Un grupo de hackers conocido por sus ataques de abrevadero contra entidades gubernamentales, se relacionó con una serie de intrusiones recientemente detectadas dirigidas a varias organizaciones en Asia Central y Medio Oriente.

La actividad maliciosa, denominada de forma colectiva como *EmissarySoldier,* se ha atribuido a un actor de amenazas llamado LuckyMouse, y se dice que ocurrió en 2020 con el objetivo de obtener información geopolítica en la región.

Los ataques involucraron la implementación de un conjunto de herramientas denominadas SysUpdate, también conocido como Soldier, en varias organizaciones violadas, incluidas agencias gubernamentales y diplomáticas, proveedores de telecomunicaciones, una empresa de medios de televisión y un banco comercial.

Lucky Mouse, también conocido como APT27 y Emissary Panda, es un grupo sofisticado de ciberespionaje que cuenta con un historial de violación de múltiples redes gubernamentales en Asia Central y Medio Oriente. El grupo también ha sido vinculado a ataques cibernéticos dirigidos a organizaciones transnacionales como la Organización de Aviación Civil Internacional (OACI) en 2019 y recientemente llamó la atención por explotar fallas de ProxyLogon para comprometer el servidor de correo electrónico de una entidad gubernamental en el Medio Oriente.

EmissarySoldier es solo el último de una serie de esfuerzos de vigilancia dirigidos a los objetivos.

> *«Con el fin de comprometer a las víctimas, LuckyMouse normalmente utiliza abrevaderos, comprometiendo los sitios web que probablemente sean visitados por sus objetivos previstos. Los operadores de LuckyMouse también realizan análisis de red para encontrar servidores vulnerables conectados a Internet dirigidos por sus víctimas previstas»,* dijo Matthieu Faou, investigador de malware de ESET.

Además, ESET también encontró algunos sistemas infectados con acceso a Internet que

ejecutan Microsoft Share Point, lo que los investigadores sospechan que ocurrió al aprovechar las vulnerabilidades de ejecución remota de código en la aplicación.

Independientemente del método utilizado para lograr un punto de apoyo inicial, la cadena de ataque culmina con la implementación de implantes personalizados posteriores al compromiso, SysUpdate o HyperBro, los cuales aprovechan el secuestro de órdenes de búsqueda de DLL para cargar cargas útiles maliciosas y frustrar la detección.

> *«El modelo tridente presenta una aplicación legítima vulnerable al secuestro de DLL, una DLL personalizada que carga la carga útil y una carga útil binaria sin procesar codificada con Shikata Ga Nai»,* dijo Faou.

Por su parte, SysUpdate funciona como una herramienta modular, con cada componente dedicado a un propósito operativo particular. Implica abusar de una aplicación benigna como cargador de una DLL maliciosa, que a su vez carga la carga útil de la primera etapa que finalmente decodifica y carga el implante de memoria en el sistema comprometido.

Desde su descubrimiento en 2018, el conjunto de herramientas ha sido objeto de numerosas revisiones dedicadas a agregar nuevas funcionalidades, lo que indica que los operadores están trabajando activamente para renovar su arsenal de malware.

> *«LuckyMouse estuvo cada vez más activo a lo largo de 2020, aparentemente atravesando un proceso de reestructuración en el que varias funciones se integraron gradualmente en el kit de herramientas SysUpdate. Esto puede ser un indicador de que los actores de amenazas detrás de LuckyMouse están cambiando gradualmente del uso de HyperBro a SysUpdate»,* dijo Faou.