FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROYECTO FINAL

Autores (Agila Elvis, Cardoza Renato, Chimbo Verónica)
Estudiantes del curso [ICBS0019-1979] – [CIBERINTELIGENCIA],
Universidad de Las Américas, Quito-Ecuador

I. RESUMEN

En este informe se realizará una investigación de CTI sobre una institución de Ecuador.

II. OBJETIVOS

- Realizar un análisis de Ciber inteligencia.

III. MATERIALES Y EQUIPOS COMPLEMENTARIOS

- Laptop
- Leak peak
- DnsDumpster

IV. PROCEDIMIENTO O DESARROLLO

***Elección de una institución de Ecuador.**

BANCO PICHINCHA

***Identificación de las necesidades de inteligencia de la institución.**

- Conocer la postura de seguridad de mis proveedores.
- Conocer la reputación de mis proveedores.
- Adelantarme a la materialización de incidentes de seguridad por medio de reportes de inteligencia que contengan indicadores de compromiso.
- Neutralización de amenazas del ciber espacio.
- Conocer los actores que amenazan mis activos (nombres, capacidades, infraestructura, posibilidad de falsos positivos).
- Automatización del proceso de inteligencia.

- Compartir inteligencia con otras instituciones de rubro.
- Detección de insiders dentro de la institución.
- Protección de Canales Digitales.
- Gestión de Riesgos Cibernéticos.

***Análisis de capacidades que debe contar la institución.**

Capacidades Tecnológicas

- Infraestructura Segura
- Sistemas de Monitoreo
- Plataformas de Inteligencia de Amenazas (TIP)
- Cifrado de Datos
- Autenticación Segura

Capacidades de Inteligencia y Análisis

- OSINT (Inteligencia de Fuentes Abiertas)
- Análisis de Malware
- Ciberinteligencia Estratégica y Operacional
- Gestión de Vulnerabilidades

Capacidades Humanas y Organizativas

- Equipo de Ciberseguridad Especializado
- Concienciación y Capacitación
- Procedimientos de Respuesta a Incidentes

Capacidades Regulatorias y de Cumplimiento

- Cumplimiento Normativo
- Gestión de Riesgos Cibernéticos
- Auditorías de Seguridad

Capacidades de Resiliencia y Continuidad del Negocio

- Planes de Continuidad y Recuperación ante Desastres
- Backups Seguros y Redundantes

***Perfilamiento de la empresa**

- Fuga de credenciales

  Las fuentes de exfiltración de información de mayor impacto para la institución son las siguientes:
  Source unavailable. (Potencialmente credenciales robadas por virus de tipo stealer, ingeniería social y otras fuentes)
  LinkedIn
  AdultFriendFinder
  Deezer.com
  Jobandtalent.com
  MyHeritage.com

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Results for pichincha.com (942)

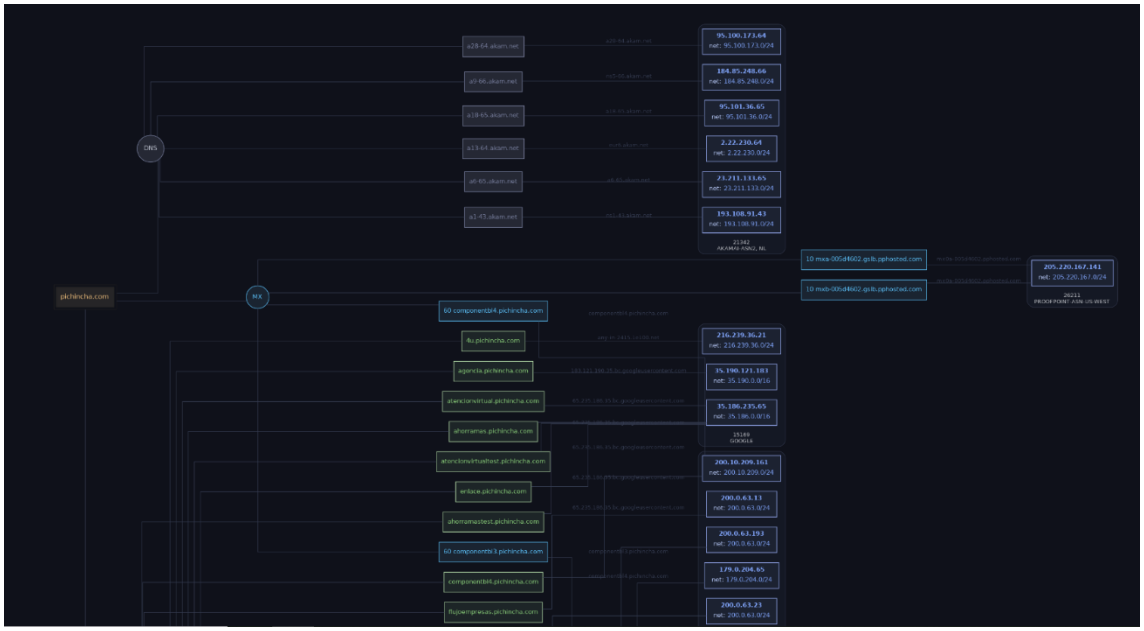
At Risk

Show 25 entries Search:

Passwords Found	Source
ivintimi@pichincha.com	Wattpad.com, Deezer.com, Trello.com, Luxottica
pvallejo@pichincha.com:lilolilo1234	MyHeritage.com, Wattpad.com, Kienthucphukhoa.net, asap.me
eorti@pichincha.com	Gatehub.net, Deezer.com, Trello.com
gaortiz@pichincha.com	Twitter.com (scraping data), Trello.com, Dubsmash.com
ntviteri@pichincha.com	Canva.com, Slideteam.net, Trello.com
erpico@pichincha.com:eliana	Collection 1, Taringa.net, Gigasize.com
lbasante@pichincha.com:pcceja	MyHeritage.com, Taringa.net
resoto@pichincha.com:qnkd6r	MyHeritage.com, Canva.com
hpazmino@pichincha.com:quimera	LinkedIn.com, flores.com.bo
jbeltran@pichincha.com	Verifications.io, Pureincubation.com

*** Identificaciones de vulneraciones y potencial exposición de portales o información sensible.**

Superficie de Ataque.



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

*** Análisis de vulnerabilidades**

El escaneo realizado muestra un **nivel de riesgo general bajo**, lo cual es positivo.

Aunque el riesgo general es bajo, es importante investigar y abordar el riesgo bajo identificado para prevenir posibles vulnerabilidades en el futuro. Es importante mantener un monitoreo regular para asegurarte de que no surjan nuevos riesgos. El escaneo indica un buen estado de seguridad, pero es crucial no descuidar el riesgo bajo identificado para mantener un entorno seguro.

*** Indagación de incidentes de ciberseguridad**

BANCO PICHINCHA

Comunicado oficial a nuestros clientes

En las últimas horas, hemos identificado un incidente de ciberseguridad en nuestros sistemas informáticos que ha inhabilitado parcialmente nuestros servicios. Hemos tomado acciones inmediatas como aislar los sistemas potencialmente afectados del resto de nuestra red y contar con expertos de ciberseguridad para asistir en la investigación.

Al momento, nuestra red de agencias, cajeros automáticos para retiros de efectivo y pagos con tarjetas de débito y crédito están operativos.

Este incidente tecnológico no afecta el desempeño financiero del banco. Reiteramos nuestro compromiso en precautelar los intereses de nuestros clientes y restablecer la atención normal a través de nuestros canales digitales en el menor tiempo posible.

Hacemos un llamado a la calma para no generar congestión y mantenerse informados a través de los canales oficiales de Banco Pichincha para evitar la propagación de rumores falsos.

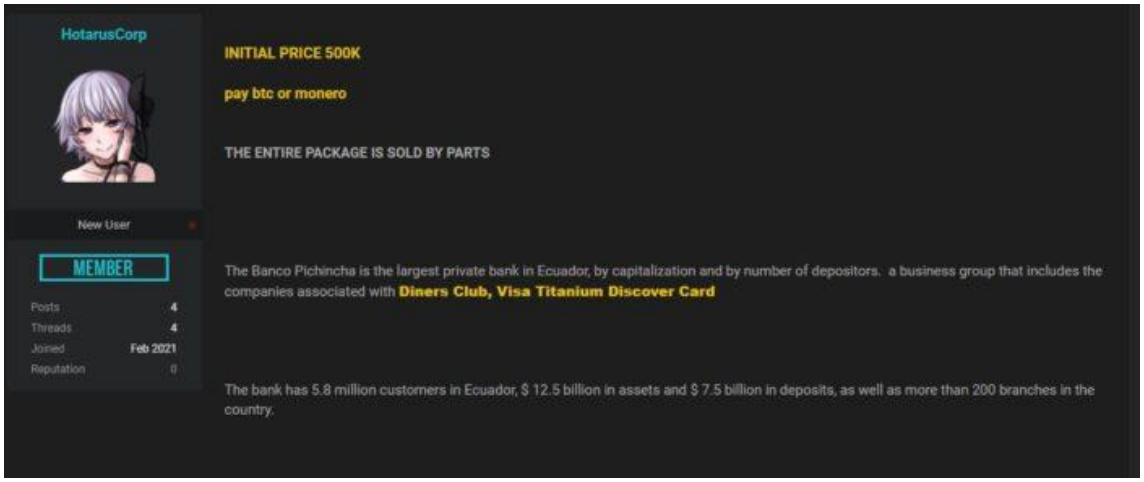
Quito, 11 de octubre de 2021

Antonio Acosta
Presidente

Santiago Bayas
Gerente General

El Banco Pichincha de Ecuador ha enfrentado varios incidentes de ciberseguridad en 2021. En febrero, se reportó una filtración masiva de datos personales de clientes debido a un acceso no autorizado a los sistemas de un proveedor de mercadeo. El grupo

