CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 228

semana del 10 al 16 de noviembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

25

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

26

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

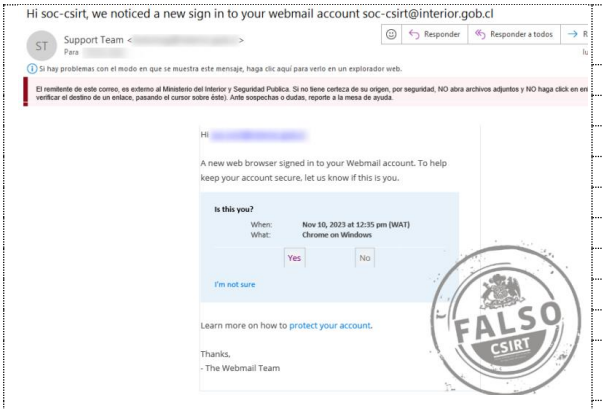
199

Las mitigaciones son útiles en productos de Microsoft.

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

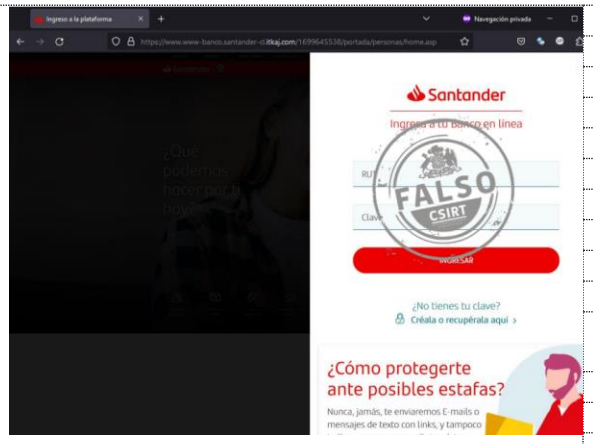


CSIRT alerta de una nueva campaña de phishing con falso mensaje de cuenta de correos	
Alerta de seguridad cibernética	8FPH23-00907-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 noviembre, 2023
Última revisión	15 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://pub-2e883b09c0a74dc48174fe1ca14292cf.r2[.]dev/mailbox-protection.html	
Dirección IP sitio falso	
[104.18.2.35]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00907-01/	

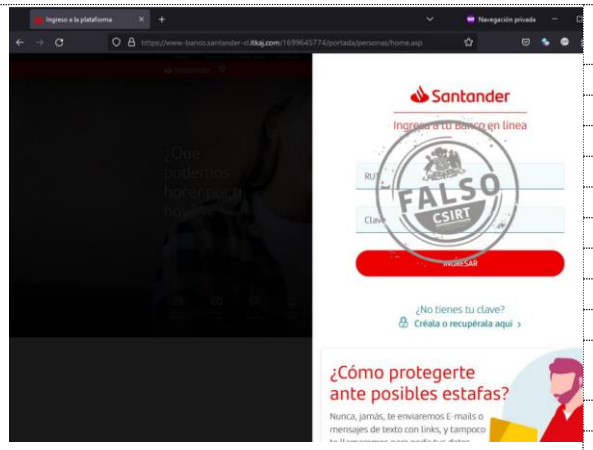
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00908-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 noviembre, 2023
Última revisión	15 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://serviestadohome[.]info/1699967769/imagenes/_personas/home/default.asp	
URL de redirección	
https://supportesmstado[.]com/activacion/cuenta-odfp/	
Dirección IP sitio falso	
[198.27.78.113]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00908-01/	

2. Sitios fraudulentos

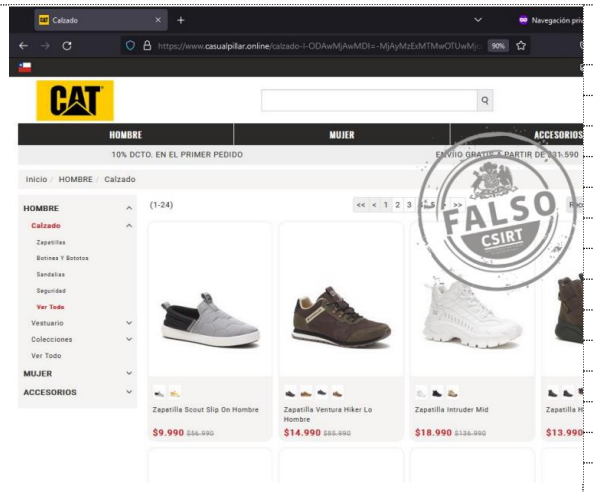
CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01548-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www-bancofalabella.cl.itkaj[.]com/1699645204/home	
Dirección IP sitio falso	
[103.163.246.230]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01548-01/	



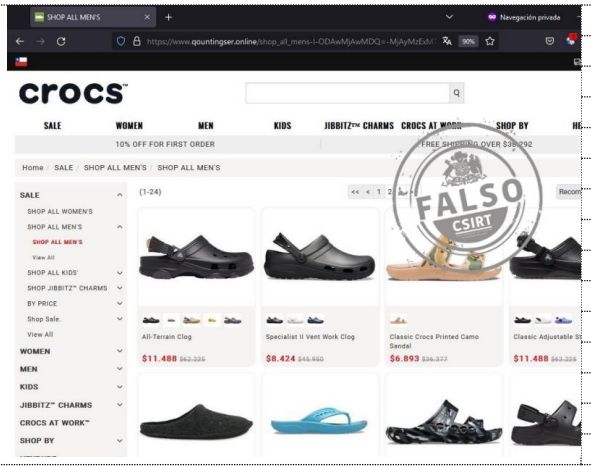
CSIRT alerta de nueva página fraudulenta que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01549-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.www-banco.santander-cl.itkaj[.]com/1699645538/portada/personas/home.asp	
Dirección IP sitio falso	
[103.163.246.230]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01549-01/	



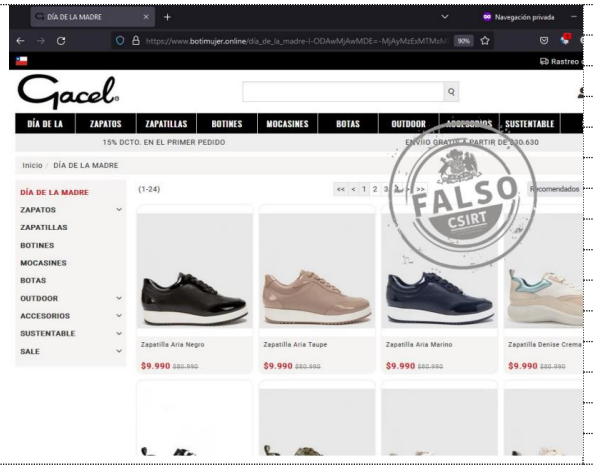
CSIRT alerta de la activación de un nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01550-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www-banco.santander-cl.itkaj[.]com/1699645774/portada/personas/home.asp	
Dirección IP sitio falso	
[103.163.246.230]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01550-01/	



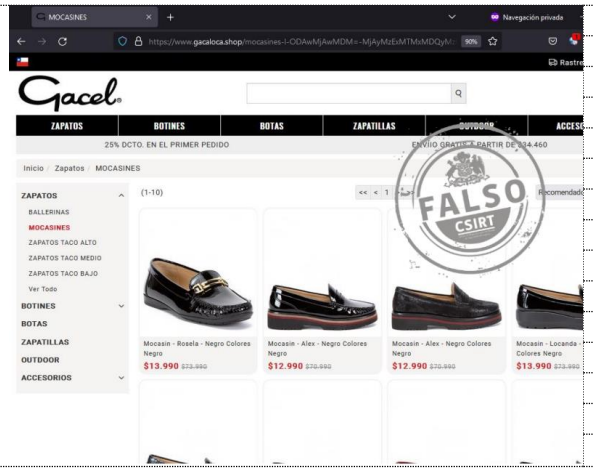
CSIRT alerta de la activación de nueva página fraudulenta que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01551-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.casualpillar[.]online	
Dirección IP sitio falso	
[199.21.150.15]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01551-01/	



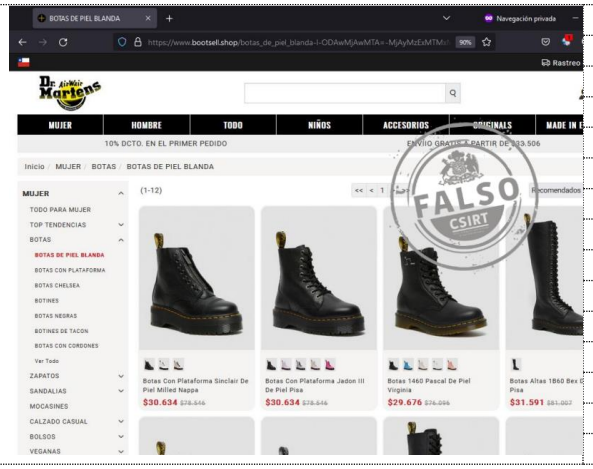
CSIRT alerta de nuevo sitio fraudulento que suplanta a Crocs	
Alerta de seguridad cibernética	8FFR23-01552-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.qountingser[.]online	
Dirección IP sitio falso	
[107.150.173.210]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01552-01/	



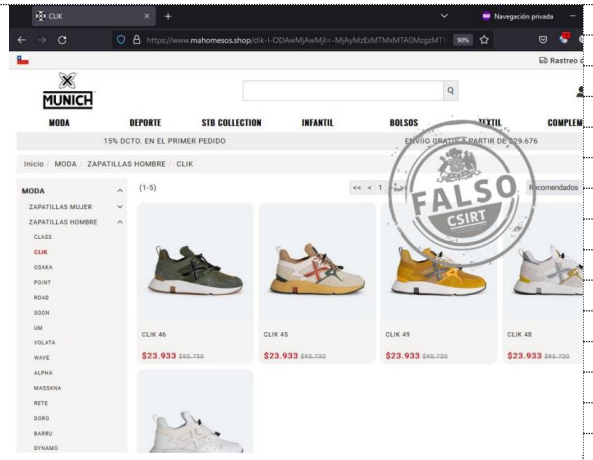
CSIRT alerta de nueva página fraudulenta que suplanta a Gacel	
Alerta de seguridad cibernética	8FFR23-01553-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.botimujer[.]online	
Dirección IP sitio falso	
[199.21.150.11]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01553-01/	



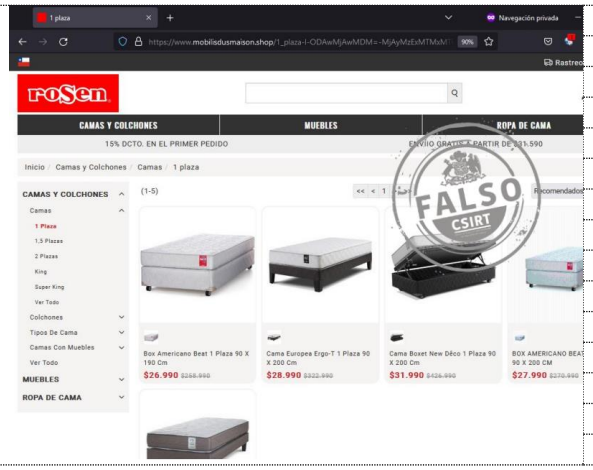
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Gacel	
Alerta de seguridad cibernética	8FFR23-01554-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.gacaloca[.]shop/	
Dirección IP sitio falso	
[199.21.150.14]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01554-01/	



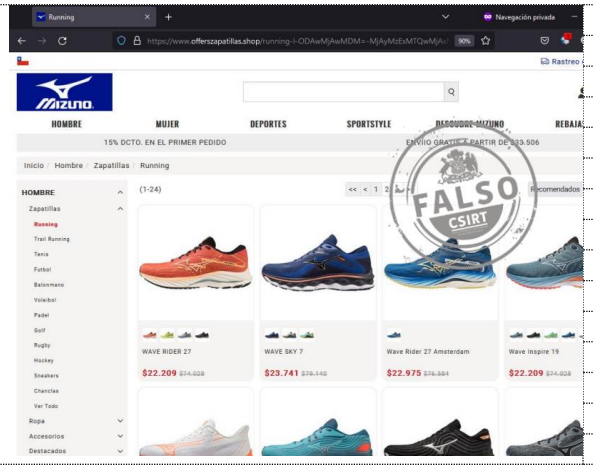
CSIRT alerta de nueva página falsa que suplanta a Dr. Martens	
Alerta de seguridad cibernética	8FFR23-01555-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.bootsell[.]shop	
Dirección IP sitio falso	
[198.144.149.116]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01555-01/	



