Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

03-06-2022 | Año 4 | N°152

Boletín de Seguridad Cibernética

Semana del 27 de mayo
al 2 de junio de 2022

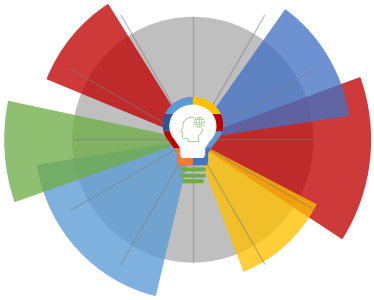
La semana en cifras

Parches

25

para vulnerabilidades

Sus mitigaciones son útiles en productos de Microsoft y Google.



Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

7

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Phishing 2
Vulnerabilidades 4
Actualidad 5
Muro de la Fama 10

Phishing

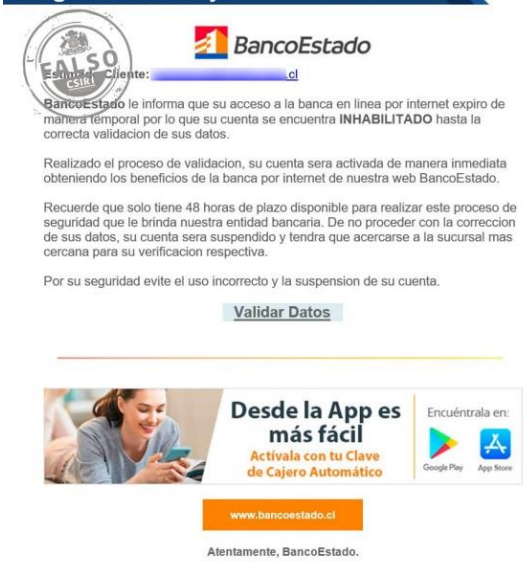
Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00532-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de mayo de 2022
Última revisión	27 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
https://bamco-ltau.cl-zzvv[.]buzz/1653598918/bancochile-web/persona/login/index.html/login	
IP	
[192.185.49.180]	
[172.67.155.66]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00532-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00532-01.pdf	

Imagen del mensaje

CSIRT advierte phishing con falso envío suplantando a CorreosChile	
Alerta de seguridad cibernética	8FPH22-00533-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2022
Última revisión	30 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
http://cmi.versatecnologia.com[.]br/js/CELLO/index/	
IP	
[101.53.144.229]	
[104.131.88.122]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00533-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00533-01-1.pdf	

Imagen del mensaje



CSIRT advierte phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00534-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2022
Última revisión	30 de mayo de 2022
Indicadores de compromiso	
URL redirección	
https://koskuflat[.]com/control/cuenta-spjw/	
URL sitio falso	
https://pr4ctik4.tarabgin[.]ir/fdasuy/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[186.64.121.148]	
[185.51.202.58]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00534-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00534-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00535-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2022
Última revisión	31 de mayo de 2022
Indicadores de compromiso	
URL Redirección	
https://noxpro2[.]com/activacion/cuenta-taiu/	
URL sitio falso	
https://cnhrd.tarabgin[.]ir/ztkug/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[168.232.165.154]	
[185.51.202.58]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00535-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00535-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00649-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2022
Última revisión	30 de mayo de 2022
CVE	
CVE-2022-1853 - CVE-2022-1854 - CVE-2022-1855 CVE-2022-1856 - CVE-2022-1857 - CVE-2022-1858 CVE-2022-1859 - CVE-2022-1860 - CVE-2022-1861 CVE-2022-1862 - CVE-2022-1863 - CVE-2022-1864 CVE-2022-1865 - CVE-2022-1866 - CVE-2022-1867 CVE-2022-1868 - CVE-2022-1869 - CVE-2022-1870 CVE-2022-1871 - CVE-2022-1872 - CVE-2022-1873 CVE-2022-1874 - CVE-2022-1875 - CVE-2022-1876	
Fabricante	
Google	
Productos afectados	
Chrome, versiones anteriores a la 102.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00649-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00649-01.pdf	

CSIRT alerta de vulnerabilidad en la Microsoft Support Diagnostic Tool	
Alerta de seguridad cibernética	9VSA22-00650-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de mayo de 2022
Última revisión	31 de mayo de 2022
CVE	
CVE-2022-30190	
Fabricante	
Microsoft	
Productos afectados	
Windows.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00650-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00650-01.pdf	

Actualidad

Alerta de Seguridad Cibernética | Agent Tesla

El CSIRT de Gobierno informó esta semana sobre un prominente RAT, denominado Agent Tesla, sus características y las mejores formas de evitar su accionar sobre los sistemas

Dejamos el texto de la alerta a continuación. También pueden encontrarlo aquí: csirt.gob.cl/noticias/alerta-agent-tesla/.

