La Botnet de EMOTET reinicia ataques en Chile y LATAM

cronup.com/la-botnet-de-emotet-reinicia-ataques-en-chile-y-latinoamerica/

November 19, 2021

Resumen Ejecutivo

En enero de 2021 la botnet de Emotet, una de las ciberamenazas más importantes del mundo, fue desmantelada en un esfuerzo en conjunto de multiples países y fuerzas policiales, sin embargo, 10 meses despues y luego de que las autoridades realizaran una desinstalación masiva del malware a nivel mundial, Emotet vuelve a mostrar signos de vida y la reconstrucción progresiva de su botnet a través de uno de sus más fieles colaboradores como es Trickbot.

Según la gente de Advanced Intelligence el regreso de Emotet ha sido tramado por un ex miembro de Ryuk, ahora parte de la pandilla de Conti, con la finalidad de dar soporte a los próximos ataques de Ransomware.

Junto a lo anterior, hemos podido evidenciar que Emotet ya se encuentra enviando campañas masivas de phishing a países en Latinoamérica como Perú, México, Paraguay, Uruguay, Colombia, Panamá, Ecuador, Argentina, El Salvador y porsupuesto Chile, entre otros.

Esto también lo hemos podido confirmar con terceros como en este Tweet de TG Soft

> 2021-11-18 #Emotet Epoch5 is spamming these countries: 🇬🇷 Greek, 🇨🇱 Chile, 🇵🇹 Portugal, 🇲🇽 Mexico, 🇵🇱Poland, 🇨🇿 Czech Rep., 🇦🇷 Argentina, 🇺🇾 Uruguay, 🇸🇰 Slovakia, 🇨🇴 Colombia, 🇪🇨 Ecuador and others.
>
> Botnet re-building in progress….
>
> — TG Soft (@VirlTeXplorer) November 18, 2021

Y en este análisis de Brad Duncan

> 2021-11-18 (Thursday) – #Emotet epoch 4 activity (emails/malware/#pcap) – https://t.co/v1k8x4MFIT – Most emails sent to Spanish-speaking recipients in central and south America, but saw one to a .gr recipient. This is the first pcap I've posted with new Emotet's HTTPS C2 traffic. pic.twitter.com/Cy8x06y20o
>
> — Brad (@malware_traffic) November 19, 2021

Actualmente Emotet cuenta con dos infraestructuras independientes que son parte de la misma botnet, a estas infraestructuras se les llama Epoch, y su caracteristica principal es que permiten a la botnet desplegarse de forma modular y mantener el control en el caso de que alguna de estas caiga.

Epoch 4 y Epoch 5 son las que se encuentran activas y ambas han comenzado a enviar campañas masivas de phishing a Latinoamérica y múltiples países alrededor del mundo.

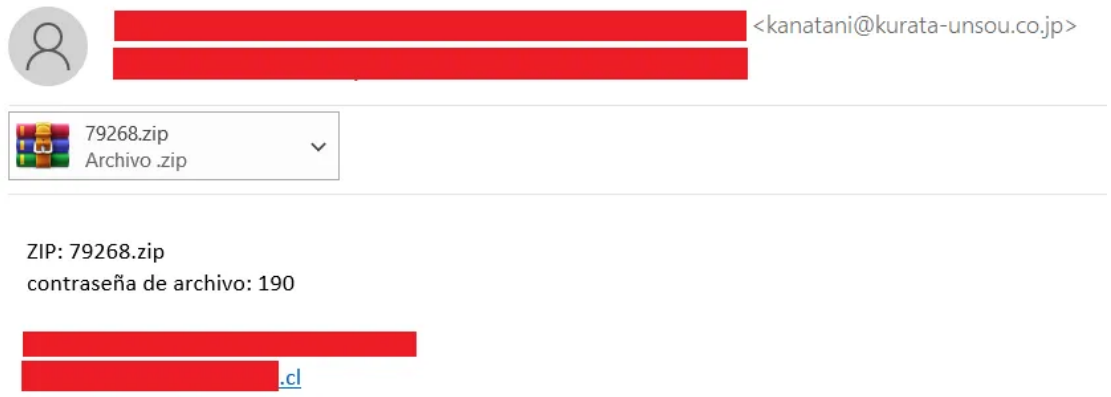
> Al momento de escribir esta alerta, CronUp ha confirmado tres incidentes en Chile por infección con este Malware.
>
> Es importante recordar que un compromiso por Emotet en la red corporativa puede derivar a un ataque de Ransomware.

