CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

INFORME EMOTET

Nueva campaña Septiembre 2019

TLP: GREEN

Septiembre de 2019

GENERALITAT VALENCIANA

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa

UNIÓN EUROPEA

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la Generalitat Valenciana por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Sumario

1 Introducción

En diversas noticias de seguridad se anticipaba una nueva campaña de Emotet debido principalmente a investigaciones realizadas donde se notaron que los operadores de Emotet dejaron de estar activos a principios de junio. Durante este tiempo no se observaron nuevas campañas y el consenso general en la comunidad fue que los servidores estaban fuera de servicio y se estaba preparando una nueva oleada de ataques. Posteriormente, sobre el 22 de agosto se observó que la infraestructura de Emotet volvía a reactivarse.

Ahora, menos de un mes después de reactivar los servidores C2, la botnet Emotet ha empezado a enviar campañas de spam a países de todo el mundo.

Los primeros correos electrónicos maliciosos con la firma de Emotet, observados el lunes 16 de septiembre por la mañana, iban dirigidos principalmente a personas, empresas y entidades gubernamentales de Alemania, el Reino Unido, Polonia, Italia y los EE. UU.

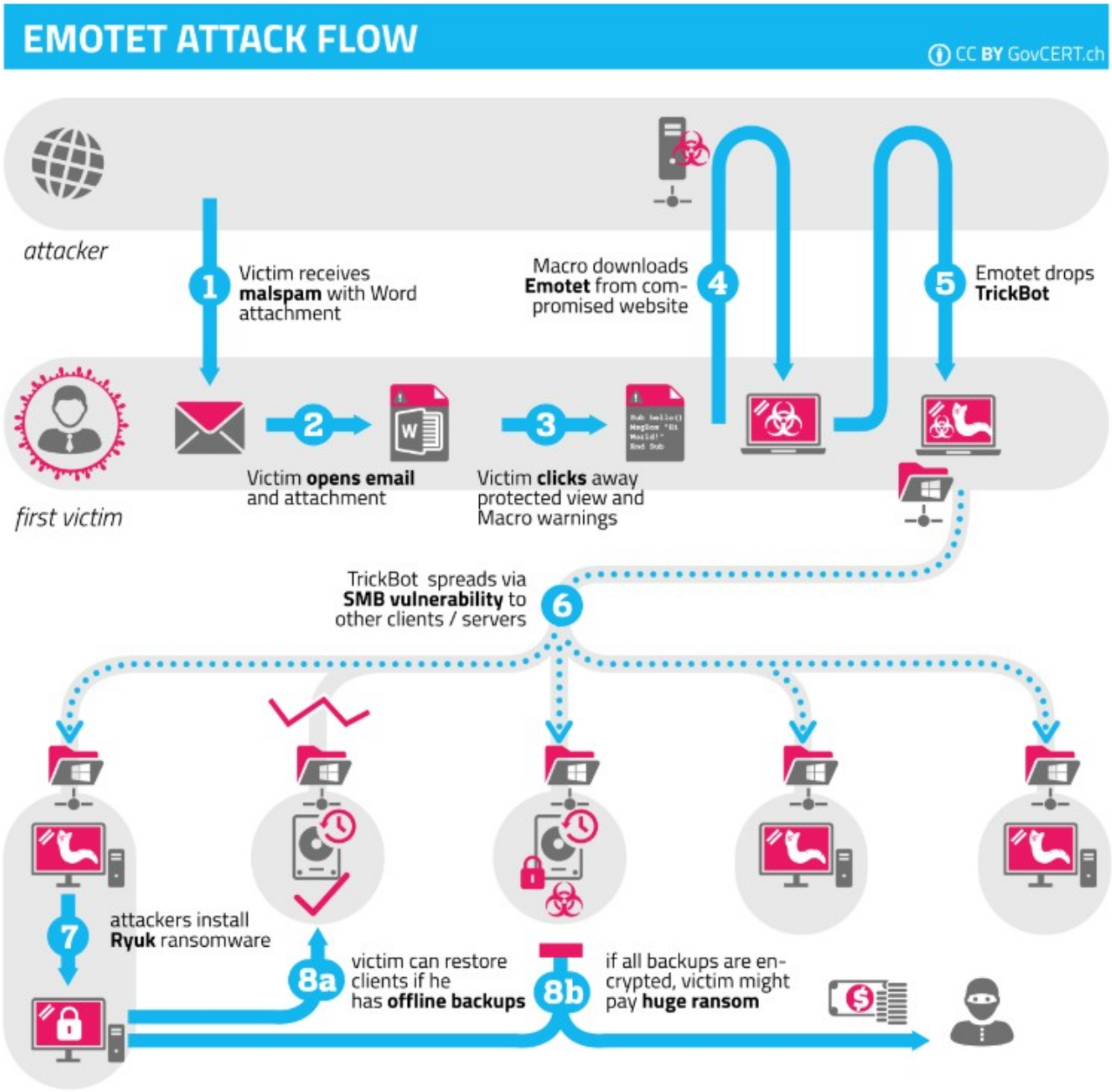
El martes 17 de septiembre comenzamos a observar, en nuestro ámbito, correos con adjuntos “.doc” y otros con enlaces externos que apuntaban a infraestructura de Emotet. Aparte según indican también pueden llegar como documentos adjuntos de JavaScript.