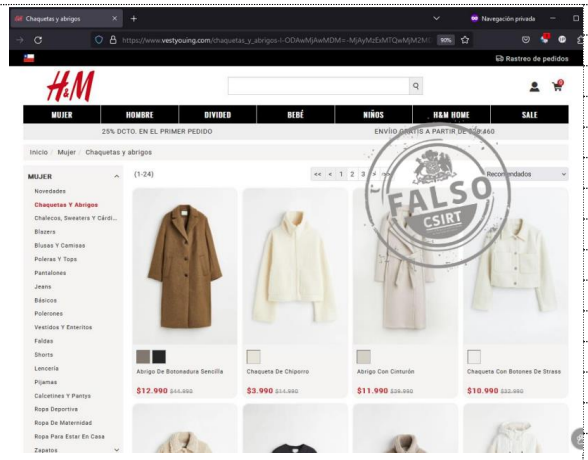
CSIRT alerta de nuevo sitio fraudulento que suplanta a zapatillas Munich	
Alerta de seguridad cibernética	8FFR23-01556-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.mahomesos[.]shop	
Dirección IP sitio falso	
[198.144.149.112]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01556-01/	



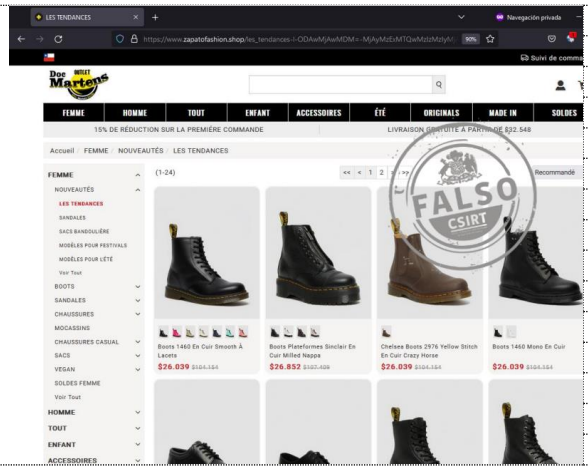
CSIRT alerta de nuevo sitio fraudulento que suplanta a Rosen	
Alerta de seguridad cibernética	8FFR23-01557-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.mobilisdusmaison[.]shop/	
Dirección IP sitio falso	
[45.141.156.89]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01557-01/	



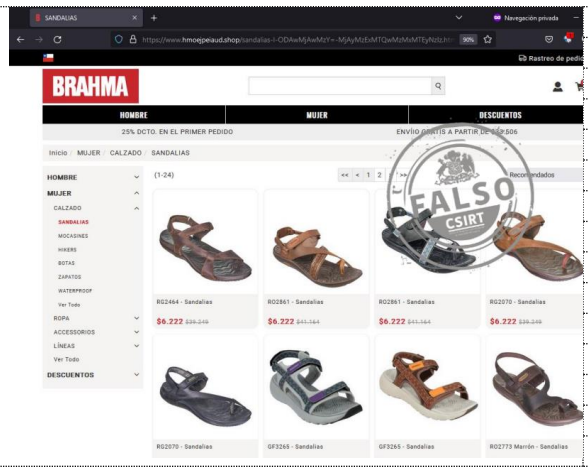
CSIRT alerta de nuevo sitio fraudulento que suplanta a Mizuno	
Alerta de seguridad cibernética	8FFR23-01558-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.offerszapatillas[.]shop	
Dirección IP sitio falso	
[45.141.156.89]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01558-01/	



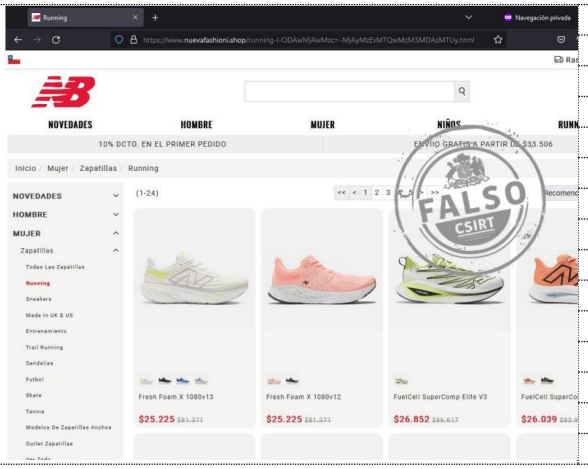
CSIRT alerta de una nueva página fraudulenta que suplanta a H&M	
Alerta de seguridad cibernética	8FFR23-01559-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.vestyouing[.]com/	
Dirección IP sitio falso	
[45.141.156.93]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01559-01/	