Distribución del Malware

Emotet se distribuye a través de correos electrónicos, utilizando para ello miles de cuentas SMTP comprometidas y suplantando a contactos conocidos o de confianza. En campañas anteriores también hemos visto el secuestro o robo de cadenas de correos, algo que seguramente veremos también muy pronto.

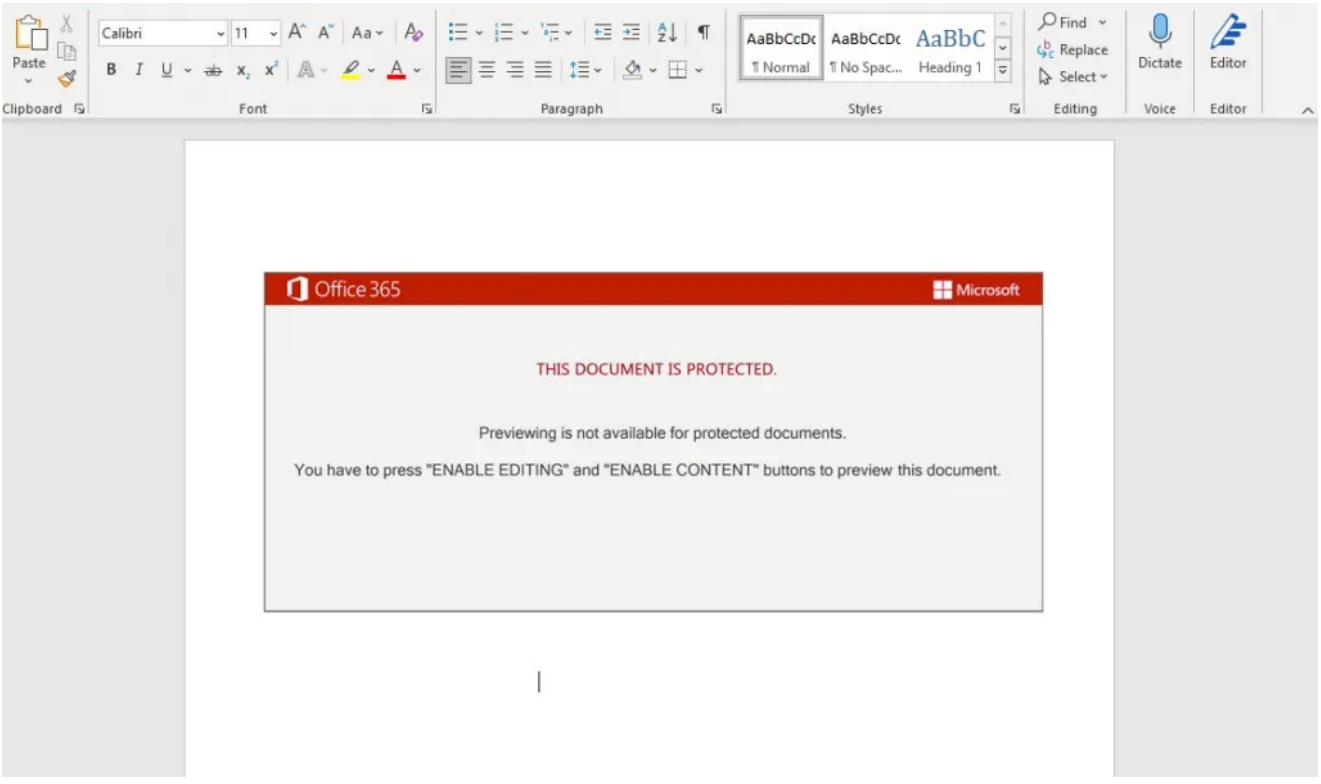
En la actualidad, el correo malicioso trae un archivo adjunto protegido con contraseña, lo que dificulta el análisis automatizado de algunas herramientas de seguridad y que en conjunto a los servidores SMTP que utilizan (organizaciones válidas) permite a los atacantes tener una mayor tasa de éxito.

A continuación, un ejemplo del correo Phishing.

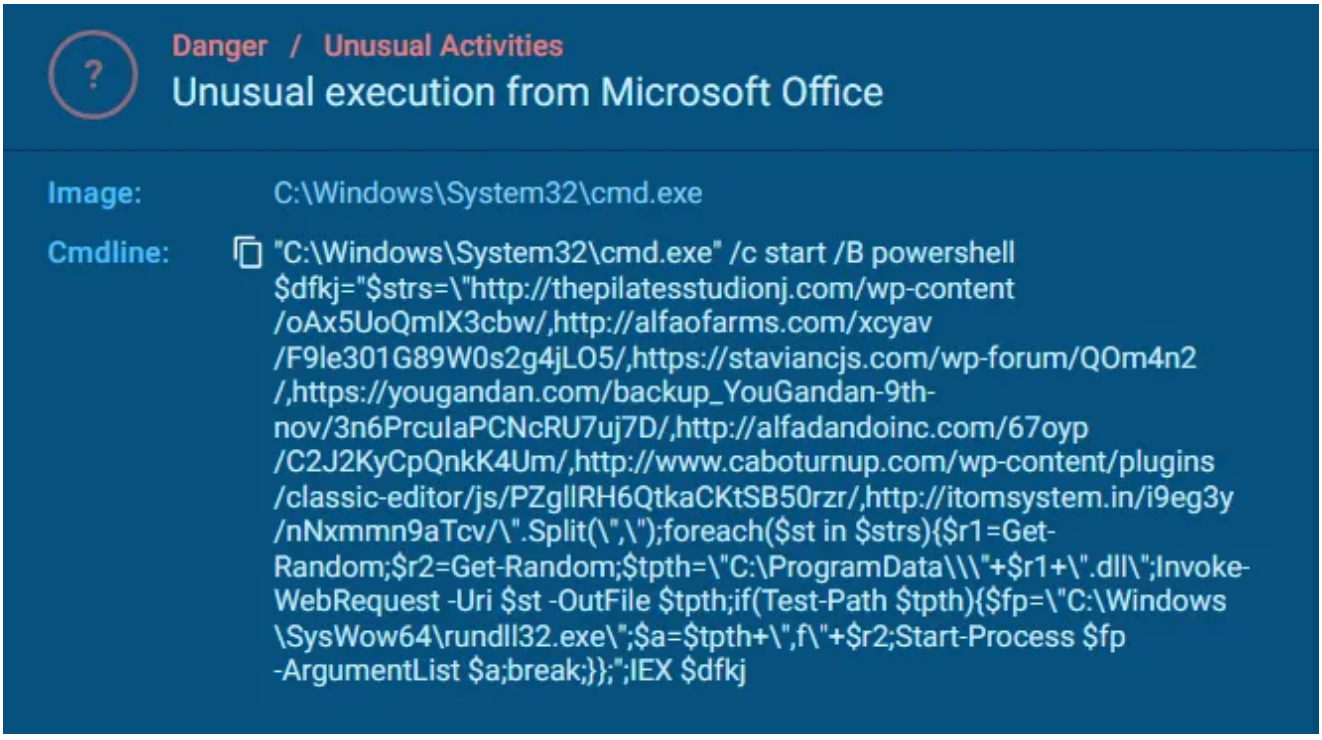


El archivo .ZIP trae un documento Microsoft Office en su interior, el que puede tener extensión .DOC, .DOCM o .XLSM entre otras. También se han visto casos donde el adjunto es directamente el documento de MS Office y en un pasado también lo hicieron con un link en el cuerpo del correo para la descarga del documento.

