Emotet, un malware basado en correo electrónico detrás de distintas campañas de spam impulsadas por botnes y ataques de ransomware, contenía una falla que permitía a los investigadores de seguridad cibernética activar un interruptor de seguridad y evitar que el malware infectara los sistemas por seis meses.

> *«La mayoría de las vulnerabilidades y exploits sobre las que lee son buenas noticias para los atacantes y malas noticias para el resto de nosotros»,* dijo James Quinn, de Binary Defense.
>
> *«Sin embargo, es importante tener en cuenta que el malware es software que también puede tener fallas. Así como los atacantes pueden explotar fallas en software legítimo para causar daño, los defensores también pueden aplicar ingeniería inversa para descubrir sus vulnerabilidades y luego explotarlas para derrotar a los malware»,* agregó.

El kill-switch estuvo activo entre el 6 de febrero de 2020 y el 6 de agosto de 2020, durante 182 días, antes de que los autores del malware parchearan su malware y cerraran la vulnerabilidad.

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

A inicios de febrero, desarrolló una nueva característica para aprovechar los dispositivos ya infectados para identificar y comprometer a nuevas víctimas conectadas a redes WiFi cercanas.

Junto con esta actualización de funciones vino un nuevo mecanismo de persistencia, según Binary Defense, que *«generó un nombre de archivo para guardar el malware en cada sistema víctima, utilizando un nombre de archivo del sistema exe o dll al azar del directorio*

system32».

El cambio en sí mismo fue sencillo: cifró el nombre del archivo con una clave XOR que luego se guardó en el valor de registro de Windows establecido en el número de serie del volumen de la víctima.

La primera versión del kill-switch desarrollado por Binary Defense, que se puso en marcha unas 37 horas después de que Emotet revelara los cambios anteriores, empleó un script de PowerShell que generaría el valor de la clave de registro para cada víctima y establecería los datos de cada valor en nulo.

De esta forma, cuando el malware buscaba el nombre del archivo en el registro, terminaría cargando un archivo exe vacío, lo que impedía que el malware se ejecutara en el sistema de destino.

> *«Cuando el malware intenta ejecutar '.exe', no podría ejecutarse porque '.' se traduce al directorio de trabajo actual para muchos sistemas operativos»,* dijo Quinn.

En una versión improvisada del kill-switch, llamada EmoCrash, Quinn dijo que pudo explotar una vulnerabilidad de desbordamiento de búfer descubierta en la rutina de instalación del malware para bloquear Emotet durante el proceso de instalación, evitando así que los usuarios se infecten.

De este modo, en lugar de restablecer el valor del registro, el script funciona identificando la arquitectura del sistema para generar el valor del registro de instalación para el número de serie del volúmen del usuario, usándolo para guardar un búfer de 832 bytes.

> *«Este pequeño búfer de datos era todo lo que se necesitaba para bloquear Emotet, e incluso podría implementarse antes de la infección (como una vacuna) o en mitad*

> *de la infección (como un interruptor de muerte). Aparecerían dos registros de fallos con ID de evento 1000 y 1001, que podrían usarse para identificar puntos finales con binarios de Emotet desactivados y muertos después de la implementación del interruptor y reiniciar la computadora»*, dijo Quinn.

Para mantenerlo en secreto de los actores de amenazas y poder parchear el código, Binary Defense dijo que se coordinó con los Equipos de Respuesta a Emergencias Informáticas (CERT) y el Equipo Cymru para distribuir el script de explotación EmoCrash a organizaciones susceptibles.

Aunque Emotet retiró su método de instalación basado en claves de registro a mediados de abril, no fue hasta el 6 de agosto cuando una actualización del cargador de malware eliminó por completo el código de valor de registro vulnerable.

> *«El 17 de julio de 2020, Emotet finalmente volvió a enviar spam luego de un período de desarrollo de varios meses. Con EmoCrash todavía activo al comienzo de su regreso completo, hasta el 6 de agosto, EmoCrash pudo brindar protección total contra Emotet»,* dijo Quinn.