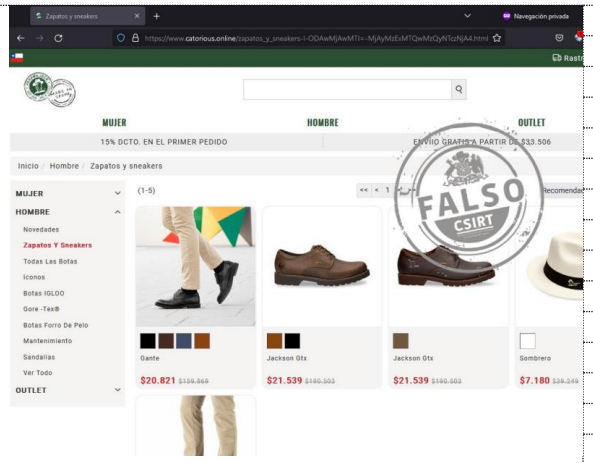
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Dr. Martens	
Alerta de seguridad cibernética	8FFR23-01560-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.zapatofashion[.]shop	
Dirección IP sitio falso	
[45.141.156.93]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01560-01/	



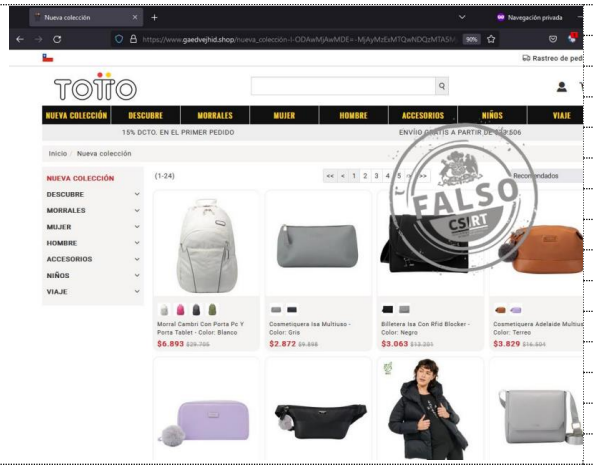
CSIRT alerta de nuevo sitio fraudulento que suplanta a sandalias Brahma	
Alerta de seguridad cibernética	8FFR23-01561-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.hmoejpeiaud[.]shop	
Dirección IP sitio falso	
[45.141.156.93]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01561-01/	



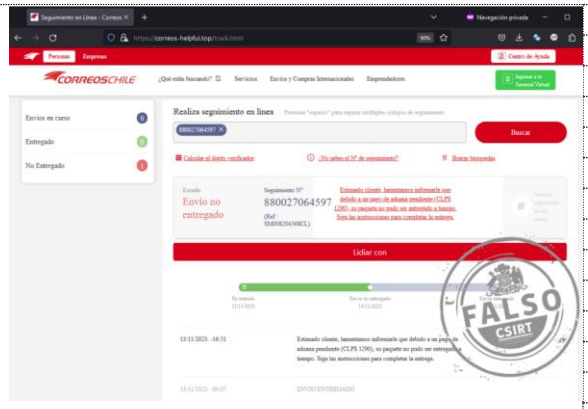
CSIRT alerta de una nueva página fraudulenta que suplanta a New Balance	
Alerta de seguridad cibernética	8FFR23-01562-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 noviembre, 2023
Última revisión	13 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.nuevafashioni[.]shop	
Dirección IP sitio falso	
[45.141.156.93]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01562-01/	