Según el informe publicado el 9 de septiembre por GovCERT.ch[1] donde se detalla el *modus operandi* se indica que se han observado ataques severos de ransomware usando estas técnicas. El vector de ataque puede ser por campañas *Malspam*, *Spear Phishing*, accesos por RDP desde internet o Citrix con credenciales débiles, y descarga de exploits alojados en webs previamente comprometidas.

Cuando el atacante obtiene el acceso a la red de la víctima, el *dropper* de Emotet analiza el entorno y a partir de ese momento, continúa la infección utilizando Trickbot y/o Ryuk, u otras según el objetivo, para etapas posteriores. Según el objetivo de la campaña, puede ser una ataque activo o bien comprometer un equipo para posteriormente vender el acceso en el mercado negro. En ambos casos, el atacante también trata de robar credenciales e infectar más sistemas para obtener un punto de apoyo más sólido en la red de las víctimas. Una vez que el atacante infecta suficientes sistemas y/o obtiene credenciales de alto nivel de privilegios (como el administrador de dominio de Windows), despliega el ransomware, cifra los datos y/o destruye los sistemas.

En ese mismo informe se muestra un gráfico con el flujo de ataque de Emotet, que coincide con nuestra investigación sobre las muestras obtenidas.

1 https://www.govcert.ch/blog/36/severe-ransomware-attacks-against-swiss-smes



Como puede observarse Emotet solo es la vía de entrada. Después utiliza Trickbot para realizar movimiento lateral a otros activos de la red utilizando vulnerabilidades como:

- Módulo de gusano SMB de Trickbot (*worm.dll* o *spreader.dll*) que explota Eternal Blue (CVE-2017-0143 / MS17-010). Este módulo utiliza la vulnerabilidad SMB antes mencionada para propagarse más y aumentar los privilegios a nivel del sistema.
- RDP Credential Stealer (Módulo *pwgrab32.dll*) de Trickbot.

- Usando la puerta trasera Empire Powershell.
- Hay otros módulos de Trickbot que pueden ser útiles para el atacante (por ejemplo *screenlocker.dll* , *systeminfo.dll* o *vncsrv.dll* cuyos nombres son bastante autoexplicativos).

Por último, cuando tienen ya identificadas varias victimas y mediante movimiento lateral han infectado activos críticos como servidores o controladores de dominio, lanzan la variante de ransomware Ryuk.

En el informe de GovCERT.ch[2] también se indican las capacidades de este ransomware así como las contramedidas aplicables para reducir el impacto del ataque.

2 Muestra

El pasado 17 de septiembre se identificó un correo remitido por la dirección "geo.operation@votbookings.com" que contenía un enlace externo hacia el dominio "delegun.com". Este descargaba un archivo "Office Open XML Document" que realmente era un documento Word que contenía macros maliciosas. Tras analizar el enlace en VirusTotal (https://www.virustotal.com/gui/url/9dce68da3da3cc38c2305aa40766b737157474f9d4ecc77f7f59be0cfd99f634/details), y posteriormente el sha-256 del archivo (https://www.virustotal.com/gui/file/f06d1abada97c93d7f65d8daddf46fdf35fedc33d27a3bd55fdc9a4687aed238/details) se detectó que efectivamente ese correo provenía de la Botnet de Emotet.

