Verne
TECHNOLOGY GROUP

Boletín de alertas

Newsletter Seguridad Verne

Vol. 29/24

ÍNDICE

EL BANCO DE ESPAÑA ADVIERTE SOBRE EL PELIGRO DE LOS PAGOS 'CONTACTLESS'

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Actualización de seguridad	Usuarios	Alta

El Banco de España ha lanzado una advertencia sobre los riesgos que conllevan los pagos contactless, o pagos sin contacto, que han incrementado su popularidad debido a la pandemia de COVID-19. Esta forma de pago, que permite realizar transacciones simplemente acercando una tarjeta, teléfono móvil o dispositivo wearable a un terminal de pago, es rápida y conveniente. Sin embargo, el Banco de España destaca que también puede ser vulnerable a ciertos tipos de fraude si no se manejan con las debidas precauciones.

Entre los principales riesgos asociados a los pagos contactless se encuentran la posibilidad de robo de datos y fraude. Debido a la naturaleza sin contacto de estas transacciones, los delincuentes pueden utilizar dispositivos de escaneo para interceptar la información de pago de una tarjeta o dispositivo móvil. Además, si un ladrón se apodera de una tarjeta contactless, podría utilizarla para realizar pagos sin necesidad de conocer el PIN, hasta un límite establecido por las entidades financieras.

Otra preocupación importante es la falta de autenticación robusta en transacciones de bajo valor, lo cual facilita que los criminales puedan realizar múltiples pagos pequeños antes de que se detecte el fraude.

Para mitigar estos riesgos, el Banco de España ofrece una serie de recomendaciones tanto para los consumidores como para las entidades financieras:

- Establecer Límites de Gasto: Las entidades financieras deben permitir a los usuarios establecer límites de gasto diario para las transacciones contactless. Esto puede ayudar a minimizar el impacto en caso de que se produzca un fraude.
- Autenticación Reforzada: Se sugiere implementar métodos de autenticación más robustos, como la autenticación biométrica (huellas dactilares, reconocimiento facial) o el uso de códigos PIN después de un cierto número de transacciones o cuando se alcanza un límite acumulado.
- Monitorización Constante: Las instituciones financieras deben vigilar continuamente las transacciones en busca de patrones sospechosos. El uso de inteligencia artificial y algoritmos avanzados puede ayudar a detectar y prevenir actividades fraudulentas de manera más eficaz.
- Educación del Usuario: Es crucial que los usuarios sean conscientes de los riesgos y sepan cómo protegerse. El Banco de España insta a los consumidores a revisar regularmente sus estados de cuenta y a reportar cualquier actividad sospechosa de inmediato.

Aparte de las recomendaciones del Banco de España, los usuarios pueden tomar medidas adicionales para protegerse:

- Uso de Fundas de Bloqueo RFID: Estas fundas impiden que los dispositivos de escaneo no autorizados puedan leer la información de las tarjetas contactless.
- Aplicaciones de Gestión de Tarjetas: Muchas aplicaciones bancarias permiten activar o desactivar la funcionalidad contactless de las tarjetas. Los usuarios pueden mantener esta funcionalidad desactivada y activarla solo cuando sea necesario.
- Revisión Frecuente de Transacciones: Revisar regularmente los extractos bancarios y las notificaciones de transacciones puede ayudar a detectar y actuar rápidamente en caso de fraude.

Los pagos contactless ofrecen una gran comodidad y rapidez, pero es esencial estar conscientes de los riesgos asociados y tomar medidas para protegerse. Las recomendaciones del Banco de España subrayan la importancia de la seguridad en las transacciones sin contacto y la necesidad de un enfoque proactivo tanto por parte de las entidades financieras como de los consumidores. Adoptar buenas prácticas y mantenerse informado puede hacer una gran diferencia en la protección contra el fraude.

