Alerta de Seguridad Informática (8FPH-00033-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 20 de Junio de 2019 | Última revisión 20 de Junio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los IoC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los IoC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

Resumen

El equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una campaña de Phishing, a través de un correo electrónico que intenta engañar al usuario para que ingrese sus credenciales de correo, mencionando que debe actualizar sus datos para evitar una funcionalidad reducida. Este correo proviene de la cuenta jguillen@proviasdes.gob.pe

Indicadores de compromisos

Url's:

http[:]//app[.]mobtizer[.]com/lp.php?lp=777c88af9c8aee11b451

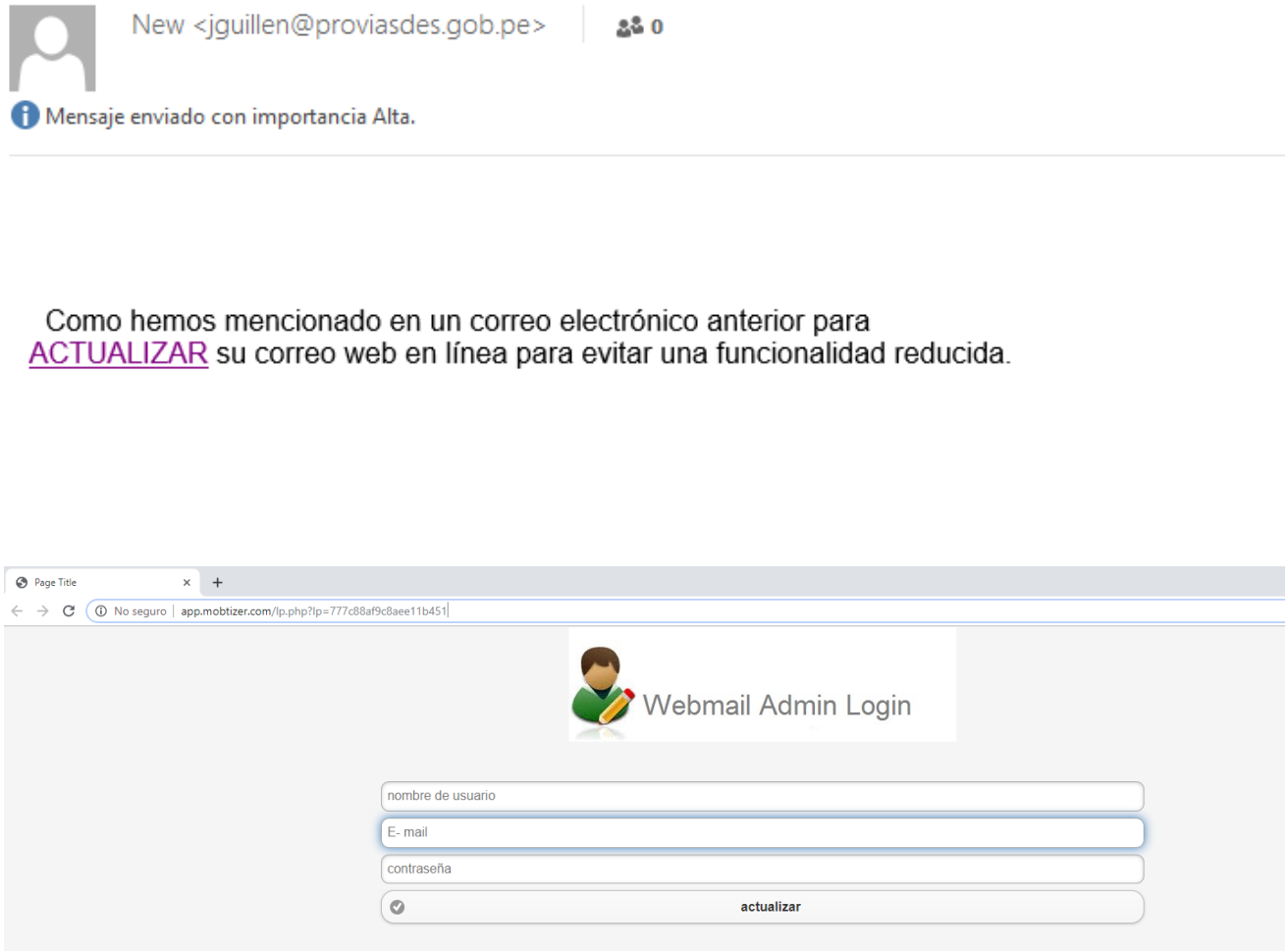
Smtp Host

mail.proviasdes.gob[.]pe [190.102.147.230])

From: (Original)

jguillen@proviasdes[.]gob[.]pe

Imagen


New <jguillen@proviasdes.gob.pe>
0
Mensaje enviado con importancia Alta.
Como hemos mencionado en un correo electrónico anterior para ACTUALIZAR su correo web en línea para evitar una funcionalidad reducida.
Page Title
No seguro | app.mobtizer.com/lp.php?lp=777c88af9c8aee11b451
Webmail Admin Login
nombre de usuario
E- mail
contraseña
actualizar

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- Evaluar el bloqueo preventivo de los indicadores de compromisos
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas
- Revisar los controles de seguridad de los AntiSpam y SandBoxing
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob