INFORMANDO DE CAMPAÑA PHISING RELACIONADO CON APPLE STORE

Se ha tenido conocimiento por parte de la Unidad de Investigación Tecnológica de la Policía Nacional de una nueva campaña de phising (captura maliciosa de datos personales) que tiene como objetivo la obtención de credenciales de tarjetas de crédito e identidad de usuarios de clientes de la Apple Store.

El phising comienza con la recepción del siguiente correo electrónico:

De: APPLE.PAGOS.CLIENTES@ds2
Fecha: 16 de noviembre de 2015, 20:02:33 CET
Para: [redacted]
Asunto: ASUNTO: COMPRA ACEPTADA - REF. 194086272212

Servicios de Atencion al Cliente de AppleStore

NOTICIA:

Estimado Cliente de AppleStore

Su compra en valor de 72.09 euros ha sido aceptada con exito.

Para cancelar este pago haga clic aqui!

Metodo Pago - Tarjeta de Credito

Abajo hay detalles importantes sobre tu pedido.

¿Preguntas?

Estamos aquí para ayudarte.

Número de pedido: 761008608537

Total Parcial: 72.09.
Embarque/Gastos Administrativos: 0,00 .
Impuesto: 0,00 .
Total: 72.09.

* Un descriptor de pago es como nuestro cobro aparecen en el saldo de su tarjeta de credito

La dirección aparente desde la que se envía este correo electrónico es APPLE.PAGOS.CLIENTES@ds2, dirección inexistente con la única intención de llevar a engaño aparentando legitimidad. De ser una dirección legítima de Apple la dirección de correo debería terminar en “apple.com”, o de algún otro dominio asociado a Apple. Una vez se pincha en el enlace se abre una página web con dirección “http://50.30.37.187/.me/me.htm”, dicha web tiene el siguiente código:

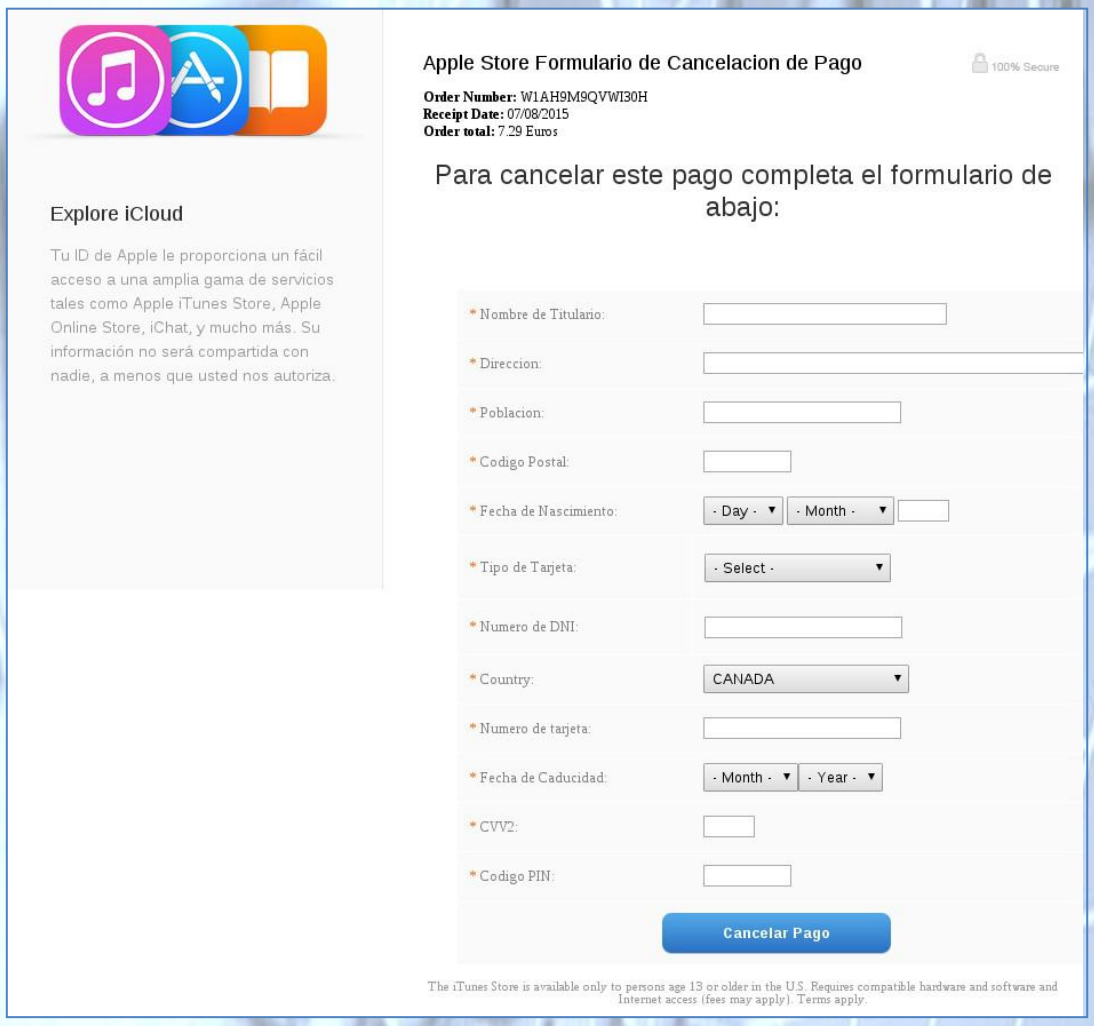
```
<script type="text/javascript">
function makeid() {
var text = "";
var possible = "abcdefghijklmnopqrstuvwxyz";
for( var i=0; i < 5; i++ )
text += possible.charAt(Math.floor(Math.random() * possible.length));
return text;
}
function welcome(s) {
s = typeof(s) != 'undefined' ? s : '';
window.location="http://particulares.appleid.apple." + makeid() + ".radionawxo.org/app/index.html"
+ s;
}
welcome("");
</script>
```

Este código nos redirige a una nueva web cuya dirección es http://particulares.appleid.apple.#####.radionawxo.org/app/index.html donde los caracteres # son una letra aleatoria (abcdefghijklmnopqrstuvwxyz)..

Esta nueva web es en la que se produce la captura de datos, como se puede ver en la captura de dicha web mostrada más adelante.

Esta web está alojada en el mismo servidor que la primera página, siendo su dirección completa “http://50.30.37.187/app/index.html”. De hecho, Google tiene ya almacenada esta dirección como una web maliciosa, avisando al usuario del riesgo de visitarla. No obstante, si se accede a través de uno de los dominios generados aleatoriamente, no es mostrado aviso alguno ya que Google no debe de tener registrados esos dominios como maliciosos.

La dirección IP 50.30.37.187 pertenece a la empresa estadounidense SERVER4YOU - Hosting Solutions International, Inc.



Apple Store Formulario de Cancelacion de Pago

100% Secure

Order Number: W1AH9M9QVWI30H
Receipt Date: 07/08/2015
Order total: 7.29 Euros

Para cancelar este pago completa el formulario de abajo:

Explore iCloud

Tu ID de Apple le proporciona un fácil acceso a una amplia gama de servicios tales como Apple iTunes Store, Apple Online Store, iChat, y mucho más. Su información no será compartida con nadie, a menos que usted nos autoriza.

* Nombre de Titulario:
* Direccion:
* Poblacion:
* Codigo Postal:
* Fecha de Nascimiento: · Day · · Month ·
* Tipo de Tarjeta: · Select ·
* Numero de DNI:
* Country: CANADA
* Numero de tarjeta:
* Fecha de Caducidad: · Month · · Year ·
* CVV2:
* Codigo PIN:

Cancelar Pago

The iTunes Store is available only to persons age 13 or older in the U.S. Requires compatible hardware and software and Internet access (fees may apply). Terms apply.

Es importante no responder nunca a solicitudes de información personal desde correos electrónicos, y mucho menos dar datos bancarios, de tarjetas de crédito o similares. Nunca bancos, o cuentas que manejan información financiera van a solicitarlo por este medio, por lo que en caso de recibir un correo electrónico de estas características o que nos redirige a páginas web que piden dicha información podremos tener casi total seguridad en que se trata de un intento fraudulento de robarnos esta información.

Ante la duda de que estemos ante un caso de phising o un correo electrónico legítimo se puede contactar con la entidad que supuestamente nos envía el correo electrónico para cotejar la legitimidad de dicha petición (por los mecanismos normales con los que se contacte con dicha entidad, no respondiendo al correo electrónico sospechoso).