Kaspersky®

INDUSTRIAL SECURITY

2014

CYBERTHREATS TO ICS SYSTEMS

YOU DON’T HAVE TO BE A TARGET
TO BECOME A VICTIM

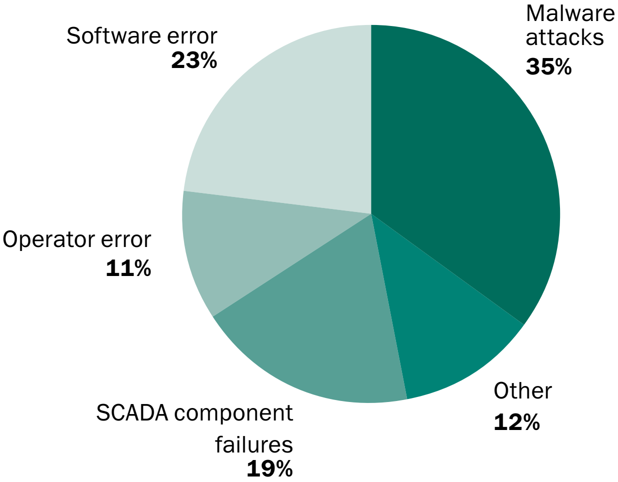
KASPERSKY lab

THE FLIP SIDE OF COMPUTERIZATION

Over the past few decades, the automation of industrial systems has been steadily gaining momentum. Business demands continuous improvements in the efficiency of production process, thus the depth of IT penetration and system connectivity grows continuously; industrial facilities are connected to corporate networks and are frequently managed remotely over the network. However, along with their benefits, these new technologies have brought new threats into the world of industrial automation, and these new threats came as a surprise. The Industrial Control Systems (ICS) in place today were designed to operate for decades, and many of them were developed without any serious regard to IT security.
The stable operation of today's industrial networks could be disrupted not only by a failure at a production unit or an operator's error, but also a software error, an accidental infection of workstations with malware or a deliberate cybercriminal attack.

Despite warnings from experts, until recently the concept of ICS security was based on the conviction that isolating a network would be sufficient to ensure security from all threats. This concept was conclusively exploded by the notorious Stuxnet: a 50 KB-sized computer worm which penetrated an isolated network via a portable USB drive, infected programmable logical controllers (PLCs) and made centrifuges physically inoperative at a nuclear facility in Iran.

The main causes of incidents in industrial networks are shown in the pie chart below (data courtesy of securityincidents.net):

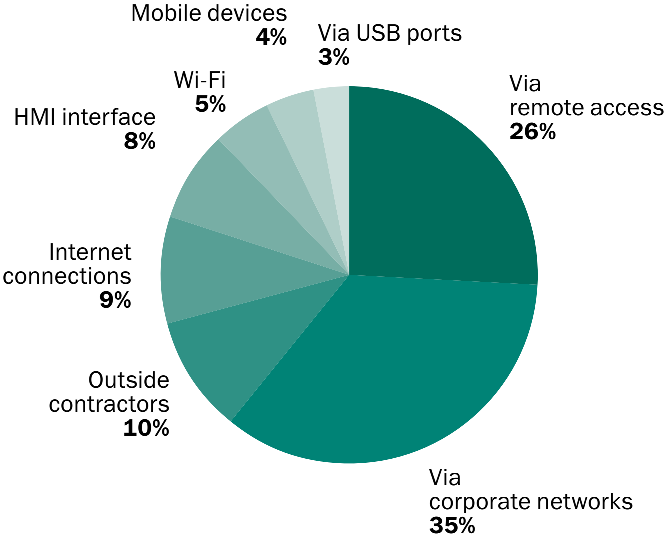


AN ISOLATED TECHNOLOGICAL NETWORK IS NO LONGER ANY GUARANTEE OF THE SECURITY OF AN INDUSTRIAL FACILITY, BE IT IT OR PHYSICAL SECURITY.

NOT JUST STUXNET

Stuxnet is the best known example of how malware can negatively affect technology processes, but it is not alone. Kaspersky Lab's studies show that many industrial computers are infected with ordinary malicious programs which follow various paths to penetrate corporate networks.

The pie chart below shows the sources from which malicious code penetrates industrial networks (data courtesy of securityincidents.net):



In industrial networks, regular malware can cause far greater damage than when it infects office or home computers. For instance, it may block the operation of critical applications, thus leading to hardware failure. The potential consequences may go far beyond even the plans of many malware writers.

