número total de afectados ni de los responsables de la estafa ante la dificultad de rastrear este tipo de ataques, para lo que se requiere la colaboración de operadoras de servicios de telecomunicación y servicios de terceros de correo electrónico.

Madrid, 29 de octubre de 2020