Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

10-09-2021 | Año 3 | N°114

Boletín de Seguridad Cibernética

Semana del 4 al 9 de septiembre de 2021

La semana en cifras

Hash

4

SHA

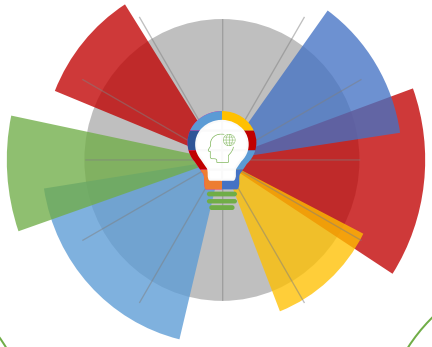
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

5

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

1

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft.

IP

4

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

Malware

CSIRT alerta de nueva campaña de malware con falso documento	
Alerta de seguridad cibernética	2CMV21-00220-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de septiembre de 2021
Última revisión	9 de septiembre de 2021
Indicadores de compromiso	
SHA256	
652BC4540760E11A3C230517E8063C55587AA29D3FA132EE9B4D050F0FA77A92 BDBFB1EB22E055C50DAA28F2F6C0CF8DC03F5FF5EBC229289FCC7739EEFAD60B	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00220-01/	
https://csirt.gob.cl/media/2021/09/2CMV21-00220-01.pdf	

CSIRT alerta de nueva campaña de malware con falso documento	
Alerta de seguridad cibernética	2CMV21-00221-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de septiembre de 2021
Última revisión	9 de septiembre de 2021
Indicadores de compromiso	
SHA256	
ED907DDF528A4DF0B078AC4B1B8949F429B59ECFC96EE4426E90A102AA6F66EF 9710BAC1236CCC3B80610209B7F03732BE51FA32BC2A4814878EC9C2CC027AC7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00221-01/	
https://csirt.gob.cl/media/2021/09/2CMV21-00221-01.pdf	

Sitios fraudulentos

Imagen del sitio

CSIRT alerta ante página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01009-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://5antand3r[.]xyz/1630675052/personas/index.asp	
IP	
[68.65.120.250]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01009-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01009-01.pdf	

Imagen del sitio

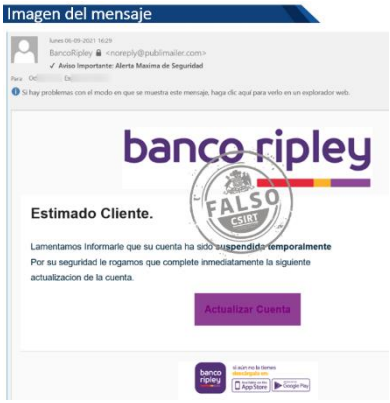
CSIRT alerta ante una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01010-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de septiembre de 2021
Última revisión	3 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://santander.bancapersonas[.]xyz/1630675134/personas/index.asp	
IP	
[198.54.115.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01010-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01010-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH21-00431-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de septiembre de 2021
Última revisión	6 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
http://clinfosupp.temp.swtest[.]ru/blo/maa9/z0n51/cc.php	
IP	
[181.114.212.148]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00431-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00431-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH21-00432-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de septiembre de 2021
Última revisión	7 de septiembre de 2021
Indicadores de compromiso	
URL redirección	
http://rimtrome[.]com/activacion/cuenta-sqcz/	
URL sitio falso	
https://forum.kmsinversiones[.]com/login	
IP	
[192.141.51.210]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00432-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00432-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad zero-day crítica en Microsoft Windows	
Alerta de seguridad cibernética	9VSA21-00488-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de septiembre de 2021
Última revisión	8 de septiembre de 2021
CVE	
CVE-2021-40444	
Fabricante	
Microsoft	
Productos afectados	
Microsoft Windows	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00488-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00488-01.pdf	

Actualidad

Alerta ante filtración de casi 500 mil credenciales de autenticación de VPN Fortinet por parte de cibercriminales internacionales

Ante la divulgación por parte de una banda de cibercriminales de casi 500 mil credenciales de autenticación de distintos productos VPN provistos por Fortinet, el CSIRT de Gobierno llama a los encargados de ciberseguridad que administren VPN de Fortinet a forzar el cambio de contraseñas, entre otras medidas urgentes que se detallan aquí: csirt.gob.cl/noticias/alerta-ante-filtracion-de-claves-de-vpn-fortinet-septiembre-2021/.

Las vulnerabilidades que habrían hecho posible el robo de las credenciales ya habían sido comunicadas por el proveedor:

CVE-2020-12812 de 2020: https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00272-01/.

CVE-2018-13379 de 2019: https://www.csirt.gob.cl/vulnerabilidades/9vsa-00032-001-csirt-comparte-actualizaciones-de-fortninet-para-varios-de-sus-productos/.

CVE-2019-5591 de 2019: https://www.fortiguard.com/psirt/FG-IR-19-037.

Amenazas Cibernéticas No. 28 | Ciberamenazas en redes industriales

Volvieron los informes de la serie Amenazas Cibernéticas al CSIRT de Gobierno. Este informe número 28 lo elaboró Matías Bendel, ingeniero certificado en CISSP y perteneciente al equipo de IBM.

El experto se aboca a explicar las implicancias de la convergencia entre los sistemas de las tecnologías de la información (TI) y las redes industriales (OT), que permite hacer más eficiente y adaptable la producción pero también expone procesos industriales a las amenazas que acechan en internet.

