Qihoo 360, una de las compañías de seguridad cibernética más destacadas, publicó hoy un nuevo informe acusando a la Agencia Central de Inteligencia de Estados Unidos (CIA), de estar detrás de una campaña de piratería de 11 años contra distintas industrias y agencias gubernamentales chinas.

Los sectores industriales específicos incluyen organizaciones de aviación, instituciones de investigación científica, compañías de petróleo e Internet, lo que de ser cierto, brinda a la CIA la capacidad de realizas *«cosas inesperadas».*

Según los investigadores, estos ataques cibernéticos se han llevado a cabo entre septiembre de 2008 y junio de 2019, y la mayoría de los objetivos se ubicaron en Beijing, Guangdong y Zhejiang.

> *«Especulamos que en los últimos once años de ataques de infiltración, la CIA puede haber captado la información comercial más clasificada de China, incluso de muchos otros países del mundo»*, dijeron los investigadores.
>
> *«Ni siquiera descarta la posibilidad de que ahora la CIA pueda rastrear el estado del vuelo global en tiempo real, la información del pasajero, la carga comercial y otra información relacionada».*

Las afirmaciones de la compañía de seguridad se basan en la conexión evidencial entre herramientas, tácticas y procedimientos utilizados por un grupo de hackers, denominado «APT-C-39», contra las industrias chinas, y las herramientas de piratería Vault 7, desarrolladas por la CIA.

La colección masiva de herramientas de piratería Vault 7, se filtró públicamente en 2017 por el sitio web WikiLeaks, que recibió la información de Joshua Adam Schulte, un ex empleado de la CIA que actualmente enfrenta cargos por filtrar información clasificada.

Qihoo 360 asegura que las herramientas de piratería desarrolladas por la CIA, como Fluxwire y Grasshopper, fueron utilizadas por el grupo APT-C-39 contra objetivos chinos algunos años antes de la fuga de información.

> *«Al comparar códigos de muestra relevantes, huellas dactilares de comportamiento y otra información, Qihoo 360 puede estar seguro de que el arma cibernética utilizada por el grupo es el arma cibernética descrita en las filtraciones de Vault 7»*, dijeron los investigadores.
>
> *«El análisis de Qihoo 360 encontró que los detalles técnicos de la mayoría de las muestras son consistentes con los del documento de Vault 7, como los comandos de control, compilación de rutas PDB, esquemas de cifrado»,* agregaron.

Además, los investigadores encontraron que el tiempo de compilación de las muestras capturadas es consistente con la zona horaria de Estados Unidos.

> *«Mediante el estudio del tiempo de compilación del malware, podemos averiguar el cronograma de trabajo del desarrollador, con el fin de conocer la zona horaria aproximada de su ubicación»,* agregaron los investigadores.

La compañía también dijo que el grupo de hackers utilizó algunas herramientas, como el complemento de ataque WISTFULTOOL, desarrollado por la Agencia de Seguridad Nacional (NSA), en sus campañas de piratería, incluso contra una gran compañía china de Internet en 2011.