La compañía rumana de seguridad cibernética Bitdefender ha lanzado un descifrador gratuito para una nueva variedad de ransomware conocida como MortalKombat.

MortalKombat es una nueva variedad de ransomware que surgió en enero de 2023. Se basa en un ransomware comercial denominado Xorist, y se ha observado en ataques dirigidos a entidades en Estados Unidos, Filipinas, Reino Unido y Turquía.

Xorist, detectado desde 2010, se distribuye como un generador de ransomware, lo que permite a los hackers crear y personalizar su propia versión del malware.

Esto incluye la nota de rescate, el nombre de archivo de la nota de rescate, la lista de extensiones de archivo objetivo, el fondo de pantalla que se usará y la extensión que se usará en los archivos cifrados.

Particularmente, MortalKombat se implementó en ataques recientes organizados por un actor de amenazas anónimo con motivación financiera como parte de una campaña de phishing dirigida a una amplia gama de organizaciones.

> *«MortalKombat encripta varios archivos en el sistema de archivos de la máquina de la víctima, como el sistema, la aplicación, la base de datos, la copia de seguridad y los archivos de la máquina virtual, así como los archivos en las ubicaciones remotas asignadas como unidades lógicas en la máquina de la víctima»,* dijo Cisco Talos.

Aunque el ransomware no muestra un comportamiento de limpieza ni elimina las instantáneas de volumen, corrompe el Explorador de Windows, desactiva la ventana de comandos Ejecutar y elimina todas las aplicaciones y carpetas del inicio de Windows.

También se sabe que corrompe los archivos eliminados en la carpeta Papelera de reciclaje y altera los nombres y tipos de archivos y realiza modificaciones en el Registro de Windows

para lograr la persistencia. Los hackers detrás de la campaña y su modelo operativo aún se desconocen.

> *«Basado en el ransomware Xorist, MortalKombat se propaga por medio de correos electrónicos de phishing y apunta a instancias RDP expuestas. El malware se planta a través del BAT Loader que también entrega el malware Laplas Clipper»*, dijo Bitdefender.

MortalKombat no es la única variante de Xorist, que ha surgido en el panorama de amenazas en los últimos meses. En noviembre de 2022, Fortinet FortiGuard Labs reveló otra versión que deja una nota de rescate en español.

El desarrollo también se produce poco más de un mes después de que Avast publicara un descifrador gratuito para el ransomware BianLian para ayudar a las víctimas del malware a recuperar archivos bloqueados sin tener que pagar a los atacantes.