



Ataques de malware y robo de datos: explican uso de plataforma para monitorear si información personal circula en la Dark Web

Académica PUCV advierte sobre los métodos de operación de ciberdelincuentes y entrega aspectos a tener en cuenta ante amenazas y riesgos

A través del uso de programas especializados para vulnerar las redes llamados malware, los ciberdelincuentes tienen la posibilidad de acceder a información personal de los usuarios, como los números de tarjetas bancarias y datos personales de identificación que están asociados a cuentas de correo, las cuales pueden ser vendidas en la Dark Web con la finalidad de cometer delitos financieros.

“Los datos que son robados se pueden transferir en distintos tipos de situaciones fraudulentas o directamente pueden ser vendidos de manera clandestina en algunos sitios no reconocidos”, indicó Pamela Hermosilla, académica de la Escuela de Ingeniería Informática de la Pontificia Universidad

Católica de Valparaíso.

Las tarjetas robadas incluyen datos adicionales como el nombre de la víctima, información de autorrelleno que permanece guardada en los navegadores y archivos del computador, los cuales son extraídos mediante los malware.

“Se trata de programas que están diseñados para infiltrarse en los sistemas, capturar información sensible como números de tarjetas, contraseñas y otros datos personales para enviar a los atacantes”, dijo la profesora de la PUCV.

¿CÓMO FUNCIONAN?

Son tres los métodos de operación más frecuentes y casi imperceptibles para infiltrarse en los dispositivos. “Mediante el

correo electrónico -a través de Phishing- simulan emails legítimos de parte de una persona, empresa o servicio de confianza, pero contienen algunos archivos o enlaces maliciosos. Otra herramienta son algunos sitios web comprometidos que, sin darse cuenta, logran instalar estos programas. Y por último, a través de descargas directamente de páginas web que contemplan malware y que capturan los datos a través del teclado, capturando pantalla o cuando se rellenan datos en formularios online”, indicó Hermosilla.

INFORME DARK WEB

Para saber si los datos personales capturados por malware circulan en la Dark Web con el riesgo de ser vendidos, Google

lanzó una herramienta para que los usuarios puedan verificar de manera gratuita si la dirección de correo está expuesta a ciberdelincuentes.

“La herramienta es un servicio diseñado para ayudar a los usuarios a proteger la información personal monitoreando la Dark Web en busca de algunos datos comprometidos. En términos generales, los recolecta utilizando algunas técnicas especializadas y luego los compara usando algoritmos avanzados. Luego notifica a los usuarios con algunas coincidencias que se puedan encontrar y entregando recomendaciones de seguridad como cambiar contraseñas, habilitar autenticación en dos pasos u otros elementos que pudieran proteger las cuentas”, explicó la profesora de Ingeniería Informática.