CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 206

semana del 9 al 15 de junio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

22

IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

23

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

101

Las mitigaciones son útiles en productos de Adobe, Microsoft y Fortinet.

HASH REPORTADOS

2

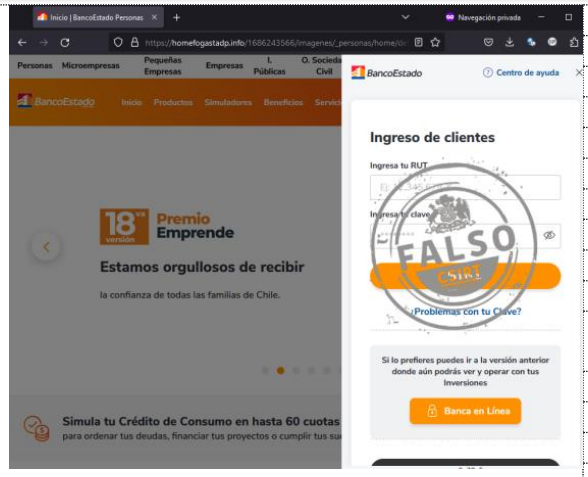
Hashes asociados a múltiples campañas de phishing con archivos que contienen malware

CONTENIDO

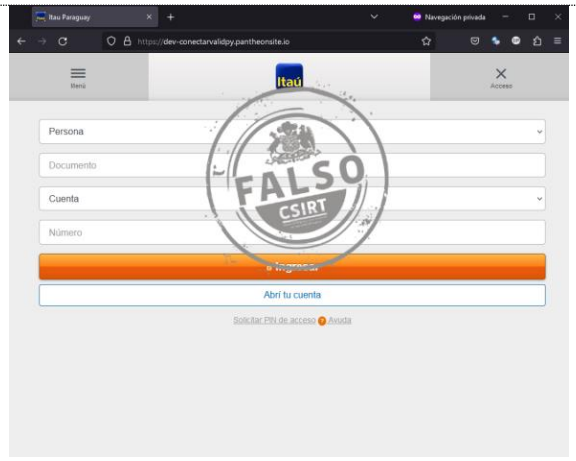
1. Sitios fraudulentos 3
2. Phishing 8
3. Ataques de fuerza bruta 10
4. Malware 11
5. Vulnerabilidades 12
6. Concientización 17
7. Recomendaciones y buenas prácticas 20
8. Muro de la Fama 21

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

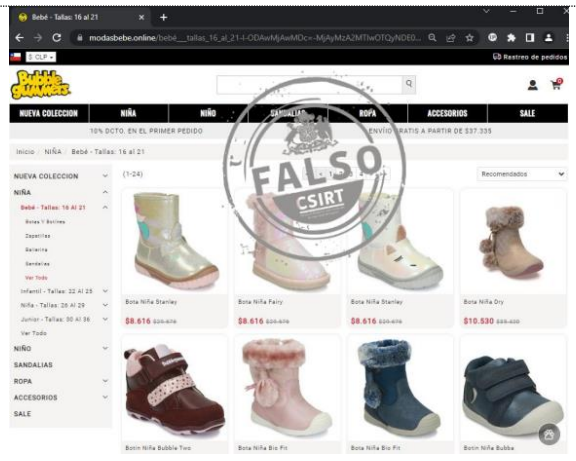
1. Sitios fraudulentos



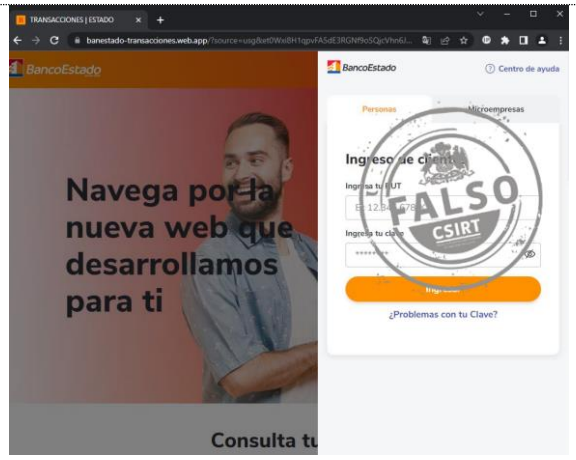
CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01396-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2023
Última revisión	9 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://homefogastadp[.]info/1686243474/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.143.106]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01396-01	



