Investigadores de Seguridad Cibernética encontraron por primera vez, una posible conexión entre la backdoor utilizada en el hackeo de SolarWinds y una cepa de malware previamente conocida.

En una nueva investigación publicada este lunes por investigadores de Kaspersky, la compañía de seguridad dijo que descubrió varias características que se superponen con otra puerta trasera conocida como Kazuar, un malware basado en .NET documentado por primera vez por Palo Alto Networks en 2017.

Revelada a inicios de diciembre, la campaña de espionaje se destacó por su escala y sigilo, y los atacantes aprovecharon la confianza asociada con el software SolarWinds Orion para infiltrarse en agencias gubernamentales y otras compañías a fin de implementar un malware personalizado con nombre en código *«Sunburst»*.

Funciones compartidas entre Sunburst y Kazuar

La atribución del compromiso de la cadena de suministro de SolarWinds ha sido difícil en parte debido a la poca o nula pista que vincula la infraestructura de ataque con campañas anteriores u otros grupos de amenazas conocidos.

El último análisis de Kaspersky sobre la puerta trasera Sunburst, reveló una serie de características compartidas entre el malware y Kazuar, lo que lleva a sospechar que:

- Tanto Sunburst como Kazuar fueron desarrollados por el mismo grupo de amenazas.
- El adversario detrás de Sunburst utilizó Kazuar como inspiración.
- Los grupos detrás de Kazuar (Turla) y Sunburst (UNC2452 o Dark Halo) obtuvieron el malware de una sola fuente.
- Los desarrolladores de Kazuar se trasladaron a otro equipo, llevándose su conjunto de herramientas con ellos.
- Los desarrolladores de Sunburst introdujeron deliberadamente estos enlaces como *«bandera falsa»* para culpar a otro grupo.

Los puntos en común compartidos entre las dos familias de malware incluyen el uso de un algoritmo de suspensión para permanecer inactivo por un período aleatorio entre las conexiones a un servidor C2, el uso extensivo del hash FNV-1a para ofuscar el código malicioso y el uso de un algoritmo hash para generar identificadores únicos de víctimas.

Mientras que Kazuar selecciona al azar un período de reposo entre dos y cuatro semanas entre las conexiones C2, Sunburst opta al azar por un período de reposo entre 12 y 14 días antes de contactar al servidor para el reconocimiento inicial. Pero los investigadores notaron que la fórmula utilizada para el cálculo del tiempo de espera sigue siendo la misma.

Vínculos de Kazuar con Turla

Kazuar es una backdoor con todas las funciones desarrollada en .NET Framework y se basa en un canal de comando y control (C2) para permitir que los actores interactúen con el sistema comprometido y exfiltren datos.

Sus características abarcan la gama típica de software espía, con soporte para ejecutar comandos maliciosos, capturar pantalla e incluso, implementar funcionalidades adicionales a través de un comando complementario.

El equipo de la Unidad 42 de Palo Alto Networks, vinculó tentativamente la herramienta al grupo de amenazas ruso Turla, también conocido como Uroburos o Snake, basándose en el hecho de que *«el linaje del código en Kazuar se remonta al menos a 2005».*

Además, el 18 de noviembre de 2020, Kazuar parece haberse sometido a un rediseño completo con un nuevo registrador de teclas y funciones de robo de contraseñas agregadas a la puerta trasera que se implementa en forma de comando del servidor C2.

Aunque es normal que los actores de amenazas sigan utilizando su conjunto de herramientas

e introduzcan funciones diseñadas para evitar los sistemas de detección y respuesta de puntos finales (EDR), los investigadores de Kaspersky plantearon la posibilidad de que los cambios se hayan introducido en respuesta a la violación de SolarWinds.

> *«Ante la sospecha de que podría descubrirse el ataque SolarWinds, el código de Kazuar se cambió para parecerse lo menos posible a la backdoor Sunburst»,* dijeron los investigadores.

CISA actualiza su aviso sobre SolarWinds

La semana pasada, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), junto con la Oficina Federal de Investigaciones (FBI), la Oficina del Director de Inteligencia Nacional (ODNI) y la Agencia de Seguridad Nacional (NSA), emitieron un comunicado conjunto en el que acusan formalmente a un adversario *«probablemente de origen ruso»* por organizar el ataque a SolarWinds.

En una actualización del 6 de enero, CISA menciona en su aviso que *«las investigaciones de respuesta a incidentes han identificado que el acceso inicial en algunos casos se obtuvo adivinando contraseñas, rociando contraseñas y credenciales administrativas inapropiadamente protegidas accesibles a través de servicios externos de acceso remoto».*

> *«Estas superposiciones de código entre Kazuar y Sunburst son interesantes y representan el primer vínculo potencial identificado a una familia de malware conocida anteriormente»,* dijeron los investigadores.
>
> *«Si bien Kazuar y Sunburst pueden estar relacionados, la naturaleza de esta relación aún no es clara. A través de un análisis más detallado, es posible que surjan pruebas que confirme uno o varios de estos puntos. Al mismo tiempo, también es posible que los desarrolladores de Sunburst fueron realmente buenos en*

> *su operación y no cometieron error alguno, siendo este enlace una falsa bandera elaborada»,* agregaron.