Alerta de Seguridad Informática (8FPH-00028-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 13 de junio de 2019 | Última revisión 13 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 serie de correos electrónicos que tienen la apariencia de casillas de Gmail, pero en realidad los correo de origen provienen de “gasatex.com” y “sinspam.com”, los que contienen un archivo adjunto en formato Word, el que se utiliza para explotar la vulnerabilidad CVE-2018-0802 de Office.

Vulnerabilidades

CVE-2018-0802

El Editor de ecuaciones en Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013 y Microsoft Office 2016 permite una vulnerabilidad de ejecución remota de código debido a la forma en que se manejan los objetos en la memoria, también conocida como "Vulnerabilidad de corrupción de memoria en Microsoft Office".

El parche está disponible en la siguiente Url de Microsoft: “https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0802”

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto, esto es, “Smtp Host”, “Subject” y las URL.

Indicadores de compromisos

Smtp Host

srvk67.allytech.com [190.210.196.67]
mia213.sinspam.com [69.25.11.213]

From:

From: "ES - Mapei Spain S.A." galciadecv@gmail.com

Subject:

Re:nuevo pedido

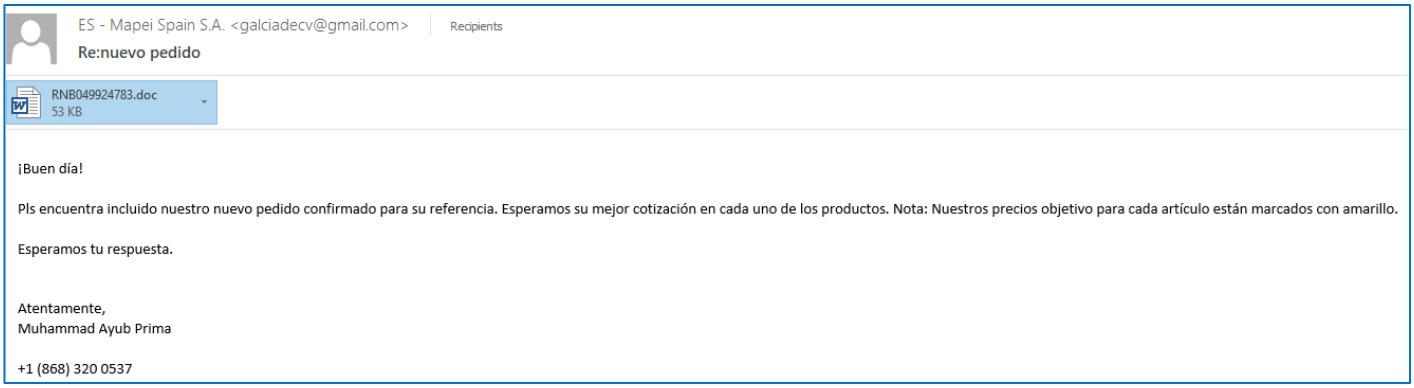
IoC

Nombre : rnb049924783.doc
Sha : MD5 8830865731ff5ab00405e9e0ce571ae3
Tamaño : 52.85 KB

Url’s:

http[:]//www.deserv[.]ie/explo/Sample 1.hta
http[:]//bit[.]ly/2Zlb3qt

Imagen



Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java, entre otras)
- Urls de Microsoft para descargar parche de seguridad “https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0802”
- 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