09/03/2022

Alerta de Seguridad Digital

[TLP: GREEN]
[PAP: GREEN]

Exfiltración de Credenciales en Internet

Teniendo en cuenta el incremento durante el último año en la comercialización en la Deep y Dark web de datos sensibles obtenidos de plataformas sobre internet, especialmente mediante la captura de credenciales de acceso empleadas por funcionarios de entidades públicas, el cual ha sido alertado en la reciente comunicación desde el CSIRT del Distrito, que contiene un listado importante de entidades probablemente comprometidas. De esta manera se hace necesario tener en cuenta y aplicar las siguientes recomendaciones con el fin de mitigar el impacto que conlleva esta amenaza y así salvaguardar la información y datos sensibles de ciudadanos, entidades públicas y privadas.
A través de estas capas adicionales de seguridad, los funcionarios de una entidad fortalecen la postura de seguridad, evitando así la fuga de datos, comprometimiento, modificación y captura de información sensible.

Debilidad identificada en la metodología usada por los usuarios:

Cuando los usuarios se autentican con su cuenta de correo personal o corporativa o inclusive con su perfil en las redes sociales en algún servicio aplicación o plataforma, es en este proceso que estos datos son capturados por tecnologías actuales como cookies, certificados digitales, navegadores web y malware y los usuarios finales no tienen las técnicas para proteger sus credenciales y los accesos a sus servicios; es por ello que nombres de usuario, contraseñas e información sensible es capturada y posteriormente ofrecida en foros clandestinos por ciberdelincuentes.

Recomendaciones específicas:

Para prevenir incidentes como fuga de datos y comprometimiento de cuentas de correo y red social siga las siguientes instrucciones para evitar ser víctima de ciberdelincuentes.

- Cambiar absolutamente todas las contraseñas de los servicios, buzones de correo, aplicaciones, redes sociales entre otros.
- Implemente contraseñas robustas, complejas, extensas y con amplia combinación de caracteres, así mismo se deben cambiar periódicamente para evitar ataques de fuerza bruta.

- Use contraseñas diferentes para cada servicio, no use la misma contraseña para los servicios que desea utilizar ya sea de procedencia online o software.
- Aunque es importante cuidar nuestras contraseñas, es más importante no ser el eslabón más débil de la cadena, los atacantes a través de técnicas de ingeniería social pueden sustraer fácilmente información de los funcionarios para comprometer cuentas, ya sea a través de mensajes de texto ofertando servicios o notificando de una supuesta transacción, hasta ataques por llamadas. telefónicas en donde ya hay un acercamiento más directo hacia la víctima.
- Revise en su cuenta de correo las configuraciones de la bandeja de entrada para descartar si se han programado reenvíos automáticos.
- Las siguientes son algunas de las soluciones halladas en el mercado y que generan un token aleatorio de único uso vigente de manera temporal, Estas soluciones se encuentran disponibles para IOS, Android, Windows y MacOS.

    - Google Authenticator
    - Duo Mobile
    - FreeOTP
    - Authy
    - Yandex.Key
    - Microoft Authenticator
- El doble factor por códigos de verificación enviados por mensajes SMS por aplicaciones de autenticación ya non confiables, algunas razones por las cuales ya no se debe fiar de códigos de verificación de SMS, son las siguientes:

    a. Otras personas pueden ver los códigos de verificación si están activadas las notificaciones en las pantallas de bloqueo.
    b. Se puede sustraer la tarjeta sim para insertarla en otro dispositivo móvil y así acceder a códigos de verificación y por ende a las contraseñas.
    c. Los mensajes SMS pueden ser interceptados por un malware hallado en el teléfono móvil.
    d. Una tarjeta SIM puede llegar a ser suplantada o clonada.
    e. Mediante acceso al protocoloSS7 se pueden interceptar llamadas y mensajes SMS.

Recomendaciones Generales

- Realizar periódicamente la evaluación de la postura de seguridad de los servicios expuestos hacia internet frente a los mecanismos de autenticación para los usuarios.
- Implemente copias de seguridad periódicas y actualizadas de modo que haya disponibilidad sobre la última versión de los datos. Salvaguarde dichas copias de seguridad de modo que no puedan ser modificadas o manipuladas.
- Es de suma importancia extender los controles de seguridad sobre los mecanismos de autenticación, las tecnologías y dispositivos empleados para el desarrollo de las actividades de trabajo en casa, remoto o teletrabajo cuando este aplique dentro del modelo de operación.

- La publicación o exposición de servicios hacia internet deben contar con certificados digitales que empleen cadenas de cifrado fuertes y a su vez que el servidor negocie con los equipos clientes a través de aplicaciones seguras y/o navegadores actualizados.
- Implemente la segmentación de red, de manera que no se pueda acceder a los equipos de red desde todos los equipos.
- Habilitar las funciones de tiempo de espera y bloqueo siempre que sea necesaria la autenticación con contraseña. Las funciones de tiempo de espera deben aumentar su duración con los intentos de inicio de sesión fallidos adicionales. Las funciones de bloqueo deben desactivar temporalmente las cuentas después de muchos intentos fallidos consecutivos. Esto puede forzar intentos de fuerza bruta más lentos, haciéndolos inviables.
- Realice jornadas de capacitación y concienciación de los usuarios, funcionarios y colaboradores, en donde se puedan observar las últimas campañas de los ciberdelincuentes junto con vectores de infección más populares.
- Establezca una directriz en donde se ordene a los funcionarios cambiar continuamente las contraseñas de las plataformas a las cuales acceden junto con características de dichas contraseñas.
- Valide continuamente funcionarios que han cambiado de cargo o han sido desvinculados de la entidad y elimine dicho perfil.
- Cambien el nombre de la SSID o de la red inalámbrica y no lo proporcione a público que no le compete, use WPA2/WPA3 para proteger las redes inalámbricas. Evite que se conecten a la red corporativa, dispositivos desconocidos, por el contrario permita el filtrado de direcciones por la dirección MAC de los equipos dentro de la entidad.
- Realice un sondeo del sitio web a fin de identificar servicios que estén abiertos, que no se usen, obsoletos o sean considerados una amenaza de la seguridad (telnet y RDP).
- Parchee sistemas operativos, antivirus y programas con las últimas actualizaciones, NO use bajo ningún motivo aplicaciones obsoletas que ya no cuenten con soporte técnico.
- No inicie sesión con su cuenta de correo o red social corporativa en servicios de uso cotidiano.

Contáctanos

Si tienes alguna consulta técnica comunicarse con ColCERT a través de los siguientes canales:

contacto@colcert.gov.co,
csirtgob@mintic.gov.co

@colCERT

Hechos QUE CONECTAN