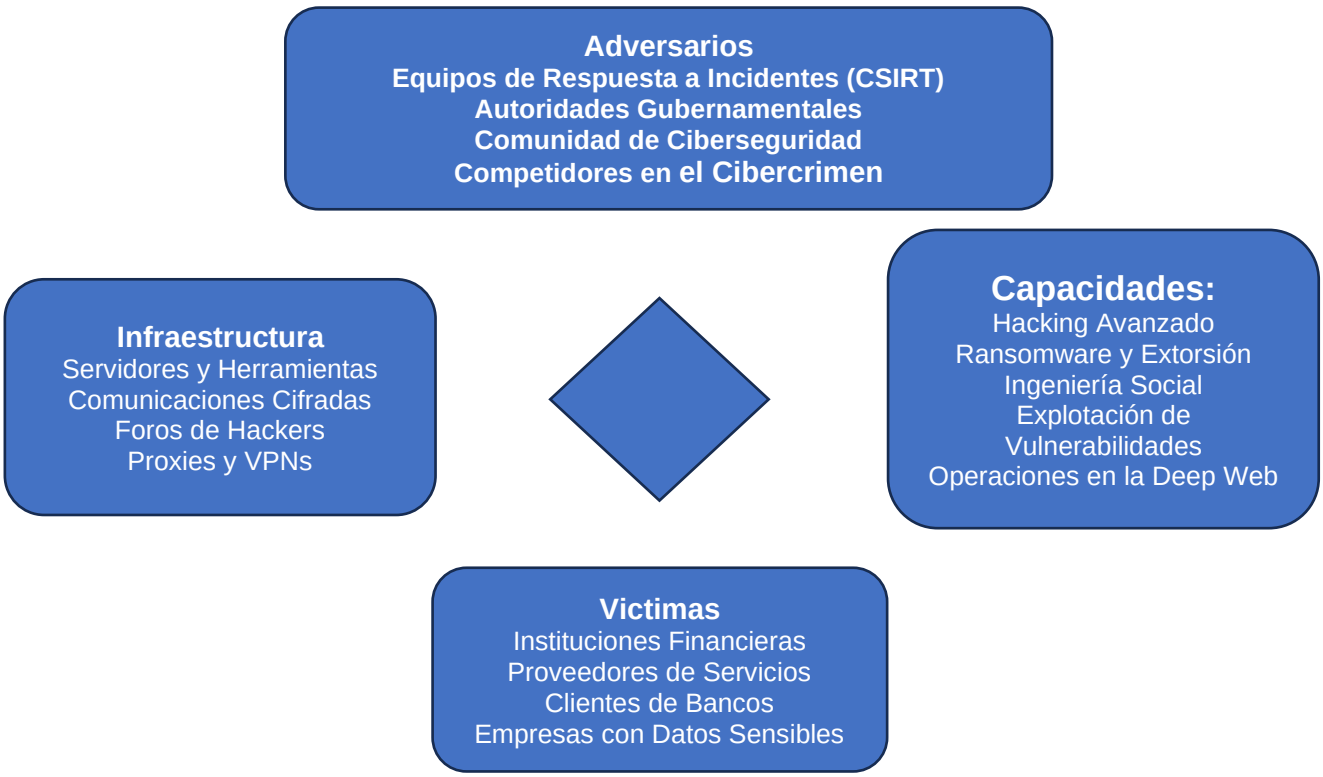
de ciberdelincuentes Hotarus Corp exigió un rescate, pero al no recibir pago, liberó la base de datos en foros de hackers. En julio, la misma base de datos fue liberada gratuitamente en la deep web. En octubre, el banco experimentó un incidente de ciberseguridad que dejó sus canales electrónicos fuera de servicio por más de 72 horas. Aunque el banco aseguró que sus sistemas no fueron vulnerados directamente, el incidente afectó significativamente sus operaciones digitales.



Los incidentes repetidos de ciberseguridad pueden erosionar la confianza de los clientes en la capacidad del banco para proteger sus datos personales y financieros. La filtración de datos y los ataques a los sistemas digitales son preocupaciones significativas para los usuarios.

A pesar de los ataques, el banco ha logrado mantener operativos sus cajeros automáticos, lo que indica una planificación de continuidad del negocio. Sin embargo, la interrupción prolongada de los servicios digitales afecta la experiencia del cliente y puede tener repercusiones financieras.