Descripción

Agent Tesla es una amenaza de tipo troyano de acceso remoto, o RAT, por su sigla en inglés. También se cuenta dentro del "Malware as a Service", o sea, malware que cualquier ciberdelincuente puede comprar listo para usar e incluso conseguirlo como una suscripción, hasta con soporte 24/7.

Está destinado principalmente a robar información de sus víctimas. Contempla varias capas de ofuscación, lo que le hace difícil de detectar (por ejemplo, puede detectar si está siendo abierta en una sandbox) y además despliega técnicas para ser una amenaza persistente, todas características que explican su extendida popularidad, siendo que data de 2014.

Capacidades

Una vez desplegado, Agent Tesla realiza numerosas operaciones de espionaje en un equipo:

- Registra lo que se digita (keylogging).
- Toma capturas de pantalla.
- Ve y copia lo que hay en el Portapapeles.
- Roba contraseñas y cookies de múltiples programas, incluyendo: decenas de buscadores web, incluyendo Google Chrome, Microsoft Edge, Mozilla Firefox y Opera; VPN como Open VPN y NordVPN y también Microsoft Outlook.
- Recopila información como nombre del equipo, sistema operativo, CPU, RAM, TCP hostname, cliente DNS, IP pública, dominio y más.
- Luego de tomar esta información, Agent Tesla la filtra al ciberdelincuente, comunicación que mantiene anónima usando un cliente TOR. Del mismo modo se comunica con su servidor de comando y control.

- También puede comunicarse con el atacante a través del protocolo SMTP de correo electrónico, o incluso por Telegram.

Indicadores de Compromiso (IOC)

Sender de Correo
3.133.219.78

9ecf32d40c78a12f43bad7283ac48a98fcdbe1f8dec70fda7df32396f0b69cbf
efac67b547566d4257e435b854da761a1f6892aef4da1c0faed3780c486a25e2
d7dc14b7811f44ecfe82059fcce4300044d34eb9a1e6cba4d25ade821294c809
250dba6f1c65b7e40d352be174ebde12de162ef61ad9be23ac155b6f0a088c5b
7a2a8ba85c73c9b5179cfe2c1598b14b774f7817a935af6d824fb39f2eea1d09
4196ac36c2e960a9c3b602394b6867e9503417a265c48552a8d5c0cfe4d17231
46c460618cb9a10c78dfaedc27e188dcc393589187d751be6e5b1183c5720e70
3d5a618b9509b6a8426aa13d8a32aa4156c4e1aa3b20ac98ab3a0fd449088d66

URL

https://terrazzaitaliana.mx/hrt/Gxuvqbqz_Skhciiey[.]bmp

Recomendaciones

- Mantener todos sus programas y especialmente antivirus, antimalware, firewall y otros software de seguridad actualizados, junto con mantener un esquema de parchados regulares.
- Reforzar todas las protecciones que debemos tener ante el phishing, principalmente nunca hacer clic en enlaces provenientes de mensajes no solicitados de email, SMS o redes sociales.
- Revisar que el mensaje provenga realmente de quien dice venir y si hay dudas llamar directamente al remitente para saber si el mensaje es real.
- Fijarse en la extensión del archivo. La última porción es la que determina de qué tipo de archivo se trata. Si dice .pdf.exe, por ejemplo, significa que es un archivo ejecutable.
- Tampoco ingresar sus credenciales a un sitio abierto desde un enlace. Mejor abrir directamente la página que queremos escribiendo su dirección en el navegador.
- No hacer descargas de archivos sospechosos, como películas o juegos piratas.
- Desactivar los macros en documentos que llegan por email.

- Evitar entregar privilegios de Administrador a usuarios, y solo acceder a como Administrador a los equipos por el tiempo que sea necesario. Evitar abrir documentos mientras se está loggeado como Administrador.

Ciberdiccionario Volumen 7

Esta semana, en un nuevo volumen de nuestro Ciberdiccionario, definimos Amenazas Avanzadas Persistentes, Análisis forense, Contraseñas robustas y Cifrado de extremo a extremo. Pueden verlo también aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-7/.

Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510 siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- María Inés Foix
- Nashla Araya
- Jorge Muñoz
- Víctor Colipí
- Francisca Alarcón
- Álex Cruz
- María Gabriela Fernández
- Franco Sanllehi
- Víctor Tapia
- Tammy Aguilera
- Isidora Agüero
- Cristián Acuña
- Gonzalo Araya
- Andrés Aldana
- Renato Cuellar

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.06.03 16:50:11 -04'00'