Cisco Endpoint IOC Attributes

The Endpoint Indication of Compromise (IOC) feature is a powerful incident response tool for scanning of post-compromise indicators across multiple computers. Endpoint IOCs are imported through the console from OpenIOC-based files written to trigger on file properties such as name, size, hash, and other attributes and system properties such as process information, running services, and Windows Registry entries. The IOC syntax can be used by incident responders to find specific artifacts or use logic to create sophisticated, correlated detections for families of malware. Endpoint IOCs have the advantage of being portable to share within your organization or in industry vertical forums and mailing lists.

As of AMP for Endpoints Windows Connector version 4.2.0.10084 the Endpoint IOC scanner now provides functionality not currently available in other competing IOC scanner software:

- The ability to match on the same file attribute (for example, file name) in a single IOC document using an AND operation. This is useful in scenarios where you are interested in finding more than one partial match for the same object type to increase the confidence of the match you are looking for.

  For example, FileItem/Filename is malware.exe AND FileItem/Filename is malware.dat.
- The ability to combine different object types in a single IOC document and trigger when both conditions are satisfied. This is useful in scenarios where you are interested in finding more than one partial match for different object types to increase the confidence of the match you are looking for.

  For example, RegistryItem/Keypath HKLM/Software/Malware AND FileItem/Filename is malware.exe.
- The ability to combine different levels of object attributes together in a single IOC document. This provides greater flexibility when creating IOC documents to improve their potential for detecting malware.

  For example, FileItem/PEInfo/ImportedModules/Name MaliciousFunction AND RegistryItem/KeyPath HKLM/Software/Malware.

The Endpoint IOC scanner is available in AMP for Endpoints Windows Connector versions 4 and higher. Running Endpoint IOC scans may require up to 1 GB of free drive space.

Sample Cisco Endpoint IOC documents are available for download:

- Asprox
- Bifrost
- Bifrost Backdoor
- Bladbindi
- Cleartext Credential Storage Enabled
- Coreshell
- CozyDuke
- CryptoTorLocker
- DarkComet
- Disabled System Restore
- Dridex
- Dridex5
- Dyre Persistence
- Executable in Registry
- Gameover
- Ghost

- Locky
- NetWiredRC
- Neutrino
- Parite
- PE Empty Section Name
- PlugX/Korplug
- PoisonIvy
- Powershell Hidden Command Execution
- Powershell Hidden Command in Registry
- Powelike
- ProfileService Exploit
- RamnitMutex
- RamnitService
- SpyEye
- Spynet
- TDSS
- TinyZBot
- Uroburos
- WiperDestoverAPT
- Xpiro Mutex
- XtremeRat
- ZxShell

Supported Endpoint IOC Attributes

IOC Attributes represent various properties on a computer that can be checked by the IOC scanner. An IOC document is made up of various attributes that have been defined by the changes a piece of malware or other intrusion may make on a compromised computer. The defined attributes are also called Indicator Terms.The IOC document can be made up of a large number of Indicator Terms that check many attributes or as few as a single term. The number of Indicator Terms defined in a document may depend on the complexity of the malware as well as tuning to reduce the chances of false-positives or false-negatives.

For example, a simple IOC document could be written to detect the presence of a file named xyz.exe in the Program Files directory. However, if you found that a legitimate application in your organization also used a file with that name, you could check for the presence of that file along with the MD5 checksum of the malicious file.

IMPORTANT!Cisco IOCs currently only support MD5 hashes and not SHA-256.

Once you have defined your IOC document using the appropriate Indicator Terms you can upload the document to the AMP for Endpoints Console. You can then have your AMP for Endpoints Connectors scan for indications of compromise using one or more IOC documents. You can upload IOC documents that contain unsupported attributes, however they will be ignored.

Endpoint IOC attributes currently supported by the AMP for Endpoints Connector are listed on the following pages.

