# Malicious object categories blocked on ICS computers by Kaspersky solutions

The malicious objects blocked by Kaspersky solutions fall into many different categories. To give a better idea of the types of threats blocked by Kaspersky products, we conducted a detailed classification.

- **Denylisted internet resources.**

  Web-antivirus protects a computer when programs installed on it (browsers, email clients, automatic application update modules and others) attempt to connect to denylisted IP addresses and URLs. Such web resources are associated in some way with distributing or controlling malware.

  Specifically, denylisted resources include, among others, those used to distribute such malware as Trojan-Spy or ransomware disguised as utilities for cracking or resetting passwords on controllers of various manufacturers, or as cracks/patches for industrial and engineering software used in industrial networks.

- **Malicious scripts and phishing pages** (JS and HTML).
- **Browser exploits.**
- **Spy Trojans, backdoors and keyloggers,**

  which appear in numerous phishing emails sent to industrial enterprises. As a rule, the ultimate goal of such attacks is to steal money.

- **Malicious documents (MSOffice + PDF) containing exploits, malicious macros or malicious links.**
- **Ransomware.**
- **Worms (Worm)**,

  which usually spread via removable media and network shares, as well as worms distributed via email (Email-Worm), network vulnerabilities (Net-Worm) and instant messengers (IM-Worm). Most worms are obsolete from the network infrastructure viewpoint. However, there are also worms like Zombaque which implement a P2P network architecture allowing threat actors to activate them at any point.

- **Virus class malware.**

  These programs include such families as Sality, Nimnul, and Virut, which have been detected for many years. Although these malicious families are considered obsolete because their command-and-control servers have long been inactive, they usually make a significant contribution to the statistics due to their self-propagation and insufficient measures taken to completely neutralize them.

- **Malicious LNK files.**

  These files are mainly blocked on removable media. They are part of the distribution mechanism for older families such as Andromeda/Gamarue, Dorkbot, Jenxcus/Dinihou and others.

  This category also includes a wide variety of LNK files with the CVE-2010-2568 vulnerability, which was first exploited to distribute the Stuxnet worm and has later been exploited to spread many other families, such as Sality, Nimnul/Ramnit, ZeuS, Vobfus, etc.

  Today, LNK files disguised as legitimate documents can be used as part of a multistage attack. They run a PowerShell script that downloads a malicious file.

  In rare cases, the malicious PowerShell script downloads binary code – a specially crafted modification of a passive TCP backdoor from the Metasploit kit – and injects the code into memory.

- **Malicious files (executables, scripts, autorun.inf, .LNK and others) that run automatically at system startup or when removable media are connected.**

  These files come from a variety of families that have one thing in common – autorun. The least harmful functionality of such files is automatically launching the browser with a predefined home page. In most cases, malicious programs that use autorun.inf are modifications of malware from old families (Palevo, Sality, Kido, etc.).

- **Malware for AutoCad.**

  It is worth noting that malware for AutoCad, specifically viruses, is mainly detected on computers that are part of industrial networks, including network shares and engineering workstations, in East Asia.

- **Web miners running in browsers.**
- **Miners in the form of executable files for Windows.**
- **Banking Trojans.**
- **Malicious files for mobile devices**

  that are blocked when such devices are connected to computers.

**Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT)** is a global project of Kaspersky 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