Alerta de seguridad informática	8FFR20-00284-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Marzo de 2020
Última revisión	25 de Marzo 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´s
crm[.]wenat[.]it/wpz/
wwmx[.]banstado[.]chile[.]com[.]byuyt[.]live
wwmx[.]banstado[.]chile[.]com[.]byuyt[.]live/imagenes/comun2008/banca-en-linea-personas[.]php?html
zs3zory[.]aplus[.]pl/www[.]bancoestado[.]cl/imagenes/comun2008/banca-en-linea-personas[.]html

IP
212[.]237[.]29[.]173
167[.]71[.]224[.]151

DOMINIOS DONDE SE ALOJA URL

Domain crm.wenat.it

crm / wenat / it / Subdomains

record type	TTL	value
A	3600	212.237.29.173

Domain wenat.it

wenat / it / Subdomains

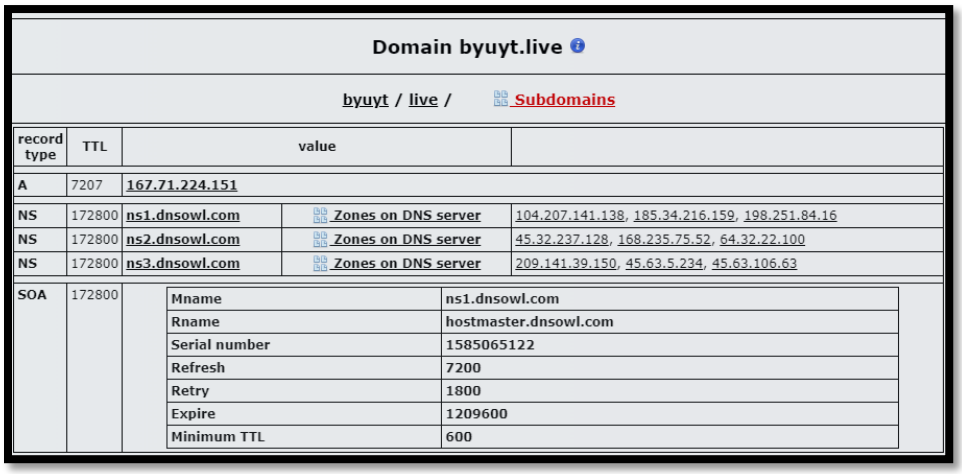
record type	TTL	value		
A	3600	46.254.36.103		
NS	14400	ns3.dyloc.com	Zones on DNS server	46.254.36.103
NS	14400	ns4.dyloc.com	Zones on DNS server	46.254.36.103
MX	3600	0 wenat.it		

SOA	14400	Mname	ns3.dyloc.com
		Rname	info.pedrali.net
		Serial number	2018061801
		Refresh	3600
		Retry	7200
		Expire	1209600
		Minimum TTL	86400

Domain wwmx.banstado.chile.com.byuyt.live

wwmx / banstado / chile / com / byuyt / live / Subdomains

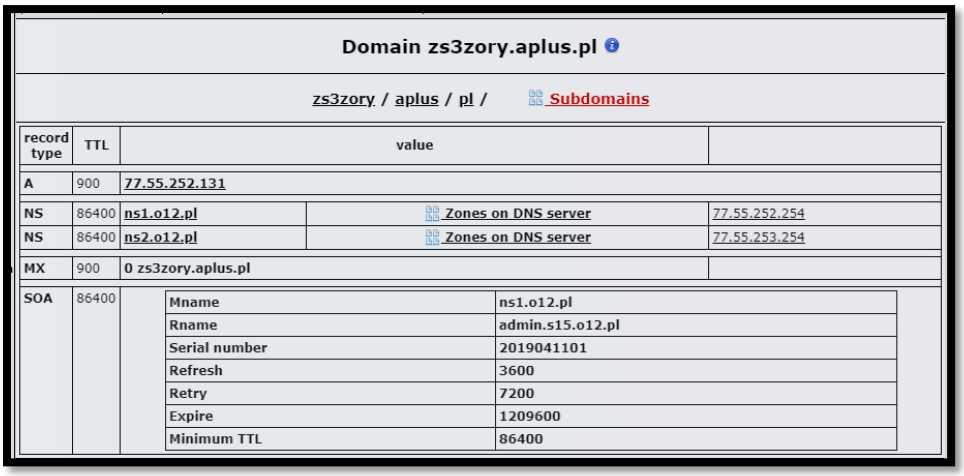
record type	TTL	value
A	7207	167.71.224.151