Attribute Supported In IOCScanner 1.0	Content Type	Description
DriverItem/DeviceItem/AttachedDeviceName	string	The filter devices (if any) attached to the device.
DriverItem/DeviceItem/AttachedDriverName	string	The filter driver (if any) servicing the attached device.
DriverItem/DeviceItem/DeviceName	string	The name of the device created by the driver.
DriverItem/DriverName	string	The driver name registered with Windows (Object Manager).
DriverItem/Md5sum	string	The string representation of the MD5 checksum of the file on disk corresponding to the driver.
DriverItem/PEInfo/Exports/DllName	string	Name of the dll (sys) exported by the driver.
DriverItem/PEInfo/Exports/ExportedFunctions/string	string	Name of a function exported by the driver.
EventLogItem/EID	integer	The event id of the Windows Event.
EventLogItem/log	string	The category of Windows Event logs (ex: System, Security, Setup, Application).
EventLogItem/message	string	The partial or full message of the Windows Event.
FileDownloadHistoryItem/FileName	string	The name of the file downloaded via the Web browser. This information can be retrieved from all users whose user directories are accessible. The extraction is browser specific. For Firefox or Chrome, this information is retrieved from all of a user's profiles.
FileItem/Created	date	The file creation time in UTC (YYYY-MM-DDTHH:MM:SSZ where T is a marker to indicate the start of the time section of the date and Z as a marker to indicate UTC).
FileItem/FileAttributes	string	The individual attributes of the file (Hidden, System etc).
FileItem/FileExtension	string	The extension of the file (exe, doc, zip, etc.).
FileItem/FileName	string	The name of the file. It can consist of wild cards and partial paths.
FileItem/FilePath	string	The path to the file on the file system. It can be a partial path.

FileItem/FullPath	string	The full path of the file. The path used is user mode paths (c:\abc\abc.exe).
FileItem/Md5sum	string	The string representation of the MD5 checksum of the file. The checksum is for the default stream of the file.
FileItem/Modified	date	The last modified time of the file in UTC (YYYY-MM-DDTHH:MM:SSZ where T is a marker to indicate the start of the time section of the date and Z as a marker to indicate UTC).
FileItem/PEInfo/BaseAddress	integer	The base address of the file as indicated in the PE header. Only executable files contain a PE header.
FileItem/PEInfo/DetectedAnomalies/string	restricted string	A string used to describe anomalies that are usually absent in clean executables. The possible values are: checksum_mismatch, checksum_is_zero, overlapping_headers, oversized_optional_header, oversized_section, section_starts_unaligned, empty_section_name, non_ascii_section_name, contains_eof_data, incorrect_image_size, invalid_entry_point, corrupted_imports.
FileItem/PEInfo/DetectedEntryPointSignature/Name	restricted string	PEiD packer detection. It uses userdb.txt and the latest signatures (all are packers) are hosted at https://code.google.com/p/reverse-engineering-scripts
FileItem/PEInfo/DetectedEntryPointSignature/Type	restricted string	The type of the PEiD signature. The possible values are: None, Packer, Installer, Compiler.
FileItem/PEInfo/DigitalSignature/CertificateSubject	string	The subject field of the certificate with which the file is digitally signed.
FileItem/PEInfo/DigitalSignature/Description	string	A description consisting of the result of SignatureExists and SignatureVerified (ex: The file is signed and signature is verified).
FileItem/PEInfo/DigitalSignature/SignatureExists	boolean string	A string (true/false) to indicate whether the file is digitally signed.
FileItem/PEInfo/DigitalSignature/SignatureVerified	boolean string	A string (true/false) to indicate whether the file is digitally signed and it is verified.
FileItem/PEInfo/Exports/DllName	string	Name of the dll exported by the executable.
FileItem/PEInfo/Exports/ExportedFunctions/string	string	Name of a function exported by the executable.

FileItem/PEInfo/Exports/ExportsTimeStamp	date	The date and time in UTC when the export table was created (YYYY-MM-DDTHH:MM:SSZ where T is a marker to indicate the start of the time section of the date and Z as a marker to indicate UTC). It is stored in the executable's export directory table.
FileItem/PEInfo/Exports/NumberOfFunctions	integer	The number of functions exported by the executable (dll).
FileItem/PEInfo/Exports/NumberOfNames	integer	The number of name pointer entries in the executable's export directory table.
FileItem/PEInfo/ImportedModules/Module/ImportedFunctions/string	string	Name of a function imported by the executable.
FileItem/PEInfo/ImportedModules/Module/Name	string	Name of the dll imported by the executable.
FileItem/PEInfo/ImportedModules/Module/NumberOfFunctions	integer	The number of functions imported by the executable.
FileItem/PEInfo/PEChecksum/PEFileRaw	integer	The CRC checksum of the executable present in the PE header.
FileItem/PEInfo/PEChecksum/PEFileAPI	integer	The CRC checksum of the executable computed using the Windows API (MapFileAndChecksum). Since this API maps the file into memory there are performance considerations. This is controlled via a configurable option, namely "UseChecksumAPI" (not visible to the user) that when true computes the Checksum using the Windows API.
FileItem/PEInfo/PEChecksum/PEComputedAPI	integer	The CRC checksum of the executable computed using the PE header.
FileItem/PEInfo/PETimeStamp	date	The date and time in UTC when the executable was created (YYYY-MM-DDTHH:MM:SSZ where T is a marker to indicate the start of the time section of the date and Z as a marker to indicate UTC).
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Language	string	To match the language, the Endpoint IOC should be created on systems where the locale specified is English. This is a constraint in our current system.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Name	string	The name of the resource.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Size	integer	The size of the resource in bytes.
FileItem/PEInfo/ResourceInfoList/ResourceInfoItem/Type	string	The type of the resource. Some of the default resource types (http://msdn.microsoft.com/en-us/library/ms648009(v=vs.85).aspx) but the additional types can be defined.

