



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

PROYECTO FINAL

Autores (Agila Elvis)

Estudiantes del curso [ICBS0019-1979] – [CIBERINTELIGENCIA],
Universidad de Las Américas, Quito-Ecuador

I. RESUMEN

Este informe presenta un análisis de Ciberinteligencia (CTI) sobre el **Banco Pichincha de Ecuador**, evaluando su postura de seguridad, las amenazas ciberneticas que enfrenta y su capacidad para detectar, mitigar y responder a incidentes. Se aplican metodologías de inteligencia de amenazas y análisis forense digital para identificar vulnerabilidades, perfilamiento de adversarios y exposición de datos sensibles.

El estudio revisa incidentes pasados, incluyendo ataques de ransomware y filtraciones de datos, y proporciona recomendaciones para fortalecer la seguridad del banco mediante auditorías, detección temprana de amenazas y colaboración con proveedores y organismos de seguridad. Se utilizan herramientas como **LeakPeek, DnsDumpster y análisis OSINT** para obtener información clave sobre la superficie de ataque del banco y sus posibles brechas de seguridad.

II. OBJETIVOS

1. Evaluar la postura de seguridad del banco mediante análisis OSINT y herramientas de inteligencia de amenazas.
2. Identificar incidentes de ciberseguridad previos y analizar su impacto en la reputación y operaciones del banco.
3. Determinar la exposición de credenciales y datos sensibles en la dark web y foros de hacking.
4. Perfilamiento de adversarios como grupos de ciberdelincuentes que han atacado la institución.
5. Analizar vulnerabilidades en los portales digitales y sistemas del banco, evaluando el nivel de riesgo de cada hallazgo.
6. Proponer estrategias de mitigación que incluyan medidas técnicas, organizativas y regulatorias para mejorar la seguridad.

III. MATERIALES Y EQUIPOS COMPLEMENTARIOS

Recomendar el fortalecimiento de la inteligencia de amenazas mediante la automatización, monitoreo continuo y colaboración con entidades de seguridad.

- Laptop
- Leak peak
- DnsDumpster
- MitreAttack
- Google Dorks
- Virus Total
- Hybryd Analysis

IV. PROCEDIMIENTO O DESARROLLO

*Elección de una institución de Ecuador.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

BANCO PICHINCHA



El Banco Pichincha, una de las principales instituciones financieras de Ecuador, desempeña un papel crucial en la economía del país al ofrecer servicios bancarios a millones de clientes. Como entidad que maneja una gran cantidad de información financiera y datos personales, enfrenta constantes desafíos en materia de ciberseguridad. La creciente sofisticación de los ataques cibernéticos y la evolución de las amenazas digitales han llevado al banco a fortalecer sus estrategias de inteligencia y defensa. Para garantizar la seguridad de su infraestructura y la protección de sus clientes, el Banco Pichincha ha identificado diversas necesidades de inteligencia clave, entre las que destacan:

1. Protección de credenciales y datos sensibles: Salvaguardando la información financiera y personal de los clientes, así como evitando accesos no autorizados a sistemas internos.
2. Monitoreo de vulnerabilidades: Evaluando continuamente sus plataformas digitales y sistemas internos para detectar y mitigar posibles intentos de explotación.
3. Gestión de la superficie de ataque: Reduciendo los activos expuestos en la red y clasificando los sistemas según su criticidad.
4. Protección contra amenazas externas: Implementando estrategias para mitigar ataques dirigidos como phishing y malware, además de monitorear foros y mercados oscuros en busca de información filtrada.

A través de estas estrategias, el Banco Pichincha busca no solo fortalecer su postura de seguridad, sino también anticiparse a incidentes, mejorar la gestión de riesgos y garantizar la confianza de sus clientes en un entorno digital cada vez más amenazante.

Capacidades de Seguridad en el Banco Pichincha

Dada la creciente amenaza del cibercrimen, el Banco Pichincha debe contar con una estrategia de seguridad robusta que le permita detectar, prevenir y responder eficazmente a incidentes. Para ello, se identifican las siguientes capacidades clave:

1. Herramientas Tecnológicas
 - Implementación de sistemas SIEM para la recopilación, análisis y correlación de eventos de seguridad en tiempo real.
 - Soluciones de gestión de identidad y acceso (IAM) para garantizar que solo usuarios autorizados accedan a los sistemas críticos.
2. Recursos Humanos
 - Personal especializado en ciberinteligencia y gestión de incidentes, capaz de identificar y mitigar amenazas avanzadas.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

- Expertos en evaluación de vulnerabilidades y auditorías de seguridad para mantener la resiliencia del banco frente a posibles ataques.
3. Respuesta a Incidentes y Continuidad del Negocio
- Protocolos de respuesta inmediata ante incidentes de seguridad para minimizar el impacto en los servicios financieros y la reputación del banco.
 - Planes de recuperación ante desastres para garantizar la continuidad de las operaciones, incluso en situaciones críticas.
4. Colaboración Externa
- Asociación con CERTs y grupos de respuesta a incidentes a nivel nacional para recibir alertas y asistencia en caso de ciberataques.
 - Participación en iniciativas internacionales de intercambio de información sobre amenazas, permitiendo al banco adelantarse a posibles ataques dirigidos.