Domain byuyt.live

byuyt / live / Subdomains

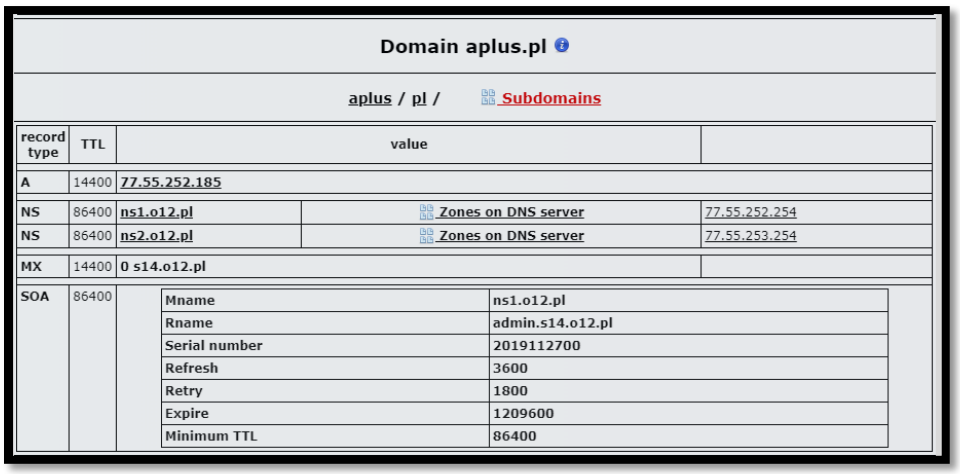
record type	TTL	value		
A	7207	167.71.224.151		
NS	172800	ns1.dnsowl.com	Zones on DNS server	104.207.141.138, 185.34.216.159, 198.251.84.16
NS	172800	ns2.dnsowl.com	Zones on DNS server	45.32.237.128, 168.235.75.52, 64.32.22.100
NS	172800	ns3.dnsowl.com	Zones on DNS server	209.141.39.150, 45.63.5.234, 45.63.106.63
SOA	172800	Mname	ns1.dnsowl.com	
		Rname	hostmaster.dnsowl.com	
		Serial number	1585065122	
		Refresh	7200	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	600	



Domain zs3zory.aplus.pl

zs3zory / aplus / pl / Subdomains

record type	TTL	value		
A	900	77.55.252.131		
NS	86400	ns1.o12.pl	Zones on DNS server	77.55.252.254
NS	86400	ns2.o12.pl	Zones on DNS server	77.55.253.254
MX	900	0 zs3zory.aplus.pl		
SOA	86400	Mname	ns1.o12.pl	
		Rname	admin.s15.o12.pl	
		Serial number	2019041101	
		Refresh	3600	
		Retry	7200	
		Expire	1209600	
		Minimum TTL	86400	



Domain aplus.pl

aplus / pl / Subdomains

record type	TTL	value		
A	14400	77.55.252.185		
NS	86400	ns1.o12.pl	Zones on DNS server	77.55.252.254
NS	86400	ns2.o12.pl	Zones on DNS server	77.55.253.254
MX	14400	0 s14.o12.pl		
SOA	86400	Mname	ns1.o12.pl	
		Rname	admin.s14.o12.pl	
		Serial number	2019112700	
		Refresh	3600	
		Retry	1800	
		Expire	1209600	
		Minimum TTL	86400	

CERTIFICADOS

Certificates

crt.sh ID	Logged At	Not Before	Not After	Matching Identities	Issuer Name
2619995560	2020-03-24	2020-03-24	2020-06-22	wwmx.banstado.chile.com.byuyt.live	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
2619844551	2020-03-24	2020-03-24	2020-06-22	wwmx.banstado.chile.com.byuyt.live	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3

