Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

16-09-2021 | Año 3 | N°115

Boletín de Seguridad Cibernética

Semana del 10 al 15 de septiembre de 2021

La semana en cifras

Hash

0

SHA

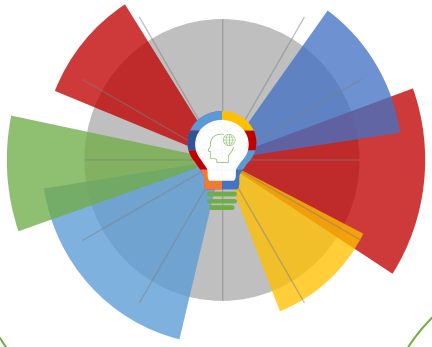
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

5

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

81

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft, Apple, Adobe, F5, Citrix y WordPress.

IP

3

Informadas

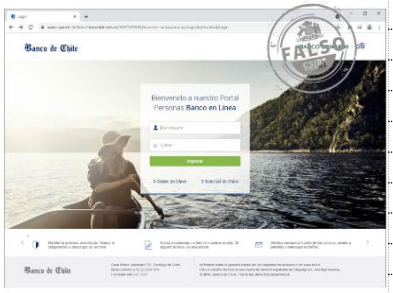
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR21-01011-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre de 2021
Indicadores de compromiso	
URL sitio falso	
https://wwv.soporte-bchile.cl.bonafidelabs[.]in/1631539133/bcochile-web/persona/login/index.html/login	
IP	
[198.136.51.114]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01011-01/	
https://www.csirt.gob.cl/media/2021/09/8FFR21-01011-01.pdf	

Phishing

Imagen del Sitio

CSIRT alerta ante campaña de smishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH21-00433-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bitly[.]com/3trinkD	
URL sitio falso	
https://inicio.web-estadon[.]fun/	
IP	
[104.21.74.85]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00433-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00433-01.pdf	

Imagen del sitio

CSIRT alerta de campaña de smishing que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH21-00434-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre de 2021
Indicadores de compromiso	
URL de SMS	
https://bitly[.]com/3k2dueU	
URL sitio falso	
http://r.banco-santander[.]ltd/r/fz09Qi2	
IP	
[104.21.65.192]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00434-01/	
https://www.csirt.gob.cl/media/2021/09/8FPH21-00434-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades en WordPress	
Alerta de seguridad cibernética	9VSA21-00489-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de septiembre de 2021
Última revisión	13 de septiembre de 2021
CVE	
CVE-2021-39200	
CVE-2021-39201	
CVE-2021-39202	
CVE-2021-39203	
Fabricante	
F5	
Productos afectados	
WordPress 5.0 a 5.8.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00489-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00489-01.pdf	

CSIRT alerta de vulnerabilidades en Citrix Hypervisor Security	
Alerta de seguridad cibernética	9VSA21-00490-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2021
Última revisión	14 de septiembre de 2021
CVE	
CVE-2021-28694	
CVE-2021-28697	
CVE-2021-28698	
CVE-2021-28699	
CVE-2021-28701	
Fabricante	
Citrix	
Productos afectados	
Citrix Hypervisor (todas las versiones)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00490-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00490-01.pdf	

CSIRT advierte de vulnerabilidades en BIG-IP APM de F5	
Alerta de seguridad cibernética	9VSA21-00491-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2021
Última revisión	14 de septiembre de 2021
CVE	
CVE-2021-23052 CVE-2021-23053	
Fabricante	
F5	
Productos afectados	
BIG-IP APM 13.1.0 – 13.1.4, 14.1.0 – 14.1.4, 15.1.0 – 15.1.2.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00491-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00491-01.pdf	

