Nro. Alerta:	EC-2022-074	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	30-mayo-2022	**Ataques previos al secuestro en cuentas de usuarios web**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Fraude
Tipo de incidente: Phishing
Nivel de riesgo: Alto

II. ALERTA

Ciberdelincuentes emplean diferentes técnicas para realizar el secuestro de cuentas de víctimas en servicios y aplicaciones web.

Figura 1.- lustración asociada a Ransomware
Fuente: Freepik

III. INTRODUCCIÓN

En la actualidad, la creación de cuentas de usuario es un parámetro transversal en diferentes sitios web; siendo el objetivo de los ataques; obtener acceso a cuentas de las víctimas (por ejemplo a sitios web y servicios en línea).

Empresas con diferentes tipos de servicio; orientadas a video conferencia, redes sociales, comercio electrónico, cloud, video hosting, aprendizaje en línea, entre otras; han mejorado diferentes parámetros para evitar el secuestro de cuentas; sin embargo, un aspecto que no se

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

ha considerado es el proceso de creación de cuentas de usuario. A continuación, se mencionan dos maneras para la creación de cuentas:

a) Ruta clásica mediante el ingreso de nombre de usuario y contraseña.
b) Ruta federada a través de un proveedor de identidad **IdP**[1]

En este sentido, aprovechando vulnerabilidades de ciertos sitios web; los ciberdelincuentes pueden secuestrar cuentas incluso antes de que las víctimas registren.

IV. VECTOR DE ATAQUE: Falta de verificación estricta en sitios web.

A continuación, se mencionan las diferentes maneras de adquirir cuentas.

Ataque de combinación federado clásico:

- El atacante usa la cuenta de correo de la víctima para crear una cuenta a través de la ruta clásica.
- El atacante espera a que la víctima cree una cuenta a través de la ruta federada utilizando la misma dirección de correo.
- Si el sitio web no tiene las garantías del caso provocaría; que, tanto el atacante como la víctima tenga acceso a la misma cuenta.

Ataque de identificador de sesión no caducado:

- El atacante usa la cuenta de correo de la víctima para crear una cuenta a través de la ruta clásica.
- El atacante mantiene una sesión activa de larga duración.
- Cuando la víctima recupera la cuenta, el atacante aún podría tener acceso si el restablecimiento de la contraseña no invalidó la sesión del atacante.

Ataque de identificador troyano:

- El atacante usa la cuenta de correo de la víctima para crear una cuenta a través de la ruta clásica y luego agrega un identificador troyano[2] a la cuenta.

[1]Almacena y gestiona las identidades digitales de los usuarios. Los factores de autenticación son Conocimiento (algo que sabes, como un nombre de usuario y una contraseña), Posesión (algo que tienes, como un teléfono inteligente) y cualidades intrínsecas (algo que eres, como tu huella dactilar o un escáner de retina).

[2] Por ejemplo, identidad federada del atacante, dirección de correo del atacante, número de teléfono controlado por el atacante.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-074	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	30-mayo-2022	**Ataques previos al secuestro en cuentas de usuarios web**	V 1.1

- Cuando la víctima restablece la contraseña, el atacante puede usar el identificador troyano para obtener acceso a la cuenta (por ejemplo, restableciendo la contraseña o solicitando un enlace de inicio de sesión único).

Ataque de cambio de correo electrónico no caducado:

- El atacante usa la cuenta de correo de la víctima para crear una cuenta a través de la ruta clásica.
- Posteriormente, realiza el proceso de cambiar la dirección de correo electrónico de la cuenta colocando la cuenta de correo del atacante.
- Como parte de este proceso, el servicio generalmente enviará una URL de verificación a la dirección de correo electrónico del atacante, pero el atacante aún no confirma el cambio.
- Después de que la víctima recuperó la cuenta y comenzó a usarla, el atacante completa el proceso de cambio de correo electrónico para tomar el control de la cuenta.

Ataque de IdP sin verificación:

- El atacante aprovecha un IdP que no verifica la propiedad de una dirección de correo electrónico al crear una identidad federada.
- Usando este IdP no verificador, el atacante crea una cuenta con el servicio de destino y espera a que la víctima cree una cuenta usando la ruta clásica.
- Si el servicio combina incorrectamente estas dos cuentas según la dirección de correo electrónico, el atacante podrá acceder a la cuenta de la víctima.

V. IMPACTO:

El impacto estará en función del servicio de destino comprometido; sin embargo, de manera general se tiene que el atacante estaría en la posibilidad de leer y modificar información confidencial asociada con la cuenta; por ejemplo, mensajes, facturación estados de cuenta, historial de uso, datos de tarjetas de crédito o realizar acciones utilizando la identidad de la víctima por ejemplo, enviar mensajes falsificados, realizar compras utilizando métodos de pago guardados, entre otros.

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- No abrir, manipular, o interactuar, con correos electrónicos altamente sospechosos que lleguen a las bandejas de correo o mensaje en redes sociales.
- Emplear autenticación multifactor.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-074	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	30-mayo-2022	**Ataques previos al secuestro en cuentas de usuarios web**	V 1.1

- Capacitar a todos los usuarios, mediante la concientización y simulaciones para reconocer e informar sobre intentos de phishing e ingeniería social.

VII. Descargo de responsabilidad

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

Cloudflare. (s.f.). *Cloudflare*. Obtenido de Cloudflare: https://www.cloudflare.com/es-es/learning/access-management/what-is-an-identity-provider/

Pavard, A., & Sudhodanan, A. (23 de 05 de 2022). *MSRC-BLOG*. Obtenido de MSRC-BLOG: https://msrc-blog.microsoft.com/2022/05/23/pre-hijacking-attacks/

Toulas, B. (23 de 05 de 2022). *Bleepingcomputer*. Obtenido de Bleepingcomputer: https://www.bleepingcomputer.com/news/security/hackers-can-hack-your-online-accounts-before-you-even-register-them/

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec