Ha surgido una nueva campaña de correo electrónico no deseado como un conducto para un cargador de malware previamente indocumentado, que permite a los atacantes obtener un punto de apoyo inicial en las redes empresariales y lanzar cargas útiles maliciosas en los sistemas comprometidos.

> *«Estas infecciones también se utilizan para facilitar la entrega de malware adicional como Quakbot y Cobalt Strike, dos de las amenazas más comunes que se observan regularmente en organizaciones de todo el mundo»*, dijeron los investigadores de Cisco Talos.

Se cree que la campaña de malspam comenzó a mediados de septiembre de 2021 a través de documentos de Microsoft Office enlazados, que cuando se abren, ejecutan una cadena de infección que lleva a que las máquinas se infecten con un malware denominado SQUIRRELWAFFLE.

Reflejando una técnica que es consistente con otros ataques de phishing de este tipo, la última operación aprovecha los hilos de correo electrónico robados para darle un velo de legitimidad y engañar a los usuarios desprevenidos para que abran los archivos adjuntos.

Además, el idioma empleado en los mensajes de respuesta coincide con el idioma utilizado en el hilo de correo electrónico original, lo que demuestra un caso de localización dinámica implementada para aumentar la probabilidad de éxito de la campaña. Los cinco idiomas principales utilizados para entregar el cargador son inglés (76%), francés (10%), alemán (7%), holandés (4%) y polaco (3%).

Los volúmenes de distribución de correo electrónico que aprovechan la nueva amenaza alcanzaron su punto máximo alrededor del 26 de septiembre, según los datos compilados por la firma de seguridad cibernética.

Aunque los servidores web previamente comprometidos, que ejecutan principalmente versiones del sistema de administración de contenido (CMS) de WordPress, funcionan como

la infraestructura de distribución de malware, una técnica interesante observada es el uso de scripts «*antibot*» para bloquear las solicitudes web que se originan en direcciones IP que no pertenecen a las víctimas, sino plataformas de análisis automatizadas y organizaciones de investigación de seguridad.

El cargador de malware, además de implementar Quakbot y la infame herramienta de prueba de penetración Cobalt Strike en los puntos finales infectados, también establece comunicaciones con un servidor remoto controlado por un atacante para recuperar cargas útiles secundarias, lo que la convierte en una potente utilidad multipropósito.

> *«Después de la eliminación de la botnet Emotet a inicios del año, los actores de amenazas criminales están llenando ese vacío. SQUIRRELWAFFLE parece ser un nuevo cargador que se aprovecha de esta brecha. Aún no está claro si SQUIRRELWAFFLE es desarrollado y distribuido por un actor de amenazas conocido o un nuevo grupo. Sin embargo, Emotet utilizó anteriormente técnicas de distribución similares»,* dijo Zscaler.