Los troyanos de acceso remoto como StrRAT y Ratty se distribuyen como una combinación de archivos Java (JAR) maliciosos, lo que una vez más destaca cómo los atacantes encuentran continuamente nuevas formas de pasar desapercibidos.

> *«Los atacantes ahora usan la técnica Polyglot para confundir las soluciones de seguridad que no validan correctamente el formato de archivo JAR»,* dijo en un informe el investigador de seguridad de Deep Instinct, Simon Kenin.

Los archivos Polyglot son archivos que combinan la sintaxis de dos o más formatos distintos de tal forma que cada formato se puede analizar sin generar ningún error.

Una de esas campañas de 2022 detectada por la compañía de ciberseguridad es el uso de formatos JAR y MSI, es decir, un archivo que es válido como instalador JAR y MSI, para implementar la carga útil StrRAT. Esto también significa que el archivo puede ser ejecutado tanto por Windows como por Java Runtime Environment (JRE) en función de cómo se interprete.

Otro ejemplo involucra el uso de políglotas CAB y JAR para entregar tanto Ratty como StrRAT. Los artefactos se propagan mediante servicios de acortamiento de URL como cutt.ly y rebrand.ly, algunos de ellos alojados en Discord.

> *«Lo especial de los archivos ZIP es que se identifican por la presencia de un registro de fin de directorio central que se encuentra al final del archivo. Esto significa que cualquier 'basura' que añadamos al principio del archivo será ignorada y el archivo seguirá siendo válido»,* dijo Kenin.

La falta de una validación adecuada de los archivos JAR da como resultado un escenario en el que el contenido adjunto malicioso puede eludir el software de seguridad y pasar desapercibido hasta que se ejecuta en los hosts comprometidos.

Esta no es la primera vez que estos políglotas con malware se detectan en la naturaleza. En noviembre de 2022, DCSO CyTec, con sede en Berlín, descubrió un ladrón de información denominado StrelaStealer que se difunde como un políglota DLL/HTML.

> *«La detección adecuada de archivos JAR debe ser tanto estática como dinámica. Es ineficiente escanear cada archivo para detectar la presencia de un registro de fin de directorio central al final del archivo»,* dijo Kenin.

> *«Los defensores deben monitorear los procesos 'java' y 'javaw'. Si dicho proceso tiene '-jar' como argumento, el nombre de archivo pasado como argumento debe tratarse como un archivo JAR independientemente de la extensión del archivo o la salida de Linux».*