FileItem/PEInfo/Sections/ActualNumberOfSections	integer	The actual number of sections present in the PE header.
FileItem/PEInfo/Sections/NumberOfSections	integer	The number of sections present in the PE header.
FileItem/PEInfo/Sections/Section/Name	string	The name of the section present in the PE header as defined by the Microsoft PE specification. It is also possible to include custom names.
FileItem/PEInfo/Sections/Section/SizeInBytes	integer	The exact size of the section in bytes.
FileItem/PEInfo/Subsystem	restricted string	The subsystem of the executable. The possible values are: Unknown, Native, Windows_GUI, Windows_CUI, OS2_CUI, POSIX_CUI, Native_Win9x_Driver, Windows_CE_GUI, EFI_Application, EFI_Boot_Service_Driver, EFI_Runtime_Driver, EFI_ROM, XBOX, Undefined.
FileItem/PEInfo/Type	restricted string	The type of the executable. Possible values are: Executable, Dll, Invalid.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Comments	string	The comments provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/CompanyName	string	The name of the company provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileDescription	string	The description of the file provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/FileVersion	string	The version of the file provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/InternalName	string	The internal name of the file provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/Language	string	To match the language, the Endpoint IOC should be created on systems where the locale specified is English. This is a constraint in our current system.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalCopyright	string	The copyright string provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/LegalTrademarks	string	The trademark string provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/OriginalFilename	string	The original name of the file provided when creating this executable.
FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductName	string	The name of the product provided when creating this executable.

FileItem/PEInfo/VersionInfoList/VersionInfoItem/ProductVersion	string	The version of the product provided when creating this executable.
FileItem/SizeInBytes	integer	The exact size of the file in bytes. Do not use the rounded off value displayed by the operating system.
FileItem/StreamList/Stream/Md5sum	string	On NTFS, file system data can be stored in more than one stream of a file. By default, there is only one stream but data can be stored in additional streams of a file. To maintain compatibility with Endpoint IOCs, the MD5sum is the string representation of MD5 checksum of the default data stream and NOT that of the actual stream.
FileItem/StreamList/Stream/Md5sumCorrect	string	On NTFS, file system data can be stored in more than one stream of a file. By default, there is only one stream but data can be stored in additional streams of a file. The string representation of MD5 checksum of the stream.
FileItem/StreamList/Stream/Name	string	On NTFS, file system data can be stored in more than one stream of a file. By default, there is only one stream but data can be stored in additional streams of a file. The name of such additional stream.
FileItem/StreamList/Stream/SizeInBytes	integer	On NTFS, file system data can be stored in more than one stream of a file. By default, there is only one stream but data can be stored in additional streams of a file. The exact size of the file in bytes of such additional stream.
PortItem/remoteIP	IP	The dotted representation of the remote IP address. It can be either an IPV4 or IPV6 address.
PrefetchItem/AccessedFileList/AccessedFile	string	The path to the file that was accessed by the application for which the prefetch entry is present.
PrefetchItem/ApplicationFileName	string	The application filename for which the prefetch entry is present.
PrefetchItem/ApplicationFullPath	string	The application full path for which the prefetch entry is present.
PrefetchItem/FullPath	string	The full path for the prefetch entry.
ProcessItem/arguments	string	The arguments that were passed to the process when it was started.
ProcessItem/HandleList/Handle/Name	string	The handle name.
ProcessItem/HandleList/Handle/Type	string	The object type the handle refers to. Typically object types like Mutant (Windows Mutex), Event are used.

