SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BOLETÍN DE ALERTA

Boletín Nro.: 2014-08

Fecha de publicación: 29/10/2014

Tema: Campaña de Pishing a través de Correo Electrónico a Instituciones Gubernamentales (.gov.py)

Descripción:

En los últimos días se ha detectado una campaña de *Pishing* a través de correo electrónico, que busca engañar principalmente a funcionarios gubernamentales relacionados a dominios .gov.py.
El asunto del mensaje es “AntiVirus” y las direcciones de correo del remitente varian, en muchos casos estan falsificadas. El mensaje indica que un virus ha sido detectado en la cuenta de correo y que para la infección se debe enviar las credenciales (usuario, contraseña y fecha de nacimiento) para evitar que la cuenta sea desactivada.

A continuación se ve un extracto del correo en cuestión:

```
Date: Wed, 29 Oct 2014 08:09:02 -0200
From: "gov.py" <.....>
Reply-to: webupgrade2014@gmail.com
To: undisclosed-recipients:;
Subject: Anti/Virus
User-Agent: Internet Messaging Program (IMP) H3 (4.3.6)
Content-Transfer-Encoding: 8bit


nos gustaría informarle que estamos llevando actualmente a cabo el
mantenimiento programado y la mejora de nuestro servicio de correo
web, y como resultado de esto un virus HTK4S se ha detectado en sus
carpetas de la cuenta, y su cuenta tiene que ser actualizado a la
nueva F-Secure HTK4S anti-virus / anti-spam versión 2014 para evitar
daños en sus archivos importantes. Llenar las columnas de abajo y
enviar de vuelta o de su cuenta de correo electrónico será suspendido
```

temporalmente de nuestros servicios.
********** **********
Nombre de usuario: .....
Contraseña: .....
Fecha de nacimiento: .....
********** ********** *
Si no lo hace dentro de las 24 horas se rinda inmediatamente a su
cuenta de correo electrónico desactivada de nuestra base de datos gov.py

Derechos de Autor 2014 gov.py
(c) Redes Todos los derechos reservados

Impacto:
Al brindar las credenciales de una cuenta de correo a terceros, estos tienen acceso a la información contenida en ella. Además de esto, también es frecuente que dichas cuentas comprometidas sean utilizadas para el envío de *spam*, con lo que toda a organización se ve afectada.

Recomendaciones:

- Nunca brindar credenciales de acceso ni información sensible a través de correo u otros medios sin verificar con certeza el uso que se le va a dar.
- Nunca abrir enlaces ni archivos adjuntos que no fueron solicitados o que no sean de total confianza.
- Recomendamos a las organizaciones implementar mecanismos anti-spam para mitigar la recepción de correos maliciosos y/o fraudulentos.
- Es importante utilizar siempre contraseñas robustas en todas sus cuentas.

En caso de que haya sido víctima de un caso de *phishing* o fraude, contacte inmediatamente a su administrador de sistemas, autoridades competentes y/o con el CERT-PY. En caso de que sus credenciales bancarias hayan sido comprometidas, contacte a la institución financiera.
Modifique las contraseñas que haya revelado. Si utiliza la misma contraseña en varias cuentas, cambie todas y no las vuelva a utilizar en un futuro.