



# ICS malware data feed

## The problem

Ensuring the cybersecurity of industrial enterprises is an increasingly difficult task given the ever-growing variety and dynamics of cyberthreats. This creates an urgent need for up-to-date data. Without it, it is difficult to detect attacks and respond to incidents on ICS computers in a timely manner.

## The solution

An ICS threat intelligence feed updated daily with data about current threats based on information received from ICS computers and incident response investigations at industrial organizations.

## Target audience

Cybersecurity teams in industrial enterprises, managed security service providers (MSSPs), computer emergency response teams (CERTs) and other similar organizations.

## The security challenges

Malware-infected systems in OT networks can cause serious and unpredictable issues for enterprises. Kaspersky ICS CERT is seeing a variety of constantly evolving malware blocked by Kaspersky solutions on ICS computers. Unfortunately, not all nodes in an OT network can be reliably protected with a modern full-fledged solution. And even when malware is blocked, company employees often lack the contextual information necessary to determine whether it is a sign of a bigger incident. In order to detect and classify attacks, quickly identify and locate affected systems, prevent the spread of malware in an OT network, and respond to incidents, it is crucial to have the most comprehensive data on current threats.

## What we offer

A constantly updated feed of ICS threat data containing IoCs that enables the identification of malware and potentially dangerous software detected by Kaspersky on ICS computers around the world. The data stream also helps identify compromised systems on ICS networks during incident response.

The data feed helps secure systems that could not be effectively secured for practical reasons [in other ways](#).

Using our data feed, the customer will be able to:

- Detect threats capable of penetrating ICS computers while they are still on the perimeter or in the IT network, thereby increasing OT network security;
- Detect attacks on ICS and related OT networks in real time;
- Identify malware infections on OT computers during incident response;
- Add Kaspersky information to local data about threats and malware detected in enterprise networks.

## What we do

The malware data feed is updated every 60 minutes with data received from [Kaspersky Security Network \(KSN\)](#) deployed on ICS computers around the world.

We verify and enrich all received data using various technologies and techniques, such as statistical analysis, Kaspersky expert systems (sandboxes, heuristics, similarity analysis, behavioral analysis, etc.), comparisons against allowlists, and manual analysis by researchers.

## What the customer gets

Data about ICS threats. It is provided in an open JSON format and can be input into various analytical and comparative tools, or reformatted into any necessary data format. The data is intended for integration with third-party SIEM systems.

The initial data file (no larger than 100 MB) is formed over three months and contains over 200,000 records. The data is updated every 60 minutes.

The threat data is presented as an IoC (MD5 hash sum) along with related metadata that can be merged with local data, especially information about files with the same MD5 hash sum:

- SHA1 and SHA256 file hash sums;
- Top file names under which malware is most often distributed;
- File size in bytes;
- File format type;
- Kaspersky name in the antivirus databases;
- File spread rating;
- Dates of the first and last events registered for this file in the threat database;
- Geographical spread of file;
- 10 IP addresses from which malicious objects were downloaded most often;

- List of URLs from which the malicious object was downloaded.

## How information about ICS threats differs from other sources

Traditionally, ICS environments have been considered separate from IT networks and isolated from the internet. Consequently, they are believed to be free from the threats that affect those environments. However, various Kaspersky products are deployed on computers in ICS and OT systems around the world, including:

- SCADA servers;
- Historian servers;
- OPC gateways;
- Stationary engineer and operator workstations;
- Mobile engineer and operator workstations;
- Human-machine interface (HMI);
- OT network administrators' computers and computers of ICS software developers.

Telemetry analysis data from these security products, as well as our research, indicate the numerous and diverse threats capable of reaching OT systems in various industries.

These threats come in many forms, including:

- Spyware, ransomware, botnet agents, backdoors, data destruction software, etc.;
- Cryptocurrency mining software, various types of self-propagating software (worms and viruses);
- Malware developed for popular engineering packages, such as AutoCAD;
- Potentially dangerous remote access tools;
- Malware targeting industrial organizations.