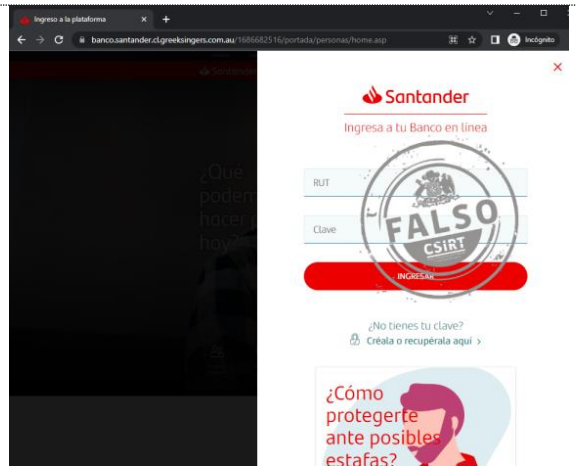
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Banco Itaú	
Alerta de seguridad cibernética	8FFR23-01397-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2023
Última revisión	9 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
http://dev-conectarvalidpy.pantheonsite.io	
Dirección IP	
[23.185.0.4]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01397-01	



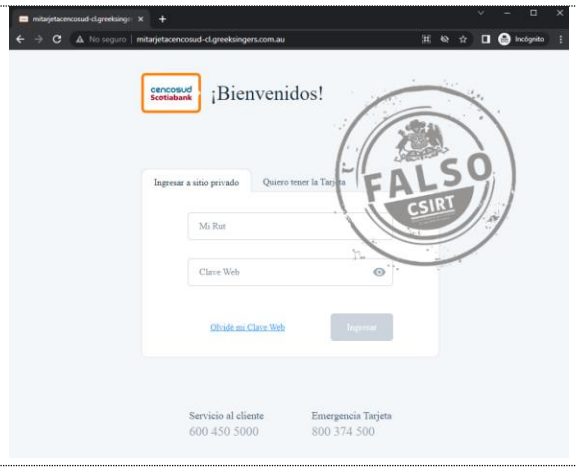
CSIRT alerta de nuevo sitio fraudulento que suplanta a Bubble Gummers	
Alerta de seguridad cibernética	8FFR23-01398-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de junio de 2023
Última revisión	12 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.modasbebe[.]online/	
Dirección IP	
[107.150.177.17]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01398-01	



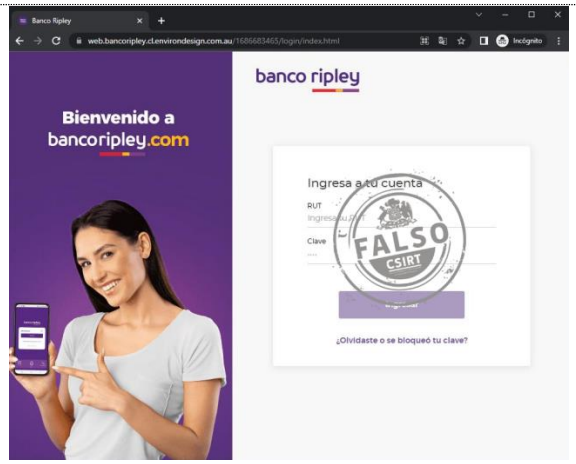
CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01399-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de junio de 2023
Última revisión	12 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://banestado-transacciones.web[.]app/?source=usg&et0Wxi8H1qpvFA5dE3RGNf9oSQjcVhn6J2ZzBbXPUyskM7raguIDYTL4wlmCOK	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01399-01	



