Instaladores falsos de herramientas de inteligencia artificial (IA) como OpenAI ChatGPT e InVideo AI están siendo utilizados como señuelo para propagar múltiples amenazas, entre ellas las familias de ransomware CyberLock y Lucky_Gh0$t, así como un nuevo malware denominado Numero.

> «El ransomware CyberLock, desarrollado en PowerShell, se enfoca principalmente en cifrar archivos específicos en el sistema de la víctima. Lucky_Gh0$t ransomware es otra variante del ransomware Yashma, que representa la sexta iteración de la serie Chaos, presentando solo ligeras modificaciones en su binario», explicó el investigador de Cisco Talos, Chetan Raghuprasad, en un informe publicado hoy.

Por otro lado, Numero es un software malicioso de carácter destructivo que afecta a las víctimas alterando los componentes de la interfaz gráfica de usuario (GUI) de Windows, dejando los equipos inutilizables.

La empresa de ciberseguridad señaló que las versiones legítimas de estas herramientas de IA son ampliamente utilizadas en ventas B2B y marketing, lo que sugiere que los delincuentes cibernéticos están dirigiendo su campaña a personas y organizaciones dentro de estos sectores.

Uno de los sitios falsos que simula ser una solución de IA es «novaleadsai[.]com», el cual aparenta ser una plataforma de monetización de prospectos llamada NovaLeads. Se sospecha que este sitio es promovido mediante técnicas de envenenamiento de SEO para mejorar artificialmente su posicionamiento en buscadores.

A los usuarios se les invita a descargar el producto ofreciendo supuestamente acceso gratuito durante el primer año, con una suscripción mensual de 95 dólares después. Sin embargo, lo que realmente se descarga es un archivo ZIP que contiene un ejecutable .NET llamado «NovaLeadsAI.exe», compilado el 2 de febrero de 2025, el mismo día en que se registró el dominio fraudulento. Este archivo actúa como un cargador que despliega el ransomware CyberLock basado en PowerShell.

El ransomware está diseñado para elevar privilegios y volver a ejecutarse con permisos de administrador si aún no los tiene, y luego cifra archivos en las particiones «C:», «D:» y «E:» que coincidan con ciertas extensiones. Posteriormente, deja una nota de rescate exigiendo un pago de $50,000 en Monero en dos billeteras distintas dentro de un plazo de tres días.

De forma llamativa, el autor del ataque afirma en la nota que los fondos serán destinados a apoyar a mujeres y niños en Palestina, Ucrania, África, Asia y otras regiones donde, según dice, *«las injusticias son una realidad diaria.»*

CATEGORY	FILE EXTENSIONS
Text Documents	.txt, .doc, .docx, .odt, .rtf, .md, .rst, .tex, .sty
Spreadsheets	.xls, .xlsx, .ods, .csv, .tsv
Presentations	.ppt, .pptx, .odp, .potx, .ppsx
PDF & eBooks	.pdf, .pdfx, .epub, .mobi, .azw, .azw3, .chm, .hlp
Images	.jpg, .jpeg, .png, .gif, .bmp, .tiff, .raw, .svg, .jfif, .ico, .webp
Audio	.mp3, .wav, .ogg, .aac, .flac, .m4a, .m4b, .caf, .mp3g
Video	.avi, .mp4, .mov, .mkv, .wmv, .webm, .3gp, .flv, .m4v, .vob, .mts, .m2ts, .ts, .mxf, .divx, .mpeg, .mpg, .ram, .rm
Archives & Disk Images	.zip, .rar, .7z, .tar, .gz, .xz, .tar.gz, .tar.bz2, .iso, .iso9660, .img, .dmg, .cdr, .zipx, .cab, .zpaq, .seam, .rar5
Executables & Scripts	.exe, .bat, .cmd, .sh, .ps1, .vbs, .js, .appx, .apk, .ipa, .deb, .rpm, .whl
Code & Programming	.html, .css, .scss, .xml, .json, .yaml, .cfg, .sql, .pl, .rb, .py, .lua, .h, .c, .cpp, .m, .swift, .java, .asm, .psm1
Database Files	.sql, .mdb, .accdb, .db, .sqlite, .sqlitedb, .db3, .sqlite3
System & Config	.log, .bak, .tmp, .swp, .ini, .plist, .xmlrpc, .dsk, .xcv
Fonts	.ttf, .otf, .woff, .woff2, .eot, .pfb
Design & Graphics	.ai, .psd, .indd, .eps, .fla, .swf
Backup & Virtual Machine	.vhd, .vmdk, .qcow2, .gho, .vpb
GIS & Maps	.gpx, .kml, .shp
Other Files	.torrent, .bup, .ifo, .bin, .dll, .msi, .sys, .qif, .pages, .key, .numbers, .rdata, .seed, .3dxml, .kdbx

> «Les pedimos que consideren que esta cantidad es pequeña en comparación con las vidas inocentes que se están perdiendo, especialmente niños que pagan el precio más alto», señala la nota. «Lamentablemente, hemos concluido que muchos no están dispuestos a ayudar de forma voluntaria, lo que hace que esta sea la única

> solución posible.»

En la etapa final del ataque, el actor malicioso utiliza la herramienta nativa de Windows «cipher.exe« con el parámetro «/w» para sobrescribir el espacio libre del disco, dificultando así la recuperación forense de archivos eliminados.