DARKGATE MALWARE EXPLOITS SAMBA FILE SHARING VULNERABILITY

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Malware	Samba	Alta

En una reciente campaña de corta duración, se descubrió que el malware DarkGate utilizaba vulnerabilidades en las comparticiones de archivos de Samba para propagar infecciones. Esta actividad se llevó a cabo durante los meses de marzo y abril de 2024, y afectó principalmente a servidores con comparticiones de archivos Samba accesibles públicamente, que alojaban archivos en Visual Basic Script (VBS) y JavaScript (JS).

DarkGate es un malware que ha evolucionado desde su primera aparición en 2018 hasta convertirse en una oferta de malware como servicio (MaaS) utilizada por un grupo selecto de clientes. Este malware tiene capacidades avanzadas, como control remoto de hosts comprometidos, ejecución de código, minería de criptomonedas, lanzamiento de shells inversos y despliegue de cargas adicionales.

La campaña documentada por investigadores de Palo Alto Networks Unit 42 comenzó con archivos de Microsoft Excel (.xlsx) que, al ser abiertos, pedían a las víctimas que hicieran clic en un botón incrustado. Este botón ejecutaba código VBS alojado en una compartición de archivos Samba, lo que iniciaba una cadena de infección que incluía la descarga y ejecución de un script en PowerShell. Este script, a su vez, descargaba un paquete de DarkGate basado en AutoHotKey.

DarkGate utiliza varias técnicas de evasión para dificultar su análisis y detección. Entre ellas, escanea programas antimalware, verifica la información de la CPU para determinar si se está ejecutando en un entorno físico o virtual, y examina los procesos en ejecución en busca de herramientas de ingeniería inversa o software de virtualización.

Además, el tráfico de comando y control (C2) de DarkGate usa solicitudes HTTP no cifradas, pero los datos están ofuscados y aparecen como texto codificado en Base64.

Este incidente subraya la capacidad de los actores maliciosos para abusar de herramientas y servicios legítimos con fines nefastos. A pesar de ser una campaña de corta duración, la utilización de comparticiones de archivos Samba públicas para distribuir malware destaca la necesidad de una ciberseguridad proactiva y robusta.

Para protegerse contra amenazas similares, se recomienda:

- Actualizar regularmente el software antimalware y habilitar las actualizaciones automáticas.
- Evitar hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocidas.
- Implementar controles de acceso y contraseñas fuertes en las comparticiones de archivos Samba.
- Considerar la encriptación de datos sensibles almacenados en estas comparticiones.
- Fomentar una cultura de conciencia de seguridad cibernética mediante la educación continua sobre mejores prácticas de ciberseguridad.

En conclusión, la evolución de DarkGate y su capacidad para adaptarse y evadir mecanismos de detección refuerzan la importancia de mantener defensas cibernéticas actualizadas y vigilantes frente a las amenazas emergentes.

BANCOS EN SINGAPUR ELIMINAN OTPS PARA INICIOS DE SESIÓN EN LÍNEA

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Actualización de seguridad	Usuarios	Media

Los bancos en Singapur han decidido eliminar el uso de contraseñas de un solo uso (OTP, por sus siglas en inglés) para los inicios de sesión en línea, reemplazándolos con tokens digitales. Esta medida será implementada para todos los usuarios que ya hayan activado los tokens digitales en sus dispositivos móviles.

La razón principal detrás de este cambio es fortalecer la seguridad de la autenticación bancaria. Los tokens digitales se consideran más seguros en comparación con los OTPs, ya que están integrados directamente en los dispositivos móviles de los usuarios y requieren una verificación más robusta, lo que dificulta el acceso no autorizado.

El aumento en los intentos de estafas de phishing ha sido una preocupación constante en Singapur. En respuesta, la Autoridad Monetaria de Singapur (MAS) y la Asociación de Bancos de Singapur (ABS) han colaborado estrechamente para desarrollar medidas que protejan mejor a los consumidores. El uso de tokens digitales se alinea con estos esfuerzos al proporcionar una capa adicional de seguridad.

Si bien este cambio puede generar inconvenientes para algunos usuarios acostumbrados a los OTPs, las instituciones bancarias aseguran que es un paso necesario para mejorar la protección contra el acceso no autorizado a las cuentas bancarias. Los clientes deberán asegurarse de tener sus dispositivos móviles configurados correctamente para utilizar los tokens digitales.

