ACADEMIA DE GUERRA AÉREA
DEPARTAMENTO DE INVESTIGACIÓN Y EXTENSIÓN

Informativo Semanal *Año VIII, Nº 4, jueves 24 de enero de 2019*

Grupo de ciberespionaje *ejecuta ataques a nivel mundial*

Los investigadores de la empresa de la seguridad informática Symantec revelaron durante diciembre pasado información relativa al grupo de espionaje cibernético que está detrás de una serie de recientes ataques contra múltiples entidades principalmente de Oriente Medio, pero también de Europa y América del Norte.

El grupo, bautizado como Seedworm, y también conocido como Muddy-Water, viene operando desde al menos 2017. Los investigadores aseguran que desde finales de septiembre de este año, los *hackers* se han infiltrado en más de 30 organizaciones, incluidas agencias gubernamentales, empresas petroleras y de gas, organizaciones no gubernamentales, y compañías informáticas y de telecomunicaciones.

La intensificada actividad informática maliciosa del grupo ha sido dirigida contra objetivos basados principalmente en Pakistán y Turquía, pero también en Arabia Saudita, Rusia, Afganistán y Jordania. Empresas con sede en Europa y EE.UU. con vínculos con Oriente Medio también se vieron afectadas.

Los investigadores de Symantec describieron a Seedworm como un grupo sofisticado que cambia continuamente sus tácticas, lo que dificulta que sea rastreado.

OBJETIVOS DE LOS ATAQUES

De acuerdo con la empresa de seguridad informática, Seedworm utiliza (y continúa actualizando) una herramienta personalizada conocida como Powermud. Se trata de una *backdoor* ("puerta trasera", en español), un especial código de programación, que permite evadir la detección en los sistemas de seguridad de las entidades que *hackean*. Seedworm es el único grupo conocido que usa esta 'puerta trasera'.

Según los investigadores, después de comprometer un sistema con Powermud, Seedworm instala una herramienta que roba contraseñas guardadas en los navegadores web y los correos electrónicos de los usuarios. Esto demuestra, según el reporte de Symantec, que el acceso al correo electrónico, a las redes sociales y a las cuentas de chat de la víctima es "uno de los objetivos probables" del grupo.

Las motivaciones de Seedworm son muy parecidas a las de numerosos grupos de espionaje cibernético: buscan obtener información procesable sobre las organizaciones y los individuos seleccionados. Además, es probable que opere para asegurar inteligencia procesable que pueda beneficiar los intereses de su patrocinador, según reseña el reporte.

Fuentes:
https://actualidad.rt.com
https://www.itdigitalsecurity.es