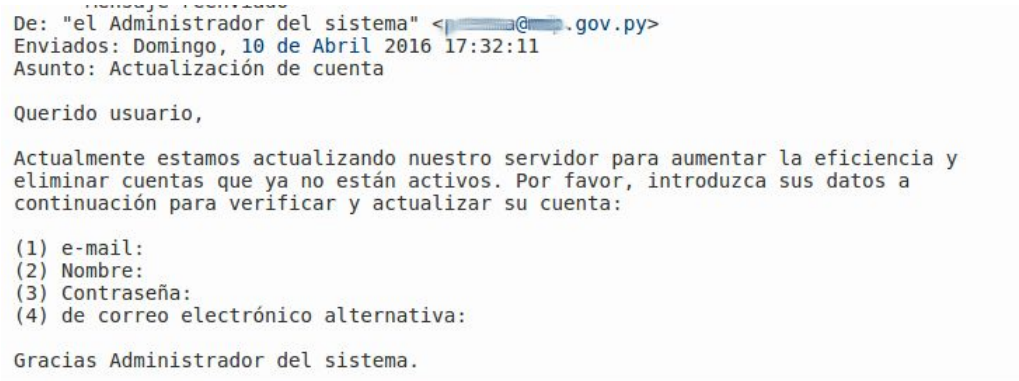
BOLETÍN DE ALERTA

Boletín Nro.: 2016-07
Fecha de publicación: 12/04/2016
Tema: Campaña de Phishing para funcionarios del Gobierno

Descripción:

En los últimos días se ha observado una campaña de phishing que apunta principalmente a funcionarios de instituciones gubernamentales. El phishing es una técnica de ingeniería social a través de la cual el ciberdelincuente busca engañar a la víctima para que la misma revele información confidencial, como por ejemplo contraseñas, PIN, etc., de modo a poder realizar posteriormente otro tipo de ataques con esa información.
La campaña de phishing observada circula a través de correos electrónicos engañosos, los cuales buscan que la víctima revele su usuario, fecha de nacimiento, contraseña y correo electrónico alternativo, haciéndoles creer que se trata de un proceso de actualización de servidor de correo enviado por un administrador de la red.
Se observaron diferentes correos electrónicos, muy similares. Algunos ejemplo de los correos electrónicos falsos que circulan son los siguientes:



De: "el Administrador del sistema" <[redacted].gov.py>
Enviados: Domingo, 10 de Abril 2016 17:32:11
Asunto: Actualización de cuenta

Querido usuario,

Actualmente estamos actualizando nuestro servidor para aumentar la eficiencia y eliminar cuentas que ya no están activos. Por favor, introduzca sus datos a continuación para verificar y actualizar su cuenta:

(1) e-mail:
(2) Nombre:
(3) Contraseña:
(4) de correo electrónico alternativa:

Gracias Administrador del sistema.

Figura 1: Ejemplo de correo de phishing

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

-----Mensaje original-----
De: Administrador de correo [mailto:[redacted].gov.py] Enviado el: domingo, 10 de abril de 2016 03:26 p.m.
Asunto: Su cuenta vencerá en 4 días.

Estimado suscriptor de la cuenta,

Bienvenido a cuenta de correo web de actualización y mantenimiento. Su Cuota Webmail ha superado el Conjunto de cuota / límite que es de 20 GB. Actualmente se está ejecutando en 23 GB debido a los archivos y carpetas ocultos en su buzón. Con el fin de seguir utilizando nuestros servicios que necesita para actualizar y volver a confirmar por correo electrónico sus datos de cuenta que se solicita a continuación para validar su buzón de correo y aumentar su cuota.

NOMBRE DE USUARIO:
FECHA DE NACIMIENTO:
ESCRIBA CONTRASEÑA:
CORREO ELECTRÓNICO ALTERNATIVO:

Para nosotros para completar esta actualización son requieren para llenar el formulario de actualización de la cuenta, debe responder a este mensaje de inmediato y entrar en detalles de su cuenta conforme a lo solicitado. La actualización permitirá una navegación más rápida para el servicio y la disminución del tiempo de carga. También tendrá la posibilidad de cargar archivos adjuntos mucho más grandes que las versiones anteriores de correo electrónico, y permite hasta 30 MB a través de la interfaz de navegador web.

Después de seguir estas instrucciones, su cuenta no será interrumpida y continuará con normalidad. Gracias por su atención a esta solicitud. Nos disculpamos por cualquier inconveniente.

¡¡¡Advertencia!!! titular de la cuenta que se niega a actualizar su / su cuenta después de 4 días de recibir esta advertencia perderá su cuenta permanentemente. La protección de su buzón de correo sigue siendo nuestra máxima prioridad y su nombre de usuario y contraseña se mantendría sin cambios tras el ejercicio de actualización.

Gracias por su comprensión.

Código de Mantenimiento: JHF5G7NBX
Copyright © 2016 Centro de Soporte Webmail Helpdest.

Figura 2: Ejemplo de correo de phishing

Impacto:

Cuando la víctima revela la información solicitada (contraseña, correo alternativo, etc.) el/los ciberdelincuente/s detrás de la campaña podrán obtener acceso a las cuentas de correo de la víctima, pudiendose revelar información sensible y/o personal. Además, el acceso a estas cuentas podrán ser utilizadas por el/los ciberdelincuente/s para otros ataques dirigidos.

Debido a la mala práctica de reutilización de contraseñas para diferentes cuentas, es posible que el/los ciberdelincuente/s pudieran obtener accesos a otro tipo de cuentas o sistemas que utilicen la misma contraseña revelada por la víctima.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Mitigación y Prevención:

Recomendamos advertir a todos los funcionarios de su institución acerca de esta campaña de phishing, instándolos a no abrir dichos correos y no revelar ninguna información sensible. Así mismo, se recomienda que, en caso de recibir un correo electrónico con las características mencionadas en este boletín, se de aviso a un responsable de su organización.

En caso de que un usuario haya caído en el engaño y haya revelado su contraseña, se recomienda cambiar esta contraseña cuanto antes, así como también realizar un análisis exhaustivo para determinar el impacto que pudiera haber generado la revelación de la misma. Si su institución hubiera sido víctima de esta campaña de phishing y algún funcionario hubiera revelado información, puede reportar el incidente al CERT-PY de modo a brindarle asesoramiento en el análisis de impacto.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py