Ciberseguridad en Banco Estado

Comisión Economía del Senado

BancoEstado
desde 1855

9 de Septiembre 2020

Agenda

- Contexto
- Antecedentes de los hechos
- Acciones efectuadas
- Avances hasta la fecha
- Programa Ciber Seguridad Banco Estado
- Próximos Pasos

Contexto Internacional

Aumento ataques a instituciones financieras

1) Desde febrero hasta abril de 2020 han crecido un 238%

2) El año 2019 cerca de 4.500 instituciones finacieras fueron atacadas

3) Instituciones financieras, gubernamentales o politicas que recibieron ataques el año 2019: Bundestag Alemán, Facebook, Uber, Banco de la reserva de Australia, Banco en Taiwan, etc.

- https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

eteque | A division of SPAMHAUS

2:25:36

jun. 2019

LIVE BOTNET THREATS WORLDWIDE

The IP address locations of servers used to control computers infected with malware

- Locations with the most intense bot activity
- Command & Control botnet servers

ber of active bots in the last 24 hours

Last 24 hrs hourly activit

Deteque researchers work constantly to update threat intelligence on your behalf.

FIND OUT MORE

TOP 10 WORST BOTNET COUNTRIES

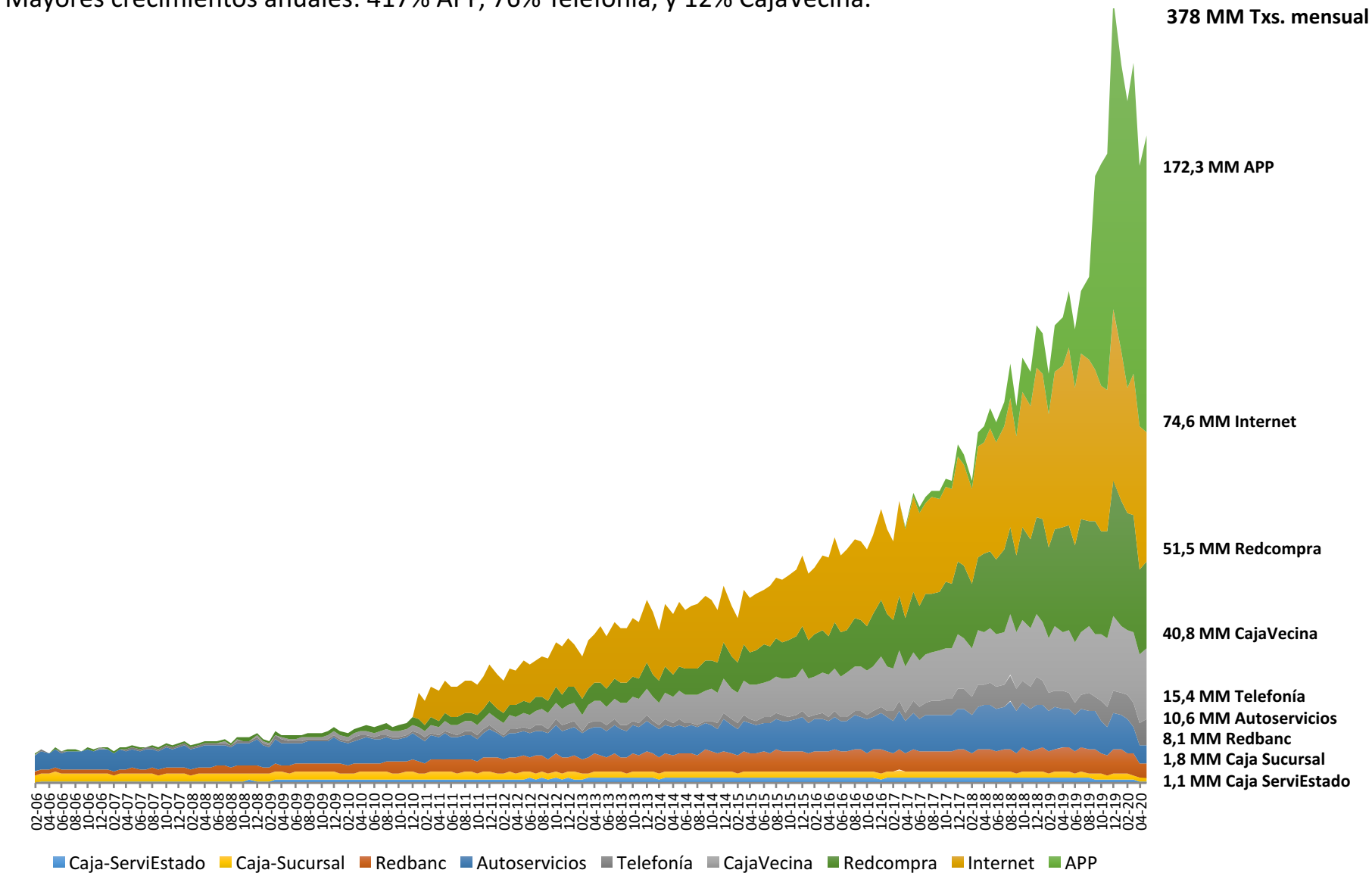
1	India	1994452
2	China	1487222
3	Viet Nam	930853

TOP 10 WORST BOTNET ISPS

1	chinanet.cn.net	973738
2	vnnic.net.vn	903111
3	amazon.com	676308

Transaccionalidad de BancoEstado – Mayo 2020
(cifras en millones de transacciones mes)

378 millones de transacciones en mayo, con una tasa de crecimiento promedio anual del 27,7%.
Mayores crecimientos anuales: 417% APP, 76% Telefonía, y 12% CajaVecina.



Fuente: Informe Resumen Estadístico de Canales Automatizados (RECA) – Mayo 2020

Antecedentes de los hechos

- Sábado 5 de Septiembre se presenta una alerta de máquina afectada.
- El equipo de Ciberseguridad procede a analizar dicha alerta y determina que es un Virus tipo RansomWare.
- Qué hace este: virus daña (encripta) archivos.
- Este Virus se encontraba presente en computadores y servidores Windows. (12.000 de un total de 24.000)
- Se ejecuta protocolo de respuesta de incidente de CiberSeguridad, que considera la activación el comité de crisis

    - Medidas de contención
    - Medición del impacto
    - Establecer el plan de recuperación

- Se contacto inmediatamente al: CSIRT, Subsecretaria de Interior, CMF, ABIF, SERNAC y PDI

Acciones efectuadas

- Medidas de contención
  - Se desconecto el Banco de Internet
  - Se Apagan Servidores mas sensibles: Swift, transacciones de alto valor.
  - Se efectua revisión Completa de los computadores y Servidores Criticos
  - Se controla la propagación
  - Se contrata apoyo especializado con Microsoft, los cuales se constituye inmediatamente.
  - Se implementan herramientas especificas de desinfección para este virus.
  - Activación de Plan de comunicación interno y externo.

- Medición del impacto
  - Este Virus afecto a plataformas Windows, principalmente canales de atención presenciales. (Sucursales Banco, Serviestado)
  - Los servicios no afectados: Son Web personas, APP Movil, Cajeros Automaticos y Caja Vecina.

- Establecer el plan de recuperación
  - Se prioriza el orden en que se restablecen los servicios
  - Se establecen distintos equipos de trabajo
  - Se establece un plan de continuidad operacional

Avances hasta la Fecha

- Malware controlado
- Proceso de desinfección
- Sistemas de Sucursales en recuperación
- Apertura de Oficinas Banco y ServiEstado
- Inteligencia de CiberSeguridad
  - Identificación de presencia del atacante.
  - Identificación de tiempo de presencia y recorrido del atacante.
- No hay afectación de Patrimonio del Banco, no hay robo a clientes.
- Hasta la fecha no existe robo de información

Avance del 2017 hasta la Fecha

Hito 1:

- Informe de BCG 2017 – Brechas y elaboración de Plan de Director de ciberseguridad

Hito 2:

- Post incidente Banco Chile – 2018
- Validación externa de plataforma Windows en materia de ciberseguridad – Remediación de Brechas

