Alerta de Seguridad Informática (8FPH-00040-001)

Nivel de Riesgo: Alto

Tipo: Phishing

Fecha de lanzamiento original: 26 de junio de 2019 | Última revisión 26 de junio 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.

Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing a través de un correo electrónico que intenta engañar a los usuarios del Banco Estado. El correo trata de persuadir a los clientes del Banco indicándoles que por motivos de seguridad han bloqueado clave de acceso a la banca en línea y ofrece la necesidad de que vuelvan a verificar su cuenta, Al hacerlo, se trata de convencer a las personas para que realicen el procedimiento ingresando a los enlaces adjuntos en el correo.

"Estos casos de phishing 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 phishing, 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"

Indicadores de compromisos

Url's:

- http[:]//www.sac.or[.]th/en/@/https://www.bancoestado.cl/?cliente=ebernala@interior.gov.cl
- https[:]//www2.bancoestado.cl.banca-en-linea.b-estado[.]com/BancoEstado/?id=ZWJlcm5hbGFAaW50ZXJpb3IuZ292LmNs

Smtp Host

w11.estado-msg[.]co [109.120.151.86]

Subdominio relacionados

f3.estado-msg[.]co [41.79.78.175]

Sender

BancoEstado.cl@w11.estado-msg[.]co

From (Falso):[1]

BancoEstado.cl BancoEstado.cl@w11.estado-msg[.]co
BancoEstado.cl@q1.estado-msg[.]co - 109.120.152.71
BancoEstado.cl@q10.estado-msg[.]co - 109.120.151.112
BancoEstado.cl@q11.estado-msg[.]co - 109.120.170.137
BancoEstado.cl@q12.estado-msg[.]co - 109.120.170.141

[1] Con aporte del Equipo Coordinador de Seguridad TI, de Aduana, se logró enriquecer esta información.

BancoEstado.cl@q13.estado-msg[.]co - 109.120.148.197
BancoEstado.cl@q14.estado-msg[.]co - 109.120.148.231
BancoEstado.cl@q15.estado-msg[.]co - 109.120.148.232
BancoEstado.cl@q16.estado-msg[.]co - 109.120.170.145
BancoEstado.cl@q17.estado-msg[.]co - 109.120.152.113
BancoEstado.cl@q18.estado-msg[.]co - 109.120.151.167
BancoEstado.cl@q19.estado-msg[.]co - 109.120.152.164
BancoEstado.cl@q2.estado-msg[.]co - 109.120.148.167
BancoEstado.cl@q3.estado-msg[.]co - 109.120.171.118
BancoEstado.cl@q4.estado-msg[.]co - 109.120.170.117
BancoEstado.cl@q5.estado-msg[.]co - 109.120.171.123
BancoEstado.cl@q8.estado-msg[.]co - 109.120.152.89
BancoEstado.cl@q9.estado-msg[.]co - 109.120.151.108
BancoEstado.cl@r10.estado-msg[.]co - 109.120.148.4
BancoEstado.cl@r11.estado-msg[.]co - 109.120.152.210
BancoEstado.cl@r12.estado-msg[.]co - 109.120.171.136
BancoEstado.cl@r13.estado-msg[.]co - 109.120.152.214
BancoEstado.cl@r14.estado-msg[.]co - 109.120.152.221
BancoEstado.cl@r15.estado-msg[.]co - 109.120.148.242
BancoEstado.cl@r16.estado-msg[.]co - 109.120.151.179
BancoEstado.cl@r17.estado-msg[.]co - 109.120.151.183
BancoEstado.cl@r18.estado-msg[.]co - 109.120.152.223
BancoEstado.cl@r19.estado-msg[.]co - 109.120.170.148
BancoEstado.cl@r2.estado-msg[.]co - 109.120.171.131
BancoEstado.cl@r20.estado-msg[.]co - 109.120.152.224
BancoEstado.cl@r3.estado-msg[.]co - 109.120.170.146
BancoEstado.cl@r4.estado-msg[.]co - 109.120.151.173
BancoEstado.cl@r5.estado-msg[.]co - 109.120.152.208
BancoEstado.cl@r6.estado-msg[.]co - 109.120.171.133
BancoEstado.cl@r7.estado-msg[.]co - 109.120.171.134
BancoEstado.cl@r8.estado-msg[.]co - 109.120.151.174
BancoEstado.cl@r9.estado-msg[.]co - 109.120.152.212

BancoEstado.cl@t1.estado-msg[.]co - 109.120.170.151
BancoEstado.cl@t10.estado-msg[.]co - 109.120.152.229
BancoEstado.cl@t11.estado-msg[.]co - 109.120.148.244
BancoEstado.cl@t12.estado-msg[.]co - 109.120.148.245
BancoEstado.cl@t13.estado-msg[.]co - 109.120.151.203
BancoEstado.cl@t14.estado-msg[.]co - 109.120.170.157
BancoEstado.cl@t15.estado-msg[.]co - 109.120.148.249
BancoEstado.cl@t16.estado-msg[.]co - 109.120.148.251
BancoEstado.cl@t18.estado-msg[.]co -109.120.170.159
BancoEstado.cl@t2.estado-msg[.]co - 109.120.152.225
BancoEstado.cl@t20.estado-msg[.]co - 109.120.171.138
BancoEstado.cl@t3.estado-msg[.]co - 109.120.151.192
BancoEstado.cl@t4.estado-msg[.]co - 109.120.151.193
BancoEstado.cl@t5.estado-msg[.]co - 109.120.152.228
BancoEstado.cl@t6.estado-msg[.]co - 109.120.170.152
BancoEstado.cl@t7.estado-msg[.]co - 109.120.148.243
BancoEstado.cl@t8.estado-msg[.]co - 109.120.171.137
BancoEstado.cl@t9.estado-msg[.]co - 109.120.170.155
BancoEstado.cl@w1.estado-msg[.]co - 109.120.171.77
BancoEstado.cl@w10.estado-msg[.]co - 109.120.171.97
BancoEstado.cl@w12.estado-msg[.]co - 109.120.166.157
BancoEstado.cl@w14.estado-msg[.]co - 109.120.148.113
BancoEstado.cl@w15.estado-msg[.]co - 109.120.166.183
BancoEstado.cl@w16.estado-msg[.]co - 109.120.166.199
BancoEstado.cl@w17.estado-msg[.]co - 109.120.170.90
BancoEstado.cl@w19.estado-msg[.]co - 109.120.171.103
BancoEstado.cl@w2.estado-msg[.]co - 109.120.166.115
BancoEstado.cl@w3.estado-msg[.]co - 109.120.151.24
BancoEstado.cl@w4.estado-msg[.]co - 109.120.151.48
BancoEstado.cl@w6.estado-msg[.]co - 109.120.170.51
BancoEstado.cl@w7.estado-msg[.]co - 109.120.170.52
BancoEstado.cl@w8.estado-msg[.]co - 109.120.151.77

BancoEstado.cl@w9.estado-msg[.]co - 109.120.170.66

Subject:

Servicio de Transferencias bloqueado: ********@********.cl

Imagen Phishing correo

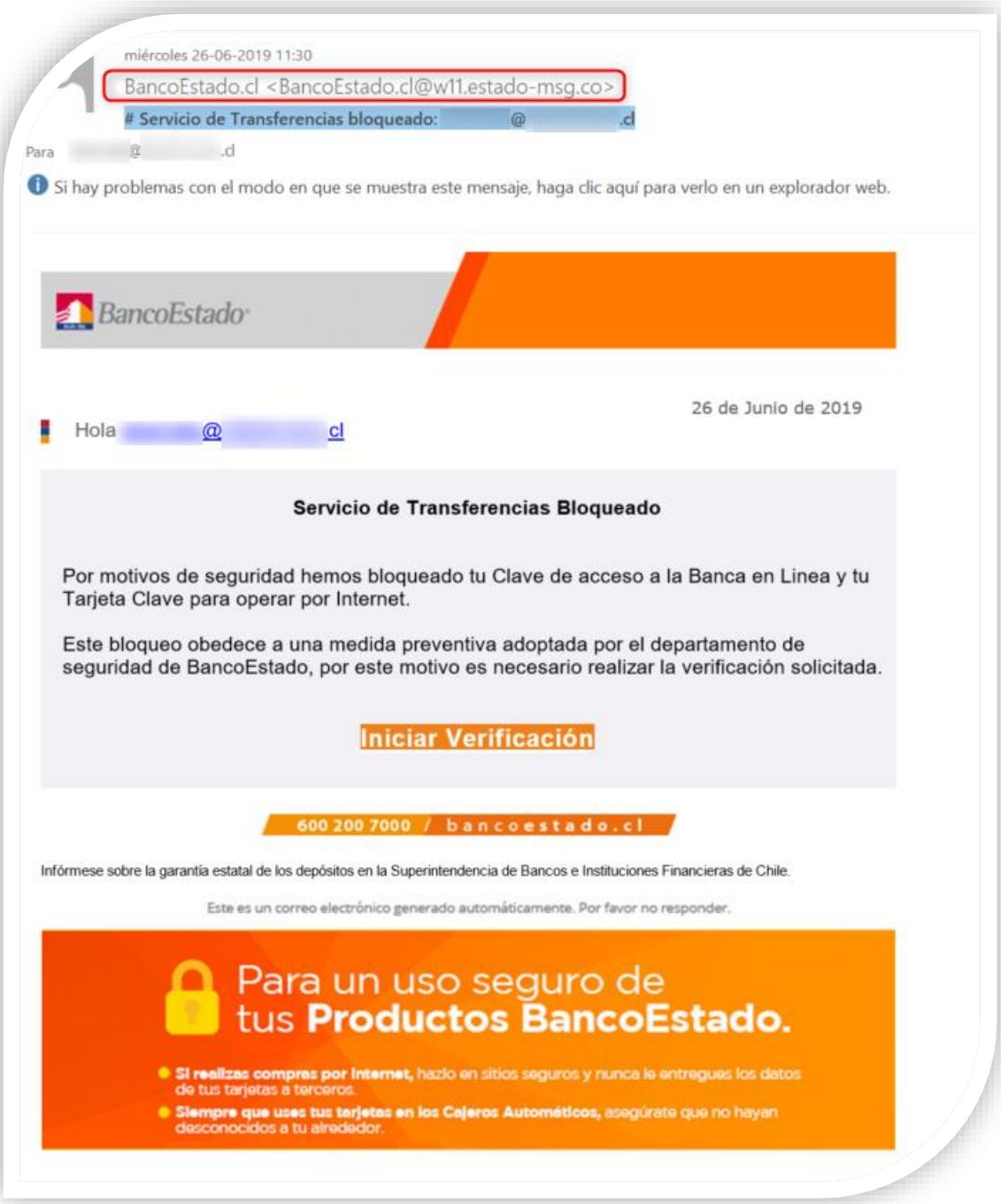
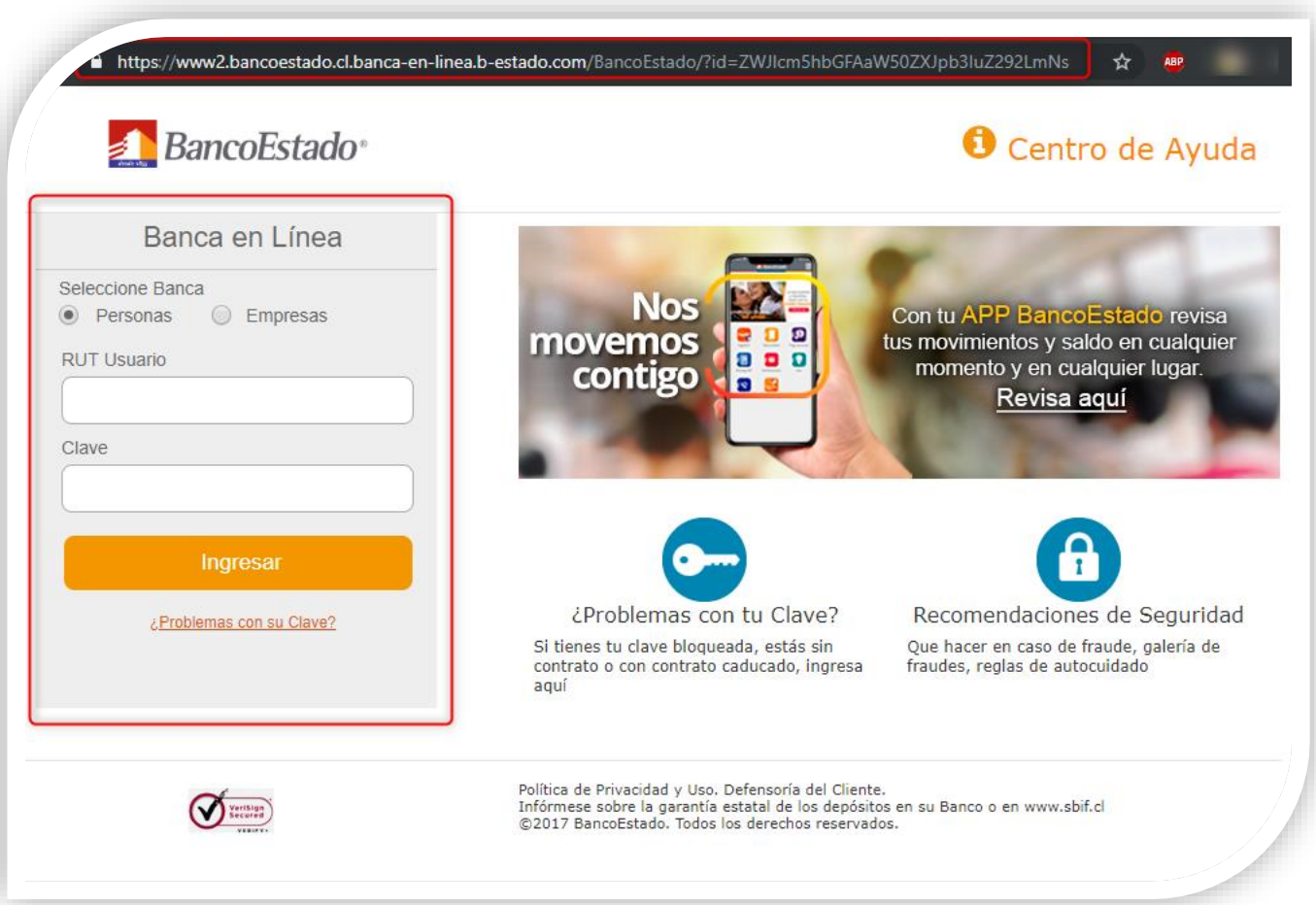


Imagen Sitio Phishing



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- 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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob