Alertan a empresas de Hacktivismo

S21sec lanzó una alerta relacionada con el sitio **filtrala.org, el cual es un portal que permite la filtración de documentos confidenciales tanto de empresas privadas como de organizaciones gubernamentales.** Las motivaciones del sitio se basan en el hacktivismo, un movimiento que, bajo el lema de la defensa de la libertad y la justicia, promueven prácticas que pueden dañar la privacidad y la operación de dichas organizaciones.

La plataforma también está activa en Twitter, con el perfil @filtrala, donde coloca consejos del tipo "cómo filtrar información de manera más segura", o invitaciones que recoge de otros perfiles orientados al activismo.

Tanto **la cuenta de Twitter como la plataforma sugieren, de forma implícita, la ilicitud de las filtraciones que hacen los usuarios**, al sugerirles formas de borrar los rastros de información o al sugerirles no enviar documentos desde la computadora que usan para trabajar. Otro consejo de los hacktivistas es el uso de TOR (The Onion Router) como medida de seguridad para anonimizar sus acciones. Dentro de su comunicación se hacen referencias a Mexicoleaks, en un intento de desviar la atención a prácticas puestas en marcha en nuestro país.

Se han encontrado también vínculos con el colectivo Anonymous, los cuales han dado muestras de una notable capacidad operacional mediante **ataques de DDoS y otro tipo de intrusiones en organizaciones de todo el mundo**. Esto es una muestra de la **delgada línea que existe entre el activismo social y el hacktivismo**, lo que debe prender las alertas de las compañías, que deben preparar sus defensas no sólo contra los riesgos que pudieran considerarse como implícitos al ecosistema tecnológico, sino contra los impuestos por corrientes políticas o ideológicas posicionados contra el sistema y todo aquello que lo representa, entre otros, la empresa.

Recomendaciones

Según S21 sec, la evolución de las **prácticas hacktivistas obliga a las empresas a dotarse de recursos que le permitan detectar actuaciones anómalas, establecer y delimitar bien los niveles de acceso a la información** y datos, supervisar los procesos de comunicación interna, sobre todo en el manejo de información confidencial, con el objeto de evitar cualquier actuación indeseada proveniente tanto de empleados desleales, como de aquellos otros inspirados en móviles de cualquier otra naturaleza.

También es importante establecer controles de documentación "por ejemplo, **no mandar documentos clasificados por correo electrónico**, ya que una vez que llega al buzón de entrada, la organización pierde por completo el control", advierte Laura Requena, responsable de Servicios Avanzados de Ciberseguridad en Latinoamérica de S21 sec.