IP DE ORIGEN DONDE SE ALOJA SITIO

Domain crm.wenat.it is located on IP address << 212.237.29.173 >>

Block start	212.237.0.0
End of block	212.237.63.255
Block size	16384 Domains in block
Block name	IT-ARUBABUSINESS-19980925
AS number	31034
Parent block	212.0.0.0 - 212.255.255.255
Organization	ORG-Ws5-RIPE

Domain wwmx.banstado.chile.com.byuyt.live is located on IP address << 167.71.224.151 >>

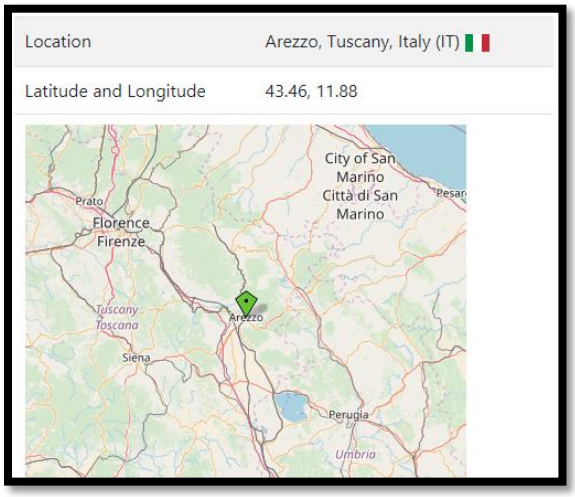
Block start	167.71.0.0
End of block	167.71.255.255
Block size	65536 Domains in block
Block name	APNET
AS number	14061
Parent block	167.0.0.0 - 167.255.255.255
Organization	TheAssociatedPress

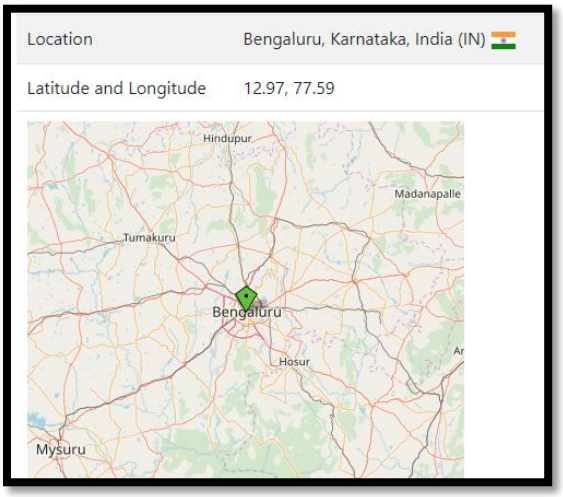
Domain zs3zory.aplus.pl is located on IP address << 77.55.252.131 >>

Block start	77.55.252.0
End of block	77.55.253.255
Block size	512 Domains in block
Block name	NAZWAPL-WEBHOSTING
AS number	15967
Parent block	77.55.0.0 - 77.55.255.255
Organization	webhosting servers

LOCALIZACIÓN

Arezzo, Tuscany, Italia
Bengaluru, Karnataka, India
Krakow, Malopolskie, Polonia





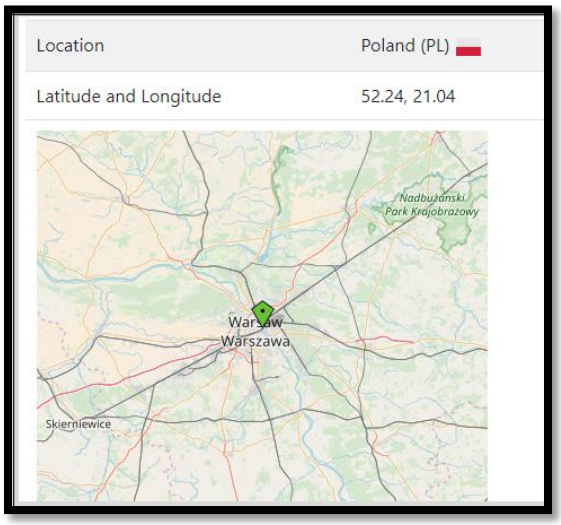
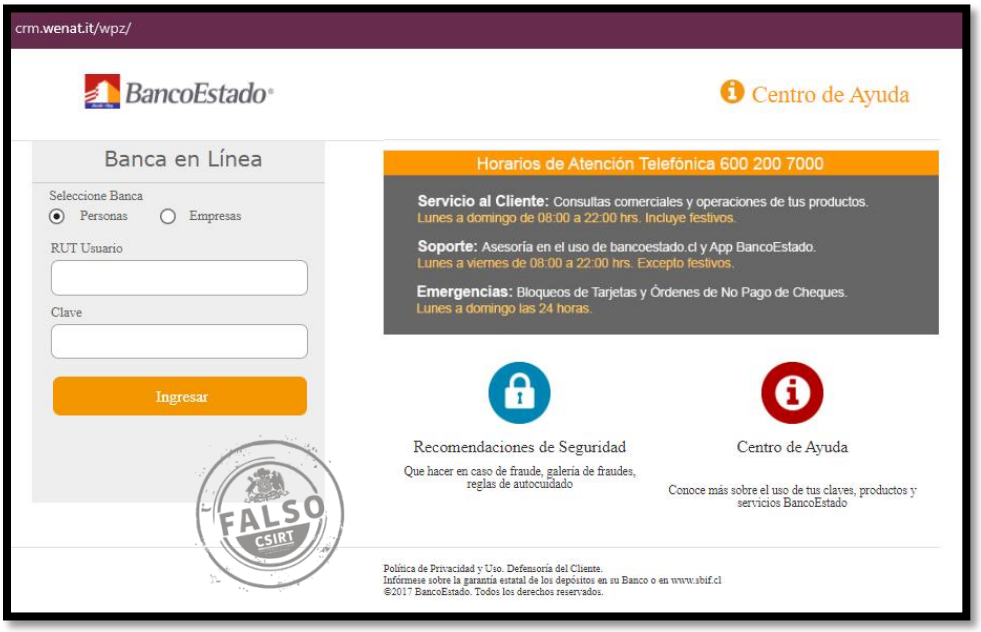
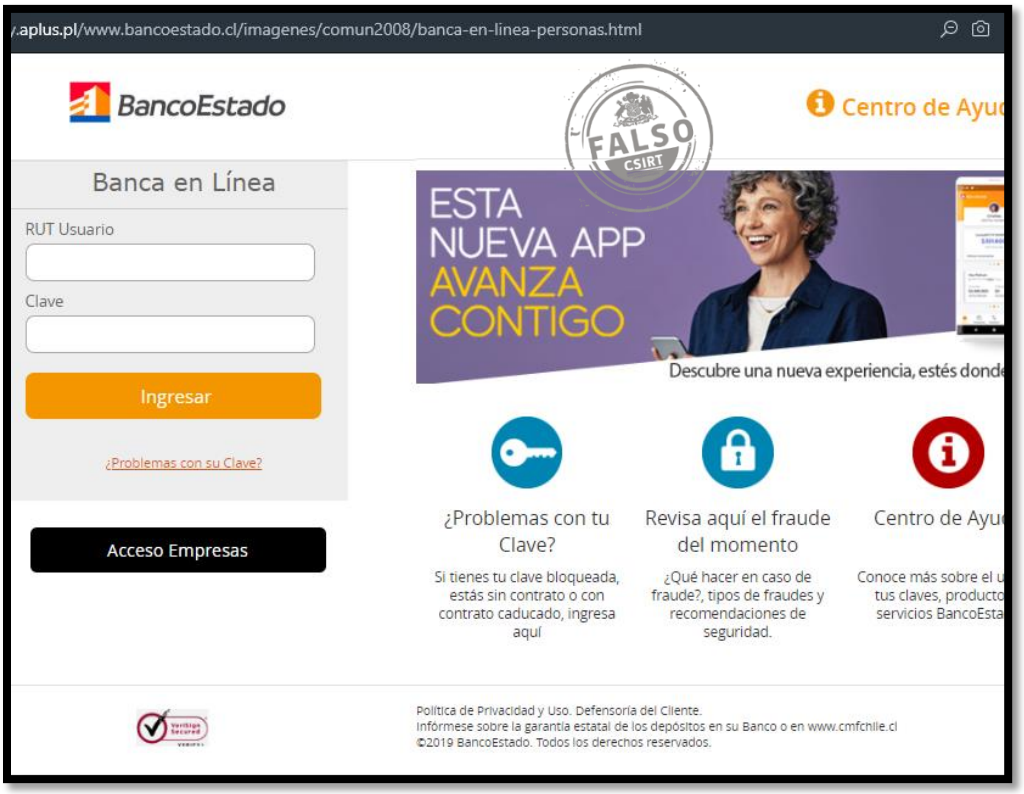


