CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 236

semana del 5 al 11 de enero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

4

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

8

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

45

Las mitigaciones son útiles en productos de Microsoft, Cisco e Ivanti.

HASH REPORTADOS

3

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

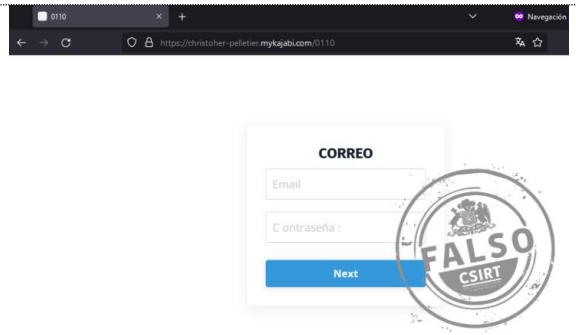
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Malware

CSIRT alerta de nueva campaña de phishing con malware, en este caso Grandoeiro	
Alerta de seguridad cibernética	2CMV23-00438-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 enero, 2024
Última revisión	8 enero, 2024
Indicadores de compromiso	
URL-Dominio	
https://espangmtes.westus2.cloudapp.azure[.]com/?25236754_966-108935108935=817902817902 https://www.dropbox[.]com/scl/fi/j3m0poowjfq9zp9glmsal/ConsultPagZDFKMQXVtlvhipmbetpeegdfYNSU.zip?rlkey=2tjq03gyi6fe4jddmo8loiarr&dl=0 http://15.229.5[.]172:24163/KvMXecvipA.xml http://15.229.5[.]172:4917/	
SHA256	
cf1dc1c23e8470735195101f8d0bbaef6e9b1550326d14c54bd9d8c9127ee59c 92bca8063250dcb09c12e00648e20acc8cd75eee2a7f1f83ab7755d0024049cd f5774d9f5e519d068c6d8bbf6cafaf0d46c51cd76c5364bdffc86ba74fd472ab	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00438-01/	

2. Sitios fraudulentos



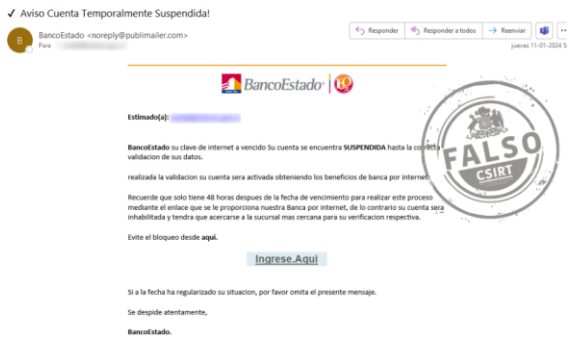
CSIRT alerta de nueva página fraudulenta que suplanta inicio de sesión de correo electrónico	
Alerta de seguridad cibernética	8FFR23-01629-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 enero, 2024
Última revisión	8 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://christoher-pelletier.mykajabi[.]com/0110	
URL de redirección	
https://new.express.adobe[.]com/webpage/ZRSKzlMNn4E05	
Dirección IP sitio falso	
[172.64.145.117]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8ffr23-01629-01/	

3. Phishing

Imagen 1: Correo Electrónico

CSIRT alerta de nueva campaña de phishing via sms (smishing) que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FPH23-00919-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 enero, 2024
Última revisión	8 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://support-appmlbancochile.bovgn5[.]online/1704727026/bchile-web/persona/login/index.html/login	
URL de redirección	
https://bit[.]ly/appmibanco	
Dirección IP sitio falso	
[162.241.85.202]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00919-01/	

CSIRT alerta de una nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00920-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 enero, 2024
Última revisión	9 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://ifepatito.khansouq[.]com/1704804454/imagenes/_personas/home/default.asp	
URL de redirección	
https://www.cajaabogadossanjuan[.]org.ar/activacion/cuenta-acbv/	
Dirección IP sitio falso	
[199.188.200.192]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00920-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH24-00921-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 enero, 2024
Última revisión	11 enero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://ucerhometadoscl[.]com/1704982755/imagenes/_personas/home/default.asp	
URL de redirección	
https://patitoqxshometado[.]com/activacion/cuenta-ildd/	
Dirección IP sitio falso	
[186.64.116.145]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00921-01/	

