07-12-2026

Malware data

Malware data refers to information or artifacts collected, analyzed, and used to identify or understand malicious software (malware). Malware is any software designed to disrupt, damage, or gain unauthorized access to computer systems. Malware data typically includes technical details about the malware's behavior, structure, and impact, such as file signatures, payloads, command-and-control (C2) communication patterns, indicators of compromise (IOCs), and more.

Malware data plays a crucial role in cybersecurity, aiding in malware detection, analysis, and prevention by security systems like antivirus software, intrusion detection systems (IDS), and threat intelligence platforms.

Malware data typically includes:

- **File-based malware data**: This includes data related to the malicious software's file, such as its hash value, file type, and structure
- **Behavioral malware data**: This refers to information about the actions a piece of malware performs after execution
- **Network-based malware data**: This includes information about how malware communicates over a network to carry out its objectives
- **Static malware analysis data**: This includes information derived from examining the malware file without executing it
- **Dynamic malware analysis data**: This includes data gathered by running the malware in a controlled environment, such as a sandbox, to observe its behavior
- **Indicators of compromise (IOCs)**: IOCs are specific pieces of data used to identify the presence of malware or malicious activity
- **Malware families and variants**: This data categorizes malware into families or variants based on shared characteristics
- **Payload information**: Payload data describes the malicious actions or objectives of malware
- **Malware delivery methods**: This includes data about how malware is distributed
- **Malware events and logs**: Data extracted from logs showing the malware's activity

The Splunk Common Information Model (CIM) add-on contains a Malware data model with fields that describe malware detection and endpoint protection management activity. The Malware data model is often used for endpoint antivirus product related events.

Before looking at documentation for specific data sources, review the Splunk Help information on general data ingestion

for Splunk Enterprise, Splunk Cloud Platform or Splunk Observability Cloud.

Add-ons and apps

- Splunk Add-on for Microsoft Security
- MalwareBazaar Connector
- MISP Connector
- Cisco Secure Malware Analytics (Threat Grid)
- Cisco Security Cloud
- Intel 471 Malware Intelligence
- PolySwarm Malware Threat Intelligence App for Splunk
- IPQS Malware And Virus File Scanner
- PAVO Malware App for Splunk
- GLIMPS Malware

Splunk Lantern articles for the Splunk platform

- Complying with General Data Protection Regulation
- Monitoring NIST SP 800-53 rev5 control families
- Detecting recurring malware on a host
- Investigating a ransomware attack
- Reconstructing a website defacement
- Recognizing improper use of system administration tools

Splunk Lantern articles for Splunk security products

- Triaging Crowdstrike malware data