



| | | | |
|--------------|---|--|---|
| Nro. Alerta: | EC-2022-0055 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  TLP:BLANCO | | |
| Fecha: | 29-marzo-2022 | EcuCERT advierte nueva campaña de suplantación de identidad "BANCO CAPITAL" | |
| | | V 1.1 | |

I. DATOS GENERALES:

| | |
|---------------------------|---|
| Clase de alerta: | Fraude |
| Tipo de incidente: | Falsificación de registros o identidad. |
| Nivel de riesgo: | Alto |

II. INTRODUCCIÓN

A través del monitoreo de fuentes abiertas empleando técnicas OSINT y plataformas de búsqueda de ciberseguridad de tipo no intrusivas y reporte de incidentes en la plataforma de EcuCERT; se ha detectado una campaña maliciosa de suplantación de identidad a nombre Del Banco Capital.

III. VECTOR DE ATAQUE:

A través de correo electrónico, se difunden los siguientes enlaces: [https://35\[.\]80\[.\]105\[.\]194//](https://35[.]80[.]105[.]194//) y [https://50\[.\]112\[.\]222\[.\]243/](https://50[.]112[.]222[.]243/) que suplantan la identidad de la página web del Banco Capital. En este sentido, se solicita a la comunidad verificar que los sitios en donde ingresan sus contraseñas pertenezcan a sitios oficiales.



IV. INDICADORES DE COMPROMISO:

A continuación, se mencionan los indicadores de compromiso asociados a la campaña maliciosa:

| | PARÁMETRO | DESCRIPCIÓN | |
|---|----------------------------------|---|---|
| 1 | URL Sitio Falso | https://35[.]80[.]105[.]194// | https://50[.]112[.]222[.]243/ |
| 2 | IP Address | 35.80.105.194 | 50.112.222.243 |
| 3 | Número de Sistema Autónomo (AS) | 16509 | 16509 |
| 4 | Organización de Sistema Autónomo | AMAZON-02 | AMAZON-02 |
| 5 | País | Estados Unidos | Estados Unidos |

Tabla 1. IOC asociados a campaña



| | | | |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-0055 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  TLP:BLANCO | | |
| Fecha: | 29-marzo-2022 | EcuCERT advierte nueva campaña de suplantación de identidad “BANCO CAPITAL” | V 1.1 |

V. IMAGEN DE LA CAMPAÑA

En referencia a [https://35\[.180\[.1105\[.1194//](https://35[.180[.1105[.1194//)

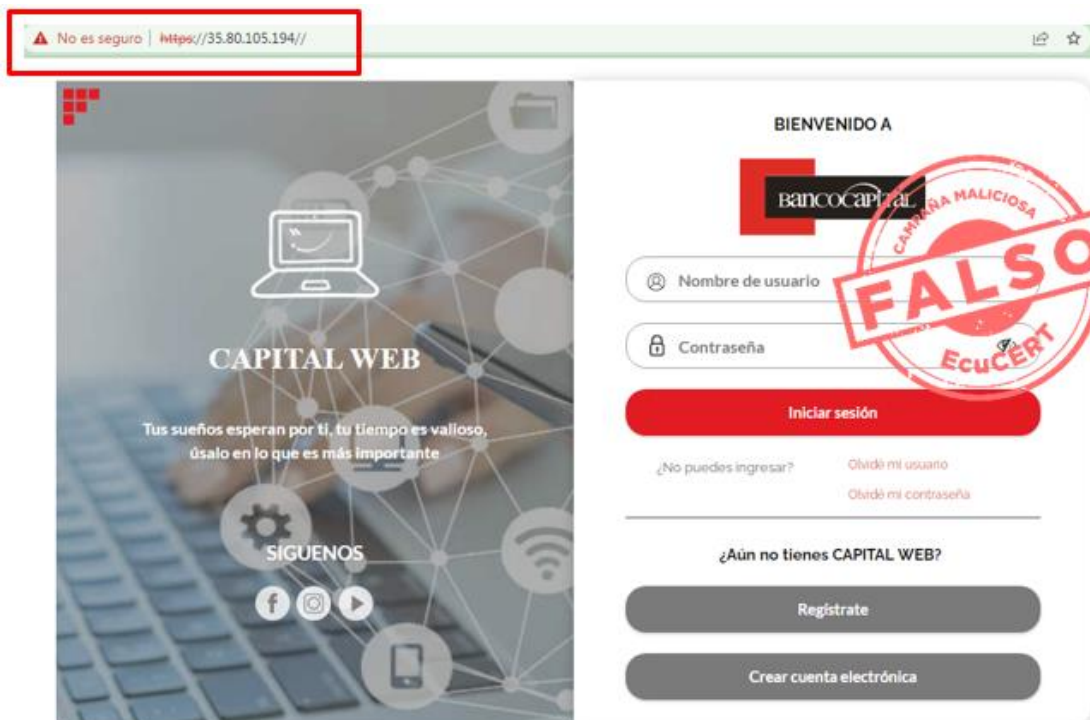




Figura 1. Campaña maliciosa a nombre de Banco Capital

| | | | |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-0055 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  TLP:BLANCO | | |
| Fecha: | 29-marzo-2022 | EcuCERT advierte nueva campaña de suplantación de identidad “BANCO CAPITAL” | |
| | | V 1.1 | |

En referencia a [https://50\[.1112\[.1222\[.1243/](https://50[.1112[.1222[.1243/) se presentan dos resultados asociados. El primer resultado es asociado a una página web solicitada desde el computador.

BIENVENIDO A




Nombre de usuario

Contraseña

Iniciar sesión

¿No puedes ingresar?
Olvidé mi usuario
Olvidé mi contraseña

¿Aún no tienes CAPITAL WEB?



Regístrate

Crear cuenta electrónica

×

Contrato ABC



Figura 2. Campaña maliciosa a nombre de Banco Capital

| | | | |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-0055 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  TLP:BLANCO | | |
| Fecha: | 29-marzo-2022 | EcuCERT advierte nueva campaña de suplantación de identidad “BANCO CAPITAL” | V 1.1 |

El segundo resultado es asociado a la apertura de dicha dirección IP desde un dispositivo móvil.



Figura 3. Campaña maliciosa a nombre de Banco Capital.

| | | | |
|--------------|--|--|---|
| Nro. Alerta: | EC-2022-0055 | CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR |  |
| TLP: |  TLP:BLANCO | | |
| Fecha: | 29-marzo-2022 | EcuCERT advierte nueva campaña de suplantación de identidad “BANCO CAPITAL” | V 1.1 |

VI. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Verificar que los sitios web que se ingresen sean los oficiales.
- No confiar en descuentos, promociones o premios ofertados por internet.
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia.
- Considerar los indicadores de compromiso descritos en el presente documento.
- Tener actualizado el sistema antivirus.
- Informarse continuamente sobre tipos de amenazas existentes.

