ArduGator

~See U Later, Alligator

Germán Quero, INSO4_A
Proyectos de Ciberseguridad

¿Qué es?

ArduGator es un conjunto de herramientas para establecer acceso persistente a un equipo que cumpla las siguientes características:

- Windows 11
- Se tiene acceso físico
- El Usuario es Administrador
- La distribución de teclado es en Español (adaptarlo a otros teclados es una obviedad)

Este objetivo se estableció por ser un conjunto de características muy común en el entorno en el que se ha desarrollado.

Adaptabilidad

El conjunto de herramientas se ha desarrollado con la adaptabilidad en mente.

Consiste en 2 herramientas muy diferenciadas:

- badUSB - arduGator
- APC Injection Malware (staged, C2) - Alligator.exe

Ambas partes se pueden utilizar por separado y con independencia en una multitud de casos de usos.

badUSB - arduGator

Consiste en un dispositivo hardware basado en un controlador AtMega32u4, concretamente una Arduino Pro Micro, que simula ser un dispositivo HID y automatiza la introducción de secuencias de teclas preprogramadas.

En este caso se utiliza como un método para descargar y ejecutar el Malware por primera vez como administrador.

Alligator.exe

Es un malware persistente y evasivo con 0 detecciones con MalwareBytes y Windows Defender.

Utiliza la técnica de APC Injection Early Bird para ejecutar código en el espacio de memoria de otro proceso.

El shellcode lo recibe de un servidor Command And Control en tiempo de ejecución para evitar ser analizado estáticamente.

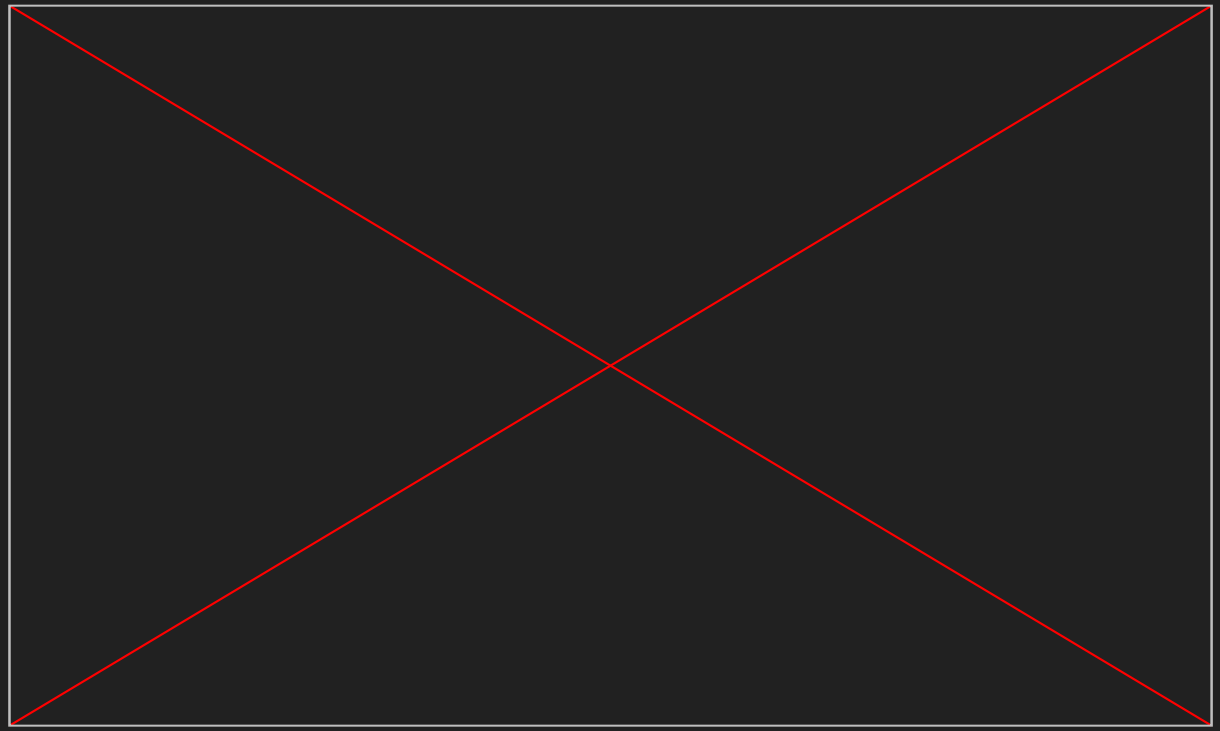
Se ha ofuscado mediante transformaciones léxicas, predicados opacos y la codificación en base64 de todos los strings hardcodeados en el ejecutable.

Casos de Uso

Se puede utilizar para ataques dirigidos donde conoces bien el sistema al que pretendes atacar, adaptándolo a las características del mismo, siempre y cuando tengas acceso físico, aunque sea durante menos de 5 segundos como veremos más adelante.

También se podría utilizar como una herramienta de Media Baiting, infectando a cualquier curioso que coja un USB desconocido del suelo y sea el admin de su propio Equipo

Ejemplos de uso



Medidas contra este tipo de ataques

- Bloquear el ordenador siempre que se vaya a quedar sin tu y solo tu supervisión (la mayoría de ataques son causados por agentes internos)
- Correcta Gestión de Permisos de Administrador (no deberías poder abrir una terminal de Admin sin contraseña)
- Antivirus Heurísticos
- Monitoreo de aplicaciones y procesos