# Boletín de Ciberseguridad

Fecha de Publicación
01/08/2022 - N.º 39
Mes de Agosto
18/07/2022 - 01/08/2022

Datasec

# Índice

## Introducción

Por medio de este boletín informativo estaremos destacando de forma quincenal, las noticias más relevantes en el ámbito de la ciberseguridad a nivel regional e internacional.

Las principales categorías de información son: vulnerabilidades tecnológicas, fraudes activos, amenazas por medios informáticos nuevos, así como recomendaciones específicas de prevención. La publicación de dichas noticias dependerá de la importancia y calidad informativa de las mismas.

A su vez se incluyen referencias técnicas y de gestión a los efectos de reducir los riesgos con anticipación y adecuada planificación.

En esta segunda quincena del mes de Julio se destacan 8 noticias de relevancia: 4 sobre vulnerabilidades tecnológicas, 2 de fraudes activos y 2 de prevención.

Aquellas noticias a tener especial recaudo son las siguientes:

Microsoft Añade Medidas de Seguridad Específicas

Microsoft refuerza medidas de seguridad contra el RDP.

Suplantación de correos del Banco Santander

Se encontró una nueva forma de ataque mediante falsos correos suplantando a Banco Santander.

Nueva Ley de Delitos Informáticos

Entró en vigencia una nueva ley de delitos informáticos suplantando la ya existente ley de 1993.


| | | |
|---|---|---|
| Linux | Malware y Rootkit para Linux | CRÍTICO |

## Descripción:

Un malware denominado Lightning Framework que se dirige a los sistemas Linux.

## Estado

Este malware se puede usar como puerta trasera usando SSH e implementar rootkits para cubrir las pistas de los atacantes.
Este malware permite diferentes formas de comunicación con el atacante. Comparada con una navaja suiza este malware todavía no fue del todo analizado y no se sabe exactamente su proveniencia.
Este malware pasa como administrador de contraseñas y claves de cifrado para evadir la detección del sistema infectado. Luego al comunicarse con el servidor comando y control este obtiene sus complementos y el módulo central.

## Remediación / Referencias

Se recomienda mantener actualizado las plataformas.
Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/07/otro-malware-y-rootkit-para-linux.html
https://developer.salesforce.com/docs/atlas.en-us.lightning.meta/lightning/intro_framework.htm

| | | |
|---|---|---|
| Adobe | Empresa Austriaca aprovecha vulnerabilidades Zero - Day | IMPORTANTE |

## Descripción

Una empresa austriaca aprovecha vulnerabilidades de Windows y Adobe de zero - day.

## Estado

La empresa austriaca vende servicios generales de seguridad y análisis de la información, utilizó varios exploit de dìa cero de Windows y Adobe en ataques limitados y altamente dirigidos contra entidades europeas y centroamericanas.

Microsoft está rastreando al actor bajo el apodo KNOTWEED, continuando con su tendencia de nombrar a los PSOA usando nombres dados a árboles y arbustos.
Se sabe que KNOTWEED incursiona tanto en operaciones de acceso y servicio como de piratería informática, ofreciendo su conjunto de herramientas a terceros y asociándose directamente en ciertos ataques.

Si bien las empresas que venden spyware comercial anuncian sus productos como un medio para abordar delitos graves, la evidencia reunida hasta ahora ha encontrado varios casos de estas herramientas siendo mal utilizadas por gobiernos autoritarios y organizaciones privadas para espiar a defensores de los derechos humanos, periodistas, disidentes y políticos.

## Remediación / Referencias

Por mayor información al respecto se puede acceder a:
https://thehackernews.com/2022/07/microsoft-uncover-austrian-company.html

| | | |
|---|---|---|
| | Filtrado de Datos de Twitter | CRÍTICO |

## Descripción:

Se filtraron 5,2 usuarios de Twitter y se pusieron a la venta.

## Estado

Twitter sufrió una filtración de datos, se utilizó una vulnerabilidad con la que se creó una base de número de teléfono y direcciones de correo.

El atacante es conocido por el sobrenombre Devil, luego de realizar este ataque compartió los usuarios robados, hasta el momento Twitter no confirma violación de datos, pero investiga la autenticidad de las afirmaciones.

Cabe destacar que al tener esta información el atacante o los compradores pueden realizar ataques dirigidos a estos usuarios.

## Remediación / Referencias

Los usuarios de Twitter deben estar atentos al recibir correos electrónicos que piden que ingrese las credenciales de inicio de sesión.

También se recomienda cambiar la contraseña y activar el 2FA en la cuenta de Twitter.

Por mayor información acceder a:
https://blog.segu-info.com.ar/2022/07/54-millones-de-usuarios-de-twitter-la.html
https://www.infobae.com/america/tecno/2022/07/26/filtraron-datos-de-mas-de-5-millones-de-usuarios-de-twitter/

| Microsoft | Microsoft Añade Medidas de Seguridad Específicas | CRÍTICO |
|---|---|---|

## Descripción:

Microsoft refuerza medidas de seguridad contra el RDP.

## Estado

Debido al aumento de ataques RDP, Microsoft decidió añadir la medida de seguridad, esta medida bloquea automáticamente las cuentas durante 10 minutos tras 10 intentos de inicio de sesión no válidos. Con esta medida se consigue complicar los ataques de fuerza bruta, desincentivándolos. No obstante, ya era posible activar esta medida en Windows, ahora esta medida de seguridad viene por defecto.

Se espera que esta medida de seguridad sea aplicada a todos los productos de Windows.