Loo Siew Yee, Directora Asistente de Política, Pagos y Crimen Financiero en MAS, enfatizó la importancia de esta medida como complemento a las buenas prácticas de ciberhigiene que los clientes deben seguir manteniendo, tales como la protección de sus credenciales bancarias.

Este cambio en el método de autenticación es parte de un esfuerzo continuo por parte de las autoridades y las instituciones financieras en Singapur para combatir las amenazas cibernéticas y asegurar un entorno bancario más seguro. A medida que las estafas se vuelven más sofisticadas, la adaptación de las medidas de seguridad es crucial para proteger a los usuarios y sus activos financieros.

MICROSOFT DESCUBRE FALLAS CRÍTICAS EN ROCKWELL AUTOMATION PANELVIEW PLUS

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Vulnerabilidad	CVE-2023-29464 CVE-2023-2071	Rockwell Automation PanelView Plus	Alta

Microsoft ha descubierto dos vulnerabilidades críticas en el sistema PanelView Plus de Rockwell Automation, designadas como CVE-2023-2071 y CVE-2023-29464, con puntajes CVSS de 9.8 y 8.2 respectivamente. Estas fallas permiten a atacantes remotos ejecutar código arbitrario y provocar condiciones de denegación de servicio (DoS). La primera vulnerabilidad implica una validación de entrada inadecuada que conduce a la ejecución remota de código, mientras que la segunda puede resultar en filtraciones de datos de memoria y DoS. Estos problemas afectan versiones específicas de FactoryTalk View Machine Edition y FactoryTalk Linx. Tanto Rockwell Automation como la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) han emitido avisos y parches para abordar estas vulnerabilidades.

CVE-2023-2071: Esta vulnerabilidad está relacionada con una validación inadecuada de entradas en la interfaz HMI de PanelView Plus. Los atacantes pueden explotar esta falla enviando entradas manipuladas, lo que les permite ejecutar código arbitrario en el sistema afectado. La explotación exitosa de esta vulnerabilidad podría otorgar control total sobre el sistema a los atacantes, permitiéndoles alterar procesos industriales críticos.

CVE-2023-29464: Esta segunda vulnerabilidad permite a los atacantes causar una condición de denegación de servicio (DoS) y potencialmente filtrar datos de memoria. La explotación de esta falla puede resultar en la interrupción de operaciones industriales, afectando la disponibilidad y confiabilidad del sistema.

Las vulnerabilidades en sistemas de automatización industrial como PanelView Plus son especialmente preocupantes debido a la naturaleza crítica de estos sistemas en procesos de manufactura y producción. La capacidad de los atacantes para comprometer estos sistemas podría tener consecuencias graves, incluyendo interrupciones en la producción, daños a equipos, y riesgos para la seguridad de los trabajadores.

Rockwell Automation ha respondido rápidamente a estos descubrimientos colaborando con Microsoft para identificar y solucionar las fallas. Se han emitido actualizaciones de seguridad y parches para las versiones afectadas de FactoryTalk View Machine Edition y FactoryTalk Linx. La Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) también ha publicado avisos de seguridad, instando a las organizaciones a aplicar los parches y seguir las mejores prácticas de ciberseguridad.

Las recomendaciones incluyen actualizar los sistemas afectados lo antes posible, revisar y ajustar las configuraciones de red para limitar el acceso no autorizado, y monitorear continuamente los sistemas en busca de actividades sospechosas. Además, se aconseja a las organizaciones realizar evaluaciones de riesgos para entender mejor cómo estas vulnerabilidades podrían impactar sus operaciones específicas.

El descubrimiento de estas vulnerabilidades subraya la importancia de la seguridad en los sistemas de automatización industrial. A medida que las industrias adoptan cada vez más tecnologías digitales y conectadas, la superficie de ataque se expande, haciendo que la ciberseguridad sea una prioridad crítica. Las colaboraciones entre proveedores de tecnología, como la de Microsoft y Rockwell Automation, son esenciales para identificar y mitigar riesgos antes de que puedan ser explotados por actores maliciosos. Es crucial que las organizaciones permanezcan vigilantes y proactivas en la protección de sus sistemas industriales contra amenazas cibernéticas emergentes.