CSIRT alerta ante vulnerabilidades críticas en productos Apple	
Alerta de seguridad cibernética	9VSA21-00492-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de septiembre de 2021
Última revisión	14 de septiembre de 2021
CVE	
CVE-2021-30858 CVE-2021-30860	
Fabricante	
Apple	
Productos afectados	
Apple Safari: 14.0 a 14.1.2 watchOS: 7.0 18R382 a 7.6.1 18U70 macOS: 10.15 19A583 a 10.15.7 19H1323 macOS: 11.0 20A2411 a 11.5.2 20G95. Apple iOS: 14.0 18A373 a 14.7.1 18G82 iPadOS: 14.0 18A373 a 14.7.1 18G82	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00492-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00492-01.pdf	

CSIRT comparte vulnerabilidades compartidas por Microsoft en su Update Tuesday de septiembre	
Alerta de seguridad cibernética	9VSA21-00493-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de septiembre de 2021
Última revisión	15 de septiembre de 2021

CVE

CVE-2021-26434	CVE-2021-36966	CVE-2021-38634	CVE-2021-38653
CVE-2021-26435	CVE-2021-36967	CVE-2021-38635	CVE-2021-38654
CVE-2021-26436	CVE-2021-36968	CVE-2021-38636	CVE-2021-38655
CVE-2021-26437	CVE-2021-36969	CVE-2021-38637	CVE-2021-38656
CVE-2021-26439	CVE-2021-36972	CVE-2021-38638	CVE-2021-38657
CVE-2021-36930	CVE-2021-36973	CVE-2021-38639	CVE-2021-38658
CVE-2021-36952	CVE-2021-36974	CVE-2021-38641	CVE-2021-38659
CVE-2021-36954	CVE-2021-36975	CVE-2021-38642	CVE-2021-38660
CVE-2021-36955	CVE-2021-38624	CVE-2021-38644	CVE-2021-38661
CVE-2021-36956	CVE-2021-38625	CVE-2021-38645	CVE-2021-38667
CVE-2021-36959	CVE-2021-38626	CVE-2021-38646	CVE-2021-38669
CVE-2021-36960	CVE-2021-38628	CVE-2021-38647	CVE-2021-38671
CVE-2021-36961	CVE-2021-38629	CVE-2021-38648	CVE-2021-40440
CVE-2021-36962	CVE-2021-38630	CVE-2021-38649	CVE-2021-40444
CVE-2021-36963	CVE-2021-38632	CVE-2021-38650	CVE-2021-40447
CVE-2021-36964	CVE-2021-38633	CVE-2021-38651	CVE-2021-40448
CVE-2021-36965		CVE-2021-38652	

Fabricante

Microsoft

Productos afectados

Accessibility Insights for Android
Azure Open Management Infrastructure
Azure Sphere
HEVC Video Extensions
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 Business Central 2020 Release Wave 2 – Update 17.10
Microsoft Dynamics 365 Business Central 2021 Release Wave 1 – Update 18.5
Microsoft Edge (Chromium-based)
Microsoft Edge for Android
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)

Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 – 16.3)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
MPEG-2 Video Extension
Visual Studio Code
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server, version 2004 (Server Core installation) Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00493-01
https://www.csirt.gob.cl/media/2021/09/9VSA21-00493-01.pdf

CSIRT alerta ante vulnerabilidades críticas en productos Apple	
Alerta de seguridad cibernética	9VSA21-00494-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de septiembre de 2021
Última revisión	15 de septiembre de 2021
CVE	
CVE-2021-30858 CVE-2021-30860	
Fabricante	
Apple	
Productos afectados	
Apple Safari: 14.0 a 14.1.2 watchOS: 7.0 18R382 a 7.6.1 18U70 macOS: 10.15 19A583 a 10.15.7 19H1323 macOS: 11.0 20A2411 a 11.5.2 20G95. Apple iOS: 14.0 18A373 a 14.7.1 18G82 iPadOS: 14.0 18A373 a 14.7.1 18G82	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00494-01	
https://www.csirt.gob.cl/media/2021/09/9VSA21-00494-01.pdf	

