Investigadores de ciberseguridad están alertando sobre un marco de comando y control (C&C) llamado Winos, que se está propagando a través de aplicaciones relacionadas con juegos, como herramientas de instalación, aceleradores de velocidad y utilidades de optimización.

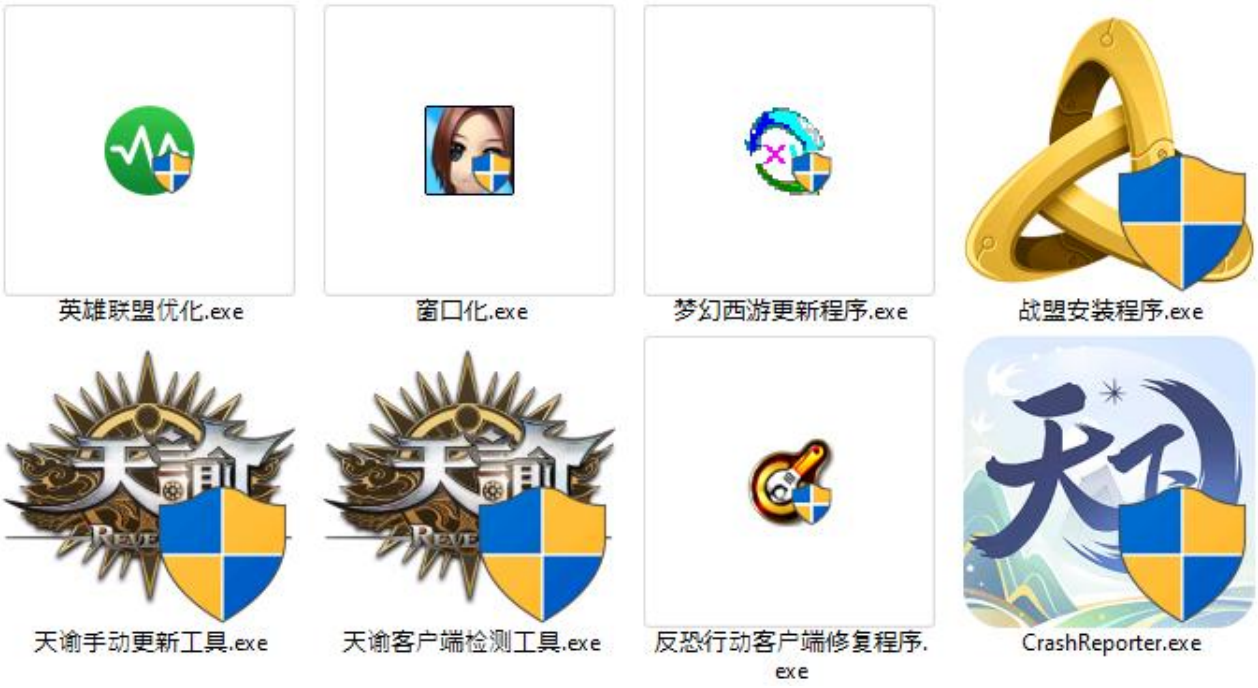
> *«Winos 4.0 es un marco malicioso avanzado que ofrece una funcionalidad integral, una arquitectura sólida y un control eficaz sobre numerosos puntos finales en línea para realizar acciones adicionales. Reconstruido a partir de Gh0st RAT, cuenta con varios componentes modulares, cada uno con una función específica»,* informó Fortinet FortiGuard Labs en un reporte.

Las campañas de distribución de Winos 4.0 fueron documentadas en junio por Trend Micro y el equipo KnownSec 404, quienes están monitoreando este grupo de actividades bajo los nombres Void Arachne y Silver Fox.

Estos ataques han sido observados atacando a usuarios de habla china, usando tácticas de optimización de motores de búsqueda de sombrero negro (SEO), redes sociales y plataformas de mensajería como Telegram para propagar el malware.

El análisis más reciente de Fortinet muestra que los usuarios que ejecutan las aplicaciones maliciosas relacionadas con juegos activan un proceso de infección en varias etapas, que comienza recuperando un archivo BMP falso desde un servidor remoto («ad59t82g[.]com»), el cual se decodifica en una biblioteca de enlaces dinámicos (DLL).

El archivo DLL configura el entorno de ejecución descargando tres archivos del mismo servidor: t3d.tmp, t4d.tmp y t5d.tmp; los dos primeros se desempaquetan para obtener la siguiente serie de cargas, incluyendo un ejecutable («u72kOdQ.exe») y tres archivos DLL, uno de los cuales es «libcef.dll».



> *«El DLL se denomina '□□□□', que significa 'Sistema de Registro de Estudiantes', lo que sugiere que el actor detrás de esta amenaza podría estar apuntando a organizaciones educativas,»* indicó Fortinet.

A continuación, el binario se utiliza para cargar «libcef.dll,» que luego extrae y ejecuta el código shell de la segunda etapa desde t5d.tmp. El malware establece contacto con su servidor de comando y control (C2) («202.79.173[.]4») a través del protocolo TCP y recupera otro DLL («□□□□.dll»).

La DLL de tercera etapa, parte de Winos 4.0, descarga datos codificados del servidor C2, así como un nuevo módulo DLL («□□□□.dll») que recolecta información del sistema, copia el contenido del portapapeles, extrae datos de extensiones de billeteras de criptomonedas como OKX Wallet y MetaMask, y habilita una función de puerta trasera para recibir más comandos del servidor.

Winos 4.0 también permite descargar complementos adicionales del servidor C2 que permiten capturar pantallas y cargar documentos sensibles desde el sistema comprometido.

> *«Winos 4.0 es un marco potente, similar a Cobalt Strike y Sliver, que soporta múltiples funciones y controla fácilmente sistemas comprometidos. Las campañas de amenazas utilizan aplicaciones relacionadas con juegos para atraer a las víctimas a descargar y ejecutar el malware sin precauciones, logrando un control profundo del sistema»,* mencionó Fortinet.