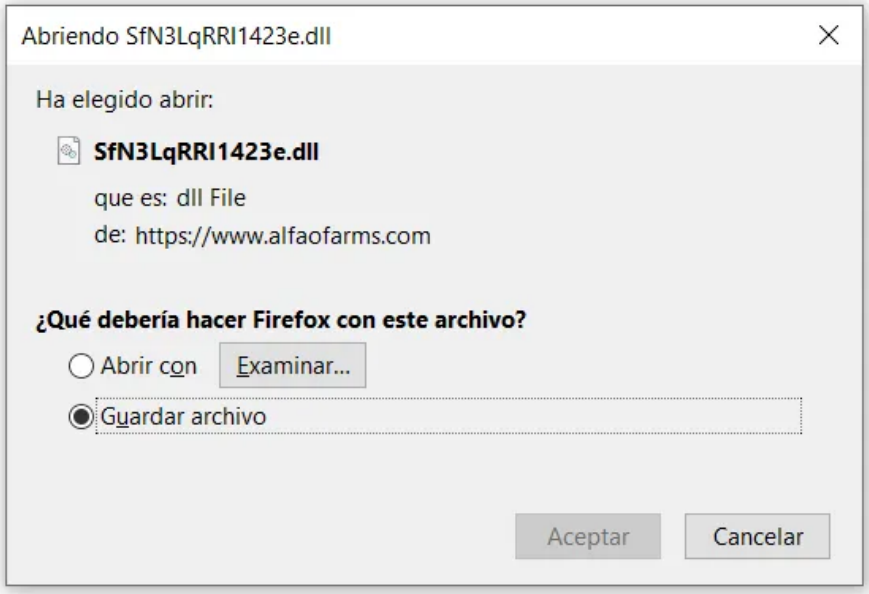
Al abrir el documento y habilitar la edición, se activa la macro y el proceso de infección del equipo. La imagen a continuación es una de las plantillas utilizadas actualmente pero pueden ser otras también.



La macro del documento ejecuta Powershell para realizar la descarga del payload final (DLL de Emotet) desde 1 de los 7 sitios distintos que vienen configurados en el documento Microsoft Office.



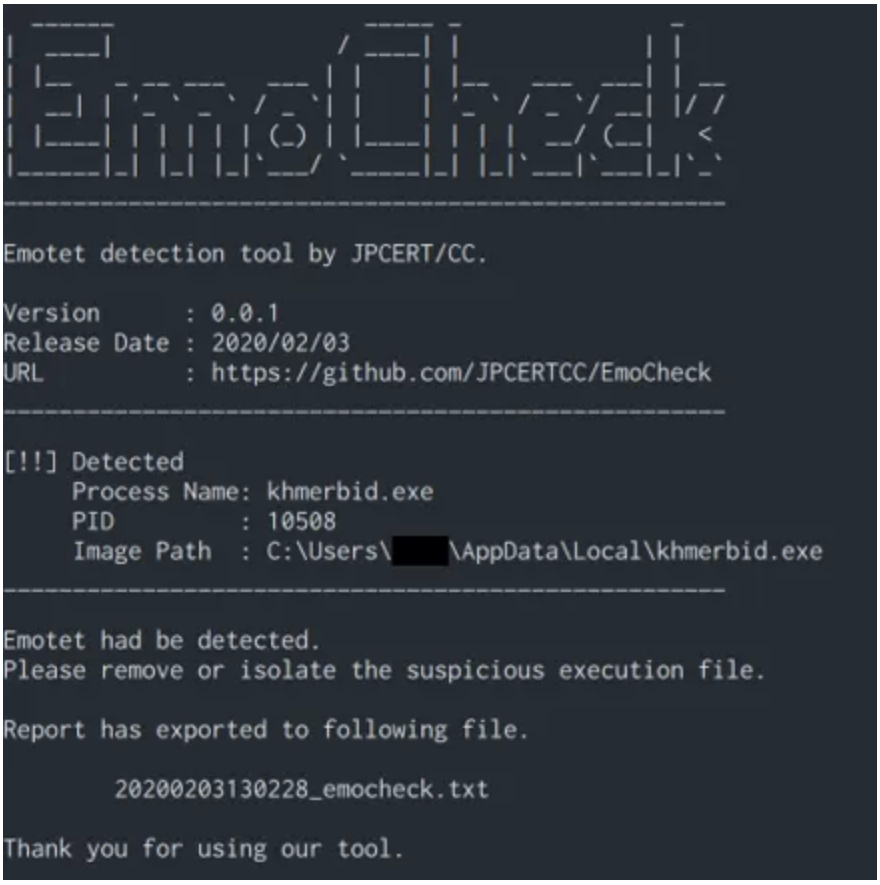
Al visitar una de estas URLs se puede apreciar la descarga de la DLL de Emotet.



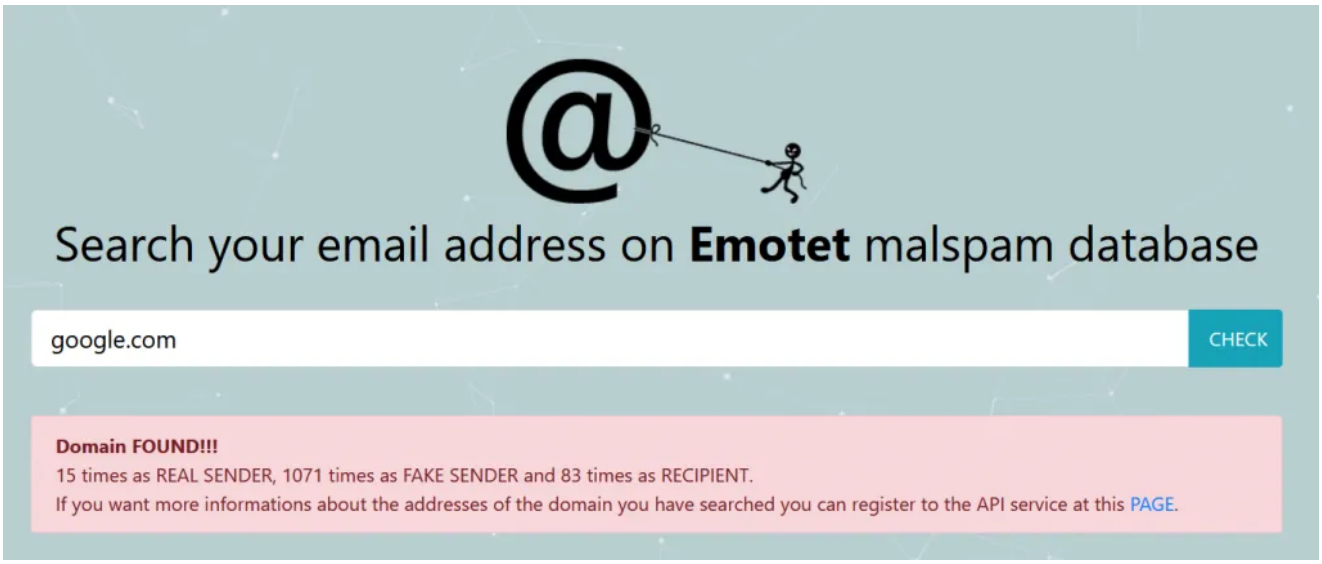
En este punto, luego de registrar la DLL, Emotet ha logrado infectar y compromer efectivamente el equipo y agregarlo a la red de computadores zombie que forman parte de la Botnet.

Herramientas y recursos

1.- **EmoCheck**, es una herramienta para la detección de Emotet en sistemas operativos Windows que ha sido desarrollada por el CERT de Japón: https://github.com/JPCERTCC/EmoCheck



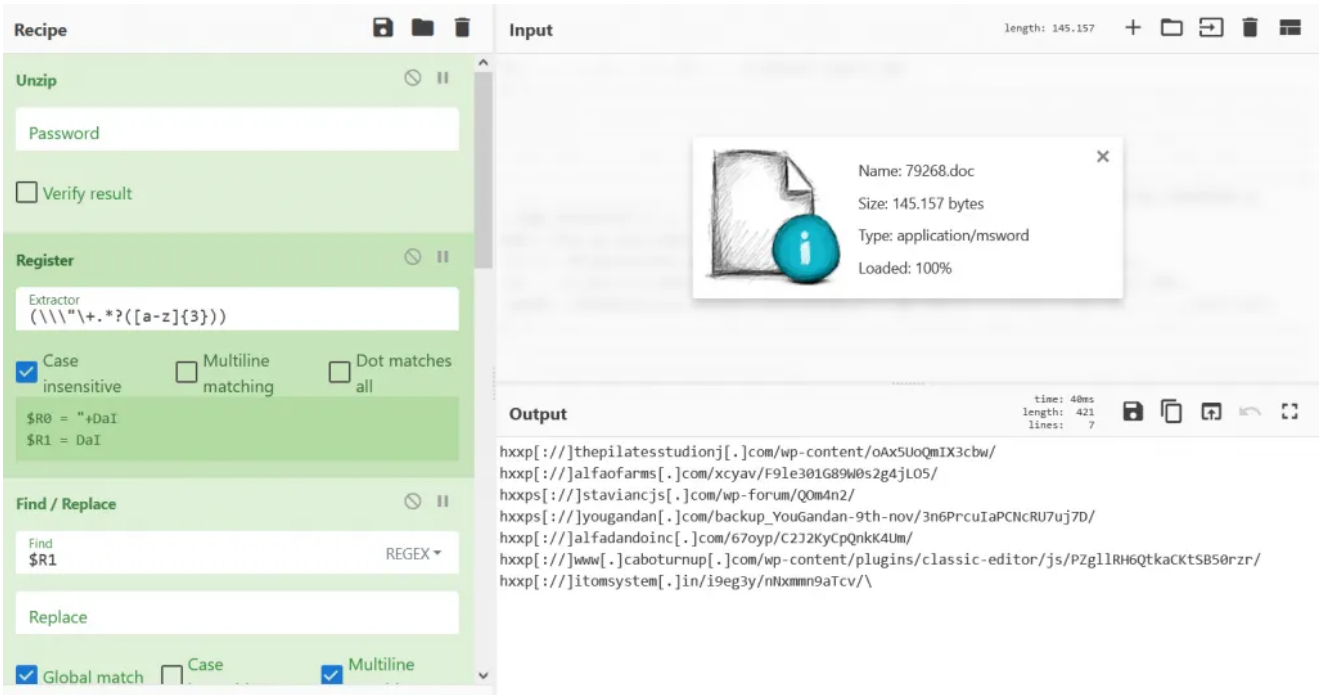
2.- **HaveIBeenEMOTET**, es un portal desarrollado por TG SOFT para detectar si un correo o dominio está en la base de datos de SPAM de Emotet: https://www.haveibeenemotet.com/



* Si, incluso Google ha sido víctima de Emotet.

3.- **CyberChef**, es una aplicación web para la encriptación, codificación, compresión y análisis de datos. Gracias a la información compartida por la gente de Cryptolaemus1 y Kostastsale hemos podido ajustar una nueva receta o «Recipe» que extrae las URLs de los documentos maliciosos (funcionando al 19-11-2021).

Utilizar desde tinyurl.com/EmotetURLs (solo debes dejar caer el documento en «Input»)



Indicadores de Compromiso

La mejor forma de protegerse frente a esta ciberamenaza es:

1.-Siguiendo al equipo de Cryptolaemus1 quienes estudian y exponen las nuevas técnicas, tácticas y procedimientos de estos atacantes.

2.-Actualizando regularmente las listas de bloqueo (C2) que disponibiliza Abuse.ch desde https://feodotracker.abuse.ch/browse/emotet/

El listado actual de servidores de comando y control activos es:

122.129.203.163
31.220.49.39
191.252.196.221
202.29.239.161
185.184.25.237
103.161.172.108
93.188.167.97
163.172.50.82
45.79.33.48
210.57.217.132
177.72.80.14
51.178.61.60
142.4.219.173
168.197.250.14

Referencias

- https://www.cronup.com/emotet-esta-de-regreso-gracias-a-la-ayuda-de-trickbot/
- https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware
- https://isc.sans.edu/diary/28044
- https://www.malware-traffic-analysis.net/2021/11/18/index.html
- https://therecord.media/emotet-botnet-returns-after-law-enforcement-mass-uninstall-operation/
- https://security-soup.net/quick-post-emotet-the-mummy-returns-again/
- https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot/

Iremos actualizando este reporte a medida que se identifiquen cambios significativos en esta amenaza. **Recuerden bloquear regularmente los nuevos C2 para mantenerse protegidos**.

Threat Intelligence Team
CronUp Ciberseguridad

Germán Fernández
Threat Researcher en CronUp Ciberseguridad
Líder Red Team & Cyber Threat Intelligence.