Los agentes de amenazas provenientes de Corea del Norte han aprovechado las recientes vulnerabilidades de seguridad descubiertas en ConnectWise ScreenConnect para implementar un nuevo tipo de malware denominado TODDLERSHARK.

Según un informe compartido por Kroll con Masterhacks, TODDLERSHARK comparte similitudes con malware conocido de Kimsuky, como BabyShark y ReconShark.

> *«El actor de amenazas logró acceder a la estación de trabajo de la víctima al explotar el asistente de configuración expuesto de la aplicación ScreenConnect»*, indicaron los investigadores de seguridad Keith Wojcieszek, George Glass y Dave Truman.
>
> *«Aprovecharon su acceso 'manos en el teclado' para utilizar cmd.exe y ejecutar mshta.exe con una URL que direcciona al malware basado en Visual Basic (VB).»*

Las vulnerabilidades específicas de ConnectWise son CVE-2024-1708 y CVE-2024-1709, que salieron a la luz el mes pasado y han sido ampliamente explotadas desde entonces por diversos actores de amenazas con el fin de distribuir mineros de criptomonedas, ransomware, troyanos de acceso remoto y malware robador.

Kimsuky, también conocido como APT43, ARCHIPELAGO, Black Banshee, Emerald Sleet (anteriormente Thallium), KTA082, Nickel Kimball y Velvet Chollima, ha ido incrementando constantemente su arsenal de malware con nuevas herramientas, siendo las más recientes GoBear y Troll Stealer.

BabyShark, descubierto por primera vez a finales de 2018, se ejecuta mediante un archivo de Aplicación HTML (HTA). Una vez activado, el malware de script VB extrae información del sistema a un servidor de control y comando (C2), mantiene la persistencia en el sistema y espera más instrucciones del operador.

Luego, en mayo de 2023, se observó que una variante de BabyShark llamada ReconShark se entregaba a individuos específicamente seleccionados a través de correos electrónicos de spear-phishing. Se estima que TODDLERSHARK representa la última evolución del mismo malware debido a similitudes en el código y comportamiento.

Este malware, además de emplear una tarea programada para persistir, está diseñado para capturar y extraer información sensible sobre los hosts comprometidos, convirtiéndose así en una herramienta valiosa para el reconocimiento.

> TODDLERSHARK *«presenta elementos de comportamiento polimórfico mediante cambios en las cadenas de identidad en el código, alteraciones en la posición del código mediante la introducción de código superfluo generado y la utilización de URL de C2 generadas de manera única, lo que podría dificultar la detección de este malware en ciertos entornos»,* señalaron los investigadores.

Este desarrollo coincide con la acusación por parte del Servicio Nacional de Inteligencia de Corea del Sur (NIS) hacia su contraparte del norte, alegando que comprometieron presuntamente los servidores de dos fabricantes nacionales de semiconductores (sin especificar) y sustrajeron datos valiosos.

Las intrusiones digitales tuvieron lugar en diciembre de 2023 y febrero de 2024. Se afirma que los agentes de amenazas dirigieron su atención a servidores expuestos a Internet y vulnerables para obtener acceso inicial, utilizando posteriormente técnicas de *«living-off-the-land»* (LotL) en lugar de desplegar malware, con el objetivo de eludir de manera más efectiva la detección.

> *«Corea del Norte podría haber iniciado preparativos para su propia producción de semiconductores debido a las dificultades para adquirir estos componentes debido a las sanciones impuestas y a la creciente demanda asociada al desarrollo de armas como misiles satelitales»,* afirmó el NIS.