Perfilamiento de la empresa

1. Fuga de Credenciales y Exposición de Datos Sensibles

El análisis muestra que múltiples cuentas de correo del dominio **pichincha.com** han sido comprometidas y expuestas en diversas plataformas. Algunas credenciales filtradas incluyen **contraseñas en texto plano** asociadas a servicios como **MyHeritage, Wattpad, Canva, Twitter, LinkedIn y Trello**. Esta filtración expone a la institución a ataques dirigidos como:

- **Fuerza bruta y reutilización de credenciales** en sistemas internos.
- **Ataques de phishing personalizados** para obtener acceso a información financiera y administrativa.
- **Movimientos laterales dentro de la infraestructura interna**, si los empleados reutilizan contraseñas en entornos corporativos.

Recomendaciones:

- Implementar un **proceso de rotación de contraseñas** obligatorio para empleados.
- Habilitar **autenticación multifactorial (MFA)** en todas las cuentas internas y sistemas sensibles.
- Utilizar **monitorización continua** para detectar accesos inusuales a sistemas corporativos.
- Realizar campañas de **concienciación en ciberseguridad** sobre el riesgo de reutilizar credenciales.

2. Identificación de Vulnerabilidades y Potencial Exposición

El hecho de que estas credenciales provengan de **plataformas de terceros** sugiere una **falta de control sobre el uso de cuentas corporativas en servicios externos**. Además, la filtración de credenciales en bases de datos expuestas podría ser explotada por cibercriminales para acceder a la infraestructura del banco.

Recomendaciones:

- **Restringir el uso de correos corporativos** en servicios no autorizados.
- Implementar **políticas de gestión de contraseñas** que incluyan el uso de administradores de contraseñas seguros.
- Realizar auditorías para verificar si las credenciales expuestas han sido utilizadas en accesos internos.

3. Superficie de Ataque y Riesgo de Exposición

La presencia de credenciales filtradas en servicios de almacenamiento en la nube y redes

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

sociales **aumenta la superficie de ataque** del banco. Un atacante podría utilizar técnicas de **ingeniería social** para obtener acceso a sistemas internos o suplantar empleados en ataques dirigidos.

Recomendaciones:

- Implementar un sistema de **detección de accesos sospechosos** con análisis de comportamiento de usuarios.
- Limitar el acceso a información sensible a través de **políticas de acceso basadas en roles (RBAC)**.
- Aplicar controles estrictos en el uso de **VPNs y redes internas** para mitigar accesos no autorizados.

4. Colaboración y Prevención de Amenazas

El banco debe fortalecer su colaboración con equipos de **respuesta a incidentes (CERTs)** y participar en iniciativas de **intercambio de inteligencia sobre amenazas** para recibir alertas tempranas sobre credenciales filtradas.

Recomendaciones:

- Integrar sistemas de **Threat Intelligence** que permitan **detectar credenciales comprometidas en tiempo real**.
- Fortalecer la cooperación con organismos de ciberseguridad nacionales e internacionales.
- Aplicar simulaciones de ataques dirigidos (**Red Teaming**) para evaluar la respuesta del banco ante una posible explotación de credenciales filtradas.

Results for pichincha.com (942)	
At Risk	
Show	entries
Passwords Found	Source
ivintimi@pichincha.com	Nettitude.com, Dezer.com, Trello.com, Luxottica
pvallejo@pichincha.com:lilolilo1234	MyHeritage.com, Nettitude.com, ClientHushPhish.net, easy-pe
eorti@pichincha.com	Dezer.com, Dezer.com, Trello.com
gaortiz@pichincha.com	Twitter.com (virusing data), Trello.com, Dubanish.com
ntviteri@pichincha.com	Canva.com, Elidetam.net, Trello.com
erpico@pichincha.com:eliana	Collection 1, Ferringi.net, Bigsize.com
lbasante@pichincha.com:pcceja	MyHeritage.com, Ferringi.net
resoto@pichincha.com:qnkd6r	MyHeritage.com, Canva.com
hpazmino@pichincha.com:quimera	LinkedIn.com, Filmes.co.bo
jbeltran@pichincha.com	Verifications.io, PureInnovation.com

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Breakdown of results and more info		
Verifications.io		
email	pichincha.com	
Collections		
email	gogomez@pichincha.com	
password	1803462926	
Collections		
email	sanpaez@pichincha.com	
password	*22Autos	
AntiPublic		
email	zaasan@pichincha.com	Activar Windows Visita Configuración para...
password	Amar2876	

Análisis de Debilidades y Posibles Tecnologías Utilizadas en Base al Escaneo DNSDumpster

El análisis de DNSDumpster proporciona información sobre los registros DNS, subdominios y direcciones IP asociadas a los sistemas del Banco Pichincha. A partir de estos datos, se pueden identificar posibles debilidades de seguridad y deducir el uso de ciertos servicios y lenguajes de programación en su infraestructura.

1. Debilidades Detectadas

1.1 Exposición de Subdominios Críticos

El escaneo muestra múltiples subdominios asociados a servicios internos y externos, incluyendo:

- component01.pichincha.com, componentb1.pichincha.com, componentb2.pichincha.com (posiblemente APIs o microservicios internos).
- exchange.pichincha.com (sistema de intercambio financiero).
- creditonline.pichincha.com (servicio de crédito en línea).
- cdn.pichincha.com, cdn-dev.pichincha.com (sistema de distribución de contenido).
- view.email.pichincha.com, cloud.email.pichincha.com, click.email.pichincha.com (servicios de correo electrónico).

Posibles vulnerabilidades:

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

- Subdomain Takeover: Si un subdominio apunta a un servicio externo no reclamado, un atacante podría tomar el control y hospedar contenido malicioso.
 - APIs expuestas: Si las APIs de los servicios financieros no tienen autenticación adecuada, podrían ser vulnerables a inyecciones SQL, ataques de fuerza bruta o API abuse.
 - Correos electrónicos expuestos: Riesgo de phishing o spoofing si no están configurados adecuadamente los registros SPF, DKIM y DMARC.
- ◆ Medidas recomendadas:
- Auditar y eliminar subdominios no utilizados para reducir la superficie de ataque.
 - Implementar autenticación y autorización en APIs para restringir accesos no autorizados.
 - Configurar correctamente los registros DNS (SPF, DKIM, DMARC) para proteger contra ataques de suplantación de identidad.

1.2 Identificación de Servicios y Posibles Tecnologías Utilizadas

1.2.1 Servidores en la Nube

El escaneo revela que varios servicios están alojados en Google Cloud Platform (GCP) y Microsoft Azure, lo que sugiere una arquitectura basada en la nube.

Posibles tecnologías usadas:

- Google Cloud Functions / Firebase: Puede implicar el uso de Node.js o Python para APIs y backend.
 - Azure App Services: Indica la posibilidad de aplicaciones en .NET (C#) o Python/Django.
- ◆ Medidas recomendadas:
- Configurar reglas estrictas de firewall para restringir accesos solo a IPs autorizadas.
 - Implementar políticas de acceso a la nube (IAM) con permisos mínimos necesarios.
 - Monitorear el tráfico de red en la nube para detectar anomalías.

1.2.2 Posibles Tecnologías en Servicios Web

Los subdominios de servicios financieros, APIs y correo electrónico sugieren el uso de las siguientes tecnologías:

- APIs REST o GraphQL: Es probable que se usen lenguajes como Python (Flask, Django), Java (Spring Boot) o Node.js (Express).

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

- Aplicaciones web bancarias: Pueden estar desarrolladas en Java (JSP, Spring) o .NET (C# y ASP.NET MVC).
- Sistemas de correo y marketing digital: Posible uso de PHP (Laravel) para paneles de administración de correos y CRM.

Posibles vulnerabilidades asociadas:

- APIs mal configuradas expuestas a inyecciones SQL, deserialización insegura o explotación de endpoints.
 - Aplicaciones en Java o PHP con vulnerabilidades como inyección de comandos o XSS.
 - Sistemas de correo en PHP vulnerables a ataques de spam o phishing.
- ◆ Medidas recomendadas:
- Ejecutar pruebas de penetración en APIs para detectar vulnerabilidades en autenticación y autorización.
 - Mantener actualizados los frameworks utilizados (Spring, Django, Laravel) para mitigar exploits conocidos.
 - Utilizar Web Application Firewalls (WAF) para bloquear ataques comunes a aplicaciones web.

2. Riesgo de Configuración de Infraestructura

2.1 Exposición de Direcciones IP

Varias IPs detectadas están asociadas a proveedores de nube, lo que indica la posibilidad de:

- Servicios mal configurados con puertos abiertos al público.
- Servidores sin medidas de hardening, permitiendo ataques de enumeración y explotación.

Posibles vulnerabilidades:

- Ataques de fuerza bruta en servicios SSH/RDP si no están protegidos con reglas de acceso.
 - Escaneos de puertos abiertos que pueden revelar versiones de software vulnerables.
 - Falta de segmentación de red, permitiendo ataques de movimiento lateral dentro de la infraestructura.
- ◆ Medidas recomendadas:

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

- Implementar políticas de acceso con listas blancas de IP para limitar conexiones externas.
- Cerrar puertos innecesarios y usar túneles VPN para accesos administrativos.
- Utilizar herramientas de monitoreo de tráfico (SIEM) para detectar intentos de acceso sospechosos.

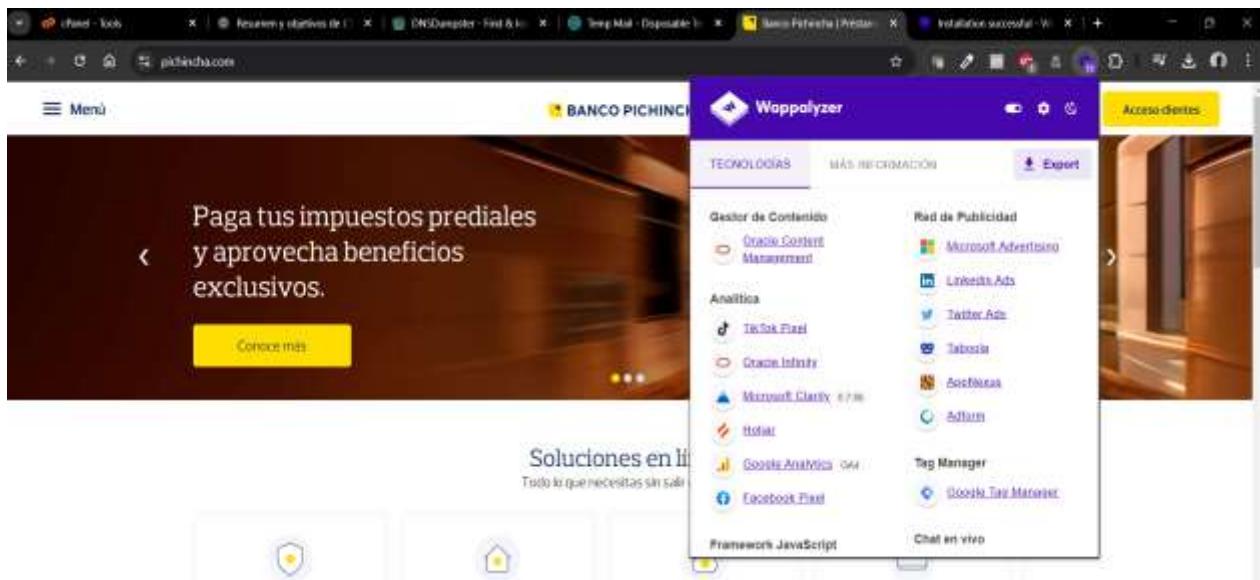


FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Análisis del Escaneo de Tecnologías con Wappalyzer en Banco Pichincha



Wappalyzer es una herramienta que detecta las tecnologías utilizadas en un sitio web, incluyendo gestores de contenido, frameworks, herramientas de analítica y publicidad, entre otros. En la captura proporcionada, el análisis revela lo siguiente:

Gestor de Contenido

Oracle Content Management

- El Banco Pichincha utiliza la plataforma de gestión de contenido (CMS) de Oracle, lo que sugiere que su sitio está construido sobre un sistema empresarial robusto y seguro.
- Esto indica que la infraestructura del sitio está basada en soluciones corporativas de Oracle, posiblemente por razones de seguridad y escalabilidad.

Posibles riesgos:

Explotación de vulnerabilidades conocidas en Oracle Content Management si no está actualizado.

Fugas de información por configuraciones incorrectas en la gestión de contenido.

◆ Medidas recomendadas:

- Monitorear actualizaciones y parches de seguridad de Oracle Content Management.
- Implementar reglas de seguridad para evitar inyección de código en el CMS.

Herramientas de Analítica Web

Las siguientes herramientas indican que el Banco Pichincha rastrea la actividad de sus usuarios para analizar el comportamiento y mejorar la experiencia del cliente:

- **TikTok Pixel:** Seguimiento de usuarios provenientes de campañas en TikTok.
- **Oracle Infinity:** Plataforma de analítica avanzada de Oracle.
- **Microsoft Clarity:** Analiza la interacción de los usuarios en la web (mapas de calor, clics).
- **Hotjar:** Registra el comportamiento de los visitantes (grabaciones de sesiones, encuestas).

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

- Google Analytics GA4: Seguimiento de métricas y tráfico del sitio.
- Facebook Pixel: Permite realizar retargeting de usuarios a través de Facebook Ads.

Medidas recomendadas:

- Asegurar que los datos de analítica no capturen información sensible (ejemplo: credenciales de acceso, datos bancarios).
- Configurar correctamente las políticas de privacidad y protección de datos para cumplir con regulaciones como GDPR o LGPD.

Redes de Publicidad

- Microsoft Advertising, LinkedIn Ads, Twitter Ads, Taboola, AppNexus, Adform

Significado:

- El Banco Pichincha utiliza campañas publicitarias digitales en diversas plataformas, lo que indica que tiene estrategias activas de marketing digital para captar clientes.
- Taboola y AppNexus sugieren que utilizan publicidad programática, lo que significa que sus anuncios se muestran en diferentes sitios web de manera automática y personalizada.

Posibles riesgos:

Uso indebido de la marca en campañas fraudulentas si no se monitorean adecuadamente.
Publicidad maliciosa (Malvertising) si no se filtran bien los proveedores de anuncios.

Medidas recomendadas:

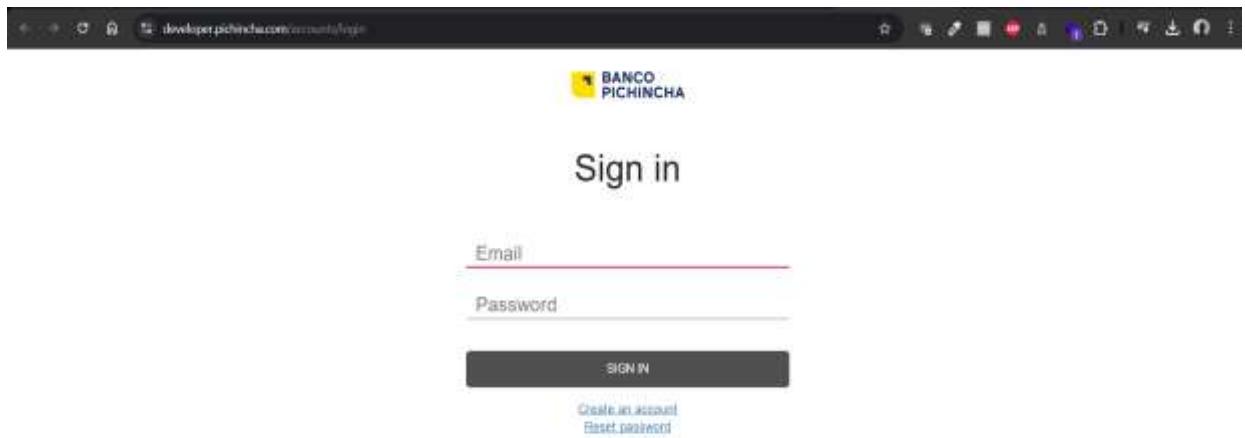
- Implementar monitoreo de fraudes publicitarios para evitar que atacantes suplanten la identidad del banco.
- Revisar periódicamente las campañas publicitarias para asegurarse de que no están dirigidas a sitios maliciosos.

Análisis del Navegador Programable

Análisis de Seguridad del Portal de Autenticación "developer.pichincha.com"

La página capturada (developer.pichincha.com/accounts/login) es un portal de autenticación del Banco Pichincha, posiblemente utilizado por desarrolladores, empleados o integraciones de API. Este tipo de interfaces pueden presentar diversas vulnerabilidades de seguridad si no están protegidas adecuadamente.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS



Falta de HTTPS Forzado (SSL/TLS)

- Si el portal no fuerza el uso de HTTPS, las credenciales pueden ser capturadas por atacantes en redes no seguras (ataques MITM - Man in the Middle).
- Verificar en el navegador si hay un candado SSL en la barra de direcciones.

Recomendación:

Forzar HTTPS con redirección automática.

Usar HSTS (HTTP Strict Transport Security) para evitar conexiones en texto plano.

Análisis de Posible Ingeniería Social y Phishing

Dado que la URL es developer.pichincha.com, parece legítima, pero un atacante podría crear una página similar para engañar a empleados.