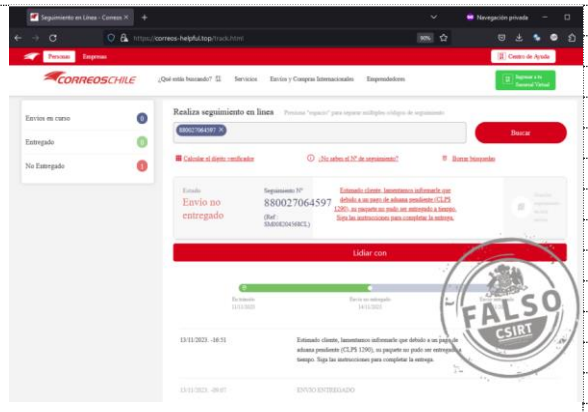
CSIRT alerta de nueva página fraudulenta que suplanta a Panama Jack	
Alerta de seguridad cibernética	8FFR23-01563-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.catorious[.]online	
Dirección IP sitio falso	
[45.141.156.93]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01563-01/	



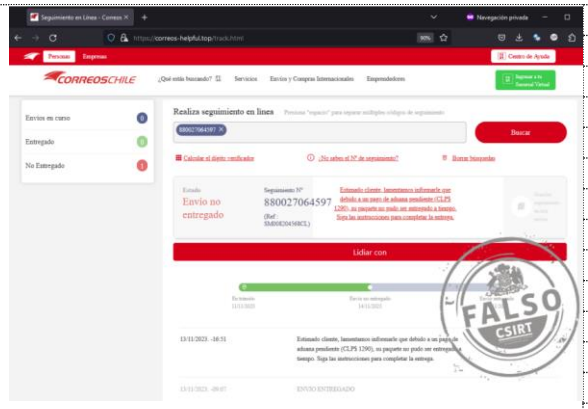
CSIRT alerta de un nuevo sitio fraudulento que suplanta a Totto	
Alerta de seguridad cibernética	8FFR23-01564-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.gaedvejhid[.]shop	
Dirección IP sitio falso	
[195.128.249.17]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01564-01/	



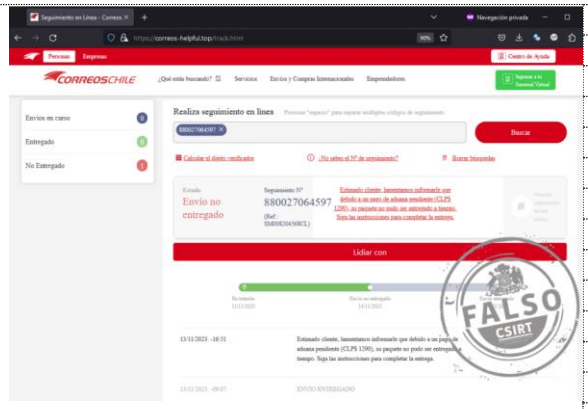
CSIRT alerta de un nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01565-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-helpful[.]top/	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01565-01/	



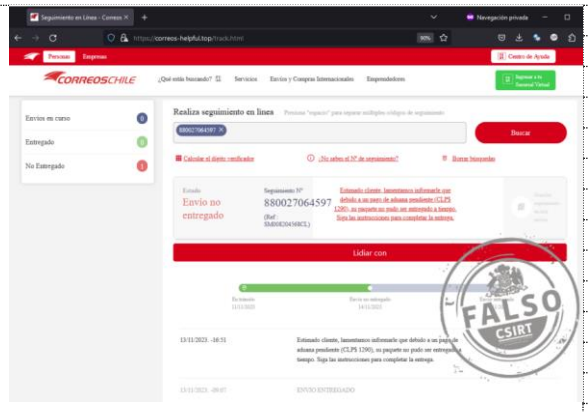
CSIRT alerta de un nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01566-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-supporting[.]top	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01566-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01567-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-assistline[.]xyz	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01567-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01568-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://correos-helpcenter.xyz	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01568-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01569-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 noviembre, 2023
Última revisión	14 noviembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://www.correos-aidpoint[.]top	
Dirección IP sitio falso	
[43.135.163.195]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01569-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades comprendidas en el Update Tuesday de Microsoft para noviembre 2023	
Alerta de seguridad cibernética	9VSA23-00935-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 noviembre, 2023
Última revisión	15 noviembre, 2023

