Alerta de seguridad informática	8FFR-00144-001
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de Diciembre de 2019
Última revisión	9 de Diciembre 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:

ccvvstore[.]xyz

Domain ccvvstore.xyz

ccvvstore / xyz / Subdomains

record type	TTL	value		
A	14400	162.241.60.177		
NS	86400	ns17.hostgator.cl	Zones on DNS server	162.241.60.176
NS	86400	ns16.hostgator.cl	Zones on DNS server	162.241.60.175
MX	14400	0 mail.ccvvstore.xyz		
TXT	14400	v=spf1 a mx include:websitewelcome.com ~all		
SOA	86400	Mname	ns16.hostgator.cl	
		Rname	root.shared16.hostgator.cl	
		Serial number	2019120202	
		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

Subject DN CN=ccvvstore.xyz

Issuer DN C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Serial 422487375321513212335509835134442056234254

Validity 2019-12-02 22:27:30 **to** 2020-03-01 22:27:30 (90 days, 0:00:00)

Names autodiscover.ccvvstore.xyz
ccvvstore.xyz
cpanel.ccvvstore.xyz
mail.ccvvstore.xyz
webdisk.ccvvstore.xyz
webmail.ccvvstore.xyz
www.ccvvstore.xyz

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

IP

162.241.60.177

Domain ccvvstore.xyz is located on IP address
<< 162.241.60.177 >>

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	46606
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	162-241-60-177.unifiedlayer.com
Domains	1 ccvvstore.xyz

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

Localización

Provo, Utah, Estados Unidos

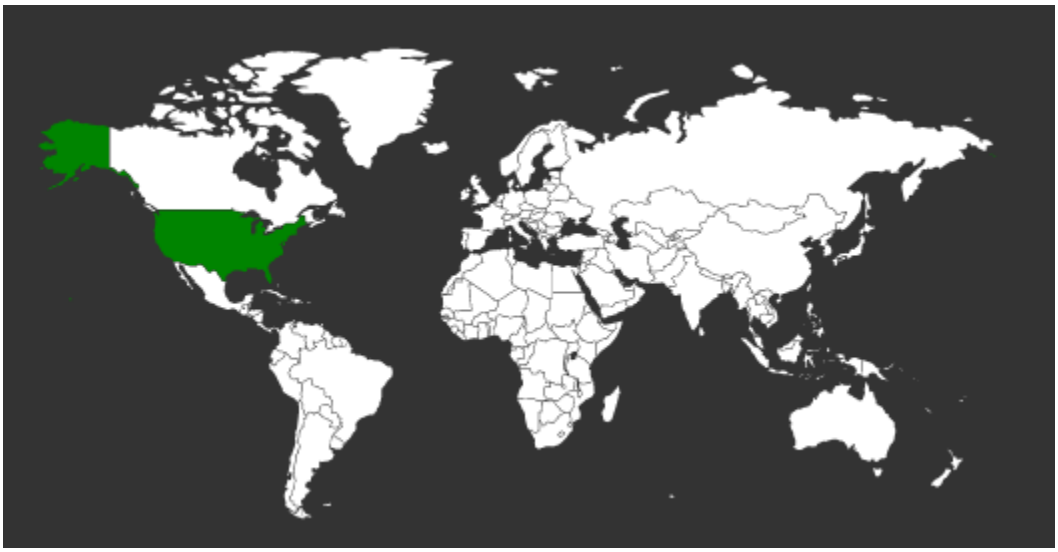
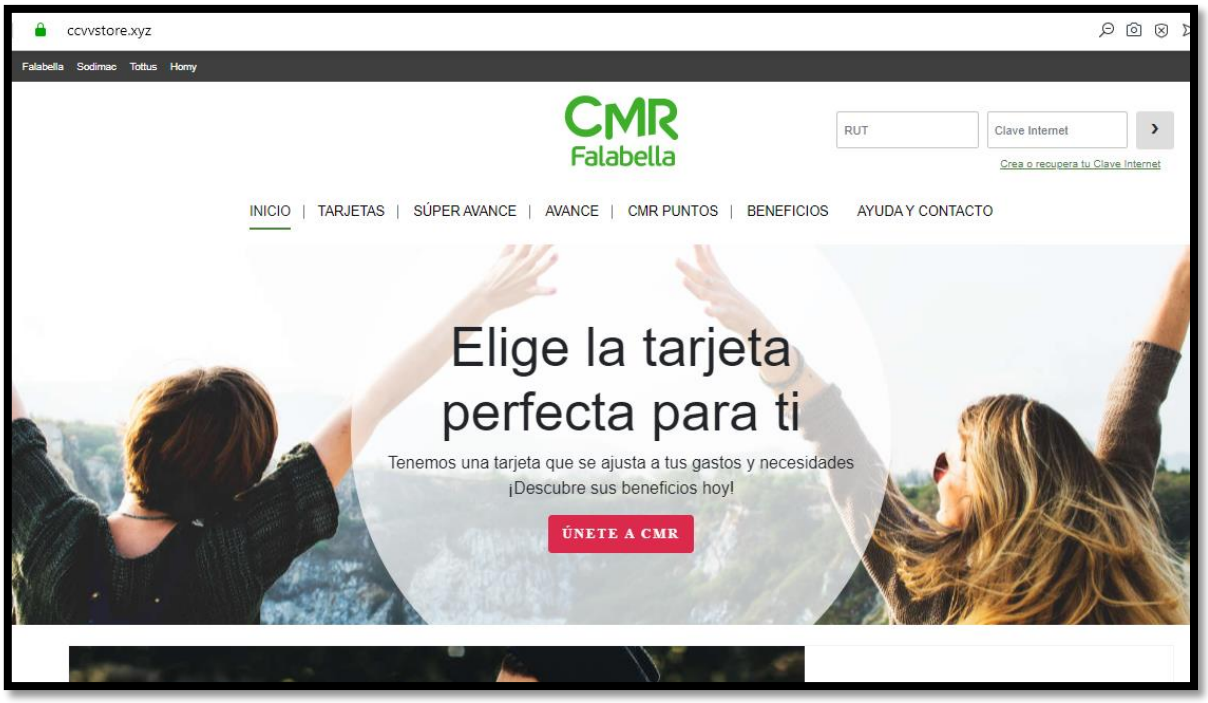


Imagen del sitio



Whois

```
Domain Name: CCVVSTORE.XYZ
Registry Domain ID: D149344481-CNIC
Registrar WHOIS Server: whois.PublicDomainRegistry.com
Registrar URL: https://publicdomainregistry.com
Updated Date: 2019-12-02T07:16:21.0Z
Creation Date: 2019-12-02T07:16:19.0Z
Registry Expiry Date: 2020-12-02T23:59:59.0Z
Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com
Registrar IANA ID: 303
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: addPeriod https://icann.org/epp#addPeriod
Registrant Organization: Privacy Protect, LLC (PrivacyProtect.org)
Registrant State/Province: MA
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: NS17.HOSTGATOR.CL
Name Server: NS16.HOSTGATOR.CL
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registrar Abuse Contact Email: abuse@publicdomainregistry.com
Registrar Abuse Contact Phone: +1.2013775952
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2019-12-06T19:03:47.0Z <<<
```

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: 2019.12.09 11:46:44 -03'00'