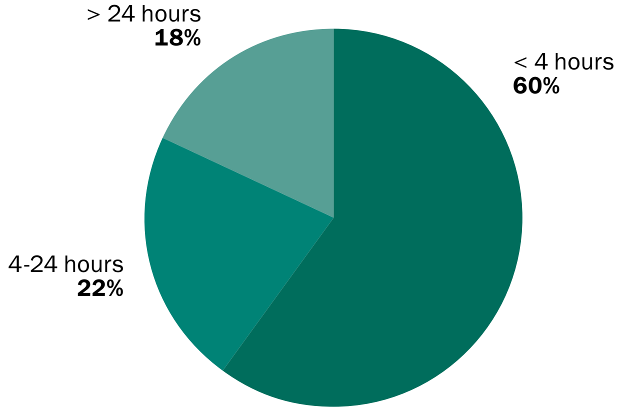
For example, cases have emerged when the Sality virus infected industrial networks — its recent modification copied the exploit of a USB vulnerability that Stuxnet also took advantage of. Although Sality contained no destructive code aimed at programmable logical controllers, its activity led to 100% CPU load on SCADA systems running under Windows.

Another example is the Conficker worm, which infected an industrial network on which Windows had not been updated. The worm sent millions of network requests, disrupting the operation of the entire industrial network.

Even computer-assisted design (CAD) tools can be used to spread malware. For instance, there is a know case when a malicious program written in AutoLisp (AutoCAD) embedded malicious code into an CAD image. When the image was opened it led to massive destruction of data.

Maintaining the reliability and safety of industrial processes requires reliable protection of its ICS against all hazards, including cyber threats.

Statistics of industrial process downtime resulting from malware incidents at industrial facilities (data courtesy of securityincidents.net):



EVEN AN ACCIDENTAL MALWARE INFECTION CAN CAUSE VERY SERIOUS CONSEQUENCES FOR AN INDUSTRIAL NETWORK.

TWO EXTREMES

Maintaining the stable, continuous and proper running of a technological process is the main task for ICS. The proper, uninterrupted operation of a technological process — be it power generation, water treatment etc. — is the key task of any industrial enterprise. If that technological process is disturbed it may lead to lost profits or even the loss of business, lives, or, in some cases, even a technological disaster.

When dealing with ICS, the popular principle is "If it ain't broken, don't fix it". This has worked well in stable environments. However, modern ICS environments cannot be called stable: they are subject to dramatic changes. Contractors reserve the capability to remotely access ICS to introduce real-time changes, update software versions and configurations; uncontrolled use of personal devices and removable media further complicates the situation. To comprehensively address this problem, ICS needs security procedures typical for standard corporate IT systems, such as auditing, testing for intrusion, scanning for vulnerabilities and training courses for the personnel. These procedures are often lacking, however.

Another extreme is many ICS systems, once they are commissioned, remain formally preserved in the same state for many years while they are in use. Strict corporate regulations and standards prohibit any changes or modifications to a once-certified system, even operating system or software security updates.

GIVEN THE SPECIFIC CHARACTERISTICS OF ICS, THERE IS NO SIMPLE SOLUTION THAT CAN ENSURE COMPREHENSIVE PROTECTION FROM THREATS.

HOW TO ENSURE ICS SECURITY?

Kaspersky Lab follows a comprehensive, process-oriented approach to ensuring the cybersecurity of industrial systems. Our security concept is based on the marriage of unique protection technologies — which do not affect the technological process — with a complex of organizational measures to ensure IT security. Kaspersky Lab's approach helps to ensure protection from both regular malware and sophisticated targeted attacks.

PROTECTION MEASURES

Today, Kaspersky Lab provides the following protection technologies which have been specifically developed for use in ICS environments:

- **Default-deny as a standard policy.** In default-deny mode, ICS works in a protected environment which only allows to run programs required for the technological process to function. All unknown and unwanted applications, including malicious programs, are blocked. Thus, a secure running environment is created with minimum load on system resources.

- **Proactive protection** against unknown malicious programs and automatic protection against exploits**.** The technology scans executable programs, assessing the security of each application by monitoring its activities when in operation.

- **"Device Control" technology** helps to manage removable devices (USB storages, GPRS modems, smartphones, USB network cards) and create limited lists of permitted devices and the users who can access them.

- **An All-in-one IT Security Console** helps to monitor and control all solutions to ensure IT security. With the single management console, admins can install, configure and manage security, and access reports.

- **Integration with SIEM** (using special connectors). Allows admins to export information about security incidents at protected nodes of the technological network into the corporate SIEM system.

ORGANIZATIONAL MEASURES

To improve IT security levels and ICS stability, Kaspersky Lab offers a set of measures as follows:

- An audit of industrial IT assets, technological processes and the methods in place to protect them.

- Threat modeling for specific industrial objects.

- Implementing technical facilities to ensure IT security.

- Trainings for employees, helping to dramatically reduce human factors in the event of an attack.

- A service to investigate incidents and eliminate their consequences.

- Recommendations on the development and update of industrial IT security regulations.

Following this approach, Kaspersky Lab is successfully working with large clients (including state organizations) across the world, implementing industrial network security projects

IF YOU NEED KASPERSKY LAB'S ASSISTANCE
IN IMPROVING IT SECURITY AT ICS, YOU CAN CONTACT US
AT INDUSTRIAL@KASPERSKY.COM.