4. Vulnerabilidades

CSIRT comparte información de nueva vulnerabilidad crítica en Ivanti EPM	
Alerta de seguridad cibernética	9VSA23-00950-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 enero, 2024
Última revisión	5 enero, 2024
CVE	
CVE-2023-39336	
Fabricante	
Ivanti	
Productos afectados	
Ivanti EPM 2021/EPM 2022 anterior a 2022 Service Update 5 (SU5).	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa23-00950-01/	

CSIRT comparte información de actualización Microsoft Update Tuesday 2024 enero		
Alerta de seguridad cibernética	9VSA24-00951-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 enero, 2024	
Última revisión	10 enero, 2024	
CVE		
CVE-2024-0056	CVE-2024-21316	CVE-2024-21309
CVE-2024-21312	CVE-2024-20660	CVE-2024-20700
CVE-2024-0057	CVE-2024-20652	CVE-2024-20699
CVE-2024-21319	CVE-2024-20658	CVE-2024-20698
CVE-2024-20677	CVE-2024-20656	CVE-2024-20696
CVE-2024-21320	CVE-2024-20653	CVE-2024-20694
CVE-2024-21318	CVE-2024-20674	CVE-2024-20691
CVE-2024-21307	CVE-2024-20672	CVE-2024-20690
CVE-2024-21306	CVE-2024-21325	CVE-2024-20662
CVE-2024-21305	CVE-2024-20666	CVE-2024-20661
CVE-2024-20697	CVE-2024-21310	CVE-2024-20657
CVE-2022-35737	CVE-2024-21314	CVE-2024-20655
CVE-2024-20692	CVE-2024-21313	CVE-2024-20654
CVE-2024-20687	CVE-2024-21311	CVE-2024-20676
CVE-2024-20683		
Fabricante		
Microsoft		
Productos afectados		
.NET 6.0		
.NET 7.0		
.NET 8.0		
Azure Storage Mover Agent		

	CBL Mariner 1.0 ARM CBL Mariner 1.0 x64 CBL Mariner 2.0 ARM CBL Mariner 2.0 x64 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 4.7.2 Microsoft .NET Framework 3.5 AND 4.8 Microsoft .NET Framework 3.5 AND 4.8.1 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 Identity Model v5.0.0 Microsoft Identity Model v5.0.0 for Nuget Microsoft Identity Model v6.0.0 Microsoft Identity Model v6.0.0 for Nuget Microsoft Identity Model v7.0.0 Microsoft Identity Model v7.0.0 for Nuget Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft Printer Metadata Troubleshooter Tool Microsoft SharePoint Enterprise Server 2016 Microsoft SharePoint Server 2019 Microsoft SharePoint Server Subscription Edition Microsoft SQL Server 2022 for x64-based Systems (CU 10) Microsoft SQL Server 2022 for x64-based Systems (GDR) 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 17.2 Microsoft Visual Studio 2022 version 17.4 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2022 version 17.8 Microsoft.Data.SqlClient 2.1 Microsoft.Data.SqlClient 3.1 Microsoft.Data.SqlClient 4.0 Microsoft.Data.SqlClient 5.1 System.Data.SqlClient 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 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 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 Server 2022, 23H2 Edition (Server Core installation)
	Enlaces para revisar el informe:
	https://csirt.gob.cl/vulnerabilidades/9vsa24-00951-01/

CSIRT comparte información de vulnerabilidad parchada por Cisco en Unity Connection	
Alerta de seguridad cibernética	9VSA24-00952-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 enero, 2024
Última revisión	11 enero, 2024
CVE	
CVE-2024-20272	
Fabricante	
Cisco	
Productos afectados	
Cisco Unity Connection 14, 12.5 y anteriores.	
Enlaces para revisar el informe:	
https://csirt.gob.cl/vulnerabilidades/9vsa23-00952-01/	

5. Noticias y concientización

Ciberconsejos | Evita caer en arriendos falsos este verano

Si buscas a través de sitios web alguna propiedad para arrendar estas vacaciones, cuidado con las falsas ofertas. Evita caer en una estafa siguiendo nuestros ciberconsejos. Más recomendaciones aquí: https://csirt.gob.cl/recomendaciones/

6. 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.

7. 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.

- Andrés Ignacio Castro Zuleta Phishing
- Felipe Vidal Phishing
- OSI - VTI UCHILE Phishing
- Fernando Enrique González Phishing
- María José Fuentes Urrutia Phishing
- Hugo Gabriel Montecinos Ataque de denegación de servicio
- Felipe Hott Delgado Exfiltracion de Informacion
- Vicente Andrés Mancilla Phishing
- Miguel Morales Saravia Phishing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.12 18:21:53 -03'00'