Hito 3:

- Ejecución activa de Plan Director de ciberseguridad

Avances 2017 hasta la Fecha

- Plan Ciberseguridad se elaboró con la asesoria de especialistas:

  - BCG
  - Microsoft
  - Fortalecimiento sistema SWIFT
  - Elaboración de Plan de Continudad Operacional
  - Creación de la Gerencia de Ciberseguridad

Plan de Ciberseguridad Banco Estado

Mitigación, detección temprana, respuesta oportuna

1. Elevar la madurez de las capacidades de SI a la par de actores comparables de la región
2. Llegar a un nivel de cobertura funcional que asegure que todos los elementos clave están siendo cubiertos
3. Enfocar en aquellos elementos que representen el mayor retorno en términos de mitigación del riesgo de SI
4. Generar un alto nivel de sensibilización de la importancia de la Seguridad de la Información y las responsabilidades de cada persona, a todo nivel en la organización
5. Adecuar el actual gobierno y organización moviéndonos hacia una dirección y dimensión que se haga cargo de los nuevos desafíos

Hemos potenciado 4 pilares fundamentales

1 Institucionalidad

- Contamos con instancias de gobierno de seguridad: Directorio, Comités de Riesgos, Procesos y Tecnología, Mesas Directivas.

- Contamos con protocolos de crisis y un equipo de respuesta ante incidentes de ciberseguridad (ERIC símil CSIRT)

- Contamos con un esquema de Políticas y Normas Específicas de Riesgo y Seguridad de la Información, aprobadas en el Comité de Riesgos y el Directorio.

- Utilizamos un marco metodológico para el control y gestión (ISO 27001/27002).

- Se creo Gerencia de Ciber Seguridad (Junio 2019).

Hemos potenciado 4 pilares fundamentales

2 Tecnología para nosotros y los clientes

- Para Clientes: diversos mecanismos para resguardo de información sensible (2da y 3ra Clave, Chip en tarjetas, entre otros).

- Para Clientes: Educación digital y de seguridad

- Infraestructura tecnológica para la protección de activos críticos expuesto al ciberespacio (Firewall, Sistema de prevención de intrusos y anti denegación de servicios)

- Planes de Continuidad Tecnológicos (DRP) y Operacionales (BCP), para enfrentar diversos escenarios de indisponibilidad tecnológica de servicios.

Hemos potenciado 4 pilares fundamentales

3 Organización para Gestión del Riesgo Operacional y Tecnológico

- Implementación de estrategia de Seguridad de la Información a nivel:
  - Estratégico (Comités),
  - Táctico (Mesas de Seguridad y Equipo de Respuesta ante Incidentes de Ciberseguridad)
  - Operacional

- Instancias de coordinación entre bancos para temas de ciberseguridad

Hemos potenciado 4 pilares fundamentales

4 Planes de Seguridad Interna

- Programa de concienciación hacia los trabajadores del Banco
- Capacitaciones especializadas en Seguridad de la Información y Ciberseguridad
- Simulaciones de ingeniería social (ej.phishing falso, USB abandonados)
- Medición nivel de adherencia cultural en ciberseguridad en BancoEstado
- Medidas restrictivas, tales como: Uso de Pendrives, accesos a sitios web, restricciones a correos externos.

Inversiones realizadas 2017 a la fecha

- Implementación de 2 Sitios de contingencia
- Nuevos Firewalls
- Boveda de Contraseña para transacciones de alto valor
- Centro de monitoreo de Seguridad
- Encriptación de Discos con información sensible
- Consultorias BCG y Microsoft

- Total: US$ 20 millones.

Próximos pasos

1) Persecución del delito
a) Informe forense Microsoft
b) Denuncia e investigación PDI
c) Querella

2) Actualización de información
a) Auditoría Interna / Externa
b) Actualización reporte BCG

3)Continuidad Ejecución Plan Director de Ciberseguridad

Ciberseguridad en Banco Estado

Comisión Economía del Senado

BancoEstado
desde 1855

9 de Septiembre 2020