Kaspersky ICS CERT

kaspersky

ICS cyberthreats in 2023

What to expect

Evgeny Goncharov

22.11.2022 Version 1.0

Cybersecurity incidents were plentiful in 2022, causing many problems for industrial infrastructure owners and operators. However, luckily, we did not see any sudden or catastrophic changes in the overall threat landscape – none that were difficult to handle, despite many colorful headlines in the media.

As we see it, the coming year looks to be much more complicated. Many people may be surprised by unexpected twists and turns, though we should already be examining these eventualities today. Below we share some of our thoughts on potential developments of 2023, though we cannot claim to be providing either a complete picture or a high degree of precision.

As we analyze the events of 2022, we must profess that we have entered an era where the most significant changes in the threat landscape for industrial enterprises and OT infrastructures are mostly determined by geopolitical trends and the related macroeconomic factors.

Cybercriminals are naturally cosmopolitan; however, they do pay close attention to political and economic trends as they chase easy profits and ensure their personal safety.

APT activity, which is traditionally ascribed to intelligence agencies of various governments, always occurs in line with developments in foreign policy and the changing goalposts inside countries and inter-governmental blocks.

Developments in the APT world

Internal and external political changes will deliver **new directions for APT activity**.

Changes in attack geography

Attack geography will inevitably change following transformations of existing and the emergence of new tactical and strategic alliances. As alliances shift, we see cybersecurity tensions arise between countries where such tensions had never existed. Yesterday's allies become today's targets.

Changes in industry focus

We are going to **see APT activity change the focus on specific industries** very soon because the evolving geopolitical realities are closely intertwined with economic changes. Therefore, we should soon see attacks targeting the following sectors representing the real economy:

- Agriculture, manufacturing of fertilizers, agricultural machinery and food products – all as a result of upcoming food crises and shifting food markets;
- Logistics and transport (including transportation of energy resources) due to the on-going changes in global logistics chains;
- The energy sector, mining and processing of mineral resources, non-ferrous and ferrous metallurgy, chemical industry, shipbuilding, instrument and machine-tool manufacturing, as the availability of these companies' products and technologies is part of the foundation for the economic security of both individual countries and political alliances;
- The alternative energy sector, specifically where it is on the geopolitical agenda;
- High-tech, pharmaceuticals and medical equipment producers, since these are integral for ensuring technological independence.

Continuing attacks on traditional targets

Naturally, we will still see APT attacks on **traditional targets**, with the main APT attack focus definitely including:

- enterprises in the military industrial complex, with geopolitical tensions, confrontations escalating to red alert status, along with the rising possibilities of military confrontations being the main drivers for the attackers;

- the government sector – we expect attacks to focus on information gathering regarding government initiatives and projects related to the growth of industrial sectors of the economy;
- critical infrastructure – attacks aiming to gain a foothold for future use, and sometimes, for instance when conflicts between specific countries are in the "hot" phase, the goal may even be to inflict immediate and direct damage.

Other changes in the threat landscape

Other important changes in the threat landscape which we already see and which we believe will increasingly contribute to the overall picture include the following:

- A rising number of hacktivists "working" to internal and external political agendas. These attacks will garner more results – quantity will begin to morph into quality.
- A growing risk of volunteer ideologically and politically motivated insiders, as well as insiders working with criminal (primarily ransomware) and APT groups – both at enterprises and among technology developers and vendors.
- Ransomware attacks on critical infrastructure will become more likely – under the auspices of hostile countries or in countries unable to respond effectively to attacks by attacking the adversary's infrastructure and conducting a full-blown investigation leading to a court case.
- Cybercriminals' hands will be untied by degrading communications between law enforcement agencies from different countries and international cooperation in cybersecurity grinding to a halt, enabling threat actors to freely attack targets in 'hostile' countries. This applies to all types of cyberthreats and is a danger for enterprises in all sectors and for all types of OT infrastructure.
- Criminal credential harvesting campaigns will increase in response to the growing demand for initial access to enterprise systems.

Risk factors due to geopolitical ebb and flow

The current situation forces industrial organizations into making an extremely complicated choice – which products and from which vendors should they be using and why.

