Alerta de seguridad informática	8FFR-00128-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Noviembre de 2019
Última revisión	27 de Noviembre de 2019

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 (CSIRT), ha identificado la activación de un portal fraudulento asociado a una IP que suplanta el sitio web oficial de **CMR Falabella**, el que podría servir para robar credenciales de usuarios de esa entidad.

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

Indicadores de Compromisos

URL´s

URL Sitio Clonado:
https[://]https-www-cmr-cl[.]bellezaycosmeticostryu[.]com/personas-chile/

Domain bellezaycosmeticostryu.com

bellezaycosmeticostryu / com / Subdomains

record type	TTL	value		
A	14400	162.241.60.14		
NS	86400	ns14.hostgator.cl	Zones on DNS server	162.241.60.12
NS	86400	ns15.hostgator.cl	Zones on DNS server	162.241.60.13
MX	14400	0 mail.bellezaycosmeticostryu.com		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname	ns14.hostgator.cl	
		Rname	root.shared14.hostgator.cl	
		Serial number	2019111104	
		Refresh	86400	
		Retry	7200	
		Expire	3600000	
		Minimum TTL	86400	

Ilustración 1 Dominio donde se Aloja Url del CMR Falabella, Falso y DNS que utiliza

Certificados

Criteria: Identity = 'bellezaycosmeticostryu.com'

Certificates

crt.sh ID	Logged At	Not Before	Not After	Issuer Name
2026467869	2019-10-21	2019-10-21	2020-01-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2021082863	2019-10-21	2019-10-21	2020-01-19	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ilustración 2 Certificado Utilizado en Url del sitio Falso del CMR Falabella

IP

162.241.60.14

Domain bellezaycosmeticostryu.com is located on IP address << 162.241.60.14 >>	
Block start	162.240.0.0
End of block	162.241.255.255
Block size	131072 Domains in block
Block name	UNIFIEDLAYER-NETWORK-16
AS number	26337
Parent block	162.0.0.0 - 162.255.255.255
Organization	UnifiedLayer
City	Provo
Region/State	Utah
Country	US , United States
Reg. date	2013-08-22
Host name	162-241-60-14.unifiedlayer.com
Domains	1 bellezaycosmeticostryu.com

Ilustración 3 Ip de Origen donde se aloja Sitio Falso del CMR Falabella

Localización

Provo, Utah, Estados Unidos

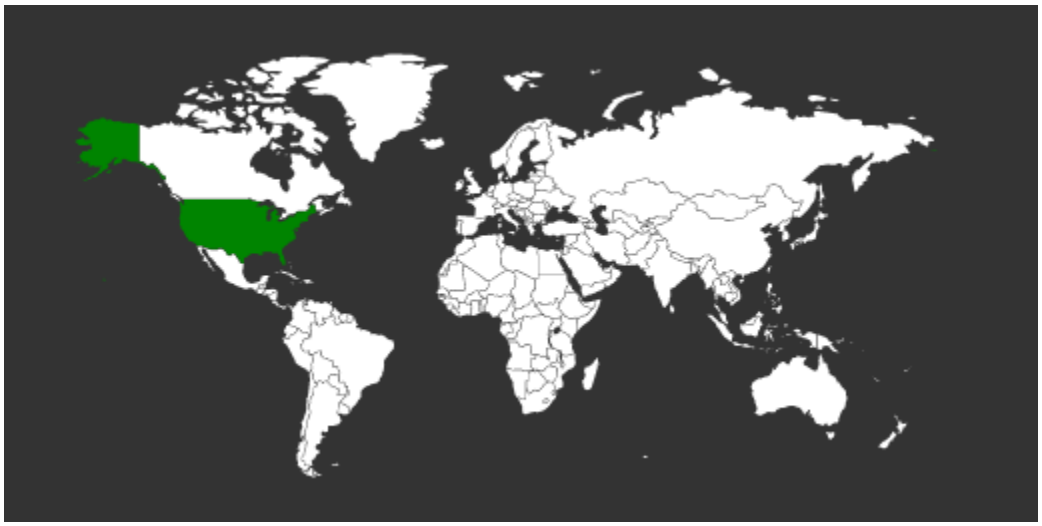

Imagen del sitio

Whois

```
Domain Name: BELLEZAYCOSMETICOSTRYU.COM
Registry Domain ID: 2445940737_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.publicdomainregistry.com
Registrar URL: www.publicdomainregistry.com
Updated Date: 2019-10-21T17:03:11Z
Creation Date: 2019-10-21T17:03:11Z
Registrar Registration Expiration Date: 2020-10-21T17:03:11Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: carlos adrian ruiz valencia
Registrant Organization:
Registrant Street: las americas , 4489 santiago
Registrant City: Santiago
Registrant State/Province: RM
Registrant Postal Code: 8320000
Registrant Country: CL
Registrant Phone: +56.909890938
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: bellezaycosmeticostryu@gmail.com
Registry Admin ID: Not Available From Registry
Admin Name: carlos adrian ruiz valencia
Admin Organization:
Admin Street: las americas , 4489 santiago
Admin City: Santiago
Admin State/Province: RM
Admin Postal Code: 8320000
Admin Country: CL
Admin Phone: +56.909890938
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: bellezaycosmeticostryu@gmail.com
Registry Tech ID: Not Available From Registry
Tech Name: carlos adrian ruiz valencia
Tech Organization:
Tech Street: las americas , 4489 santiago
Tech City: Santiago
Tech State/Province: RM
Tech Postal Code: 8320000
Tech Country: CL
Tech Phone: +56.909890938
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: bellezaycosmeticostryu@gmail.com
Name Server: ns14.hostgator.cl
Name Server: ns15.hostgator.cl
DNSSEC: Unsigned
```

Recomendaciones

- Evitar acceder al sitio anteriormente indicado e informar a los usuarios sobre su existencia, para evitar que se conviertan en víctimas del fraude.
- Ser precavidos frente a este tipo de páginas fraudulentas.
- Bloquear en los proxy o sistemas de control de contenido, hacia la URL maliciosa
- 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

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.11.27 16:21:02 -03'00'