Kaspersky: así espían los países

El último informe publicado por **Kaspersky Lab,** la firma de seguridad nacida en Rusia, asegura que Estados-nación están respaldando a agentes de amenazas para hackear a otros grupos para robar datos de las víctimas, tomar prestadas herramientas y técnicas, y reutilizar entre ellos su infraestructura, dificultando a los investigadores de seguridad la obtención de inteligencia para combatir estas amenazas, según el **Equipo Global de Investigación y Análisis** de la firma.

Kaspersky Lab cree que **tales ataques posiblemente sean implementados principalmente por grupos respaldados por estados-nación,** y dirigidos a agentes extranjeros o menos competentes. Es importante que los investigadores de seguridad de TI aprendan a detectar e interpretar los signos de estos ataques, para que puedan presentar su inteligencia en su contexto, dice el estudio.

Hay dos estrategias principales, según los expertos: ataques pasivos implican interceptar los datos en tránsito de otros grupos, por ejemplo, cuando se mueven entre las víctimas y los servidores de mando y control, estos son casi imposibles de detectar. El enfoque activo implica infiltrarse en la infraestructura maliciosa de otro agente de amenazas.

El equipo ha encontrado una serie de artefactos extraños e inesperados al investigar a agentes de amenaza específicos que sugieren que estos ataques activos ya están ocurriendo públicamente como **backdoors** o puertas traseras instaladas en la infraestructura de control y mando (C&C) de otra entidad

Uno de ellos fue encontrado en 2013, cuando se analizaba un servidor utilizado por NetTraveler, una campaña en idioma chino dirigida a activistas y organizaciones en Asia. La segunda fue encontrada en 2014, cuando se investigaba un sitio web hackeado y usado por Crouching Yeti (también conocido como Energetic Bear), un agente de amenazas en idioma ruso que ataca al

sector industrial desde 2010. Los investigadores notaron que, durante un breve período de tiempo, el panel de administración de la red C&C fue modificado con una etiqueta que apuntaba a una dirección IP remota en China (probablemente una señal falsa).

Algunos agentes de amenazas, más que robarlas, comparten víctimas. Este es un enfoque arriesgado si uno de los grupos es menos avanzado y lo descubren, ya que el inevitable análisis forense que sigue también revelará a los otros intrusos. En noviembre de 2014, Kaspersky Lab informó que un servidor perteneciente a una institución de investigación en Medio Oriente, conocido como el Magnet of Threats**, alojó simultáneamente implantes para los agentes de amenazas altamente avanzados Regin y Equation Group (de idioma inglés)**, Turla e ItaDuke (en ruso), así como Animal Farm (en francés) y Careto (en español). De hecho, este servidor fue el punto de partida para el descubrimiento del Equation Group.