Pueden enterarse de todos los detalles aquí: https://www.csirt.gob.cl/reportes/ciberamenazas-en-redes-industriales-amenazas-ciberneticas-no-28/.

La Implementación del Mes | No. 3 Seguridad Aplicada: Wazuh

Septiembre traen el tercer volumen de La Implementación del Mes, dedicada a Wazuh. Esta es una solución de monitoreo de seguridad gratuita, de código abierto y lista para la detección de amenazas, monitoreo de integridad, respuesta a incidentes y cumplimiento.

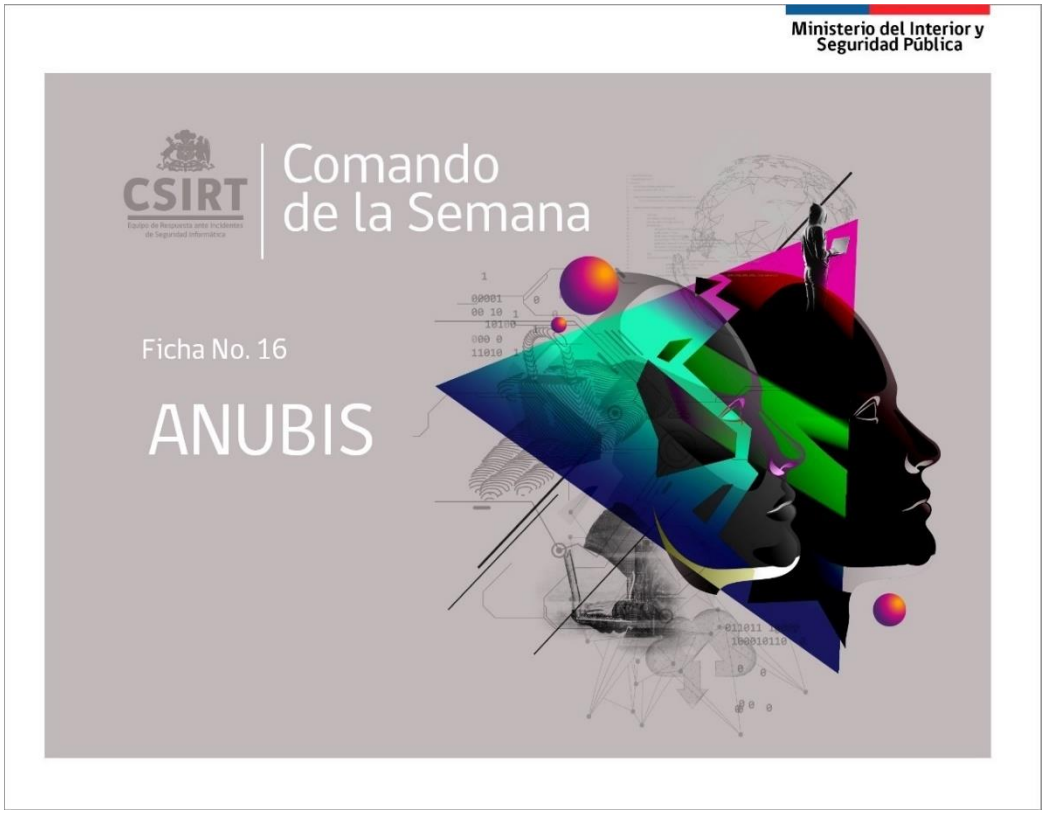
Wazuh se utiliza para recopilar, agregar, indexar y analizar datos de seguridad, lo que ayuda a las instituciones a detectar intrusiones, amenazas y anomalías de comportamiento. Pueden enterarse de todos los detalles aquí: https://www.csirt.gob.cl/estadisticas/la-implementacion-del-mes-no-3/.

El Comando de la Semana | No. 16 Anubis

Para comenzar septiembre en El Comando de la Semana les traemos nada menos que a una deidad egipcia, Anubis. Esta es una herramienta de recopilación de información y enumeración de subdominios, desde una variedad de fuentes, incluidos HackerTarget, DNSDumpster, certificados x509, VirusTotal, Google, Pkey, Sublist3r, Shodan y NetCraft. Anubis también tiene un proyecto hermano, AnubisDB, que sirve como un repositorio centralizado de subdominios.

El objetivo de estos comandos que compartimos semanalmente no es reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Pueden encontrar el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-16/.



El Control de la Semana | No. 10 Controles contra Códigos Maliciosos

La Ficha de Control Normativo de esta semana trata sobre controles contra códigos maliciosos, parte de la implementación de la Política General de Seguridad de la Información en una organización. Esta a su vez debe estar armonizada con una adecuada política específica de Seguridad de las Operaciones, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Dentro de aquella Política de Seguridad de las Operaciones deberemos implementar una serie de directrices para evitar el ingreso de software malicioso (malware) a nuestra institución.

Por lo anterior, en el documento descargable a continuación, encontrarán los detalles más importantes a tener en consideración al momento de definir nuestros controles contra códigos maliciosos.

Pueden descargar esta nueva ficha semanal, aquí: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-10/.

Recomendaciones y buenas prácticas

Recomendaciones generales de seguridad

- 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 +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Francisco Javier Gutiérrez
- Tomás Eduardo Gaete Fischer
- Gonzalo Arturo Villegas Soto
- Camilo Córdova
- Álvaro Villalón
- Matías Alejandro Fredes Galarce

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.16 12:38:55 -03'00'