ProcessItem/name	string	The process name.
ProcessItem/path	string	The path to the file corresponding to the process.
ProcessItem/PortList/PortItem/localPort	integer	Specify a single port or range of ports (ex:10000 TO 15000).
ProcessItem/SectionList/MemorySection/DigitalSignature/SignatureVerified	boolean string	A string (true/false) to indicate whether the file is digitally signed and verified.
ProcessItem/SectionList/MemorySection/Md5sum	string	The string representation of the MD5 checksum of the memory section.
ProcessItem/SectionList/MemorySection/Name	string	The section name in the process.
ProcessItem/SectionList/MemorySection/PEInfo/Exports/ExportedFunctions/string	string	In case the memory section is an executable, the name of the exported function.
ProcessItem/SectionList/MemorySection/PEInfo/ImportedModules/Module/Name	string	In case the memory section is an executable, the name of the module that is imported.
ProcessItem/SectionList/MemorySection/PEInfo/Sections/Section/Name	string	In case the memory section is an executable, the name of the section in the PE header of that executable.
RegistryItem/Hive	restricted string	The string representing the registry hives (http://msdn.microsoft.com/en-us/library/windows/desktop/ms724877(v=vs.85).aspx). Possible values are HKEY_USERS, HKEY_CURRENT_CONFIG, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE\SAM, HKEY_LOCAL_MACHINE\Security, HKEY_LOCAL_MACHINE\Software, HKEY_LOCAL_MACHINE\System, HKEY_USERS\.DEFAULT, HKEY_LOCAL_MACHINE\BCD00000000.
RegistryItem/KeyPath	string	The full path of the registry key (not including the hive).
RegistryItem/Path	string	The partial path of the registry key.
RegistryItem/ReportedLengthInBytes	integer	The size in bytes used to store the registry value.
RegistryItem/Text	string	The actual registry value.

RegistryItem/Type	restricted string	The string value representing the registry type. Possible values are REG_NONE, REG_SZ, REG_EXPAND_SZ, REG_BINARY, REG_DWORD, REG_DWORD_BIG_ENDIAN, REG_LINK, REG_MULTI_SZ, REG_RESOURCE_LIST, REG_FULL_RESOURCE_DESCRIPTOR, REG_RESOURCE_REQUIREMENTS_LIST, REG_QWORD, REG_INVALID_TYPE, REG_KEY.
RegistryItem/Value	string	The actual registry value represented as base64. Used when registry value is binary.
RegistryItem/ValueName	string	The registry value name.
ServiceItem/arguments	string	The arguments that were passed to the service when it was started.
ServiceItem/description	string	The description used to typically describe the job that the service does
ServiceItem/descriptiveName	string	The display name (friendly name) of the service.
ServiceItem/name	string	The name registered with Windows Service Control Manager (SCM). The service can be an in-process service or an out-of-process service. In an in-process service there will be a service dll present and the path is typically the svchost.exe.
ServiceItem/path	string	The path to the executable registered as the service. This is the executable that runs as part of the service.
ServiceItem/pathCertificateIssuer	string	The issuer of the certificate with which the file corresponding to the service is digitally signed.
ServiceItem/pathCertificateSubject	string	The subject field of the certificate with which the file corresponding to the service is digitally signed.
ServiceItem/pathmd5sum	string	The string representation of the MD5 checksum of the file on disk corresponding to the service.
ServiceItem/pathSignatureExists	boolean string	A string (true/false) to indicate whether the file is digitally signed.
ServiceItem/pathSignatureVerified	boolean string	A string (true/false) to indicate whether the file is digitally signed and verified.
ServiceItem/serviceDLL	string	The path to the in-process service dll registered as the service. This service runs inside the svchost proces.

ServiceItem/serviceDLLCertificateIssuer	string	The issuer of the certificate with which the dll file corresponding to the in-process service is digitally signed.
ServiceItem/serviceDLLCertificateSubject	string	The subject field of the certificate with which the dll file corresponding to the in-process service is digitally signed.
ServiceItem/serviceDLLmd5sum	string	The string representation of the MD5 checksum of the dll file on disk corresponding to the in-process service.
ServiceItem/serviceDLLSignatureExists	boolean string	A string (true/false) to indicate whether the dll file corresponding to the in-process service is digitally signed.
ServiceItem/serviceDLLSignatureVerified	boolean string	A string (true/false) to indicate whether the dll file corresponding to the in-process service is digitally signed and verified.
ServiceItem/status	restricted string	The status of the service. The possible values are: SERVICE_CONTINUE_PENDING, SERVICE_PAUSE_PENDING, SERVICE_PAUSED, SERVICE_RUNNING, SERVICE_START_PENDING, SERVICE_STOP_PENDING, SERVICE_STOPPED.
SystemRestoreItem/OriginalFileName	string	The original name of the file before the System restore point was created.
TaskItem/ActionList/Action/ExecProgramPath	string	The path of the executable registered to run with Windows Task Scheduler.
TaskItem/ApplicationName	string	The name of the executable registered to run with Windows Task Scheduler.
TaskItem/Name	string	The name of the task registered with Windows Task Scheduler.