En el análisis de este tipo de documento se observa el uso de una macro maliciosa que ejecuta un powershell, codificado en base64, que contiene los enlaces para las descarga del código dañino. Los enlaces detectados para esta muestra son:

- hxxps://www.59055[.]cn/wp-content/f7c18_onqapey8-49048/
- hxxps://www.xinlou[.]info/wp-content/zomusjj_rgsps3-791960/
- hxxps://larissalinhares.com[.]br/wp-admin/ttzTQwatYY
- hxxps://toptarotist[.]nl/cgi-bin/r1y59l_283xx-97329804/
- hxxp://www.robotechcity[.]com/wp-content/nyCCqximrj/

2 https://www.govcert.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

El correo completo es el siguiente:

-----Mensaje original-----

De: PECME [mailto:geo.operation@votbookings.com]

Enviado el: martes, 17 de septiembre de 2019 10:55

Para: PECME

Asunto: PAGOS FACTURAS

Buenas tardes,

Et passo els documents sol·licitats

hxxps://deleogun[.]com/paclm/bZIuaFhVQlDwWFAAVqunuPzofQ/

Gracias,

PECME

Como puede observarse en el correo no se trata de un spam o phishing mal hecho que descargue el documento malicioso, sino que se trata de un intento de suplantación del organismo PECME, que envía correos a otros usuarios corporativos, de esta manera es más fácil que engañen a quien recibe el correo pues supondrá que ha sido enviado por algún compañero. Además, el correo no está en idiomas genéricos como el inglés sino que está en castellano y valenciano, lo cual aún da más confianza al receptor del correo.

En estos momentos se está analizando la muestra en el laboratorio de malware de CSIRT-CV para contrastar los datos observados en informes recientes de Emotet.

Vista la incidencia de la campaña, no sólo en nuestro ámbito sino en general, se buscó toda la información posible sobre Emotet y se recabaron los IOC que se exponen en el apartado de IOC.

Tras recabar todos los IOC, se añadieron a un analizador de tráfico y tras su ejecución se observaron ciertos equipos contactando con algunos de los dominios usados por Emotet para la descarga del documento malicioso. Concretamente estos dominios son:

- solivagantfoodie[.]com
- hanifbaba[.]com
- kattegattcenter[.]se

En uno de los casos la usuaria ha confirmado que abrió un correo extraño a las horas que

notificamos.

Además hemos observado en equipos comprometidos que se está usando módulo para enviar correos al exterior de forma masiva con adjuntos maliciosos del tipo "*.doc*". Los correos iban dirigidos a servidores de correo externos usando el puerto 587 de smtps. También se ha observado en equipos comprometidos solicitudes al recurso "*whoami.php*" de una de las IP que aparece en el apartado IOC. Concretamente la petición es (*hxxp://104.236.185[.]25:8080/whoami.php)*, según se indica está relacionado con "*Spam C2s*"

Por último hemos observado que un equipo ha generado la siguiente alerta en el IDS "*ETPRO TROJAN Observed Trickbot Style SSL Cert (Internet Widgets Pty Ltd)*". El contacto con las direcciones IP externas está activo actualmente según Feodo Tracker, y contiene muestras de malware relacionados con TrickBot:

https://feodotracker.abuse.ch/browse/host/190.13.160.19

https://feodotracker.abuse.ch/browse/host/186.42.98.254

Toda la información genérica ha sido obtenida, a través de los siguientes enlaces:

- https://twitter.com/hashtag/emotet
- https://blog.malwarebytes.com/botnets/2019/09/emotet-is-back-botnet-springs-back-to-life-with-new-spam-campaign/
- https://app.any.run/tasks/590eb66a-89e4-4aad-86ab-1f344f93e2ee/
- https://www.bleepingcomputer.com/news/security/emotet-revived-with-large-spam-campaigns-around-the-world/
- https://www.zdnet.com/article/emotet-todays-most-dangerous-botnet-comes-back-to-life/
- https://www.govcert.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

3 IOC

Los IOC se han obtenido desde los siguientes enlaces:

- https://pastebin.com/u/jroosen
- https://pastebin.com/VnnwwP4y
- https://pastebin.com/nUxnxSg4
- https://pastebin.com/cZ0RUx9V

- https://pastebin.com/a5uQnG9b
- IP Trickbot: 190.13.160.19, 186.42.98.254, 190.152.4.98, 190.154.203.218, 170.238.117.187, 170.233.120.53 y 189.80.134.122.
- hxxps://bhubaneswarambulance.com/wp-content/tg3p20/
- hxxps://indonesiaexp.com/wp-admin/ar3468/
- hxxp://purepropertiesobx.com/menusa/edt222/
- hxxp://sidanah.com/wp-admin/6dtjzp2161/
- hxxps://potoretocreative.com/wp-admin/n7/

Indicar que las muestras analizadas presentan dominios o IP reflejados en los enlaces anteriormente mencionados. Estamos en proceso de análisis de muestras para obtener más información acerca de esta nueva campaña.