Nro. Alerta:	EC-2022-079	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	**EcuCERT advierte sobre campaña de suplantación de identidad "COOPERATIVA JEP"**	V 1.2

I. DATOS GENERALES:

Clase de alerta: Phishing
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 detectó una campaña maliciosa de suplantación de identidad a nombre de la Cooperativa de Ahorro y Crédito JEP.

III. VECTOR DE ATAQUE:

El enlace: **"hxxps://dev[-]juventud[-]ecuatoriana-jep[.]pantheonsite[.]io/JEP"**, suplanta la identidad de la página web de la Cooperativa JEP., misma que se encontraba alojada en la siguiente dirección IP 23.185.0.4. 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 (IOCs):

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

No.	PARÁMETRO	DESCRIPCIÓN
1	URL sitio falso	https://dev-juventud-ecuatoriana-jep.pantheonsite.io/JEP
2	IP Address	23.185.0.4
3	Número de Sistema Autónomo (AS)	54113
4	Organización de Sistema Autónomo	FASTLY
5	Nombre de la organización	Pantheon (Plataforma de Hosting web)
6	País	Estados Unidos

Tabla Nro. 1. IOCs asociados a campaña

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-079	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	**EcuCERT advierte sobre campaña de suplantación de identidad "COOPERATIVA JEP"**	V 1.2

V. IMAGEN DE LA CAMPAÑA:

En referencia al enlace: **"hxxps://dev[-]juventud[-]ecuatoriana-jep[.]pantheonsite[.]io/JEP"**

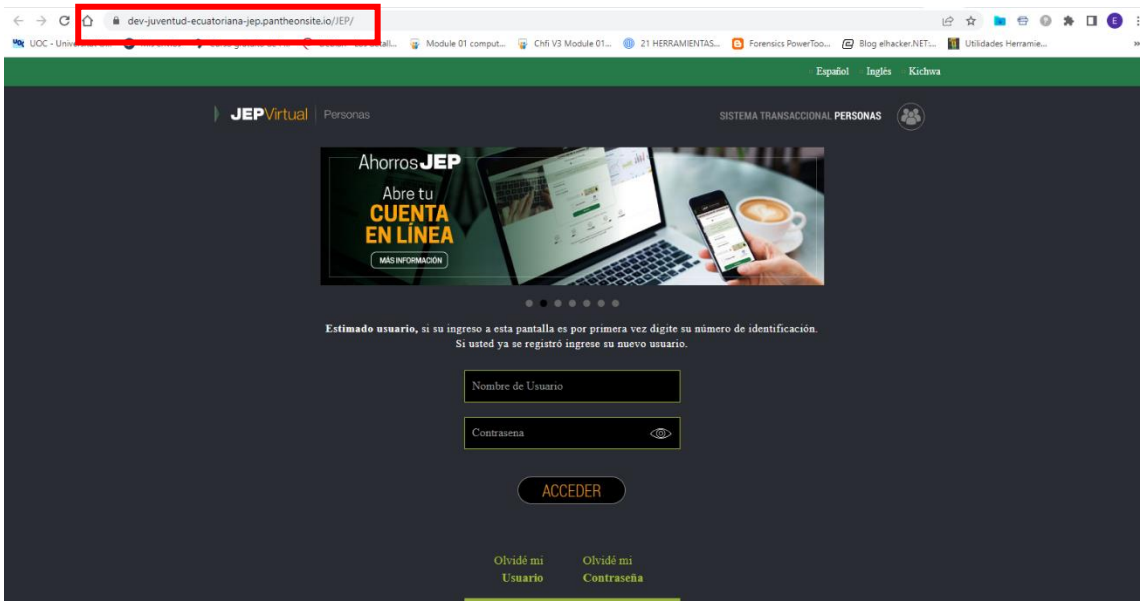

Figura Nro. 1. Campaña maliciosa a nombre de Cooperativa JEP

VI. IDENTIFCICAIÓN DE SITIOS FALSOS:

Para poder identificar URL falsas hay que conocer cómo están constituidas las direcciones web. A manera de ejemplo en el enlace **https://a_b_c.jep.coop/** se tiene lo siguiente:

«https»:	Protocolo utilizado para acceder al sitio web.
«://»:	Símbolos de separación entre el protocolo y el dominio.
«a_b_c»:	Nombre de subdominio del sitio.
«jep»:	Nombre del dominio del sitio web. Se debe poner atención en esta parte del dominio, ya que los ciberdelincuentes no lo pueden copiar.
«.coop»:	Es la extensión del dominio (Otras extensiones ser: com, edu, org, etc.)

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-079	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	20-julio-2022	**EcuCERT advierte sobre campaña de suplantación de identidad "COOPERATIVA JEP"**	V 1.2

Los ciberdelincuentes, crean **subdominios** que se **parecen al dominio** para engañar a las víctimas. En este caso:

- **https://dev-juventud-ecuatoriana-jep.pantheonsite.io,**
  - **dev-juventud-ecuatoriana-jep** subdominio fraudulento que pretende engañar al usuario.
  - **pantheonsite.io** dominio real del sitio, que no corresponde al dominio de la Cooperativa JEP.

VII. 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.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta, se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec