El Buró Federal de Investigaciones de Estados Unidos (FBI), confirmó este sábado que hackers no identificados violaron uno de sus servidores de correo electrónico para enviar mensajes falsos sobre un *«sofisticado ataque en cadena».*

El incidente, que fue revelado públicamente por primera vez por la organización sin fines de lucro de inteligencia de amenazas SpamHaus, involucró el envío de correos electrónicos de advertencia fraudulentos con el asunto *«Urgente: actor de amenazas en los sistemas»,* que se originó de la dirección de correo electrónico legítima del FBI: *«eims@ic.fbi[.]gov»,* que enmarca el ataque a Vinny Troia, un investigador de seguridad y fundador de las compañías de inteligencia de la dark web Night Lion Security y Shadowbyte, al mismo tiempo que afirma que está afiliado a un equipo de piratería llamado TheDarkOverlord.

SpamHaus citó sus propios datos de telemetría para afirmar que las explosiones de correo electrónico ocurrieron en dos oleadas de «spam», una poco antes de las 5:00 am UTC y otra poco después de las 7:00 am UTC.

Sin embargo, según el investigador de Kryptos Logic, Marcus Hutchins, el objetivo parece ser desacreditar a Troia.

> *«Vinny Troia escribió un libro que revela información sobre el grupo de piratería TheDarkOverlord. Poco después, alguien comenzó a borrar los clústeres de ElasticSearch dejando atrás su nombre. Más tarde, su Twitter fue hackeado, luego su sitio web. Ahora un servidor de correo electrónico del FBI hackeado está enviando esto»*, tuiteó Hutchins.

Brian Krebs, de Krebs on Security, quién también recibió una misiva independiente del atacante, detalló en un informe independiente que *«los mensajes de spam se enviaron abusando de un código inseguro en un portal en línea del FBI diseñado para compartir información con las autoridades policiales estatales y locales».*

Pompompurin dijo a Krebs que la violación se llevó a cabo aprovechando una falla en el

Portal Empresarial de Aplicación de la Ley (LEEP) del FBI, que no solo permitía a cualquier individuo solicitar una cuenta, sino que también filtró la contraseña de un solo uso que se envía al solicitante para confirmar su registro, lo que le permite interceptar y manipular las solicitudes HTTP con su propio mensaje falso a miles de direcciones de correo electrónico.

> *«El FBI está al tato de una mala configuración de software que temporalmente permitió un actor capaz de aprovechar el Cumplimiento de la Ley Enterprise Portal (LEEP) para enviar correos electrónicos falsos. Si bien el correo electrónico legítimo se originó en un servidor operado por el FBI, ese servidor estaba dedicado a enviar notificaciones para LEEP y no formaba parte del servicio de correo electrónico corporativo del FBI. Ningún actor pudo acceder o comprometer ningún dato o PII en la red del FBI»,* dijo la agencia en un comunicado.