Un nuevo grupo de atacantes persistente y altamente capaz ha estado apuntando a las principales entidades públicas y privadas de alto perfil en Estados Unidos, como parte de una serie de ataques de intrusión cibernética dirigidos mediante la explotación de servidores de Microsoft Internet Information Services (IIS) orientados a Internet para infiltrarse en sus redes.

La compañía israelí de seguridad cibernética Sygnia, que identificó la campaña, está rastreando al avanzado y sigiloso adversario bajo el sobrenombre de *«Mantis Religiosa» o «TG1021»*.

> *«TG1021 utiliza un marco de malware personalizado, construido alrededor de un núcleo común, hecho a la medida para los servidores IIS. El conjunto de herramientas es completamente volátil, se carga de forma reflectante en la memoria de una máquina afectada y deja poco o ningún rastro en los objetivos infectados. El actor de amenazas también utiliza una puerta trasera sigilosa adicional y varios módulos posteriores a la explotación para realizar el reconocimiento de la red, elevar los privilegios y moverse lateralmente dentro de las redes»*, dijeron los investigadores.

Además de exhibir capacidades que muestran un esfuerzo significativo para evitar la detección al interferir activamente con los mecanismos de registro y evadir con éxito los sistemas comerciales de detección y respuesta de puntos finales (EDR), se sabe que el actor de amenazas aprovecha un conjunto de exploits de aplicaciones web ASP.NET para obtener ventaja y un punto de apoyo inicial, además de una puerta trasera de los servidores mediante la ejecución de un implante sofisticado llamado «NodeIISWeb», que está diseñado para cargar archivos DLL personalizados, así como para interceptar y manejar las solicitudes HTTP recibidas por el servidor.

Las vulnerabilidades que aprovechan los atacantes incluyen:

- Exploit de RCE de encuesta de casilla de verificación (CVE-2021-27852)

- Explotación de deserialización VIEWSTATE
- Altserialización Deserialización insegura
- Exploit de Telerik-UI (CVE-2019-18935 y CVE-2017-11317)

La investigación de Sygnia acerca de las tácticas, técnicas y procedimientos (TTP) de TG1021, descubrió *«superposiciones importantes»* con las de un actor patrocinado por la nación llamado *«Compromisos de copiar y pegar»,* como se detalla en un aviso publicado por el Centro Australiano de Seguridad Cibernética (ACSC) en junio de 2020, que describió una campaña cibernética dirigida a la infraestructura de cara al público principalmente a través del uso de fallas sin parches en los servidores IIS y UI de Telerik. Sin embargo, todavía no se ha realizado una atribución formal.

> *«Praying Mantis, que se ha observado apuntando a entidades públicas y privadas de alto perfil en dos mercados occidentales importantes, ejemplifica una tendencia creciente de ciberdelincuentes que utilizan métodos de ataques sofisticados de estado-nación para atacar organizaciones comerciales. Las actividades forenses continuas y la respuesta oportuna a incidentes son esenciales para identificar y defender eficazmente las redes de ataques de actores de amenazas similares»,* dijeron los investigadores.