Autoridades de hasta ocho países desmantelaron la infraestructura de Emotet, un malware de Windows basado en correo electrónico detrás de varias campañas de spam impulsadas por botnets y ataques de ransomware durante los últimos diez años.

La eliminación coordinada de la botnet este martes, denominada *«Operation Ladybird»*, es el resultado de un esfuerzo conjunto entre las autoridades de los Países Bajos, Alemania, Estados Unidos, Reino Unido, Francia, Lituania, Canadá y Ucrania, para tomar el control de los servidores que se utilizaron para ejecutar y mantener la red del malware.

> *«La infraestructura de Emotet actuó esencialmente como una puerta principal para los sistemas informáticos a escala global. Lo que hizo a Emotet tan peligroso es que el malware se ofreció en alquiler a otros ciberdelincuentes para instalar otros tipos de malware, como troyanos bancarios o ransomware, en la computadora de la víctima»*, dijo la Europol.

Desde su identificación por primera vez en 2014, Emotet ha evolucionado desde sus raíces como un ladrón de credenciales y un troyano bancario hasta una poderosa *«navaja suiza»* que puede servir como descargador, ladrón de información y spam, dependiendo de cómo se implemente.

Conocido por estar en constante desarrollo, el servicio de ciberdelincuencia se actualiza regularmente para mejorar el sigilo, la persistencia y agregar nuevas capacidades de espionaje a través de una amplia gama de módulos, incluyendo un difusor de WiFi para identificar y comprometer a nuevas víctimas conectadas a redes WiFi cercanas.

El año pasado, el malware se vinculó a varias campañas de spam impulsadas por botnets e incluso fue capaz de entregar cargas útiles más peligrosas como TrickBot y Ryuk, alquilando su botnet de máquinas comprometidas a otros grupos de malware.

> *«El grupo Emotet logró llevar el correo electrónico como vector de ataque al*

> *siguiente nivel»*, dijo Europol.

## 700 servidores Emotet incautados

La Agencia Nacional del Crimen del Reino Unido (NCA), dijo que la operación tomó casi dos años para mapear la infraestructura de Emotet, con múltiples propiedades en la ciudad ucraniana de Kharkiv allanadas para confiscar equipos informáticos utilizados por los hackers.

El Departamento de Policía Cibernética de Ucrania también arrestó a dos personas presuntamente involucradas en el mantenimiento de la infraestructura de la botnet, ambos enfrentan 12 años de prisión en caso de ser declarados culpables.

> *«El análisis de las cuentas utilizadas por el grupo detrás de Emotet, mostró que 10.5 millones de dólares fueron movidos durante un período de dos años en una única plataforma de moneda virtual. Casi 500,000 dólares se habían gastado por el grupo durante el mismo período para mantener su infraestructura criminal»*, dijo la NCA.

A nivel mundial, los daños relacionados con Emotet han costado al rededor de 2,500 millones de dólares, según las autoridades ucranianas.

Con por lo menos 700 servidores operados por Emotet en todo el mundo, ahora eliminados desde el interior, las máquinas infectadas por el malware están configuradas para ser dirigidas a esta infraestructura policial, evitando de este modo una mayor explotación.

La Policía Nacional Holandesa lanzó una herramienta para verificar los posibles riesgos, basada en un conjunto de datos que contiene 600 mil direcciones de correo electrónico, nombres de usuario y contraseñas que se identificaron durante la operación.

## Limpieza de Emotet en masa el 25 de abril de 2021

La policía holandesa incautó dos servidores centrales ubicados en el país, y dijo que ha implementado una actualización de software para neutralizar la amenaza que representa Emotet de forma efectiva.

*«Todos los sistemas informáticos infectados recuperarán automáticamente la actualización allí, después de lo cual, la infección de Emotet se pondrá en cuarentena»,* dijo un investigador apodado milkcream. Se espera que Emotet se elimine de todas las máquinas comprometidas el 25 de abril de 2021 a las 12:00 hora local.

Hasta ahora, el servicio Abuse.ch Feodo Tracker muestra que al menos 20 servidores Emotet siguen en línea.

> *«Una combinación de herramientas de ciberseguridad actualizadas y conciencia de ciberseguridad es esencial para evitar ser víctima de botnets sofisticadas como Emotet»,* dijo Europol.
>
> *«Los usuarios deben revisar cuidadosamente su correo electrónico y evitar abrir mensajes y especialmente archivos adjuntos de remitentes desconocidos. Si un mensaje parece demasiado bueno para ser verdad, probablemente lo sea y los correos electrónicos que imploran un sentido de urgencia deben evitarse a toda costa»*, agregó.