Ciberdelincuentes envían falsos CV contaminados con virus

Actualmente, los cibercriminales están intentando infectar con malware a empresas de América Latina a través del envío de falsos currículums que contienen un troyano de acceso remoto.

ESET, compañía especializada en detección proactiva de amenazas, comparte ejemplos de esta práctica y acerca algunos a tener en cuenta para identificar estos engaños y así mantener los sistemas protegidos.

La compañía comparte algunos de los ejemplos de currículums con malware que son enviados a diferentes empresas de la región:

A simple vista estos emails parecen legítimos; de hecho, la dirección de correo en ambos casos parecería no ser falsa, y la redacción no presenta errores de ortografía o gramática que sirvan de alarma.

Así y todo, según ESET, siempre hay pequeños detalles que permiten detectar cuándo un mail puede estar distribuyendo contenido malicioso.

“En el caso del mail enviado supuestamente por Mariana Alvarez, llama la atención que no esté dirigido a ninguna persona en particular (algo que se repite en el ejemplo de Catalina Muñoz). Y que, además, no se incluya el nombre en el saludo. Pero lo más llamativo, en ambos ejemplos, es que el archivo adjunto está en formato .zip, y el peso de este.”, comenta Camilo Gutiérrez Amaya, jefe del Laboratorio de Investigación de ESET Latinoamérica.

En caso de descargar el falso currículum, el usuario se estará infectando con malware y otorgando así al ciberatacante la posibilidad de que obtenga información sensible vinculada a sus credenciales de acceso al correo.

Igualmente, también quedan expuestos los datos de homebanking y tarjetas de crédito, sin olvidar la posibilidad de que el atacante acceda a información confidencial de la empresa.

Además, se le puede permitir instalar software no autorizado para cometer otro tipo de delitos, como encriptar archivos o bloquear el acceso a los sistemas de toda la organización.

“Para mitigar el riesgo de ser víctima de este tipo de ataque es importante sistematizar buenas prácticas, y como organización o empresa también es relevante tomar cartas en el asunto desde la protección de los sistemas, así como brindar capacitaciones a sus colaboradores para detectar intentos de phishing”, agrega el investigador de ESET Latinoamérica.

Aspectos que deben generar atención

Cuando se recibe un correo -sobre todo si es inesperado- hay varios detalles y señales que pueden hablar de un intento de phishing. Antes de hacer clic, el equipo de ESET recomienda chequear dos detalles:

- La redacción y ortografía en el asunto y contenido del mensaje. Si bien gracias a la Inteligencia Artificial, los ciberatacantes logran redactar mensajes cada vez más coherentes y elaborados, siempre es bueno dar una leída a conciencia y verificar que no haya errores que levanten sospecha.
- La extensión del archivo –si es .jpg, pdf, o similar– que debe, al menos, tener concordancia con el documento que el mail dice adjuntar. Como vemos en los ejemplos de esta campaña, los supuestos curriculums son en realidad archivos .zip (un archivo comprimido).

En cuanto a la protección extra, es fundamental para la detección contar con una solución de seguridad robusta y confiable, que pueda brindar protección contra este y otro tipo de ataques de malware.

“Enviar un currículum a una organización para postularse a algún puesto de trabajo es una práctica cotidiana, pero también se ha convertido en otra práctica muy común entre los cibercriminales para infectar a las empresas con malware, indica Gutiérrez Amaya.

Y añade que es importante «tomar conciencia de que esto está sucediendo actualmente y capacitarse para detectar correos maliciosos, es el primer paso que deben dar las empresas para estar protegidas.”, concluye el ejecutivo.

Con información de 800 noticias