CVE			
CVE-2023-36560	CVE-2023-36437	CVE-2023-36720	CVE-2023-35349
CVE-2023-36049	CVE-2023-36410	CVE-2023-36724	CVE-2023-36785
CVE-2023-36017	CVE-2023-36045	CVE-2023-36725	CVE-2023-36564
CVE-2023-36030	CVE-2023-36041	CVE-2023-36431	CVE-2023-36565
CVE-2023-36558	CVE-2023-36050	CVE-2023-36434	CVE-2023-36567
CVE-2023-36025	CVE-2023-36422	CVE-2023-36433	CVE-2023-36571
CVE-2023-36052	CVE-2023-38177	CVE-2023-36557	CVE-2023-36572
CVE-2023-38151	CVE-2023-36027	CVE-2023-36778	CVE-2023-36573
CVE-2023-36398	CVE-2023-5996	CVE-2023-36436	CVE-2023-36574
CVE-2023-36035	CVE-2023-36024	CVE-2023-36576	CVE-2023-36575
CVE-2023-36031	CVE-2023-36014	CVE-2023-36598	CVE-2023-36577
CVE-2023-36036	CVE-2023-5859	CVE-2023-36438	CVE-2023-36578
CVE-2023-36399	CVE-2023-5858	CVE-2023-36563	CVE-2023-36579
CVE-2023-36037	CVE-2023-5857	CVE-2023-36722	CVE-2023-36581
CVE-2023-36042	CVE-2023-5856	CVE-2023-36569	CVE-2023-36582
CVE-2023-36394	CVE-2023-5855	CVE-2023-36570	CVE-2023-36583
CVE-2023-36413	CVE-2023-5854	CVE-2023-36731	CVE-2023-36584
CVE-2023-36424	CVE-2023-5853	CVE-2023-36732	CVE-2023-36585
CVE-2023-36439	CVE-2023-5852	CVE-2023-36566	CVE-2023-36589
CVE-2023-36007	CVE-2023-5851	CVE-2023-41763	CVE-2023-36590
CVE-2023-36393	CVE-2023-5850	CVE-2023-36414	CVE-2023-36591
CVE-2023-36028	CVE-2023-5849	CVE-2023-36561	CVE-2023-36592
CVE-2023-36396	CVE-2023-5482	CVE-2023-44487	CVE-2023-36593
CVE-2023-36719	CVE-2023-5480	CVE-2023-36780	CVE-2023-36594
CVE-2023-36403	CVE-2023-36034	CVE-2023-36420	CVE-2023-36596
CVE-2023-36423	CVE-2023-36022	CVE-2023-36568	CVE-2023-36603
CVE-2023-36046	CVE-2023-36029	CVE-2023-36721	CVE-2023-36605
CVE-2023-36406	CVE-2023-5472	CVE-2023-36417	CVE-2023-36606
CVE-2023-36407	CVE-2023-44323	CVE-2023-36418	CVE-2023-36697
CVE-2023-36392	CVE-2023-36409	CVE-2023-36419	CVE-2023-36698
CVE-2023-36427	CVE-2023-38545	CVE-2023-36730	CVE-2023-36701
CVE-2023-36404	CVE-2023-38039	CVE-2023-36429	CVE-2023-36702
CVE-2023-36395	CVE-2023-5487	CVE-2023-36717	CVE-2023-36703
CVE-2023-36408	CVE-2023-5486	CVE-2023-36718	CVE-2023-36704
CVE-2023-36047	CVE-2023-5485	CVE-2023-36726	CVE-2023-36706
CVE-2023-24023	CVE-2023-5484	CVE-2023-36737	CVE-2023-36707
CVE-2023-36405	CVE-2023-5483	CVE-2023-36415	CVE-2023-36709
CVE-2023-36400	CVE-2023-5481	CVE-2023-36416	CVE-2023-36710
CVE-2023-36705	CVE-2023-5479	CVE-2023-36723	CVE-2023-36711
CVE-2023-36401	CVE-2023-5478	CVE-2023-36728	CVE-2023-36712
CVE-2023-36428	CVE-2023-5477	CVE-2023-41773	CVE-2023-36713
CVE-2023-36402	CVE-2023-5476	CVE-2023-41772	CVE-2023-36729