*** Perfilamiento de adversarios**



Análisis del Perfil de Hotarus Corp

- Hotarus Corp se enfoca en instituciones financieras y sus proveedores, buscando datos sensibles que puedan monetizar mediante extorsión o venta en la deep web.
- Utilizan una combinación de hacking técnico y explotación de terceros para acceder a redes corporativas. Su capacidad para operar en la deep web les permite evadir la detección y mantener el anonimato.
- Sus ataques tienen un alto impacto en la reputación y la confianza de las instituciones financieras, además de exponer a los clientes a riesgos de fraude y robo de identidad.
- Las instituciones afectadas deben fortalecer la seguridad de sus proveedores, implementar monitoreo continuo y colaborar con autoridades para rastrear y desmantelar la infraestructura del grupo.

V. CONCLUSIÓN Y RECOMENDACIÓN

Conclusión:

El caso del Banco Pichincha subraya la importancia de una estrategia integral de ciberseguridad que incluya la protección de sistemas internos y externos, la detección temprana de amenazas y una respuesta rápida y efectiva a incidentes. La colaboración con proveedores, autoridades y la comunidad de ciberseguridad es crucial para mitigar riesgos y proteger los datos de los clientes. Además, la inversión en concientización y capacitación del personal puede reducir significativamente la superficie de ataque y mejorar la resiliencia frente a futuros ciberataques.

Recomendaciones:

- Realizar auditorías de seguridad periódicas a proveedores externos
- Incluir cláusulas de seguridad en los contratos con proveedores para garantizar el cumplimiento de estándares de ciberseguridad.
- Implementar sistemas de detección de intrusiones (IDS) y monitoreo de redes para identificar actividades sospechosas.
- Capacitar a empleados y proveedores en prácticas de seguridad, como la identificación de phishing.
- Participar en comunidades de intercambio de inteligencia sobre amenazas para mantenerse actualizado sobre nuevas tácticas y técnicas.

VI. BIBLIOGRAFÍA COMPLEMENTARIA

1. **El Comercio** (2021). *Banco Pichincha enfrenta ciberataque: Canales electrónicos sin servicio por más de 72 horas*.
   Disponible en: https://www.elcomercio.com/actualidad/negocios/banco-pichincha-ciberseguridad-ciberataque-hackeo.html
   (Artículo principal utilizado como fuente para los detalles del incidente del Banco Pichincha).

2. **MITRE ATT&CK Framework**.
   Disponible en: https://attack.mitre.org/

(Marco de referencia utilizado para analizar las tácticas, técnicas y procedimientos (TTPs) de los ciberataques).

3. **NIST Cybersecurity Framework**.
   Disponible en: https://www.nist.gov/cyberframework
   (Referencia para las recomendaciones de mejora en la gestión de ciberseguridad).

4. **Europol** (2021). *Internet Organized Crime Threat Assessment (IOCTA)*.
   Disponible en: https://www.europol.europa.eu/iocta-report
   (Informe sobre tendencias de cibercrimen y grupos de hackers).

5. **Krebs on Security**.
   Disponible en: https://krebsonsecurity.com/
   (Blog especializado en ciberseguridad que analiza incidentes y grupos de ciberdelincuentes).

6. **Dark Reading**.
   Disponible en: https://www.darkreading.com/
   (Portal de noticias y análisis sobre ciberseguridad).

7. **IBM Security X-Force Threat Intelligence Index**.
   Disponible en: https://www.ibm.com/security/data-breach/threat-intelligence
   (Informe anual sobre tendencias de ciberamenazas y grupos de hackers).

8. **CISA (Cybersecurity and Infrastructure Security Agency)**.
   Disponible en: https://www.cisa.gov/
   (Recursos y guías para la gestión de incidentes de ciberseguridad).

9. **OWASP (Open Web Application Security Project)**.
   Disponible en: https://owasp.org/
   (Referencia para buenas prácticas en la protección de aplicaciones y sistemas).

10. **Hotarus Corp y grupos de hackers**:

    Información basada en reportes de medios y análisis de incidentes públicos. No hay una fuente oficial específica, pero se utilizaron referencias de **El Comercio** y otros medios ecuatorianos.

11. **Modelo de Diamante para Análisis de Amenazas**:

    Caltagirone, S., Pendergast, A., & Betz, C. (2013). *The Diamond Model of Intrusion Analysis*.
    Disponible en: https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
    (Marco teórico utilizado para el perfilamiento de adversarios).

12. **Deep Web y Foros de Hackers**:

    Información basada en reportes de medios y análisis de inteligencia de amenazas. No hay una fuente única, pero se utilizaron referencias de **Krebs on Security** y **Dark Reading**.