PRESIDENCIA DEL CONSEJO DE MINISTROS

Oficina Nacional de GOBIERNOELECTRÓNICO e INFORMÁTICA

BOLETÍN DE ALERTA ANTIVIRUS

Centro de Consulta e Investigación sobre Seguridad de la Información

Edición Nº 148/ 29 de Diciembre de 2008

Visite el Portal del Estado Peruano: www.peru.gob.pe

INDICE

FUENTES

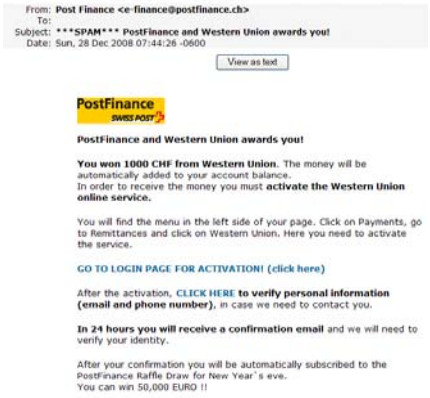
- Alerta Antivirus
- Per Antivirus
- Sophos

FALSO MENSAJE POSTFINANCE_PHISHING

PostFinance_Phishing es un falso mensaje de correo reportado el 28 de Diciembre del 2008, que está siendo enviado a miles de usuarios en todo el mundo, mediante el cual se ofrece un "premio" de 1000 CHF que es código ISO del franco zuizo y equivale a una significativa suma de Euros. Intenta robar información de la cuentas de Western Unión, y descarga un malware en su sistema.

Se envía a equipos con Windows 95/98/NT/2000/XP/Vista y Server 2003.

La técnica empleada para este tipo de fraude electrónico se denomina "phishing". La misma que hace uso de la "ingeniería social"



From: Post Finance <e-finance@postfinance.ch>
To:
Subject: ***SPAM*** PostFinance and Western Union awards you!
Date: Sun, 28 Dec 2008 07:44:26 -0600

View as text

PostFinance
SWISS POST

PostFinance and Western Union awards you!

You won 1000 CHF from Western Union. The money will be automatically added to your account balance.
In order to receive the money you must **activate the Western Union online service.**

You will find the menu in the left side of your page. Click on Payments, go to Remittances and click on Western Union. Here you need to activate the service.

GO TO LOGIN PAGE FOR ACTIVATION! (click here)

After the activation, **CLICK HERE to verify personal information (email and phone number),** in case we need to contact you.

In 24 hours you will receive a confirmation email and we will need to verify your identity.

After your confirmation you will be automatically subscribed to the PostFinance Raffle Draw for New Year`s eve.
You can win 50,000 EURO !!

Recomendaciones importantes:.

- o No haga click en ninguno de lo enlaces (ni siquiera por curiosidad)
- o Elimine este mensaje y no lo guarde en ninguna carpeta.
- o Borre el cache, cookies e historial del menu de Herramientas de su navegador despues de ejecutado los pasos anteriores.

TROYANO TROJ/ZBOT.ACY

Zbot.ACY es un troyano reportado el 27 de Diciembre del 2008, residente en memoria que se propaga al visitar determinadas páginas web, que han sido vulneradas y a las que se ha insertado un archivo de nombre up.exe que está comprimido y con atributo de descarga automática.

Infecta a Windows 95/98/NT/2000/XP y Server 2003, está desarrollado en Assembler con una extensión de 55,296 y no está encriptado.

Roba información de servidores de sistemas financieros configurados con contraseñas débiles, descarga malwares y tiene un peligroso componente Rootkit.

Al ingresar a un sistema se copia a la carpeta %System% con el nombre de Twext.exe y para evitar su fácil detección le agrega código "basura".

Al siguiente inicio del equipo, el troyano infecta los archivos originales Winlogon.exe y Svchost.exe e intenta conectarse a una dirección web.

El troyano intenta robar información de varias entidades financieras.

TROYANO TROJ/CHROMEINJECT

Chromeinject es un troyano que se propaga usando servicios de Internet. Infecta Windows 95/98/Me/NT/2000/XP/Vista y Server 2003 que usen el navegador Mozilla FireFox. Está desarrollado en Assembler.