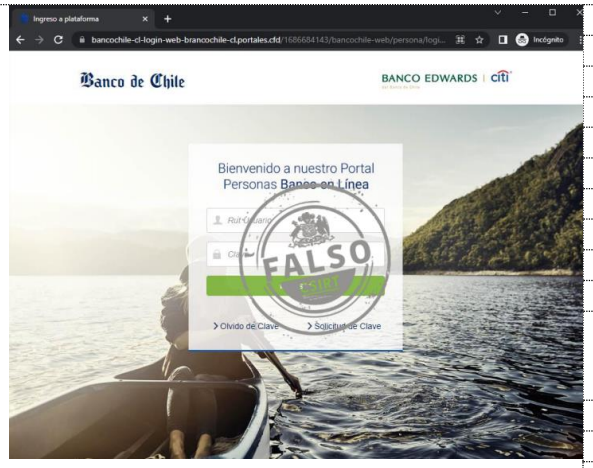
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01400-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://bit[.]ly/3MVVOPm?l=www.santander.cl https://eilders[.]nl/bancosantander/cuenta-kdjs/ https://banco.santander.cl.greeksingers[.]com.au/1686682516/portada/personas/home.asp	
Dirección IP	
[103.226.222.162]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01400-01	



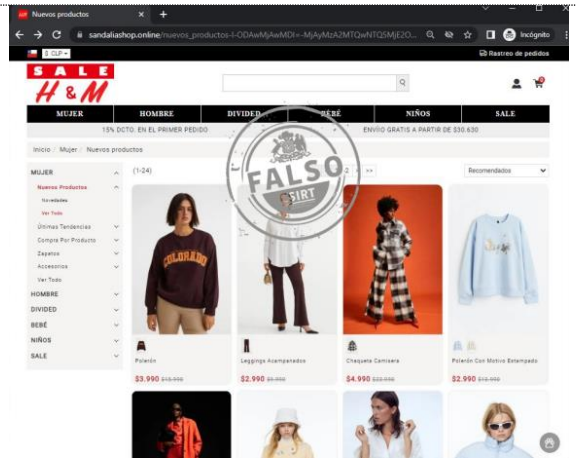
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FFR23-01401-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
http://mitarjetacencosud-cl.greeksingers[.]com.au/	
Dirección IP	
[103.226.222.162]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01401-01	



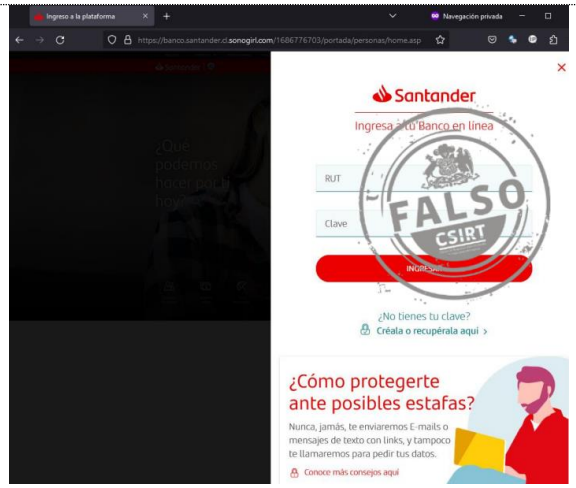
CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01402-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.web.bancoripley.cl.environdesign[.]com.au/1686683465/login/index.html	
Dirección IP	
[103.226.222.162]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01402-01	



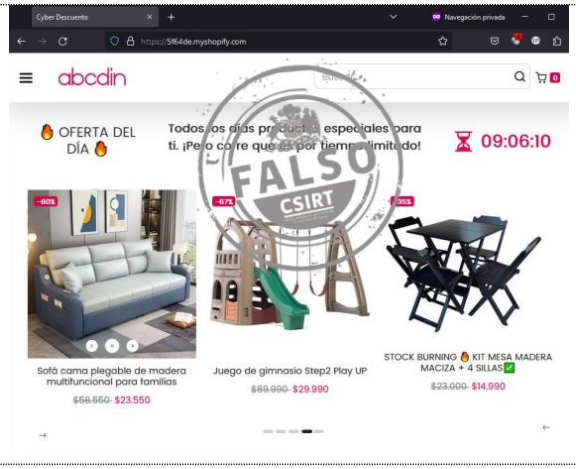
CSIRT alerta de nueva página fraudulenta que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01403-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://consumos[.]one/ https://bancochile-cl-login-web-brancochile-cl.portales[.]cfd/1686684143/bancochile-web/persona/login/index.html/login	
Dirección IP	
[104.21.9.98]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01403-01	



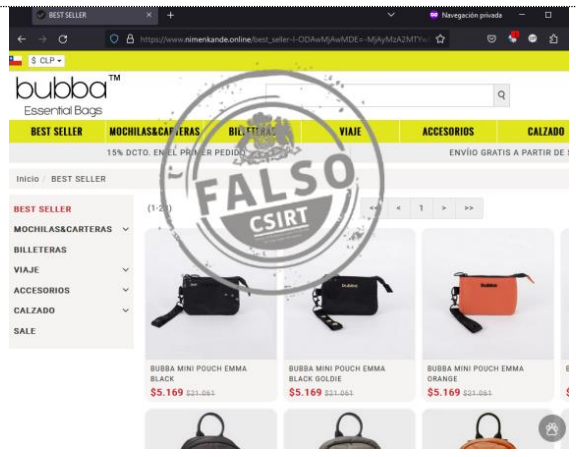
CSIRT alerta ante nueva página fraudulenta que suplanta a H&M	
Alerta de seguridad cibernética	8FFR23-01404-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2023
Última revisión	14 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.sandaliashop[.]online/	
Dirección IP	
[23.252.68.249]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01404-01	



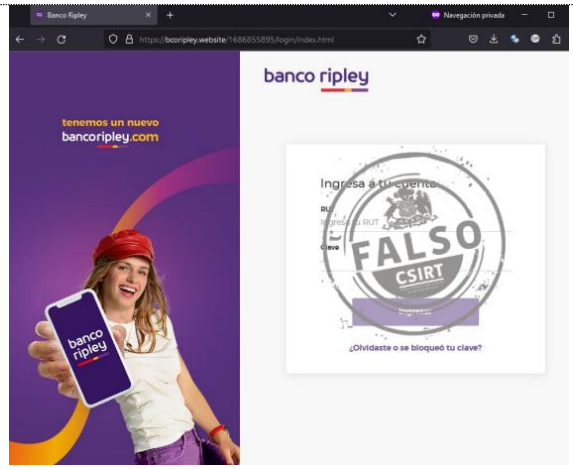
CSIRT alerta ante nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01405-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://banco.santander.cl.sonogirl[.]com/1686776703/portada/personas/home.asp	
Dirección IP	
[192.185.74.39]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01405-01	



CSIRT alerta ante sitio fraudulento que suplanta a ABCDin	
Alerta de seguridad cibernética	8FFR23-01406-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://5f64de.myshopify[.]com/	
Dirección IP	
[23.227.38.74]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01406-01	



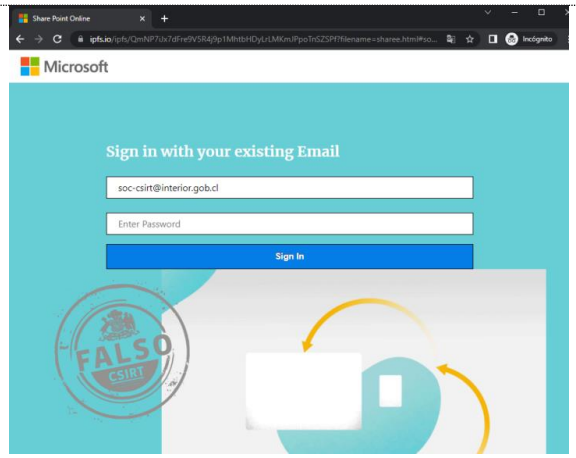
CSIRT alerta ante nueva página falsa que suplanta a Bubba Bags	
Alerta de seguridad cibernética	8FFR23-01407-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://www.nimenkande[.]online	
Dirección IP	
[23.252.71.136]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01407-01	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01408-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL sitio falso	
https://t[.]co/wqukED5Eyg https://pltf[.]website/ https://bcoripley[.]website/1686855895/login/index.html	
Dirección IP	
[68.65.120.219]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR23-01408-01	

2. Phishing

CSIRT alerta de nueva campaña de phishing, que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00833-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2023
Última revisión	9 de junio de 2023
URL redirección	
https://bit[.]ly/3J45YfF?l=www.santander.cl http://amazon1234[.]com/bancosantander/cuenta-ofis/	
URL sitio falso	
https://banco.santander.cl.paperhands[.]com.au/1686316960/portada/personas/home.asp	
Dirección IP	
[103.226.222.162]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00833-01/	



CSIRT alerta ante nueva campaña de phishing que suplanta a Microsoft SharePoint	
Alerta de seguridad cibernética	8FPH23-00834-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://boundlessdao.com/wp-content/shipdoc/#test@csirt.gob.cl	
URL sitio falso	
https://ipfs.io/ipfs/QmNP7iJx7dFre9V5R4j9p1MhtbHDyLrLMKmJPpoTnSZSPf?filename=sharee.html#test@csirt.gob.cl	
Dirección IP sitio falso	
[209.94.90.1]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00834-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00835-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de junio de 2023
Última revisión	15 de junio de 2023
Indicadores de compromiso	
URL redirección	
https://reachercontact[.]com/activacion/cuenta-zksc/	
URL sitio falso	
https://comunistable[.]com/1686775462/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[213.136.93.171]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8FPH23-00835-01/	

3. Ataques de fuerza bruta

CSIRT alerta de ataques de fuerza bruta contra SMTP	
Alerta de seguridad cibernética	4IIA22-00067-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2023
Última revisión	9 de junio de 2023
Indicadores de compromiso	
Direcciones IP	
80.94.95.242 45.66.230.176 107.182.128.12 194.85.249.206 185.252.179.55 193.56.29.186	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iia22-00067-01/	

4. Malware

CSIRT alerta de nueva campaña de phishing con malware, en email que suplanta al BancoEstado	
Alerta de seguridad cibernética	2CMV23-00418-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de junio de 2023
Última revisión	9 de junio de 2023
Indicadores de compromiso	
URL-Dominio	
http://savory.com[.]bd/imagify-backup/167_Hpxmebnuzgs 193.239.84[.]153:9184 217.16.85[.]25 info@znidarsic[.]si	
SHA256	
797a26c77e77386595b546a20e2654c9e7c2c14294390a2e2a9eee715b9a392c b5336f410d43416162e091970d023d3d4f6b93276bbeab99412056dfc1a78aa2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00418-01/	

5. Vulnerabilidades

CSIRT informa de vulnerabilidad crítica parchada en VPN Fortinet SSL	
Alerta de seguridad cibernética	9VSA23-00846-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de junio de 2023
Última revisión	12 de junio de 2023
CVE	
CVE-2023-27997	
Fabricantes	
Fortinet	
Productos afectados	
FortiGate SSL.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00846-01/	

CSIRT alerta de nuevas vulnerabilidades parchadas por Fortinet	
Alerta de seguridad cibernética	9VSA23-00847-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de junio de 2023
Última revisión	13 de junio de 2023
CVE	
CVE-2023-27997	
CVE-2023-29180	
CVE-2023-22640	
CVE-2023-29181	
CVE-2023-29179	
CVE-2023-22641	
Fabricante	
Fortinet	
Productos afectados	
FortiGate SSL.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00847-01/	

CSIRT comparte vulnerabilidades parchadas en el Update Tuesday de Microsoft para junio 2023	
Alerta de seguridad cibernética	9VSA23-00843-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de junio de 2023
Última revisión	14 de junio de 2023

CVE

CVE-2023-32030	CVE-2023-33139	CVE-2023-32010
CVE-2023-29326	CVE-2023-27910	CVE-2023-32009
CVE-2023-24895	CVE-2023-27909	CVE-2023-32008
CVE-2023-24936	CVE-2023-29012	CVE-2023-29373
CVE-2023-29331	CVE-2023-29011	CVE-2023-29372
CVE-2023-24897	CVE-2023-25815	CVE-2023-29371
CVE-2023-29337	CVE-2023-32024	CVE-2023-29370
CVE-2023-33140	CVE-2023-33137	CVE-2023-29369
CVE-2023-29357	CVE-2023-33133	CVE-2023-29368
CVE-2023-33142	CVE-2023-33132	CVE-2023-29367
CVE-2023-29353	CVE-2023-33131	CVE-2023-29366
CVE-2023-32031	CVE-2023-33130	CVE-2023-29365
CVE-2023-28310	CVE-2023-33129	CVE-2023-29364
CVE-2023-33146	CVE-2023-32029	CVE-2023-29363
CVE-2023-33145	CVE-2023-32022	CVE-2023-29362
CVE-2023-33144	CVE-2023-32021	CVE-2023-29361
CVE-2023-21569	CVE-2023-32020	CVE-2023-29360
CVE-2023-21565	CVE-2023-32019	CVE-2023-29359
CVE-2023-33141	CVE-2023-32018	CVE-2023-29358
CVE-2023-27911	CVE-2023-32017	CVE-2023-29355
CVE-2023-33128	CVE-2023-32016	CVE-2023-29352
CVE-2023-32032	CVE-2023-32015	CVE-2023-29351
CVE-2023-33126	CVE-2023-32014	CVE-2023-29346
CVE-2023-33135	CVE-2023-32013	CVE-2023-24896
CVE-2023-29007	CVE-2023-32012	CVE-2023-24937
CVE-2023-25652	CVE-2023-32011	CVE-2023-24938

Fabricantes

Microsoft

Productos afectados

.NET 6.0
.NET 7.0
Azure DevOps Server 2020.1.2
Azure DevOps Server 2022
Azure DevOps Server 2022.0.1
Dynamics 365 for Finance and Operations
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 and 4.6.2
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5 AND 4.8.1
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.6.2

	Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 Microsoft .NET Framework 4.8 Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Edge (Chromium-based) 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 Exchange Server 2016 Cumulative Update 23 Microsoft Exchange Server 2019 Cumulative Update 12 Microsoft Exchange Server 2019 Cumulative Update 13 Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for Mac Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft Office Online Server Microsoft OneNote for Universal Microsoft Outlook 2013 (32-bit editions) Microsoft Outlook 2013 (64-bit editions) Microsoft Outlook 2013 RT Service Pack 1 Microsoft Outlook 2016 (32-bit edition) Microsoft Outlook 2016 (64-bit edition) Microsoft Power Apps Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft Visual Studio 2013 Update 5 Microsoft Visual Studio 2015 Update 3 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 2022 version 17.0 Microsoft Visual Studio 2022 version 17.2 Microsoft Visual Studio 2022 version 17.4 Microsoft Visual Studio 2022 version 17.5 Microsoft Visual Studio 2022 version 17.6 NuGet 6.0.4 NuGet 6.2.3 NuGet 6.3.2 NuGet 6.4.1 NuGet 6.5.0 NuGet 6.6.0 Remote Desktop client for Windows Desktop Sysinternals Suite 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 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems 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 Sysinternals Process Monitor YARP 2.0
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00843-01/

CSIRT comparte información de varias vulnerabilidades parchadas por Adobe		
Alerta de seguridad cibernética	9VSA23-00849-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	14 de junio de 2023	
Última revisión	14 de junio de 2023	
CVE		
CVE-2023-29304	CVE-2023-29289	CVE-2023-29295
CVE-2023-29307	CVE-2023-29290	CVE-2023-29296
CVE-2023-29322	CVE-2023-29291	CVE-2023-29297
CVE-2023-29302	CVE-2023-29292	CVE-2023-22248
CVE-2023-29287	CVE-2023-29293	CVE-2023-29321
CVE-2023-29288	CVE-2023-29294	
Fabricantes		
Adobe		
Productos afectados		
Adobe Experience Manager (AEM) 6.5.17.0 y anteriores.		

	Adobe Commerce 2.4.6 y anteriores, 2.4.5-p2 y anteriores, 2.4.4-p3 y anteriores, 2.4.3-ext-2 y anteriores, 2.4.2-ext-2 y anteriores, 2.4.1-ext-2 y anteriores, 2.4.0-ext-2 y anteriores, 2.3.7-p4-ext-2 y anteriores. Magento Open Source 2.4.6 y anteriores, 2.4.5-p2 y anteriores, 2.4.4-p3 y anteriores. Adobe Animate 2022 22.0.9 y anteriores. Adobe Animate 2023 23.0.1 y anteriores.
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00849-01/

6. Concientización

Día Mundial Contra el Ciberacoso

En el #StopCyberbullyingDay (que se observa cada tercer viernes de junio) revivimos la charla "Cómo identificar el ciberacoso y cómo abordarlo" que realizamos el CSIRT de Gobierno y la Fundación Katy Summer: https://www.csirt.gob.cl/noticias/charla-ciberacoso-katy-summer-2023/.

La Tercera: "Gobierno alerta sobre aumento de los fraudes con falsas facturas"

Compartimos con La Tercera un informe sobre el resurgimiento de peligrosas estafas a través del envío de facturas falsas por email, junto con nuestros consejos para no caer en estos engaños. La nota completa puede ser leída aquí: https://www.latercera.com/nacional/noticia/gobierno-alerta-sobre-aumento-de-los-fraudes-con-falsas-facturas/UAPRTIWPABDHNFDLTCHH535OZA/.

Participación en nota sobre medidas de precaución digital ante el aumento de pagos digitales

El Mercurio contactó a la Coordinación Nacional de Ciberseguridad para ser una de sus fuentes en una nota sobre pagos digitales y seguridad, este lunes 16 de junio en su cuerpo B, Economía y Negocios: https://digital.elmercurio.com/2023/06/12/B/6F49RCLH#zoom=page-width

B 2 ECONOMÍA Y NEGOCIOS EL MERCURIO LUNES 12 DE JUNIO DE 2023

En medio de aumento de preocupación en la industria financiera por los fraudes:

Identidad digital, reforma al Registro Civil y autenticación surgen como posibles fórmulas para elevar seguridad en pago con celular

CATALINA MUÑOZ-KAPPES

Según expertos, la solución para prevenir robos con engaño, al usar los *smartphones* como medio de pago, radica en poder garantizar que la persona es quien dice ser.

Conadecus aclara que ante un fraude electrónico quien debe responder es la entidad bancaria, ya que ellos son los responsables de brindar seguridad al prestar el servicio.

RESPONSABILIDAD
La Asociación Chilena de Telecomunicaciones afirma que estos no son fraudes telefónicos, sino que "fraudes bancarios cometidos por teléfono", por lo que los medios digitales de pago deben aportar la seguridad.

La masificación de los métodos de pago a través del celular, vía transferencias por aplicaciones bancarias o código QR, ha vuelto cada vez más importante la seguridad en estos dispositivos. Si bien la Ley 21.234, conocida como la ley de fraude, limita la responsabilidad del usuario frente a estos delitos, debiendo asumirla la entidad bancaria, el aumento de estos eventos hace necesario avanzar en mecanismos de prevención.

Antonio Olivares, abogado de la Corporación Nacional de Consumidores y Usuarios (Conadecus), indica que frente a un fraude electrónico es responsable el consumidor en caso de que él haya sido extremadamente negligente. Pero en principio quien responde es el banco, ya que "es el que tiene que entregar seguridad al prestar el servicio".

También podría ser responsable la empresa de telecomunicaciones, dice Olivares, ya que se han registrado casos en que las firmas han entregado copias de números de teléfono a personas que no son el titular de la línea telefónica. Con esto, los delincuentes pueden acceder al mensaje de texto de confirmación que envían algunos servicios bancarios para verificar que la persona es quien dice ser. "Esto es una infracción, pero se podrían tener mayores estándares en beneficio de los consumidores", señala Olivares.