Actualidad

Comenzaron las inscripciones para el Segundo Simposio de Ciberseguridad para Funcionarios Públicos, realizado por el CSIRT de Gobierno

Como CSIRT de Gobierno nos complace invitar a la comunidad nacional de la ciberseguridad a participar este martes 28 de septiembre de nuestro Segundo Simposio de Ciberseguridad para Funcionarios Públicos, dirigido principalmente a los encargados de ciberseguridad de organismos del Estado pero abierto a todos quienes quieran participar (inscripciones aquí: https://simposio-ciberseguridad.csirt.gob.cl).

Las clases y talleres del simposio, realizadas todas por funcionarios del CSIRT de Gobierno tocarán una serie de temas, como el uso de herramientas *open source*, los conceptos clave que determinan la seguridad de las páginas web, los controles para mitigar las amenazas de ciberseguridad y los procedimientos necesarios para conseguir la revocación de nombres de dominio.

Los cupos disponibles son limitados y se asignaran por orden de inscripción. La inscripción debe verificarse con el correo institucional o corporativo.

Fecha: Martes 28 de septiembre de 2021.

Horario: Desde las 09:00 horas. La agenda detallada y más información aquí: https://www.csirt.gob.cl/noticias/comienzan-las-inscripciones-para-el-segundo-simposio-de-ciberseguridad-para-funcionarios-publicos-realizado-por-el-csirt-de-gobierno/.

Los invitamos a registrarse en el siguiente link: https://simposio-ciberseguridad.csirt.gob.cl/ .

Agenda/Simposio 2021

am	08:45	**Registro en la Plataforma**	
	9:00-9:15	**Ceremonia de apertura.**	Juan Francisco Galli Basili, Subsecretario del Interior
	9:15-10:00	**Charla 1**	Director CSIRT Sr Carlos Landeros
	10:00-10:55	**Taller 1: Usando un SIEM (opensource): WAZUH**	Hernan Espinoza Analista CSIRT
	11:00- 11:55	**Taller 2: Usando un HONEY-POT (opensource): T-POT**	Miguel Kurte Analista CSIRT
pm	12:00- 12:30	**Charla 2: Seguridad en sitios web (introducción teórica) [1/3]**	Natalia Perez Analista CSIRT
	12:35- 13:35	**Taller 3 (primera parte): Seguridad en sitio web (herramientas y verificación práctica) [2/3]**	Juan Sanhueza Analista CSIRT
	14:30-15:25	**Taller 3 (segunda parte): Seguridad en sitio web (herramientas y verificación práctica) [3/3]**	Juan Sanhueza Analista CSIRT
	15:30- 16:25	**Charla 3: Controles para mitigar amenazas en ciberseguridad (30 controles prioritarios)**	Gonzalo Conch Analista CSIRT
	16:30- 17:25	**Revocación de nombres de dominio**	Cristobal Hammersley Abogado CSIRT
	17:30-17:40	**Cierre del evento**	

El Comando de la Semana | No. 17 Sublist3r

Esta semana, el comando protagonista fue Sublist3r, herramienta de Python diseñada para enumerar subdominios de sitios web que usa OSINT. Así, ayuda a los probadores de penetración y cazadores de errores a recopilar subdominios usando motores de búsqueda como Google, Yahoo, Bing, Baidu y Ask.

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.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-17/.

El Control de la Semana | No. 11 Respaldo de la información

La Ficha de Control Normativo de esta semana trata sobre controles que entregan los lineamientos para desarrollar una adecuada estrategia de respaldo de la información de nuestra organización.

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-11/.

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.

- Pedro Arnaldo Rodríguez Brito
- Francisco Javier Gutiérrez
- Francisca Camila Araya Ravanal
- Matías Nicolás Marchant Bórquez
- José Ignacio Parra
- Rodrigo Cortés

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.16 13:36:39 -03'00'