Un actor de amenazas de habla china desconocido hasta ahora, ha sido vinculado a una operación evasiva de larga duración dirigida a objetivos del sudeste asiático desde julio de 2020, con el fin de implementar un rootkit en modo kernel en sistemas Windows comprometidos.

También se dice que los ataques montados por el grupo de hacking apodado como GhostEmperor por Kaspersky, ha utilizado un *«marco de malware sofisticado de múltiples etapas»* que permite proporcionar persistencia y control remoto sobre los hosts objetivo.

La compañía rusa de seguridad cibernética nombró al rootkit como Demodex, con infecciones reportadas en varias entidades de alto perfil en Malasia, Tailandia, Vietnam e Indonesia, además de valores atípicos ubicados en Egipto, Etiopía y Afganistán.

> *«Demodex se utiliza para ocultar los artefactos del malware en modo de usuario de los investigadores y las soluciones de seguridad, al tiempo que demuestran un interesante esquema de carga sin documentar que involucra el componente de modo kernel de un proyecto de código abierto llamado Cheat Engine para eludir el mecanismo de ejecución de la firma del controlador de Windows»,* dijeron los investigadores de Kaspersky.

Se ha descubierto que las infecciones de GhostEmperor aprovechan múltiples rutas de intrusión que culminan en la ejecución de malware en la memoria, siendo la principal de ellas la explotación de vulnerabilidades conocidas en servidores públicos como Apache, Windows IIS, Oracle y Microsoft Exchange, incluidos los exploits de ProxyLogon que salió a la luz en marzo de 2021, para ganar un punto de apoyo inicial y pivotar lateralmente a otras partes de la red de la víctima, incluso en máquinas que ejecutan versiones recientes del sistema operativo Windows 10.

Luego de una violación exitosa, las cadenas de infección seleccionadas que dieron como resultado la implementación del rootkit se llevaron a cabo de forma remota a través de otro sistema en la misma red utilizando software legítimo como WMI o PsExec, lo que llevó a la ejecución de un implante en memoria capaz de instalar más cargas útiles durante el tiempo de ejecución.

A pesar de su dependencia de la ofuscación y otros métodos de detección y evasión para eludir el descubrimiento y el análisis, Demodex evita el mecanismo de aplicación de la firma del controlador de Microsoft para permitir la ejecución de código arbitrario sin firmar en el espacio del kernel al aprovechar un controlador firmado legítimo y de código abierto llamado «dbk64.sys», que se envía junto con Cheat Engine, una aplicación utilizada para introducir trampas en los videojuegos.

> *«Con una operación de larga duración, víctimas de alto perfil y un conjunto de herramientas avanzadas, el actor subyacente es altamente calificado y hábil en su oficio, los cuales son evidentes a través del uso de un amplio conjunto de anti-sofisticadas e inusuales técnicas forenses y anti-análisis»,* dijeron los investigadores.

La revelación surge como un actor de amenaza vinculada en China con el nombre en código TAG-28, que se ha descubierto detrás de las intrusiones contra medios de comunicación indios y agencias gubernamentales, como el Times Group, la Autoridad de Identificación Única de la India (UIDAI), y el departamento de policía del estado de Madhya Pradesh.

Recorded Future, a inicios de la semana, también descubrió actividad maliciosa dirigida a un servidor de correo de Roshan, uno de los proveedores de telecomunicaciones más grandes de Afganistán, que atribuyó a cuatro actores distintos patrocinados por el estado chino: RedFoxtrot, Calypso APT, así como a dos clústeres separados que utilizan puertas traseras asociados con los grupos Winnti y PlugX.