Penetration vectors used by such malware to infiltrate ICS computers include:

- Specialist online forums for engineers working on production lines, including those where patches, programs for hacking engineering and industrial software, or patched/hacked engineering and ICS software are distributed;
- Phishing attacks targeting industrial organizations;
- Phishing attacks primarily targeting industrial organizations or organizations in a specific sector, as well as attacks targeting a specific organization, including [malicious mailings from compromised mailboxes, suppliers, customers, and technology and business partners](#);

- OT nodes unprotected by antivirus solutions that become sources of multiple repeat infections, often with older malware rarely seen in IT networks;
- Infected portable data sources (USB drives);
- Attacks on contractors and third-party service providers with remote or local access to the OT network;
- Attacks through software and ICS equipment vendor supply chains.

This distinguishes the threat landscape of industrial OT networks from that of IT infrastructures\*, even though attacks on industrial enterprises primarily employ general-purpose malicious tools. [Attackers typically use modified binary samples in attacks, employing various obfuscation techniques and modification of binary code to reduce the likelihood of detection.](#)

\*Over 70% of the malware samples that we detect on ICS systems are rarely, if ever, seen in IT networks and are therefore not included in the Enterprise threat data stream. For this reason, some solutions not designed for the ICS environment may lack signatures for these malware samples.

In addition to the specifics of the overall ICS threat landscape, we also see noticeable differences by region and industry. The data stream contains threats detected on computers from various industries, including (but not limited to):

- Automotive;
- Building automation;
- Energy;
- Food and beverage;
- Healthcare and pharmaceuticals;
- Manufacturing;
- Oil and gas;
- Metallurgy;
- Mining;
- Transportation and logistics;
- Utilities;
- Waste recycling/utilization.

The feed also includes data from attacked OT systems related to the following types of infrastructure:

- Engineering and ICS integration;
- ICS software development;
- Building automation;
- Biometric authentication systems in OT and physical access control.

## Use case scenarios

### Detecting malware and attacks with the potential to penetrate the ICS environment

Comparing data in the feed with SIEM data collected from the network perimeter, end nodes and sandboxes. Specifically:

- Comparing hash sums from the ICS Threat Intelligence Malware Data Feed with MD5 hash sums of files that are:
  - Moving through the network perimeter (proxy servers, SMTP, FTP, SMB);
  - Detected/registered on end nodes (by antivirus solutions, application launch software and/or during audits);
  - Analyzed in sandboxes.
- Comparing IPs and URLs from the ICS Threat Intelligence Malware Data Feed with IP and URL from:
  - Incoming and outgoing connections registered on the network perimeter (firewalls, IDS, IPS, proxy servers);
  - Incoming and outgoing connections registered on endpoints (local firewalls, IDS and IPS);
  - Detected as a result of dynamic file analysis in sandboxes;
  - Extracted from emails.

### Identifying malware infections on ICS computers during cybersecurity audits and incident investigations

Data in the feed is useful for locating malware infections on ICS computers. This includes:

- Detected during analysis of the computer's file system;
- Detected in event logs of antivirus solutions, application launch software, etc.;
- Detected in copies of network traffic;
- Detected in event logs of firewalls, IDS, IPS, proxy servers and sandboxes;
- Detected in process memory snapshots.

## Threat data enrichment

During incident detection or investigations, personnel often require additional information about detected threats. Metadata about the threats and IoCs found in the feed can significantly simplify an investigation by:

- Prioritizing the incident based on the degree of attack targeting;

- Connecting disparate facts related to the incident to create a more complete picture of the attack;
- Locating related events, malware components, attempted attacks and/or cases of infection in other systems within the organization.

[Request a consultation](#)

## Learn more

- [Dynamics of external and internal threats to industrial control systems. Q2 2025](#)
- [Threat landscape for industrial automation systems. Q1 2026](#)
- [Campaigns abusing corporate trusted infrastructure hunt for corporate credentials on ICS networks](#)

## Related services

- Analysis of known ICS vulnerabilities for critical information security decision-making
- ICS vulnerability and threat intelligence
- Incident response at industrial enterprises
- Digital forensics and incident response in ICS. Training
- Development of incident response handbook and training

[Request a consultation](#)

**Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT)**

is a global Kaspersky project aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

[Kaspersky ICS CERT](#)

[ics-cert@kaspersky.com](mailto:ics-cert@kaspersky.com)