El grupo de amenazas persistentes avanzadas (APT) conocido como ToddyCat ha sido relacionado con un nuevo conjunto de herramientas maliciosas diseñadas para la extracción de datos, lo que proporciona una comprensión más profunda de las tácticas y capacidades de este grupo de piratas informáticos.

Los descubrimientos provienen de la empresa de ciberseguridad Kaspersky, que ya había arrojado luz sobre este adversario el año pasado, vinculándolo a ataques contra entidades de alto perfil en Europa y Asia durante casi tres años.

Aunque el arsenal de este grupo incluye prominentemente el troyano Ninja y un acceso trasero llamado Samurai, investigaciones adicionales han revelado una serie completamente nueva de software malicioso desarrollado y mantenido por este actor para lograr persistencia, llevar a cabo operaciones con archivos y cargar cargas útiles adicionales en tiempo de ejecución.

Esto incluye una serie de cargadores con la capacidad de lanzar el troyano Ninja como segunda etapa, una herramienta denominada LoFiSe para identificar y recolectar archivos de interés, un cargador de Dropbox para guardar datos robados en Dropbox y Pcexter para exfiltrar archivos de archivo a Microsoft OneDrive.

También se ha observado que ToddyCat utiliza scripts personalizados para la recopilación de datos, un acceso trasero pasivo que recibe comandos a través de paquetes UDP, Cobalt Strike para la fase posterior a la explotación y credenciales de administradores de dominio comprometidas para facilitar el movimiento lateral y llevar a cabo sus actividades de espionaje.

> *«Observamos variantes de scripts diseñadas exclusivamente para recopilar datos y copiar archivos en carpetas específicas, pero sin incluirlos en archivos comprimidos»,* destacó Kaspersky.

> *«En estos casos, el actor ejecutó el script en el host remoto utilizando la técnica estándar de ejecución de tareas remotas. Los archivos recolectados se transferían manualmente al host de exfiltración utilizando la utilidad xcopy y, finalmente, se comprimían utilizando el programa 7z».*

Esta información surge en un momento en que Check Point ha revelado que gobiernos y entidades de telecomunicaciones en Asia han sido blanco de una campaña en curso desde 2021 que utiliza una amplia variedad de malware «*desechables*» para evadir la detección y entregar malware en la siguiente etapa.

Según la empresa de ciberseguridad, esta actividad se basa en infraestructura que se superpone con la utilizada por ToddyCat.