Respecto a cómo las empresas de telecomunicaciones pueden contribuir a prevenir estos delitos, Alfonso Gómez, CEO de Telefónica Hispam, comenta que "tenemos que trabajar muy de cerca con la banca. Es un frente que tenemos que atacar colectivamente (...) tiene que ser un trabajo mancomunado, del sector público y de los sectores involucrados en cada uno de los casos".

Sin embargo, desde ChileTelcos, Asociación Chilena de Telecomunicaciones, afirman que estos no son fraudes telefónicos, sino que "fraudes bancarios cometidos por teléfono" y que los medios de pagos digitales deben contar con las medidas necesarias para proteger a los usuarios. "Esa responsabilidad de las entidades financieras es indelegable", aseveran.

Por otro lado, afirman que para prevenir estos hechos es importante la educación de los usuarios. También que los medios de acreditación de identidad solo puede proveerlos el Estado, "lo que nos lleva a pensar en un e-rut o la masificación de la clave única".

Raíz del problema

Según el senador Kenneth Pugh, el problema radica en que "Chile se ha quedado en la prehistoria digital. Lo que hay ahora son credenciales, nombre de usuario y clave, y eso es muy básico, no da las garantías suficientes y por eso están ocurriendo todos los fraudes".

Señala que existen formas para quebrar el sistema, desde adivinar la clave, porque es muy simple, hasta usar ataques de fuerza bruta y de diccionario para tener acceso. "Todo eso es frágil. Se refuerza el sistema cuando se tienen factores de autenticación que permitan asegurar de que efectivamente es la persona. Mientras eso no exista, los fraudes van a ir aumentado cada vez más".

Carolina Pizarro, directora de ciberseguridad de NTT Data, explica que las contraseñas móviles de cuatro dígitos pueden ser "hackeadas" por un ciberdelincuente en menos de cuatro segundos. Indica que la doble autenticación que piden las aplicaciones bancarias da un poco más de seguridad dentro de los dispositivos, pero que "tampoco es infalible". Hoy se necesitan al menos tres autenticaciones "para empezar a decir que está siendo seguro", según Pizarro, como dos contraseñas y un código variable para hacer una transacción, o incorporar elementos de biometría, como la huella dactilar o los rasgos faciales.

Es por esto que el senador Pugh enfatiza en que Chile necesita un sistema de identidad digital robusto, que solo puede ser entregado por el Estado, para lo que se requiere "una reforma profunda al Registro Civil", ya que este "no tiene la capacidad para autenticar a las personas".

Explica que en países donde esto está implementado, como Estonia, las personas pueden hacer el 99% de sus trámites de manera virtual. Además de la credencial, los ciudadanos portan un chip que se puede insertar en un computador para verificar su identidad. A su vez, si es necesario, el sistema les puede pedir confirmación mediante el número telefónico, que está en una base de datos del Registro Civil, o encendiendo la cámara para hacer un reconocimiento facial.

Si bien esta es una preocupación creciente, desde la Coordinación Nacional de Ciberseguridad afirman que "no es un problema mayor desde el punto de vista de la seguridad", ya que usualmente la motivación de los ladrones es simplemente revender el teléfono. Por eso recalcan que es importante tener el celular con contraseña, ya que en caso contrario los delincuentes pueden hacerse pasar por la víctima para solicitar dinero a los contactos.

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 que los sitios web a los que se ingrese sean los oficiales.

8. 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 campañas de phishing, malware y/o sitios fraudulentos.

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.

- Sugy Nam
- Hellis Leiva
- Fernando Flores Tobar
- René Valdés
- Catalina Inés Sanhueza Rivera
- Jorge Aquiles Anticoi Carrasco
- Rigoberto Cancino
- Gabriel Torres Yarza
- Fernando Valenzuela

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.06.16 16:26:21 -04'00'