Alerta de seguridad cibernética	8FFR20-00431-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Mayo de 2020
Última revisión	26 de Mayo de 2020

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 **Banco Estado** , 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 compromiso

URL

acceso[.]bacoestado[.]win

IP

95[.]179[.]254[.]172

Dominios donde se aloja url

Domain bacoestado.win

bacoestado / win / Subdomains

record type	TTL	value		
NS	172800	ns1.dnsowl.com	Zones on DNS server	198.251.84.16, 104.207.141.138, 185.34.216.159
NS	172800	ns2.dnsowl.com	Zones on DNS server	168.235.75.52, 45.32.237.128, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	45.63.106.63, 209.141.39.150, 45.63.5.234

SOA	172800		
		Mname	ns1.dnsowl.com
		Rname	hostmaster.dnsowl.com
		Serial number	1590436612
		Refresh	7200
		Retry	1800
		Expire	1209600
		Minimum TTL	600

Certificados

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2809865581	2020-05-15	2020-05-15	2020-08-13	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2724688039	2020-04-15	2020-04-15	2020-07-14	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2698740302	2020-04-15	2020-04-15	2020-07-14	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2690356744	2020-04-11	2020-04-11	2020-07-10	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2690357196	2020-04-11	2020-04-11	2020-07-10	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2677491719	2020-04-07	2020-04-07	2020-07-06	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2677106927	2020-04-07	2020-04-07	2020-07-06	acceso.bacoestado.win	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

Ip de origen donde se aloja sitio

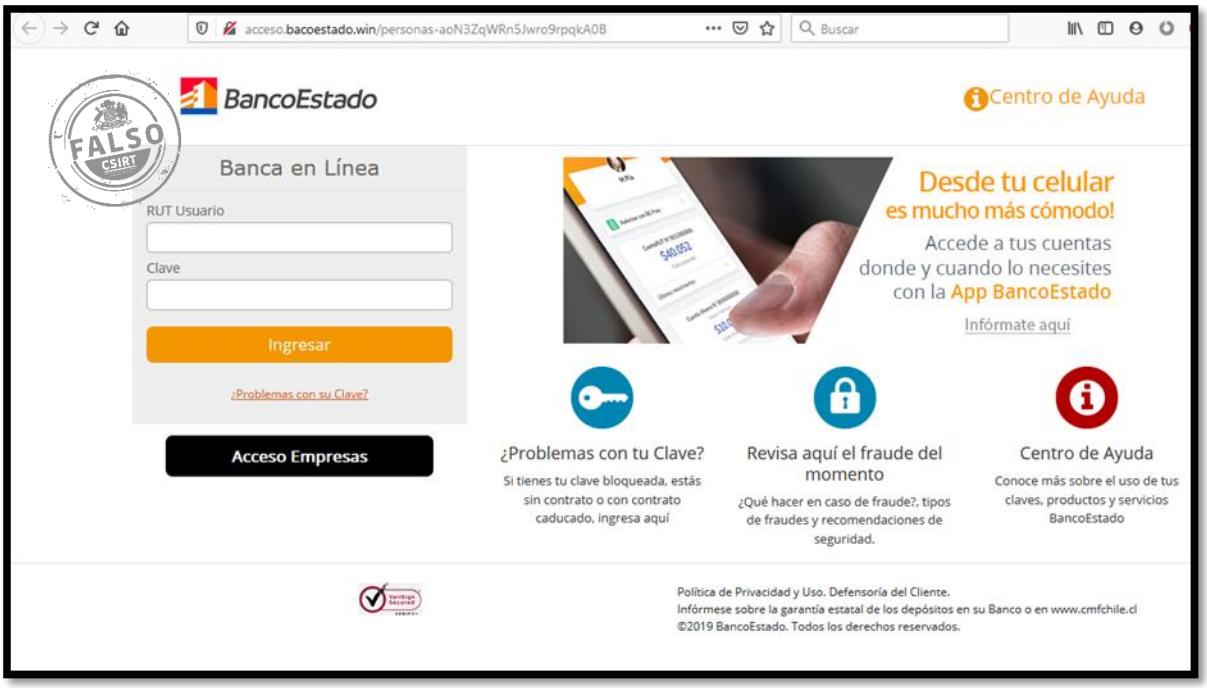
Domain acceso.bacoestado.win is located on IP address << 95.179.254.172 >>

Block start	95.179.254.0
End of block	95.179.255.255
Block size	512 Domains in block
Block name	NET-V4-95-179-128-0-17
AS number	20473
Parent block	95.179.128.0 - 95.179.255.255
Organization	Hanauer Landstraße 302 60314 Frankfurt am Main Germany

Localización

Amsterdam, Holanda del Norte, Países Bajos

Imagen del sitio



Whois

```
Domain Name: bacoestado.win
Registry Domain ID: DFA306D155A4349F5B2671D37E389098F-NSR
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-05-20T07:00:00Z
Creation Date: 2020-04-05T07:00:00Z
Registrar Registration Expiration Date: 2021-04-05T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransfer
Prohibited
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: See PrivacyGuardian.org
Registrant Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Registrant City: Phoenix
Registrant State/Province: AZ
Registrant Postal Code: 85016
Registrant Country: US
Registrant Phone: +1.3478717726
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: pw-3e06066dbf9ac5c92644cf83a597357c@privacyguardian.org
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: See PrivacyGuardian.org
Admin Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Admin City: Phoenix
Admin State/Province: AZ
Admin Postal Code: 85016
Admin Country: US
Admin Phone: +1.3478717726
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: pw-3e06066dbf9ac5c92644cf83a597357c@privacyguardian.org
Registry Tech ID:
```

```
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: See PrivacyGuardian.org
Tech Street: 1928 E. Highland Ave. Ste F104 PMB# 255
Tech City: Phoenix
Tech State/Province: AZ
Tech Postal Code: 85016
Tech Country: US
Tech Phone: +1.3478717726
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: pw-3e06066dbf9ac5c92644cf83a597357c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2020-05-25T07:00:00Z <<<
```

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.