Un nuevo tipo de ransomware llamado Big Head está siendo distribuido como parte de una campaña de malvertising que se presenta como falsas actualizaciones de Microsoft Windows e instaladores de Word.

El ransomware Big Head fue documentado por primera vez por Fortinet FortiGuard Labs el mes pasado, cuando se descubrieron múltiples variantes del ransomware diseñadas para cifrar los archivos en las máquinas de las víctimas a cambio de un pago en criptomonedas.

> *«Una variante del ransomware Big Head muestra una falsa actualización de Windows, lo que sugiere que el ransomware también fue distribuido como una actualización falsa de Windows. Una de las variantes tiene el ícono de Microsoft Word y probablemente fue distribuido como software falsificado»,* señalaron los investigadores de Fortinet en ese momento.

La mayoría de las muestras de Big Head han sido enviadas hasta ahora desde los Estados Unidos, España, Francia y Turquía.

En un nuevo análisis del ransomware basado en .NET, Trend Micro detalló su funcionamiento interno, destacando su capacidad para desplegar tres archivos binarios encriptados: 1.exe para propagar el malware, archive.exe para facilitar las comunicaciones a través de Telegram y Xarch.exe para cifrar los archivos y mostrar una falsa actualización de Windows.

«El malware muestra una interfaz falsa de actualización de Windows para engañar a la víctima y hacerle creer que la actividad maliciosa es un proceso legítimo de actualización de software, con el porcentaje de progreso aumentando en intervalos de 100 segundos», explicó la empresa de ciberseguridad.

Big Head no difiere de otras familias de ransomware en el sentido de que elimina las copias de seguridad, finaliza varios procesos y realiza verificaciones para determinar si se está ejecutando en un entorno virtualizado antes de proceder al cifrado de los archivos.

Además, el malware desactiva el Administrador de tareas para evitar que los usuarios terminen o investiguen su proceso y se detiene automáticamente si el idioma de la máquina coincide con el ruso, bielorruso, ucraniano, kazajo, kirguiso, armenio, georgiano, tártaro y uzbeco. También incorpora una función de autodestrucción para borrar su presencia.

Trend Micro informó haber detectado un segundo componente de Big Head con comportamientos tanto de ransomware como de robo de información, siendo este último el cual aprovecha el Stealer de código abierto WorldWind para recolectar el historial del navegador web, listas de directorios, procesos en ejecución, claves de producto e información de red.

También se descubrió una tercera variante de Big Head que incorpora un infectador de archivos llamado Neshta, utilizado para insertar código malicioso en ejecutables en el host infectado.

> *«La inclusión de Neshta en el despliegue del ransomware también puede servir como una técnica de camuflaje para la carga útil final del ransomware Big Head»,* indicaron los investigadores de Trend Micro.

> *«Esta técnica puede hacer que el malware parezca un tipo de amenaza diferente, como un virus, lo cual puede desviar la priorización de las soluciones de seguridad que se enfocan principalmente en la detección de ransomware».*

Actualmente, se desconoce la identidad del actor de amenazas detrás de Big Head, pero Trend Micro mencionó haber identificado un canal de YouTube con el nombre *«aplikasi premium cuma cuma»*, lo que sugiere que el adversario probablemente sea de origen

indonesio.

> *«Los equipos de seguridad deben mantenerse preparados ante las diversas funcionalidades del malware. Esta naturaleza polifacética otorga al malware el potencial de causar un daño significativo una vez que esté completamente operativo, lo que dificulta la defensa de los sistemas, ya que cada vector de ataque requiere atención individual».*