CVE-2023-36425	CVE-2023-5475	CVE-2023-41771	CVE-2023-41774
CVE-2023-36397	CVE-2023-5474	CVE-2023-41770	CVE-2023-41769
CVE-2023-36038	CVE-2023-5473	CVE-2023-41768	CVE-2023-41766
CVE-2023-36016	CVE-2023-5218	CVE-2023-41767	CVE-2023-41765
CVE-2023-36018	CVE-2023-36559	CVE-2023-36743	CVE-2023-36789
CVE-2023-36021	CVE-2023-38171	CVE-2023-36776	CVE-2023-36786
CVE-2023-36043	CVE-2023-36435	CVE-2023-36790	CVE-2023-38159
CVE-2023-36033	CVE-2023-36602	CVE-2023-38166	
CVE-2023-36039	CVE-2023-29348	CVE-2023-36902	

Fabricante

Microsoft

Productos afectados

.NET 8.0
ASP.NET Core 8.0
az logicapp config appsettings set
Azure DevOps Server 2020.1.2
Azure HDInsight
Azure Identity SDK for .NET
Azure Identity SDK for JavaScript
Azure Network Watcher VM Extension
Azure Pipelines Agent
Azure RTOS GUIX Studio
Host Integration Server 2020
Jupyter Extension for Visual Studio Code
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 3.5.1
Microsoft Common Data Model SDK for C#
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Edge (Chromium-based)
Microsoft Edge (Chromium-based) Extended Stable
Microsoft Edge for Android
Microsoft Excel 2016 (64-bit edition)
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Exchange Server 2019 Cumulative Update 13
Microsoft ODBC Driver 18 for SQL Server on MacOS
Microsoft Office 2016 (64-bit edition)
Microsoft Office for Universal
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft SharePoint Server Subscription Edition
Microsoft SQL Server 2019 for x64-based Systems (CU 22)
Microsoft SQL Server 2022 for x64-based Systems (CU 8)
Microsoft Visual Studio 2022 version 17.4
On-Prem Data Gateway
PowerShell 7.3
PowerShell 7.3
Send Customer Voice survey from Dynamics 365 app
Skype for Business Server 2015 CU13
Skype for Business Server 2019 CU7
System Center Operations Manager (SCOM) 2016
Windows 10 for 32-bit Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 21H2 for x64-based Systems

	Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows Defender Antimalware Platform Windows Server 2008 for x64-based Systems Service Pack 2 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 (Server Core installation) Windows Server 2012 R2 (Server Core installation) Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022, 23H2 Edition (Server Core installation)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00935-01/

4. Noticias y concientización

Inscríbete en la competencia de ciberseguridad "SheSecures"

Desde el 28 al 30 de marzo de 2024, se llevará a cabo esta competencia dirigida sólo para mujeres desde los 16 años que vivan en Chile y quieran desarrollar sus habilidades técnicas e ingresar a la industria de ciberseguridad.

Más información e inscripciones aquí: https://shesecures-chile.hackrocks.com/

Eliminación cuentas de correo electrónico

Para entregar un mejor servicio y responder a las necesidades de la comunidad, el CSIRT de Gobierno eliminó y reemplazó algunas cuentas de correo electrónico, quedando de la siguiente manera:

- La cuenta soc@interior.gob.cl fue eliminada y reemplazada por incidentes@interior.gob.cl. A través de este correo se deben notificar incidentes, incluyendo el DS 273, solicitar ayuda técnica, reportar problemas y requerir escaneos a sitios web de las instituciones públicas.

- La cuenta legalcsirt@interior.gob.cl fue eliminada y reemplazada por csirt-legal@interior.gob.cl para requerimientos legales o judiciales.

- La cuenta comunicaciones@interior.gob.cl fue eliminada y reemplazada por csirt-comunicaciones@interior.gob.cl, cuenta a la que pueden pedir información general, servicios, capacitaciones, requerimientos para eventos o actividades de ciberseguridad.

Así también se dieron de baja las cuentas scan-csirt@interior.gob.cl y soc-csirt@interior.gob.cl

La nota completa: https://www.csirt.gob.cl/noticias/eliminacion-cuentas-de-correo-electronico/

5. 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.

6. 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.

- Adrián Muñoz - Phishing
- Luis Miranda Vasquez - Phishing
- Luis Lamoliatte Vargas - Phishing
- Samuel Ricardo Paschuan Vega - Phishing
- Vicente Soto - Phishing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.17 18:11:00 -03'00'