Kaspersky publicó una investigación este miércoles, en la que afirma que un grupo chino de amenazas ha desarrollado nuevas capacidades para apuntar a sistemas con espacios de aire en un intento de filtrar datos sensibles para espionaje.

La APT, conocida como Cycldek, Goblin Panda o Conimes, emplea un extenso conjunto de herramientas para el movimiento lateral y robo de información en las redes de víctimas, que incluyen herramientas personalizadas, tácticas y procedimientos previamente no reportados en ataques contra agencias gubernamentales en Vietnam, Tailandia y Laos.

> *«Una de las herramientas recientemente reveladas se llama USBCulprit, y se encontró que depende de los medios USB para filtrar los datos de las víctimas. Esto puede sugerir que Cycldek está tratando de llegar a redes con espacios de aire en entornos de víctimas o depende de la presencia física para el mismo propósito»,* dijo Kaspersky.

Observado por primera vez por CrowdStrike en 2013, Cycldek tiene una larga historia señalando los sectores de defensa, energía y gobierno en el sudeste asiático, particularmente Vietnam, utilizando documentos señuelo que explotan vulnerabilidades conocidas (como CVE-2012-0158, CVE-2017-11882, CVE-2018-0802) en Microsoft Office para colocar un malware llamado NewCore RAT.

El análisis de Kaspersky de NewCore reveló dos variantes diferentes, denominadas BlueCore y RedCore, centradas alrededor de dos grupos de actividad, con similitudes tanto en código como en infraestructura, pero también contienen características que son exclusivas de RedCore, es decir, un keylogger y un registrador RDP que captura detalles acerca de usuarios conectados a un sistema por medio de RDP.

> *«Cada grupo de actividad tenía un enfoque geográfico diferente. Los operadores detrás del clúster BlueCore invirtieron la mayor parte de sus esfuerzos en objetivos vietnamitas con varios valores atípicos en Laos y Tailandia, mientras que los*

> *operadores del clúster RedCore comenzaron con un enfoque en Vietnam y se desviaron a Laos a fines de 2018»*, agregaron los investigadores.

Los implantes BlueCore y Redcore descargaron una variedad de herramientas adicionales para facilitar el movimiento lateral (HDoor) y extraer información (JsonCookies y ChromePass) de los sistemas comprometidos.

El principal de ellos es un malware llamado USBCulprit, que es capaz de escanear una serie de rutas, recopilar documentos con extensiones específicas (.pdf, .doc, .wps, .docx, .ppt, .xls, .xlsx, .pptx, .rtf) y exportarlos a una unidad USB conectada.

Además, el malware está programado para copiarse de forma selectiva en ciertas unidades extraíbles para que pueda moverse lateralmente a otros sistemas con espacio de aire cada vez que se inserta una unidad USB infectada en otra máquina.

Un análisis de telemetría de Kaspersky descubrió que la primera instancia del binario data de 2014, con las últimas muestras registradas a finales de 2019.

El mecanismo de infección inicial se basa en el aprovechamiento de binarios maliciosos que imitan componentes antivirus legítimos para cargar USBCulprit en lo que se denomina secuestro de órdenes de búsqueda de DLL, antes de proceder a la recopilación de información relevante, guardarla en forma de un archivo RAR cifrado y filtrar los datos a un dispositivo extraíble conectado.

> *«Las características del malware pueden dar lugar a varias suposiciones sobre su propósito y casos de uso, uno de los cuales es alcanzar y obtener los datos de máquinas con espacios de aire. Esto explicaría la falta de comunicación de red en el malware y el uso de solo medios extraíbles como forma de transferir datos entrantes y salientes».*

En última instancia, las similitudes y diferencias entre las dos piezas de malware son indicativas del hecho de que los actores detrás de los clústeres comparten código e infraestructura, mientras operan como dos ramificaciones distintas en una sola entidad más grande.

> *«Cycldek es un ejemplo de un actor que tiene una capacidad más amplia de lo que se percibe públicamente. Si bien las descripciones más conocidas de su actividad dan la impresión de un grupo marginal con capacidades inferiores, la gama de herramientas y el intervalo de tiempo de las operaciones muestran que el grupo tiene un amplio punto de apoyo dentro de las redes de objetivos de alto perfil en el sudeste asiático»,* concluyó Kaspersky.