Alerta de Seguridad Informática (2CMV-00010-001)

Nivel de Riesgo: Alto

Tipo: Malware

Fecha de lanzamiento original: 21 de junio de 2019 | Última revisión 21 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 engañar que existe una reserva hotelera, donde debe terminar la transacción, solicitando por el atacante descargar documento adjunto formato Word “detalle de la reserva.docx”, el que se utiliza para explotar la vulnerabilidad CVE-2017-8570 de Office.

Vulnerabilidades

CVE-2017-8570

Microsoft Office permite una vulnerabilidad de ejecución remota de código debido a la forma en la que gestiona los objetos en la memoria. Esto también se conoce como "Microsoft Office Remote Code Execution Vulnerability.

El parche está disponible en la siguiente Url de Microsoft: “https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8570”

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

turkiye.narinhosting[.]com [185.171.24.49]

From:

sandro carlos recepakduman@turkochat[.]com

Subject:

detalles de la reserva002

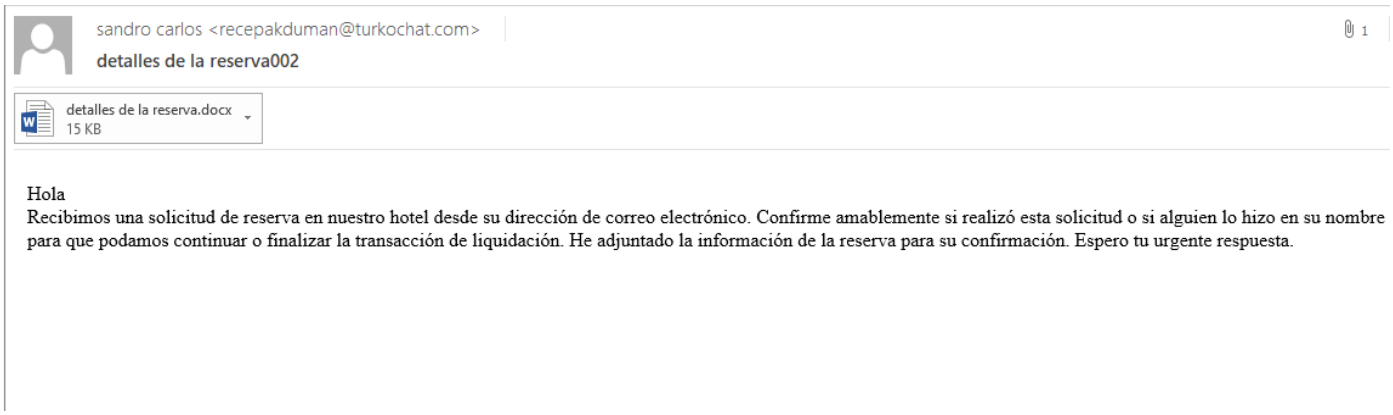
Archivo Adjunto

Archivo	:	detalles de la reserva.docx
MD5	:	d8d5c69e3ab5114f4bbbbd2ac873874d
SHA-1	:	833e6a4b117eada755860e59f6a994bb45c5e924
SHA-256	:	564953cb780453d03584cd3f5b68ea30c438c696025290f38c0c77dc304bcaf9

Url's:

http[:]//doughnut-snack[.]live/bpvpl.tar.gz
http[:]//greenroomstudio[.]live/app/
http[:]//mikelsonallen300.duckdns[.]org/is-ready
http[:]//greenroomstudio[.]live/app
http[:]//doughnut-snack[.]live/klplu.tar.gz
http[:]//doughnut-snack[.]live/mapv.tar.gz
http[:]//greenroomstudio[.]live/app/css.doc
http[:]//unknownsoft.duckdns[.]org/is-ready

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-2017-8570”
- 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