Esta medida de protección podría ser explotada por los grupos de ciberdelincuentes para orquestar un ataque de denegación de servicio (DoS), pero con esta medida de seguridad Microsoft prevé disminuir estos ataques.

## Remediación / Referencias

Se recomienda actualizar Windows.
Por mayor información acceder a:
https://docs.microsoft.com/es-es/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol
https://blog.segu-info.com.ar/2022/07/microsoft-refuerza-rdp-contra-ataques.html


| | | |
|---|---|---|
| Santander | Suplantación de correos del Banco Santander | IMPORTANTE |

## Descripción

Se encontró una nueva forma de ataque mediante falsos correos suplantando a Banco Santander

## Estado

Los usuarios del Banco Santander pueden recibir mensajes explicando que se le ha bloqueado la cuenta debido a una falla en el Banco y para poder desbloquearla debe de ingresar al link adjunto e ingresar la información pedida. Mensajes parecidos a estos no provienen del Banco Santander, los atacantes utilizan este medio para poder obtener los datos de las víctimas, credenciales y así acceder a su cuenta.

## Remediación / Referencias

Se recomienda no abrir correos ni mensajes de dudosa procedencia, desconfiar de los enlaces y archivos en los mensajes o correo y mantener actualizadas las plataformas.
Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/alertas/8fph22-00561-01/
https://www.santander.com.uy/si-sospech%C3%A1s-reportalo

| Microsoft | Ciberataques por el bloqueo de Macros | CRÍTICO |
|---|---|---|

## Descripción

Microsoft ha realizado un bloqueo de macros, de forma predeterminada, permitiendo nuevas formas de realizar ataques.

## Estado

Microsoft bloqueó los macros. Al no existir macros lo usuarios buscan formas alternativas en archivos contenedores como pueden ser ISO, .RAR y LNK (archivos de acceso directo a Windows).

Los atacantes utilizan estas alternativas para poder distribuir archivos que contengan malware.
Los malware se distribuyen mediante email, utilizando ingeniería social y enviando el archivo a los usuarios que confían.

## Remediación / Referencias

Se recomienda no compartir información de seguridad personal con otros, evaluar de donde salen los mails que le fueron enviados y no descargar archivos que no son de fuentes confiables.

Por mayor información al respecto se puede acceder a:
https://docs.microsoft.com/es-es/microsoft-365/security/intelligence/macro-malware?view=o365-worldwide
https://thehackernews.com/2022/07/hackers-opting-new-attack-methods-after.html


| | | |
|---|---|---|
| | Consejos por estafas mediante Whatsapp | PREVENCIÓN |

## Descripción

Debido al aumento de estafas por Whatsapp INCIBE comparte consejos para prevenir.

## Afectados

WhatsApp cuenta con miles de usuarios alrededor del mundo, convirtiéndose en objetivo para los atacantes el secuestro de Whatsapp, donde, con ayuda de las víctimas, logran tomar control del Whatsapp.
Al intentar ingresar a Whatsapp por primera vez, este pide un código de verificación que es enviado por SMS al teléfono al que se quiere acceder, es ese momento los atacantes mandan un mensaje a la víctima pidiendo ese código de verificación que lo ha enviado sin querer a ese celular, si la víctima le entrega el código de verificación se concluye en secuestro del Whatsapp permitiendo a los atacantes ingresar. Debido a esto, mercurio sacó unos consejos para poder no caer en estos ataques.

## Remediación / Referencias

Se recomienda leer el manual de consejos:
https://www.csirt.gob.cl/recomendaciones/ciberconsejos-como-prevenir-el-secuestro-de-whatsapp/
Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/noticias/el-mercurio-estafas-whatsapp/

| CSIRT | Nueva Ley de Delitos Informáticos | PREVENCIÓN |
|---|---|---|

## Descripción

Entró en vigencia una nueva ley de delitos informáticos suplantando la ya existente ley de 1993.

## Afectados

La nueva ley que entró en vigencia en Chile facilita la persecución de los delincuentes informáticos a través de las fronteras internacionales, también redefinen los tipos legales y agregando agravantes.

Algunos agravantes que se pueden leer es esta ley son el abuso de confianza en caso de administrar sistemas informáticos, también se considera agravante si al realizar un ataque este perjudica a servicios públicos y el desarrollo normal de los procesos electorales.

## Remediación / Referencias

Se recomienda leer la ley, la puedes encontrar en PDF en el siguiente link:
https://www.diariooficial.interior.gob.cl/publicaciones/2022/06/20/43283/01/2145558.pdf
Por mayor información al respecto se puede acceder a:
https://www.csirt.gob.cl/noticias/nueva-ley-de-delitos-informaticos-entro-en-vigor/

## Conclusiones

Los logros a nivel constitucional de leyes de protección de datos y de delitos informáticos como la que logró decretarse en Chile, es un evento muy importante y destacable a nivel latinoamericano y mundial.

Todos los avances que desde las directivas gubernamentales y empresariales se encaminan en pavimentar y recorrer juntos los senderos de la confianza garantizada, a través de asegurar la información, permitirá que la evolución florezca. De esta manera es que se lleva a estados más elevados de seguridad y confianza en conjunto, que permiten crecimientos de relaciones comerciales, así como crear valor en todos los procesos organizacionales.

Las leyes y reglamentos que se extiendan a ámbitos legales y de demás jurisprudencia, es fundamental para contrarrestar todos los aspectos que son más humanos en las relaciones con la información y los medios digitales.

Enhorabuena por los ciudadanos de Chile por sus avances y a seguir avanzando en estos temas que nos ocupan a todos.