Investigadores de seguridad cibernética detallaron este martes un ataque de correo electrónico masivo organizado por un grupo de hackers, que afecta a una amplia gama de industrias, con una de sus operaciones específicas de la región dirigida principalmente a Alemania y Austria.

La compañía de seguridad empresarial Proofpoint, vinculó la campaña de malware con gran confianza a TA505, que es el nombre asignado al grupo de amenazas con motivaciones financieras que ha estado activo en el negocio del ciberdelito desde al menos 2014, y está detrás del troyano bancario Dridex y un arsenal de otras herramientas maliciosas como FlawedAmmyy, FlawedGrace, la botnet Neutrino y el ransomware Locky, entre otras.

La empresa de seguridad cibernética Morphisec Labs, está rastreando la misma cadena de ataques bajo el nombre independiente de MirrorBlast.

Se cree que los ataques comenzaron como una serie de oleadas de correo electrónico de bajo volumen, entregando solo varios miles de mensajes en cada fase, antes de aumentar a fines de septiembre y tan recientemente como el 13 de octubre, lo que resultó en decenas a cientos de miles de correos electrónicos.

> *«Muchas de las campañas, especialmente las de gran volumen, se parecen mucho a la actividad histórica de TA505 de 2019 y 2020. Los puntos en común incluyen convenciones de nombres de dominio similares, señuelos de correo electrónico, señuelos de archivos de Excel y la entrega del troyano de acceso remoto FlawedGrace»,* dijeron los investigadores.

El grupo cuenta con una pista de registro de golpear a los institutos de investigación, bancos, comercios minoristas, empresas de energía, instituciones sanitarias, líneas aéreas y agencias gubernamentales, con las actividades maliciosas normalmente comenzando a partir de los archivos adjuntos con malware y cordones de apertura en los mensajes de phishing presuntamente estando relacionado con actualización de COVID-19, reclamos de seguros o notificaciones sobre archivos compartidos de Microsoft OneDrive.

> *«Con el tiempo, TA505 evolucionó de un socio menor a una operación criminal madura, autosuficiente y versátil con un amplio espectro de objetivos. A lo largo de los años, el grupo se basó en gran medida en terceros servicios de fiestas y herramientas para respaldar sus actividades fraudulentas, sin embargo, el grupo ahora opera principalmente de forma independiente desde la infección inicial hasta la monetización»*, dijo NCC Group.

Sin embargo, el éxito de la última campaña depende de que los usuarios habiliten las macros después de abrir archivos adjuntos maliciosos de Excel, después de que se descargue un archivo MSI ofuscado para buscar los cargadores de la siguiente etapa antes de la entrega de una versión actualizada de FlawedGrace RAT, que incorpora soporte para cadenas encriptadas y llamadas API ofuscadas.

FlawedGrace, observado por primera vez en noviembre de 2017, es un troyano de acceso remoto con todas las funciones escrito en C++, que está diseñado deliberadamente para frustrar la ingeniería inversa y el análisis. Cuenta con una lista de capacidades que le permiten establecer comunicaciones con un servidor de comando y control para recibir instrucciones y exfiltrar los resultados de esos comandos al servidor.

La ola de ataques de octubre del actor también es significativa por su cambio de táctica, que incluye el uso de cargadores intermedios rediseñados con secuencias de comandos en lenguajes de programación inusuales como Rebol y KiXtart en lugar de Get2, un descargador previamente implementado por el grupo para realizar reconocimiento, y descargar e instalar cargas útiles RAT de etapa final.

> *«TA505 es un actor de amenazas establecido que está motivado financieramente y es conocido por realizar campañas de correo electrónico malicioso en una escala sin precedentes. El grupo cambia regularmente sus TTP y son considerados pioneros en el mundo del ciberdelito. Este actor de amenazas no limita su conjunto de objetivos y, de hecho, es un oportunista igual a las geografías y verticales que elige atacar»*, dijo Proofpoint.

> *«Esto combinado con la capacidad de TA505 para ser flexible, enfocándose en lo que es más lucrativo y cambiando sus TTP según sea necesario, hace que el actor sea una amenaza continua»*, agregaron los investigadores.