CUIDADO CON LO QUE TIRAS A LA BASURA: ESTÁN USANDO DATOS DE PAQUETES DE ENVÍO PARA DIVERSOS TIMOS

CATEGORÍA	NOMBRE VULNERABILIDAD	BRECHA	Criticidad
Ciberseguridad	Phishing	Usuarios	Alta

La práctica conocida como 'dumpster diving' implica buscar en la basura para recuperar información valiosa que pueda ser utilizada en ciberataques. Aunque muchas personas no lo consideran, cuando se tira un paquete de una tienda en línea como Amazon, la etiqueta adherida contiene varios datos personales que podrían ser utilizados en su contra para estafarlas. Estos datos pueden ser explotados por estafadores que los utilizan para realizar fraudes y engaños.

El término 'dumpster diving' se refiere a la búsqueda de información personal en la basura que puede ser utilizada para cometer fraudes. Cuando una persona desecha un paquete con una etiqueta que contiene su nombre, dirección y posiblemente otros datos, esta información se vuelve accesible para cualquier persona que recupere el paquete de la basura. Los estafadores pueden utilizar estos datos para contactarte bajo el pretexto de ser la tienda en la que compraste el artículo. A través de correos electrónicos o llamadas telefónicas, pueden alegar que hay un problema con tu compra o que tienes derecho a algún descuento adicional, entre otras excusas, con el objetivo de obtener más información personal y financiera.

Una vez que los estafadores tienen acceso a tus datos personales a través de etiquetas de paquetes desechadas, pueden realizar varios tipos de fraudes. Pueden hacerse pasar por representantes de tiendas, entidades bancarias u otros servicios, solicitándote información adicional bajo el pretexto de solucionar un problema o brindarte un beneficio. Esta técnica de ingeniería social es efectiva porque las víctimas tienden a confiar en la autenticidad del contacto al reconocer la compra real del artículo.

El objetivo final de estos estafadores es obtener información más sensible, como detalles bancarios, contraseñas y otros datos personales que puedan ser utilizados para acceder a cuentas financieras o realizar transacciones fraudulentas.

Los estafadores buscan en la basura información confiable que pueda ser utilizada en ciberataques. Pueden recuperar una amplia gama de documentos y datos, incluyendo facturas, números de teléfono, direcciones y, en algunos casos, incluso números de tarjetas bancarias. Esta información puede ser utilizada para construir un perfil detallado de la víctima, facilitando ataques de phishing y otras formas de fraude.

Para minimizar el riesgo de ser víctima de estas estafas, es fundamental asegurarse de que ninguna información personal identificable se deseche sin ser destruida adecuadamente. Esto incluye etiquetas de paquetes, documentos financieros y cualquier otro papel que contenga datos personales. Las prácticas recomendadas incluyen triturar documentos antes de desecharlos y borrar o cubrir cualquier información personal de los paquetes.

Además, es importante estar alerta a correos electrónicos y llamadas sospechosas, especialmente aquellas que soliciten información personal o financiera. Verificar siempre la autenticidad del contacto a través de canales oficiales antes de proporcionar cualquier dato.

El ‘dumpster diving’ es una táctica sencilla pero efectiva que los estafadores utilizan para obtener información personal y cometer fraudes. La conciencia y la adopción de medidas de seguridad adecuadas al desechar documentos y paquetes pueden reducir significativamente el riesgo de caer en estas estafas. Es vital destruir cualquier información personal antes de tirarla y mantenerse vigilante ante intentos de phishing y otros engaños. La protección de los datos personales comienza con la gestión cuidadosa de lo que se desecha en la basura

.

> SERVICIOS VERNE PARA PYMES

¿TE GUSTARÍA AMPLIAR INFORMACIÓN O RECIBIR ASESORAMIENTO DE UN ESPECIALISTA?

www.vernegroup.com

CONTACTA