On the one hand, we are seeing **failing trust relationships** in supply chains for both products and services (including OEM), which in turn increases the risks in using many of the products companies are used to:

- It becomes more difficult to deploy security updates when vendors end support for products or leave the market.
- This is equally applicable to degrading quality of security solutions when regular updates cease due to security vendors leaving the market.
- We cannot totally rule out the possibility of political pressure being applied to weaponize products, technologies and services of some minor market players. When it comes to global market leaders and respected vendors, however, we believe this to be extremely unlikely.

On the other hand, searching for alternative solutions can be extremely complicated. Products from local vendors, whose **secure development culture**, as we have often found, is usually significantly inferior to that of global leaders, are likely to have 'silly' security errors and **zero-day vulnerabilities**, rendering them easy prey for both cybercriminals and hacktivists.

Organizations based in countries where the political situation does not require addressing the above issues, should still consider the **risk factors which affect everyone**:

- The quality of threat detection decreases as IS developers lose some markets, resulting in the expected loss of some of their qualified IS experts. This is a real risk factor for all security vendors experiencing political pressure.
- The communication breakdowns between IS developers and researchers located on opposite sides of the new 'iron curtain' or even on the same side (due to increased competition on local markets) will undoubtedly decrease the detection rates of security solutions that are currently being developed.
- Decreasing CTI quality – unfounded politically motivated cyberthreat attribution, exaggerated threats, lower statement validity criteria due to political pressure and in an attempt to utilize the government's political narrative to earn additional profits.
- Government attempts to consolidate information about incidents, threats and vulnerabilities and to limit access to this information detract from overall awareness, since information may sometimes be kept under wraps without good reasons.
  And at the same time, this results in an increased risk of confidential data leaks (example: PoC of an RCE published by mistake in a national vulnerability database). This issue could be addressed by building broad cybersecurity capacity in the public sector to ensure that responsible

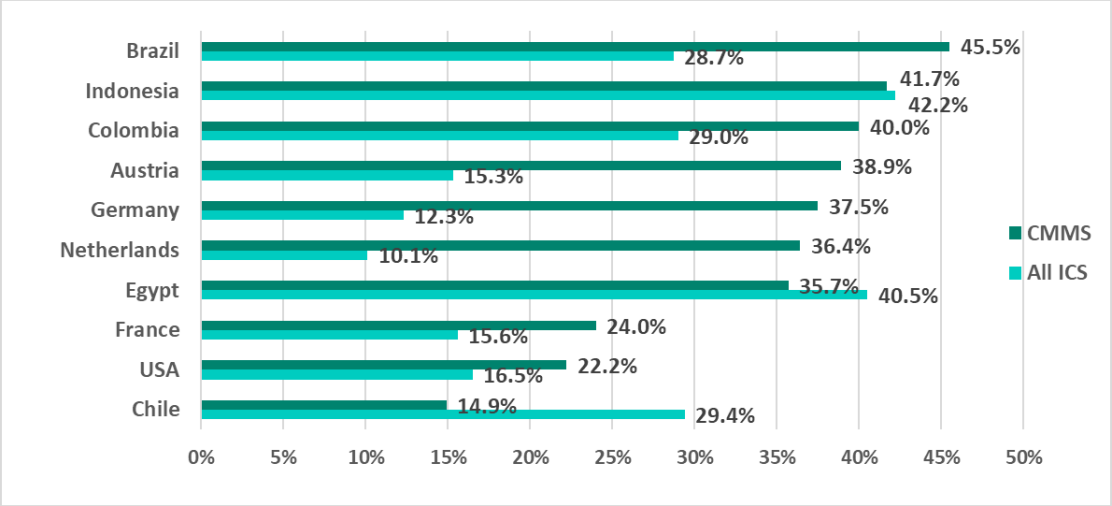
treatment of sensitive cybersecurity information and efficient coordinated vulnerability disclosure can always be guaranteed.

- Additional IS risks due to the growing role of governments in the operations of industrial enterprises, including connections to government clouds and services, which may sometimes be less protected than some of the best private ones.

Additional technical and technological risk factors

- Digitalization in a race for higher efficiency – IIoT and SmartXXX (including predictive maintenance systems and digital twin technology) leads to significantly increased attack surfaces. This is confirmed by the attack statistics on CMMS (Computerized Maintenance Management Systems).

