File Types That are Scanned by Cisco Secure Endpoint on Public Cloud

Contents

Introduction

This document provides a list of the files that are checked against the Public Cloud. There are different levels of reporting between the Cisco Secure Endpoint, Event Console, and Device Trajectory. Although a file is scanned at the connector level, only certain files are queried against the Public Cloud. This narrowing of events is not to hide visibility, but to accent the more important indications of compromise and not weigh down the system with inconsequential files.

File Types That are Scanned by Cisco Secure Endpoint on Public Cloud

Supported File Types Looked Up Against the Cloud

Windows

- 7ZSFX
- ELF
- ENCRYPTED_SCRIPT
- HTML_APP
- HWP3
- HWPOLE2
- LNK
- MBR
- MSCAB
- MSEXE
- MSOLE2
- OOXML_PPT
- OOXML_HWP
- OOXML_WORD
- OOXML_XL
- PDF
- POWERSHELL
- REGISTRY

- SCRIPT
- SETUP_INFO
- SWF
- WINDOWS_SCRIPT
- XML_HWP
- XML_WORD
- XML_XL
- ZIP

Mac and Linux

- DMG
- ELF
- JAVA
- MACHO
- MACHO_UNIBIN
- MSCAB
- MSEXE
- MSOLE2
- OOXML_PPT
- OOXML_WORD
- OOXML_XL
- PDF
- SWF
- XAR
- ZIP

Android Connector

- APK Files

Filetypes not visible in Device Trajectory

- AU3
- XZ
- CRYPTFF
- MSCHM
- RARSFX
- ZIPSFX

Archives filetypes that are scanned but not queried against the cloud

(The contents of the archives are queried against the cloud, not the archive itself)

- 7Z
- 7ZSFX
- ARJ
- ARFSFX