COVID-19

Staying cyber secure

La pandemia del COVID-19 ha cambiado nuestras vidas. Existe una preocupación significativa en nuestra gente y con esta preocupación viene un deseo de tener más información, seguridad y apoyo. Los grupos de crimen organizado están explotando los miedos, incertezas y dudas que genera el COVID-19, atacando a los individuos y negocios en una variedad de maneras.

Las amenazas existentes

Desde mediados de febrero, el equipo global de KPMG Cyber ha identificados una diversidad de ataques phishing que provienen de lo que parece ser una infraestructura criminal que explota la incertidumbre y miedo al COVID-19 para hacer que las víctimas accedan a sitios webs falso y allí poder robas sus credenciales Office 365.

Algunos ejemplos de estas campañas incluyen:

- Emails/phishings con información del COVID-19, que contienen adjuntos con códigos malignos, los cuales al ser abiertos explotan una vulnerabilidad en los productos Microsoft Office, que permite ejecutar comandos de manera arbitraria sobre la computadora afectada.
- Emails/phishings con información de salud relativa al COVID-19, adjuntada en documentos Word que incluyen macros malignas, que realizan la descarga del virus Emotet o Trickbot.
- Emails/phishings múltiples con vínculos a sitios de salud falso que solicitan las credenciales de los usuarios.
- Una selección de recomendaciones que pretenden proporcionar a los clientes actualizaciones sobre la disrupción de servicios debido al COVID-19 y que conducen a la descarga de programas malignos.
- Emails aparentemente provenientes de organismos gubernamentales y/o organizaciones internacionales, que proporcionan precauciones contra el COVID-19, pero incluyen en el correo programas malignos.
- Emails falsos sobre descuentos especiales en la declaración de impuestos, debido al COVID-19, que buscan capturan información de aquellas víctimas que abren el correo y acceden a los sitios web falsos incluidos.

Muchos grupos del crimen organizado han cambiado sus tácticas para usar materiales relacionados con el COVID-19, incluyendo actualizaciones de la evolución de la pandemia, curas falsas, paquetes fiscales, beneficios de emergencia y escasez de suministros.

Algunos indicadores que deben aumentar su sospecha:

- Gramática, ortografía y puntuación pobre.
- Deficiencias en el diseño y calidad del mensaje.
- Dirigidos de manera genérica como "Estimado Sr(a)", "Hola", "Estimado cliente", "Estimado contribuyente".
- Incluye un sentido de urgencia falso. Ejemplo: "oferta disponible para las primeras 100 personas".
- Solicita directamente información personal.

La respuesta

Existen algunas actividades clave que puede desarrollar para reducir el riesgo a su organización y sus empleados, particularmente cuando exista teletrabajo.

- Aumentar la conciencia sobre estas amenazas en su equipo de trabajo y cómo han explotado la sensibilidad hacia el COVID-19.
- Diseñar y compartir prácticas sobre cómo mantenerse seguros durante el teletrabajo, de acuerdo con el enfoque que haya adoptado su organización ante la pandemia.
- Asegurarse de utilizar contraseñas robustas y preferiblemente doble autenticación para todos los accesos remotos, especialmente para Office 365.

- Proporcione a los teletrabajadores una guía directa sobre cómo utilizar las soluciones de teletrabajo, incluyendo mecanismos para permanecer seguros y tips contra el phishing.

- Asegurarse de que todas las computadoras tengan un antivirus operativo y actualizado, así como también un firewall.

- Habilitar una línea de ayuda o chat de fácil acceso que proporcione recomendaciones de seguridad o permita reportar cualquier evento sospechoso.

- Una selección de recomendaciones que pretenden proporcionar a los clientes actualizaciones sobre la disrupción de servicios debido al COVID-19 y que conducen a la descarga de programas malignos.

- Para reducir el impacto asociado al robo, habilite cifrado en los dispositivos móviles, incluyendo especialmente las laptops.

- Considere deshabilitar los puertos USB y habilitar una herramienta de colaboración para facilitar el intercambio de información.

Además, asegúrese de que sus procesos financieros incorporen la reconfirmación de los pagos significación durante la pandemia de COVID-19. Esta reconfirmación puede ayudar a protegerse contra ataques de falsificación de correo electrónico corporativo. Idealmente, use un canal diferente como llamar o enviar mensajes de texto para confirmar una solicitud de correo electrónico.

En el ambiente de TI, asegúrese de aplicar parches de seguridad críticos y actualizar firewalls y software antivirus, incluidas las computadoras portátiles en uso para el trabajo remoto.

Es muy probable que el crimen organizado utilice cualquier nueva vulnerabilidad de TI para vulnerar la seguridad de su empresa, especialmente durante esta pandemia.

Asegúrese de realizar una copia de seguridad de todos los sistemas críticos, de manera regular, y de validar la integridad de estas copias. Esto como medida de respuesta ante un posible incremento de las amenazas por ransomware, explotando la temática del COVID-19 como trasfondo.

Contactos

Juan Manzano
Director de Cyber & CIO Advisory
T: +58 212 277 41 32
E: jmanzano@KPMG.com

Iván Briceño
Socio Líder de Risk Consulting - Advisory
T: +58 212 277 41 39
E: ibriceno@kpmg.com

kpmg.com/ve

@KPMG_VE | KPMG en Venezuela | KPMG en Venezuela | @kpmg_ve | KPMG Venezuela