Top 10 countries ranked by the percentage of CMMS attacked in H1 2022



It is significant that in this Top 10 ranking by the percentage of attacked CMMS in H1 2022 we see the traditionally 'secure' countries which are not seen in rankings based on the overall percentage of OT computers attacked in the country or based on the percentage of attacked OT computers by sector.

- Rising energy carrier prices and the resulting rises in hardware prices, on the one hand, will force many enterprises to abandon plans to deploy on premise infrastructure in favor of cloud services from third party vendors (which increases IS risks). In addition, this will negatively impact budgets allocated for IT/OT security.
- The deployment of various unmanned vehicles and units (trucks, drones, agricultural equipment and so forth), which can be abused as either targets or tools for attacks.

Most noteworthy techniques and tactics in future attacks

Let's not indulge in any fantastic suppositions about tactics and techniques used by the most advanced attackers, such as APTs connected to intelligence agencies in leading countries, as we can then be waylaid by unexpected twists and turns. Let's also not discuss the tactics and techniques used by the numerous threat actors at the other end of the spectrum – the least qualified ones, since it is unlikely that they will come up with something interesting or new, and the security solutions already in place at most organizations can effectively block their attacks.

Let's focus instead on the middle of the spectrum – the techniques and tactics used by the more active APT groups, whose activity is usually ascribed as being in line with the interests of countries in the Middle East and the Far East, as well as being used by more advanced cybercriminals, such as ransomware gangs.

Based on our experience of investigating such attacks and the related incidents, we believe that ICS cybersecurity specialists need to focus on the following tactics and techniques:

- Phishing pages and scripts embedded on legitimate sites.
- The use of Trojanized "cracked" distribution packages, "patches" and key generators for commonly used and specialist software (this will be stimulated by rising license costs and the departure of vendors from certain markets due to political pressure).
- Phishing emails about current events with especially dramatic subjects, including events the root causes of which are political in nature.
- Documents stolen in previous attacks on related or partner organizations being used as bait in phishing emails.
- The distribution of phishing emails disguised as legitimate work correspondence via compromised mailboxes.
- N-day vulnerabilities – these will be closed even more slowly as security updates for some solutions will become less accessible.
- Exploiting foolish configuration errors (such as failing to change default passwords) and zero-day vulnerabilities in products from 'new' vendors, including local ones. Mass rollouts of such products are inevitable, despite the serious doubts about the developers' security maturity.
  For instance, recommendations such as "enter password xyz in the password field" can be found in installation instructions and user manuals in a surprising number of products from small 'local' vendors. Furthermore,

you will rarely find information about vulnerabilities inherited from common components and OEM technologies on such vendors' websites.
- Exploiting inherent security flaws in cloud services from 'local' service providers and government information systems (see above).
- Exploiting configuration errors in security solutions. This includes the possibility of disabling an antivirus product without entering an administrator password (antivirus is almost useless if an attacker can easily disable it). Another instance would be the weak security of the IS solution centralized management systems. In this case, IS solutions are not only easy to bypass, but they can also be used to move laterally – for instance to deliver malware or to gain access to 'isolated' network segments and to bypass access control rules.
- Using popular cloud services as CnC – even after an attack is identified, the victim might still be unable to block it because important business processes could depend on the cloud.
- Exploiting vulnerabilities in legitimate software, for instance, using DLL Hijacking and BYOVD (Bring Your Own Vulnerable Driver) to bypass endpoint security solutions.
- Distributing malware via removable media to overcome air gaps, in those instances where air gaps actually do exist.

Some final thoughts

When writing about potential future issues, we did not aim to describe a full set of potential threats. Instead, we attempted to convey the impression of a global character of upcoming developments and to encourage our readers to assess those issues (including similar ones not mentioned specifically in this paper) which are most relevant to their organization.

We included only those developments and described only those risks which we believe to be most widespread and generally applicable to many organizations in many countries. Therefore, we kept the predictions less specific on purpose.

Only you can determine which threats are relevant for you. Naturally, if you need some assistance with this rather complicated task, we are always ready to help.

Our predictions are the sum of the opinions of our entire team based on our collective experience in researching vulnerabilities and attacks and investigating incidents, as well as our personal vision of the main vectors driving changes in the threat landscape. We will be very glad if any of our negative predictions do not come true in 2023.

We are always happy to discuss our ideas and we welcome your questions at ics-cert@kaspersky.com.

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