IMAGEN DEL SITIO




aplus.pl/www.bancoestado.cl/imagenes/comun2008/banca-en-linea-personas.html
BancoEstado
FALSO
CSIRT
Centro de Ayu
Banca en Línea
RUT Usuario
Clave
Ingresar
¿Problemas con su Clave?
Acceso Empresas
ESTA NUEVA APP AVANZA CONTIGO
Descubre una nueva experiencia, estés dond
¿Problemas con tu Clave?
Si tienes tu clave bloqueada, estás sin contrato o con contrato caducado, ingresa aquí
Revisa aquí el fraude del momento
¿Qué hacer en caso de fraude?, tipos de fraudes y recomendaciones de seguridad.
Centro de Ayu
Conoce más sobre el u
tus claves, producto
servicios BancoEsta
Política de Privacidad y Uso. Defensoría del Cliente.
Infórmese sobre la garantía estatal de los depósitos en su Banco o en www.cmfchile.cl
©2019 BancoEstado. Todos los derechos reservados.

WHOIS

```
Domain:             wenat.it
Status:             ok
Signed:             no
Created:            2018-04-26 14:15:36
Last Update:        2019-05-12 01:04:41
Expire Date:        2020-04-26

Registrant
  Organization:     Meno22percento S.r.l.
  Address:          via Lungadige Panvinio n°3
                    Verona
                    37100
                    VR
                    IT
  Created:          2018-04-26 14:15:28
  Last Update:      2018-04-26 14:15:28

Admin Contact
  Name:             Livio Di Blasi
  Organization:     Meno22percento S.r.l.
  Address:          via Lungadige Panvinio n°3
                    Verona
                    37100
                    VR
                    IT
  Created:          2018-04-26 14:15:28
  Last Update:      2018-04-26 14:15:28

Technical Contacts
  Name:             hidden
  Organization:     hidden

Registrar
  Organization:     Servizi Internet S.r.l.
  Name:             REGDOM-REG
  Web:              http://www.regdom.it/
  DNSSEC:           no


Nameservers
  ns3.dyloc.com
  ns4.dyloc.com
```

```
Domain Name: byuyt.live
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: https://www.namesilo.com/
Updated Date: 2020-03-24T07:00:00Z
Creation Date: 2020-03-24T07:00:00Z
Registrar Registration Expiration Date: 2021-03-24T07:00:00Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse@namesilo.com
Registrar Abuse Contact Phone: +1.4805240066
Domain Status: ok https://www.icann.org/epp#ok
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-482f3ce134d2f94627c4fdd5682b0e1c@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-482f3ce134d2f94627c4fdd5682b0e1c@privacyguardian.org
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 Email: pw-482f3ce134d2f94627c4fdd5682b0e1c@privacyguardian.org
Name Server: NS1.DNSOWL.COM
Name Server: NS2.DNSOWL.COM
Name Server: NS3.DNSOWL.COM
DNSSEC: unsigned
```

```
DOMAIN NAME:            aplus.pl
registrant type:        organization
nameservers:            ns1.ol2.pl. [77.55.252.254]
                        ns2.ol2.pl. [77.55.253.254]
created:                2004.05.12 17:57:55
last modified:          2019.12.13 08:30:24
renewal date:           2030.05.12 17:57:55

no option

dnssec:                 Unsigned


REGISTRAR:
nazwa.pl sp. z o.o.
ul. Mieczysława Medweckiego 17
31-870 Kraków
Polska/Poland
+48.801 33 22 33
+48.22 454 48 10
+48.22 454 48 08
kontakt@nazwa.pl
www.nazwa.pl
```

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 AntiSam y SandBoxing.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.25 13:03:31 -03'00'