

Alerta de seguridad cibernética	8FFR21-00963-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Junio de 2021
Última revisión	11 de Junio de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Estos casos de fraude no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado fraude, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile (CSIRT de Gobierno), ha identificado la activación de una página fraudulenta que hace pasar por la plataforma Amazon, lo que podría servir para robar credenciales de usuarios.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

[https://lordandpost\[.\]info/clamz/](https://lordandpost[.]info/clamz/)

Certificado Digital

Fecha Válido	10-06-2021
Fecha Término	08-09-2021
Emitido	R3

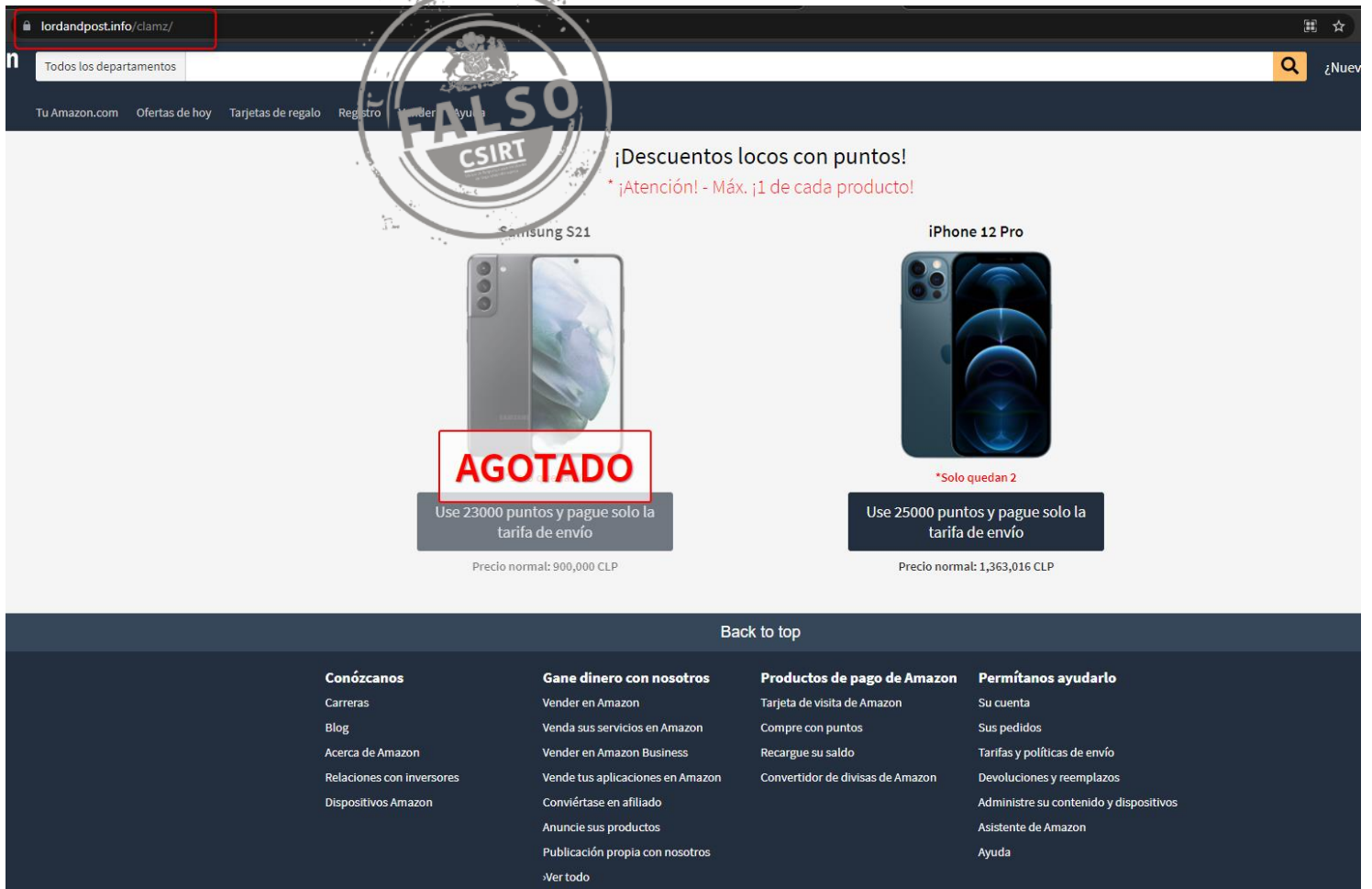
Datos Alojamiento

IP	[207.174.214.152]
Número de Sistema Autónomo (AS)	394695
Etiqueta del Sistema Autónomo	PUBLIC-DOMAIN-REGISTRY
País	US
Registrador	ARIN

Datos del Dominio

Nombre de Dominio	lordandpost[.]info
Creado	29-11-2011
Expira	25-12-2024
Información del Registrador	PDR Ltd. d/b/a PublicDomainRegistry.com
ID IANA	303
Correo Electrónico	abuse-contact@publicdomainregistry.com
Name Server	ns1.md-49.webhostbox.net ns2.md-49.webhostbox.net

Imagen del sitio



lordandpost.info/clamz/

Todos los departamentos

Tu Amazon.com Ofertas de hoy Tarjetas de regalo Registro Ayuda

FALSO
CSIRT

¡Descuentos locos con puntos!
* ¡Atención! - Máx. ¡1 de cada producto!

Samsung S21

iPhone 12 Pro

AGOTADO

Use 23000 puntos y pague solo la tarifa de envío

Precio normal: 900,000 CLP

*Solo quedan 2

Use 25000 puntos y pague solo la tarifa de envío

Precio normal: 1,363,016 CLP

Back to top

<p>Conózanos</p> <ul style="list-style-type: none"> Carreras Blog Acerca de Amazon Relaciones con inversores Dispositivos Amazon 	<p>Gane dinero con nosotros</p> <ul style="list-style-type: none"> Vender en Amazon Venda sus servicios en Amazon Vender en Amazon Business Vende tus aplicaciones en Amazon Conviértase en afiliado Anuncie sus productos Publicación propia con nosotros Ver todo 	<p>Productos de pago de Amazon</p> <ul style="list-style-type: none"> Tarjeta de visita de Amazon Compre con puntos Recargue su saldo Convertidor de divisas de Amazon 	<p>Permítanos ayudarlo</p> <ul style="list-style-type: none"> Su cuenta Sus pedidos Tarifas y políticas de envío Devoluciones y reemplazos Administre su contenido y dispositivos Asistente de Amazon Ayuda
--	--	---	---

Recomendaciones

- 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.