Cisco Talos también detectó a un atacante distribuyendo el ransomware Lucky_Gh0$t haciéndose pasar por un instalador de una versión premium de ChatGPT.

> «El instalador SFX malicioso incluía una carpeta con el ejecutable del ransomware Lucky_Gh0$t bajo el nombre 'dwn.exe', que imita al legítimo ejecutable de Microsoft 'dwm.exe',» dijo Raghuprasad. «La carpeta también contenía herramientas legítimas de IA de código abierto de Microsoft, disponibles en su repositorio de GitHub, pensadas para desarrolladores y científicos de datos que trabajan con IA, especialmente en el ecosistema de Azure.»

Si el usuario ejecuta el instalador SFX, el script incrustado activa el ransomware. Esta variante del ransomware Yashma, Lucky_Gh0$t, cifra archivos que tengan un tamaño inferior a 1.2 GB, pero antes elimina las copias sombra de volumen y respaldos del sistema.

Aquí tienes la traducción al español con una redacción diferente, manteniendo las citas originales intactas:

La nota de rescate que se presenta al final del ataque incluye un identificador personal único para la desencriptación y da instrucciones a las víctimas para que se comuniquen mediante la aplicación de mensajería Session con el fin de realizar el pago y obtener el programa de descifrado.

Además, los actores maliciosos están aprovechando el auge de las herramientas de inteligencia artificial para difundir un instalador falso de InVideo AI, una plataforma de

creación de videos impulsada por IA, con el objetivo de desplegar un malware destructivo conocido como Numero.

Este instalador fraudulento funciona como un «dropper» que contiene tres elementos: un archivo por lotes (batch) de Windows, un script en Visual Basic, y el ejecutable del malware Numero. Cuando el usuario ejecuta el instalador, el archivo por lotes se inicia en un bucle infinito a través del shell de Windows, ejecutando el malware y luego pausándolo durante 60 segundos mediante el script de VB con `cscript`.

> «Tras reanudar la ejecución, el archivo por lotes finaliza el proceso del malware Numero y lo vuelve a iniciar», explicó Talos. «Al implementar el bucle infinito, el malware Numero se ejecuta de forma continua en el equipo de la víctima.»

Numero, un ejecutable de 32 bits para Windows escrito en C++, verifica si hay herramientas de análisis o depuración de malware activas entre los procesos del sistema. Si no detecta ninguna, sobrescribe la ventana del escritorio (título, botones y contenido) con la cadena numérica «1234567890». Este malware fue compilado el 24 de enero de 2025.

Esta revelación coincide con una investigación publicada por Mandiant, empresa propiedad de Google, que detalla una campaña de «malvertising» (publicidad maliciosa) donde se colocan anuncios engañosos en Facebook y LinkedIn, los cuales redirigen a sitios falsos que imitan herramientas legítimas de generación de video con IA como Luma AI, Canva Dream Lab y Kling AI, entre otras.

Esta operación, también documentada recientemente por Morphisec y Check Point, ha sido atribuida a un grupo de amenazas rastreado por la tecnológica como UNC6032, que se sospecha opera desde Vietnam. La campaña estaría activa al menos desde mediados de 2024.

El ataque sigue un patrón específico: usuarios desprevenidos ingresan a estos sitios y se les solicita escribir un prompt para generar un video. No obstante, como se ha observado antes,

el contenido del prompt no importa, ya que el objetivo principal del sitio es iniciar la descarga de una carga útil (payload) desarrollada en Rust llamada STARKVEIL.

> «[STARKVEIL] despliega tres familias de malware modulares, enfocadas principalmente en el robo de información y capaces de descargar complementos adicionales para ampliar sus funciones», indicó Mandiant. «La presencia de múltiples cargas útiles similares sugiere un mecanismo de respaldo, que permite que el ataque continúe incluso si algunas son detectadas o bloqueadas por sistemas de seguridad.»

Las tres familias de malware que STARKVEIL distribuye son:

- GRIMPULL: un descargador que utiliza una conexión TOR para obtener payloads adicionales escritos en .NET, los cuales son descifrados, descomprimidos y cargados directamente en la memoria como ensamblados .NET.
- FROSTRIFT: una puerta trasera desarrollada en .NET que recopila información del sistema, detalles sobre programas instalados y escanea 48 extensiones relacionadas con gestores de contraseñas, autenticadores y billeteras de criptomonedas en navegadores basados en Chromium.
- XWorm: un troyano de acceso remoto (RAT) conocido, también en .NET, con capacidades de registro de teclas, ejecución de comandos, captura de pantalla, recolección de datos y notificación a los atacantes vía Telegram.

Además, STARKVEIL actúa como medio para iniciar un dropper adicional escrito en Python, llamado COILHATCH, cuya función es cargar y ejecutar las tres cargas útiles anteriores utilizando la técnica de DLL side-loading.

> *«Estas herramientas de IA ya no apuntan únicamente a diseñadores gráficos; cualquier persona puede caer en la trampa de un anuncio aparentemente inofensivo. La curiosidad por probar la última novedad en IA puede convertir a*

> *cualquiera en víctima»,* advirtió Mandiant.