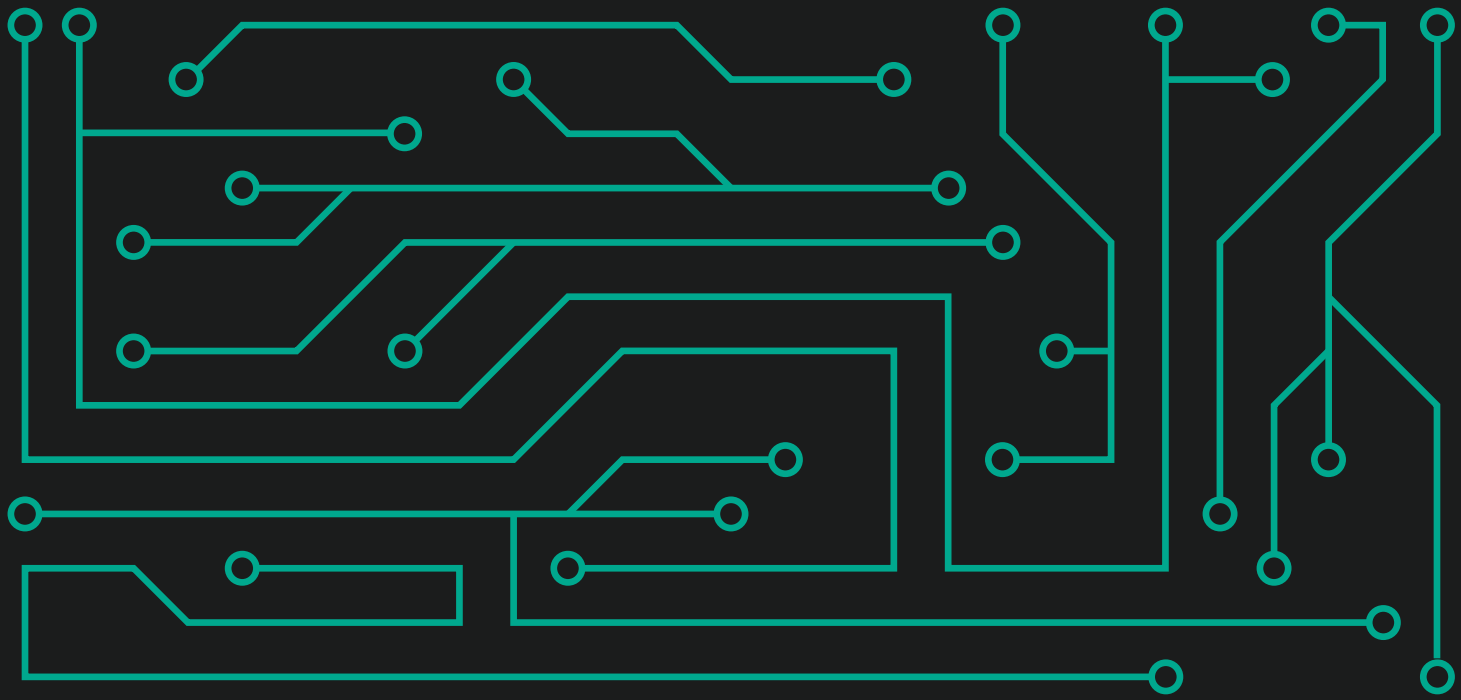
KASPERSKY lab

Kaspersky Security Bulletin:

THREAT PREDICTIONS FOR INDUSTRIAL SECURITY IN 2019



The past few years have been very intense and eventful when it comes to incidents affecting the information security of industrial systems. That includes new vulnerabilities, new threat vectors, accidental infections of industrial systems and detected targeted attacks. In response, last year we developed some Threat Predictions for Industrial Security in 2018, outlining the trends most likely to unfold in the year ahead.

The industrial cybersecurity threat landscape moves at a slower and more rigid pace than the information technology threat landscape in general. Attacks on ICS are still hard to monetize. Industrial organizations are still out of scope for the majority of cybercriminals. They are a relatively new target for adversaries who have already started attacking them. These are still applying existing tools and tactics to their attacks. That is why the majority of the industrial threat predictions from last year are still unfolding, although some of them have already come true.

Kaspersky Lab specialists have spent a few years investigating the cyberthreat landscape for industrial organizations and trying to bring their expertise and technology to OT environments. We are still on a long journey, with various to difficulties cope with and problems yet to solve. Constantly keeping in contact with many researchers in other security organizations and some ICS security pioneers from inside industrial companies; we have come to the conclusion that some of the difficulties we face are common to the industry. Solving some of those is mandatory to make the world more secure and safe.

So, although the fog of 2018's predictions and threat landscape has yet to clear, we decided to focus on the major problems likely to affect the work of professionals involved in industrial systems in 2019.

TOP FOUR CYBERSECURITY CHALLENGES FACING INDUSTRIAL ENTERPRISES IN 2019

1. The ever-increasing attack surface

The increasing amount of automation systems, the variety of automation tools, number of organizations and individuals with direct or remote access to automation systems, as well as the emergence of communication channels for monitoring and remote control between previously independent objects – all expand the opportunities for criminals to plan and execute their attacks.

2. Growing interest of cybercriminals and special services

A decrease in profitability and increase in risks from cyberattacks aimed at traditional victims is pushing criminals to search for new targets, including those within industrial organizations.

At the same time, special services in many countries, as well as other organized groups – motivated by internal and external political interests – and financially-motivated groups, are actively engaged in the research and development of techniques to implement espionage and terrorist attacks aimed at industrial enterprises.

Taking into account the current geopolitical context, the development of industrial enterprises' automation systems, and the transition to new management processes and models of production and economic activity, this situation will continue to develop in the coming years, negatively affecting industrial organizations.

3. The underestimation of general threat levels

A lack of public access to information about information security issues within industrial enterprises, coupled with the relative rarity of targeted attacks on automation systems, an excessive belief in emergency protection systems and the denial of objective reality is having a negative effect on the assessment of threat levels by owners and operators of industrial enterprises and their personnel.

4. The misunderstanding of threat specifics and the suboptimal choice of protection options

In the world of industrial cybersecurity, several high–profile incidents carried out with the help of targeted attacks against a very limited number of victims, created an information landscape that formed fully the idea of a potential threat – both among information security researchers and security developers, and among potential users of these tools.

However, the professional reporting of these incidents was often too difficult to understand by the majority of potential users, and was devoid of important OT details. The information field formed in these conditions, including the absence of a daily need to deflect the attacks aimed at automated control systems, gave developers a chance to create products that might protect better from the artificial scenarios thought up by researchers themselves, than from real world day-to-day threats. This could leave the automation systems of industrial enterprises vulnerable to real life attacks, including random ones and targeted attack campaigns organized by cyber criminals.