Ejemplo de ataque:

- Un atacante envía un correo falso con "Actualización de seguridad - Banco Pichincha".
- La víctima accede a developer-pichincha.com (dominio fraudulento).
- Introduce sus credenciales en el sitio falso, permitiendo que el atacante acceda a su cuenta real.

Recomendación:

Verificar que la URL es legítima antes de ingresar credenciales.
Implementar MFA obligatorio para todas las cuentas.
Usar protecciones anti-phishing en correos electrónicos.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Análisis de vulnerabilidades

→ Scan summary



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.

El sistema evaluado tiene una buena postura de seguridad con bajo riesgo general. Debe investigarse la vulnerabilidad de bajo riesgo y los hallazgos informativos para garantizar un entorno más seguro. Se recomienda realizar auditorías de seguridad periódicas y pruebas de penetración para fortalecer aún más la seguridad.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

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 prevenir 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.

The screenshot shows a forum post from a user named 'HotarusCorp' (Member) with the title 'INITIAL PRICE 500K'. The post contains the text: 'pay btc or monero' and 'THE ENTIRE PACKAGE IS SOLD BY PARTS'. Below the post, there is a note: 'The Banco Pichincha is the largest private bank in Ecuador, by capitalization and by number of depositors. a business group that includes the companies associated with Diners Club, Visa Titanium Discover Card'. At the bottom, it says: 'The bank has 5.8 million customers in Ecuador, \$ 12.5 billion in assets and \$ 7.5 billion in deposits, as well as more than 200 branches in the country.'

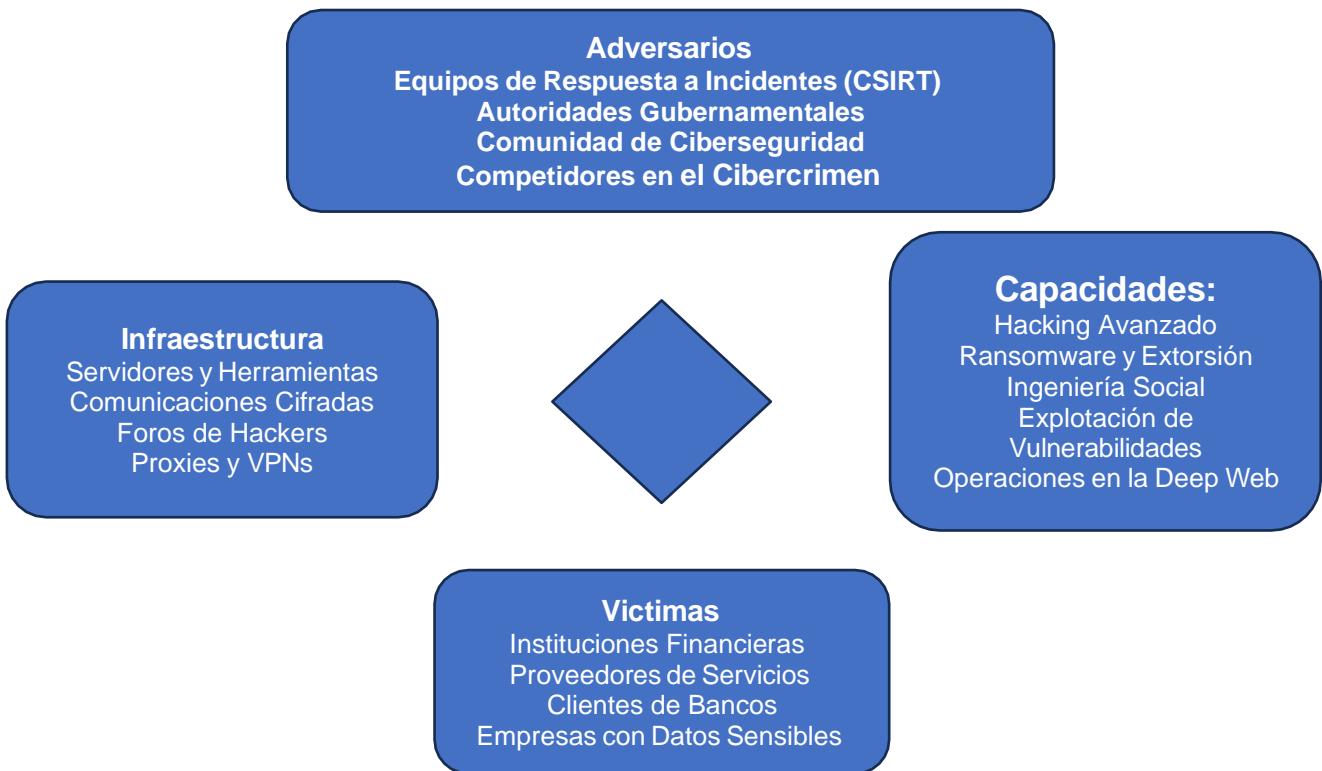
Los incidentes repetidos de ciberseguridad pueden erosionar la confianza de los clientes en la capacidad del banco para proteger sus datos personales y financieros. La filtración de datos y los ataques a los sistemas digitales son preocupaciones significativas para los usuarios.

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,

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

la interrupción prolongada de los servicios digitales afecta la experiencia del cliente y puede tener repercusiones financieras.

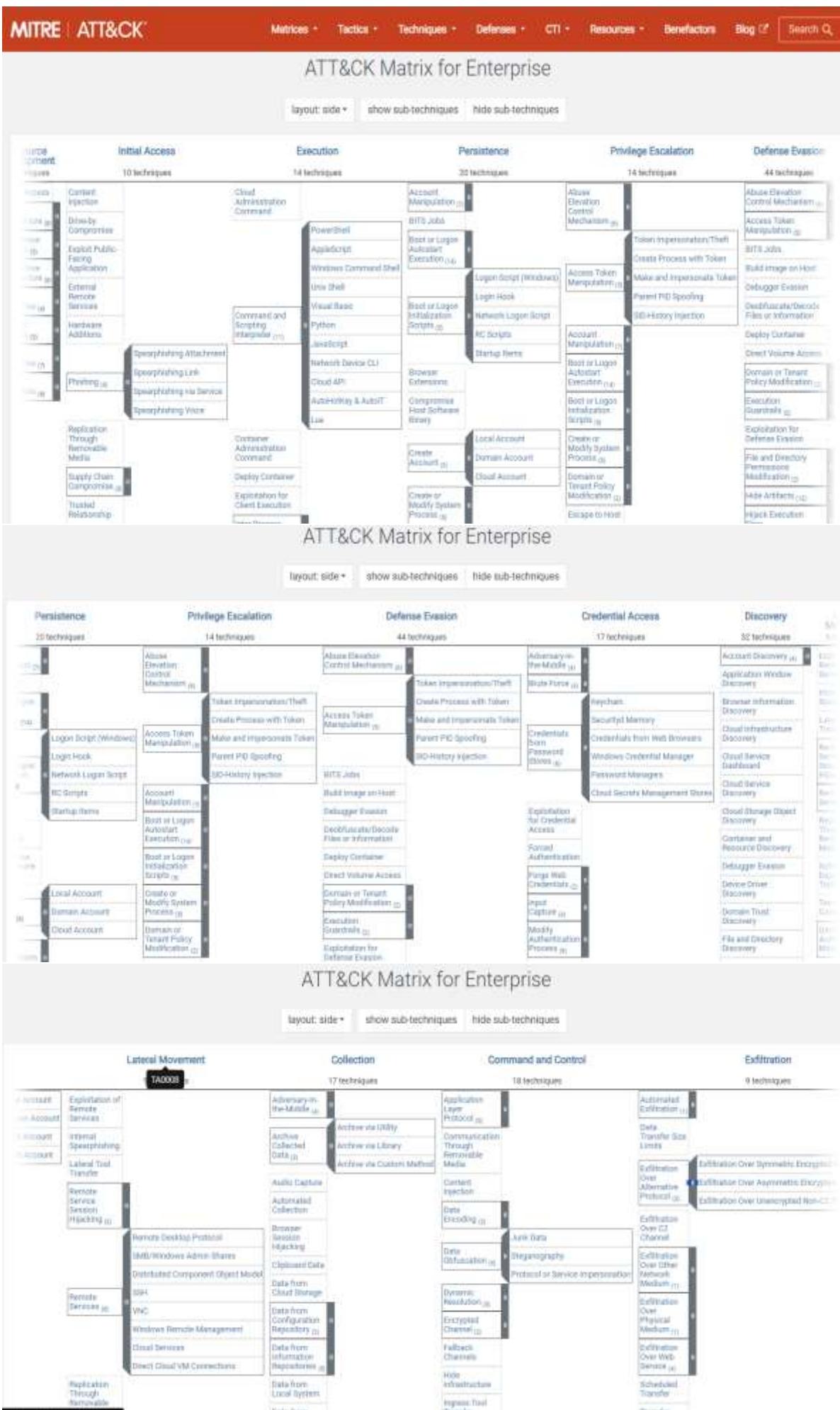
* Perfilamiento de adversarios



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.

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Tácticas y Técnicas Principales en la Matriz usadas por el grupo identificado en el análisis de Hotarus Corp

1. Acceso Inicial (Initial Access)

Cómo los atacantes obtienen acceso a la red o sistema objetivo.

- Phishing (Spearphishing, Phishing vía Servicio, Phishing con Archivos)
- Explotación de Aplicaciones Públicas
- Servicios Remotos Externos (RDP, SSH)
- Compromiso de la Cadena de Suministro
- Adición de Hardware Malicioso

Medidas de mitigación: Autenticación multifactor, segmentación de red, concienciación en ciberseguridad.

2. Ejecución (Execution)

Cómo los atacantes ejecutan código en los sistemas comprometidos.

- Uso de PowerShell, Windows Command Shell, Python, JavaScript
- Abuso de APIs en la Nube
- Scripts en Red (RC Scripts, Logon Scripts)
- Exploración a través de Exploits en Aplicaciones

Medidas de mitigación: Restricción de ejecución de scripts, monitoreo de procesos sospechosos.

3. Persistencia (Persistence)

Métodos usados por atacantes para mantener acceso en el sistema.

- Manipulación de Cuentas (crear/modificar cuentas)
- Instalación de extensiones en navegadores
- Compromiso de Binarios del Sistema
- Ejecución Automática al Inicio (Boot/Logon Autostart Execution)

Medidas de mitigación: Control de integridad de archivos, listas blancas de aplicaciones.

4. Escalada de Privilegios (Privilege Escalation)

Cómo los atacantes obtienen mayores permisos en un sistema.

- Abuso de Control de Elevación de Privilegios
- Manipulación de Tokens de Acceso
- Ejecución de Procesos con Permisos Elevados
- Spoofing de PID (Parent Process ID Spoofing)

Medidas de mitigación: Uso de privilegios mínimos, auditorías de seguridad periódicas.

5. Evasión de Defensa (Defense Evasion)

Técnicas para evitar la detección por soluciones de seguridad.

- Manipulación de Tokens de Acceso
- Modificación de Permisos de Archivos y Directorios
- Evitar Depuradores y Sandboxes
- Modificación de Políticas de Dominio o Tenant

Medidas de mitigación: Monitoreo de cambios en archivos, control de acceso basado en roles.

6. Acceso a Credenciales (Credential Access)

Cómo los atacantes roban credenciales de usuario y administrador.

- Volcado de Credenciales del SO (LSASS, SAM, NTDS.dit)
- Captura de Entrada del Usuario (Keylogging)
- Abuso de Autenticación en la Nube
- Ataques de Fuerza Bruta o Spray de Contraseñas

Medidas de mitigación: Autenticación multifactor, uso de administradores de contraseñas.

7. Movimiento Lateral (Lateral Movement)

Cómo los atacantes se desplazan dentro de la red.

- Uso de Servicios Remotos (SMB, RDP, SSH)
- Transferencia de Herramientas de Ataque
- Compromiso de Cuentas Administrativas
- Uso de Herramientas del Sistema Operativo (PsExec, WMI)

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

Medidas de mitigación: Segmentación de red, registros de auditoría, detección de anomalías.

8. Recopilación (Collection)

Cómo los atacantes extraen información valiosa del sistema objetivo.

- Captura de Capturas de Pantalla
- Registro de Keystrokes (Keylogging)
- Escaneo de Archivos Sensibles
- Acceso a Cámaras y Micrófonos

Medidas de mitigación: Restricciones en el acceso a hardware y monitoreo de actividades.

9. Exfiltración (Exfiltration)

Cómo los atacantes extraen datos fuera del entorno comprometido.

- Transferencia de Archivos a la Nube o a Servidores C2
- Compresión y Encriptación de Datos antes de la Exfiltración
- Uso de Canales de Comunicación Encubiertos

Medidas de mitigación: Monitoreo de tráfico, prevención de fuga de datos (DLP).

10. Comando y Control (Command and Control)

Cómo los atacantes mantienen comunicación con sistemas comprometidos.

- Uso de Canales Encriptados
- Túneles de Red Ofuscados
- Abuso de Servicios Legítimos (DNS, HTTPS, WebSockets)
- Uso de Redes de Anonimización (Tor, VPNs, Proxies)

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. El informe evidencia que, aunque el Banco Pichincha ha fortalecido su seguridad, **aún existen brechas de seguridad que deben ser abordadas de inmediato.**

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.



FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

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/iocat-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:**

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

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**.