ZLoader, el malware que atacó a 2.000 víctimas en 111 países

11/01/2022

Una nueva campaña de malware que aprovecha la verificación de la firma digital de Microsoft para robar información sensible de las víctimas, fue descubierto por Check Point Research (CPR), la división de Inteligencia de Amenazas de Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder de soluciones de ciberseguridad a nivel mundial.

Llamado ZLoader, el malware es un troyano bancario que utiliza la inyección web para robar cookies, contraseñas y cualquier otro dato sensible. Anteriormente, ZLoader era conocido porque entregaba ransomware y llegó al radar de CISA en septiembre de 2021 como una amenaza en la distribución del ransomware Conti.

Durante el mismo mes, Microsoft señaló cómo los operadores de ZLoader estaban comprando anuncios de palabras clave de Google para distribuir varias cepas de malware, incluido el ransomware Ryuk. Hoy, los investigadores publican un informe que detalla el resurgimiento de ZLoader en una campaña que se ha cobrado más de 2.000 víctimas en 111 países. CPR atribuye la campaña al grupo de ciberdelincuentes MalSmoke.

La cadena de la infección

El ataque comienza con la instalación de un programa legítimo de gestión remota que se hace pasar por una instalación de Java.

Tras esta instalación, el ciberdelincuente tiene acceso completo al sistema y es capaz de cargar/descargar archivos y también ejecutar scripts, por lo que carga y ejecuta unos scripts que descargan más scripts que ejecutan mshta.exe con el archivo appContast.dll como parámetro.

El archivo appContast.dll está firmado por Microsoft, aunque se ha añadido más datos al final del archivo.

La información añadida descarga y ejecuta la carga útil final de Zloader, robando credenciales de usuario y documentación privada de las víctimas.

«La gente debe saber que no puede confiar en la firma digital de un archivo. Lo que encontramos fue una nueva campaña de ZLoader que explota la verificación de la firma digital de Microsoft para robar información sensible de los usuarios. Comenzamos a ver pruebas de esta nueva campaña alrededor de noviembre de 2021. Los atacantes, que atribuimos a MalSmoke, buscan el robo de credenciales de usuario e información privada de las víctimas. Hasta ahora, hemos contabilizado más de 2.000 víctimas en 111 países. Con todo, parece que los

autores de la campaña de Zloader consiguen evadir los sistemas de control y siguen actualizando sus métodos semanalmente. Recomendamos encarecidamente a los usuarios a que apliquen la actualización de Microsoft para la verificación estricta de Authenticode, que no se aplica por defecto", destaca Kobi Eisenkraft, Malware Researcher de Check Point Software.

Consejos de seguridad

- Aplicar la actualización de Microsoft para la verificación estricta de Authenticode. No se aplica por defecto.
- No instalar programas de fuentes o sitios desconocidos.
- No pulsar sobre enlaces ni abrir archivos adjuntos desconocidos que se reciban por correo.

Fuente: Ámbito