Alerta de Seguridad Informática (2CMV-00012-001)

Nivel de Riesgo: Alto

Tipo: Malware

Fecha de lanzamiento original: 03 de julio de 2019 | Última revisión 03 de Julio 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 intentan engañar a los usuarios adjuntando documentos de compras pendientes, los que solicitan la descarga de un documento adjunto en formato Word bajo los nombres “Shipping doc.doc.rtf” y “Shipping doc.doc.rtf”, el que se utiliza para explotar las vulnerabilidades CVE-2018-0802 y CVE-2017-0199 de Office. Además, existe un script en los documentos que es ejecutado por PowerShell el que descarga y ejecuta archivos maliciosos. Al ser infectado, el equipo realiza comunicaciones al servidor de comando y control (C&C).

Vulnerabilidades

CVE-2018-0802

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0802

“Resumen”

Existe una vulnerabilidad de ejecución remota de código en el software de Microsoft Office, que no puede manejar correctamente los objetos en la memoria. Un atacante podría ejecutar código arbitrario. Si el usuario actual ha iniciado sesión con derechos de usuario administrativos, un atacante podría tomar el control del sistema afectado. Un atacante podría entonces instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario. Los usuarios cuyas cuentas están configuradas para tener menos derechos de usuario podrían verse menos afectados que los usuarios que operan con derechos de usuario administrador.

CVE-2017-0199

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

“Resumen”

Existe una vulnerabilidad de ejecución remota de código en la forma en que Microsoft Office y WordPad analizan archivos. Un atacante podría tomar el control de un sistema afectado. Un atacante podría entonces instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario. La explotación de esta vulnerabilidad requiere que un usuario abra o obtenga una vista previa de un archivo especialmente diseñado con una versión afectada de Microsoft Office o WordPad.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto

Indicadores de compromisos

Smtp Host

server15158[.]comalis[.]net [91.191.151.58]
acestarcomph[.]wsiph2[.]com [45.33.104.46]

From:

SaaIkhlas@gmail[.]com
lisazry@ecuworldwide[.]com

Subject:

RE: SHIPPING DOCS
Re(4): FW: Re(2): new order 2019
new order 2019

Archivo Adjunto

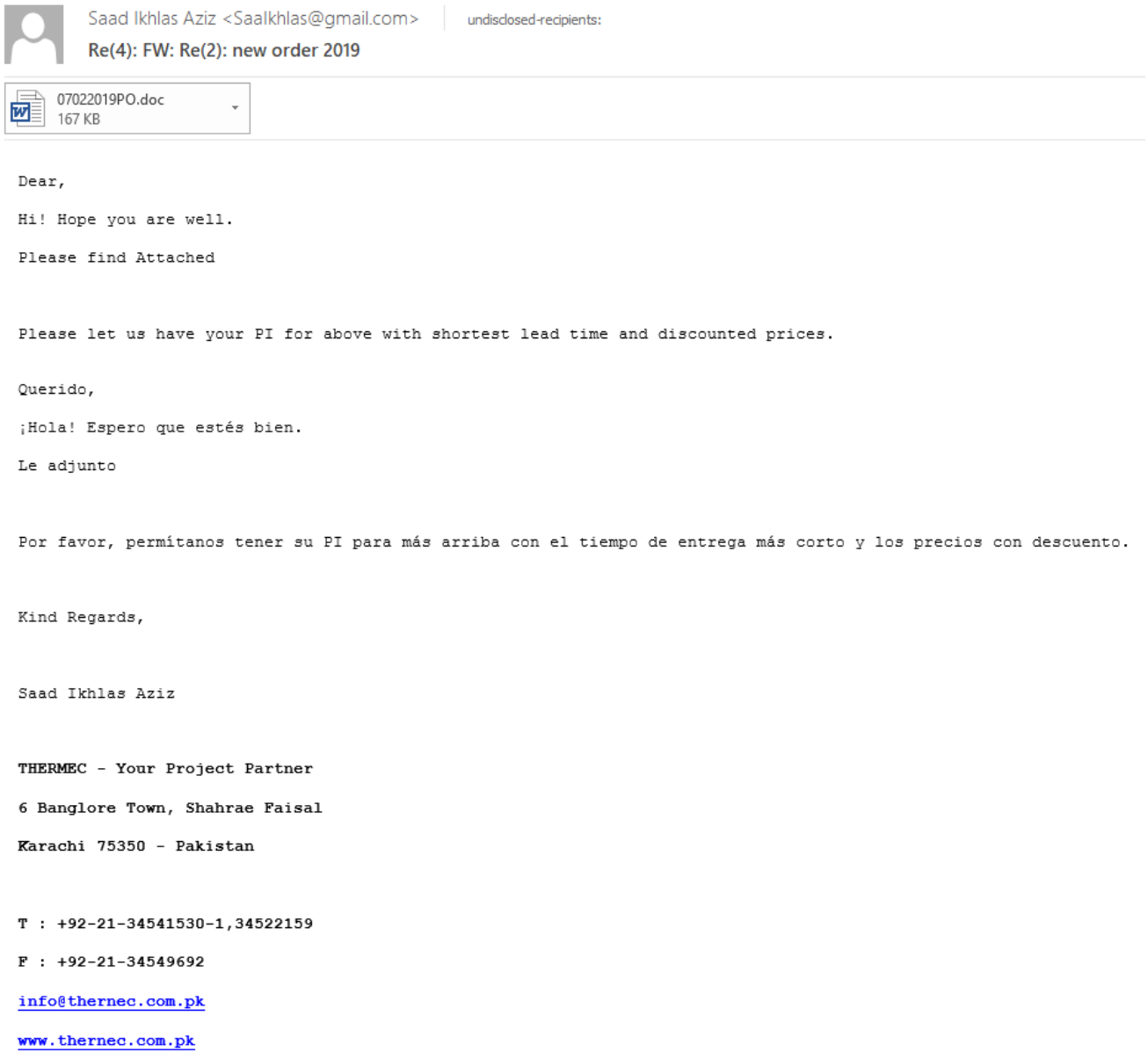
Archivo	:	07022019PO.doc
MD5	:	d5c64e4141ff4a2274f35915077b20b4
SHA-256	:	b086d462fa649284d139452f479708be9605f9d6

Archivo	:	Shipping doc.doc.rtf
MD5	:	1ff4a87cd3a91ae22ef241ced4b51438
SHA-1	:	e738fc100209ec00fa16d544b4f2755beb284b51

Url's:

http[:]//betalco[.]biz/PoQPvOnPEamMQIRK/gate[.]php
http[:]//www.deserv[.]ie/ameno/Sample[.]hta
http[:]//www.deserv[.]ie/amen/amen[.]dfg
http[:]//bit[.]ly/325yMgK

Imagen



Saad Ikhlas Aziz <Saalkhlas@gmail.com> undisclosed-recipients:

Re(4): FW: Re(2): new order 2019

07022019PO.doc
167 KB

Dear,

Hi! Hope you are well.

Please find Attached

Please let us have your PI for above with shortest lead time and discounted prices.

Querido,

¡Hola! Espero que estés bien.

Le adjunto

Por favor, permítanos tener su PI para más arriba con el tiempo de entrega más corto y los precios con descuento.

Kind Regards,

Saad Ikhlas Aziz

THERMEC - Your Project Partner

6 Banglore Town, Shahrae Faisal

Karachi 75350 - Pakistan

T : +92-21-34541530-1,34522159

F : +92-21-34549692

info@thernec.com.pk

www.thernec.com.pk

ECU WORLDWIDE (GUANGZHOU) LIMITED SHENZHEN BRANCH <lisazry@ecuworldwide.com>

RE: SHIPPING DOCS

Shipping doc.doc
43 KB

Dear Sir / Ma'am,

Hello.

We are pleased to send the shipping documents,

please see as per attached file.

I hope your confirmation reply when you receive this notice.

Kind regards,

Lisa Zheng Ru Yan

Document Clerk - Operation

ECU WORLDWIDE (GUANGZHOU) LIMITED SHENZHEN BRANCH
Unit 901-902, 9/F
Caiwuwei Jinlong Building
Hongbao Road, Luohu District

518 000 Shenzhen (China)
D: +86 760 88780815-810
E: lisazry@ecuworldwide.com
W: www.ecuworldwide.com

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-2017-0199
    - 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