Al ingresar a un sistema busca la presencia del navegador Mozilla Firefox y se copia a las rutas:

%SystemDrive%\[Ruta_a_FireFox]\plugins\npbasic.dll
%SystemDrive%\[Ruta_a_FireFox]\plugins\npbasic.dll1
%Temp%\[RANDOM FILE NAME].tmp

Luego modifica los siguientes archivos para robar información sensible del sistema.:

%SystemDrive%\[Ruta_a_FireFox]\chrome\chrome\content\browser.js
%SystemDrive%\[Ruta_a_FireFox]\chrome\chrome\content\browser.xul
%SystemDrive%\[Ruta_a_FireFox]\chrome\browser.manifest

El troyano roba información cuando los siguientes dominios son accedidos usando Mozilla Firefox:

53.com	ccm.es
abbeynational.co.uk	chase.com
adelaidebank.com.au	citizensbankonline.com
akbank.com	clavenet.net
anbusiness.com	co-operativebank.co.uk
anbusiness.com	co-operativebankonline.co.uk
anz.com	credem.it
areasegura.banif.es	csebanking.it
arquia.es	e-gold.com
banca.cajaen.es	elmonte.es
bancaeuro.it	fibancmediolanum.es
bancagenerali.it	fineco.it
bancaintesa.it	in-biz.it
bancajaproximaempresas.com	intelvia.cajamurcia.es
bancamarch.es	isideonline.it
bancamediolanum.it	islamic-bank.com
bancogallego.es	itibank.co.uk
bancoherrero.com	iwbank.it
bancopastor.es	kfhonline.com
bancopopular.es	lloydstsb.co.uk
banesto.es	my.if.com
banking.*.de	mybankoffshore.alil.co.im
banking.first-direct.com	mybusinessbank.co.uk
bankoa.es	nationet.com
bankofamerica	natwestibanking.com
banksa.com	net.kutxa.net
banquepopulaire.fr	online.co.uk
barclays.com	online.hbs.net.au
bbvanetoffice.com	onlinebanking.nationalcity.com*'
bcp.it	openbank.es
bgnetplus.com	paypal.com
boq.com.au	pncs.com.au
bv-i.bancodevalencia.es	popso.it
caixa*.es	poste.it
caixamanlleu.es	procreditbank.bg
caixasabadell.net	quiubi.it
caja*.es	sabadellatlantico.com
carifvg.com	schwab.com
cariparma.it	secservizi.it
cariparo.it	smile.co.uk
carisbo.it	suncorpmetway.com.au
carnet.cajarioja.es	suntrust.com
caterallenonline.co.uk	tdcanadatrust.com
fmbcc.bcc.it	unibanking.it
gbw2.it	unipolbanca.it
gruposantander.es	uno-e.com
gruppocarige.it/grps/vbank/jsp/login.jsp	usbank.com
halifax-online.co.uk	wachovia.com
hsbc.co	wamu.com
ibank.cahoot.com	wellsfargo.com
ibercajadirecto.com	westpac.com.au
	www.qccu.com.au

Finalmente el troyano envía las información extraída a los siguienteS dominios:

- http://www.yandeeex.ru
- http://www.sss.re

LISTA DE ANTIVIRUS

NOMBRE DEL ANTIVIRUS	PAGINA WEB
Panda Software	http://www.pandasoftware.es/
Per Antivirus	http://www.perantivirus.com/
The Hacker	http://www.hacksoft.com.pe/
AVAST Antivirus	http://www.antivir.com/support.htm
Zap Antivirus	http://www.zapantivirus.com
Sophos Antivirus	http://esp.sophos.com/
Norton Antivirus (NAV)	http://www.sarc.com/avcenter/download.html
Antiviral Toolkit Pro (AVP)	http://www.kaspersky.com/
ESafe	http://www.esafe.com/download/virusig.html
Antivirus Enterprise Protection	http://www.commandcom.com/html/files.html
InoculateIT	http://support.cai.com/Download/virussig.html
McAfee VirusScan	http://download.mcafee.com/updates/updates.asp
AVG Antivirus	http://www.grisoft.com/us/us_index.php
Symantec	http://www.symantec.com/
TrenMicro	http://www.trendmicro.com/download/pattern.asp
BitDefender	http://www.bitdefender-es.com
Antivirus	http://www.antivirus.com

CUALQUIER CONSULTA ENVIAR UN CORREO AL CENTRO DE CONSULTA E INVESTIGACION SOBRE SEGURIDAD DE LA INFORMACION - CCISI

ccisi@pcm.gob.pe
Teléfono : 2744356 – 106