Alertan de un virus “indetectable” que controla ya 100.000 ordenadores

El malware llamado Ramnit ha infectado a miles de dispositivos sin que los antivirus pudieran detectarlo.

Al comprar un nuevo ordenador, antes de ponerte a descargar programas y aplicaciones como si no hubiese un mañana, debes extremar las medidas de seguridad. Por lo tanto, es imprescindible tener activado un antivirus. Sin embargo, hay que tener en cuenta qué tipo de antivirus es y cuánto protege realmente. Porque algunos actúan solamente cuando entras en webs de dudoso prestigio o pinchas en los enlaces de emails de desconocidos. Pero hay algunos malware que no son detectados fácilmente.

Así, expertos y analistas en ciberseguridad han detectado una

nueva campaña masiva del malware llamado Ramnit que pasa desapercibido y, por tanto, no suele detectarse mediante antivirus. Este troyano fue detectado por primera vez en 2011 y afecta a sistemas operativos Windows.

Según informa Check Point, una compañía de soluciones de seguridad, entre mayo y julio ha llegado a infectar ya a más de 100.000 ordenadores. Se trata de una nueva configuración que ha estado activa desde el 6 de marzo de 2018, la cual no ha llamado la atención hasta el momento que se ha lanzado la advertencia.

Actividades criminales

Por otro lado, hay constancia de que Ramnit se ha utilizado desde 2011 para llevar a cabo actividades criminales. Entre ellas, se encuentra la monitorización de la navegación web del sistema infectado, y la detección de la visita de sitios de banca online y la manipulación de webs de banca online con el objetivo de parecer legítimas.

Aunque también se dedica a robar cookies de sesión de los navegadores web para poder suplantar a la víctima en sitios seguros, al escaneo de discos duros del ordenador, robar archivos en base a palabras clave o contraseñas y recopilación de las credenciales de acceso de clientes FTP.

Según Check Point, el malware hace que los equipos que están infectados operen como una botnet altamente centralizada. Asimismo, el virus crea una cadena de procesos para inyectar su código en los dispositivos objetivo. En primer lugar, inyecta el código en el proceso recién creado usando una técnica de vaciado de procesos. Tras ello, el malware recurre a una aplicación predeterminada para abrir archivos con la extensión .html y a partir de ese momento realiza las principales acciones.

Fuente: losreplicantes.