Developments and trends in the ICS threat landscape in Europe, Q1 2022 – Q1 2023

This report is based on an analysis of statistical data collected through the Kaspersky Security Network (KSN), a distributed antivirus network. The data was received from those KSN users who have given their voluntary consent to have data anonymously transferred from their computers and processed for the purpose described in the KSN Agreement for the Kaspersky product installed on their computer.

The information transferred by the user includes only the types and categories of data described in the relevant KSN Agreement. This information not only assists in analyzing the threat landscape, but is also needed to detect new threats, including targeted attacks and advanced persistent threats (APT).

Executive Summary

In Q1 2023, regions of Europe continued to be the ones least affected by attacks on OT computers. Western and Northern Europe ranked **14th** and **13th** out of 14 regions worldwide in terms of the percentage of OT computers on which malicious objects were detected. Southern and Eastern Europe ranked **10th** and **9th**, respectively.

Countries: Although the average numbers for the region were low, the percentage of attacked OT computers varied from **6.66%** in Luxembourg to **35.3%** in Serbia.

The most significant increases in the percentage of attacked OT computers, compared to the previous quarter's values, were observed in the following countries:

- United Kingdom, **+2.5 p.p.**
- Albania, **+2.4 p.p.**
- Belgium, **+2.3 p.p.**

Threats: Malicious scripts and phishing pages, denylisted internet resources, and **spyware** were the types of threats most frequently detected on OT computers.

The percentage of threats distributed via the **internet** increased in 3 out of 4 European regions, with an average increase of **+1.2 p.p.** Eastern Europe was the only region that showed a decrease in internet threats.

Internet threats: In Q1 2023, the internet remained the dominant source of threats for OT computers in Europe. Denylisted internet resources, malicious scripts, and phishing pages were the most prevalent sources of this type of threat.

Industries: The rates of attacked OT computers in Q1 2023 for the industries selected for this report were as follows:

- **Energy:** The rates of attacked OT computers in the Energy sector varied from **10.8%** in Western Europe to **17%** in Southern Europe. Northern Europe experienced a significant rise of **+2.5 p.p.**
- **ICS Engineering & integration:** This industry was the most attacked in Northern Europe, with a rate of **21.2%**. The percentage of ICS computers attacked nearly doubled compared to the values in Q4 2022. It was also the second most attacked industry across Europe.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

- **Building Automation:** In Q1 2023, this industry had the highest attack rate among all European regions, averaging **27.4%**. Southern Europe had the highest percentage at **39.3%**, indicating a significant risk for OT environments. After four quarters of a downtrend since the beginning of 2022, the attack percentage increased by an average of **+7.4 p.p.** across the regions, compared to an average decrease of **-3.3 p.p.** in Q4 2022. The new wave of ongoing phishing campaigns in Southern Europe was the most likely reason for such a significant growth.
- **Manufacturing:** The percentage values for Q1 2023 remained close to those in Q4 2022. Southern and Eastern Europe saw a decreasing trend throughout 2022, while Western and Northern regions experienced a bounce-back with an average increase of **+0.8 p.p.**

For more information, please contact: ics-cert@kaspersky.com

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

Methodology

The statistical data presented in this report was received from OT computers protected by Kaspersky products that Kaspersky ICS CERT categorizes as part of the industrial infrastructure at organizations. This group includes Windows computers that perform one or several of the following functions:

- Supervisory control and data acquisition (SCADA) servers;
- Data storage servers (Historian);
- Data gateways (OPC);
- Stationary workstations of engineers and operators;
- Mobile workstations of engineers and operators;
- Human Machine Interface (HMI);
- Computers used for industrial network administration;
- Computers used to develop software for industrial automation.

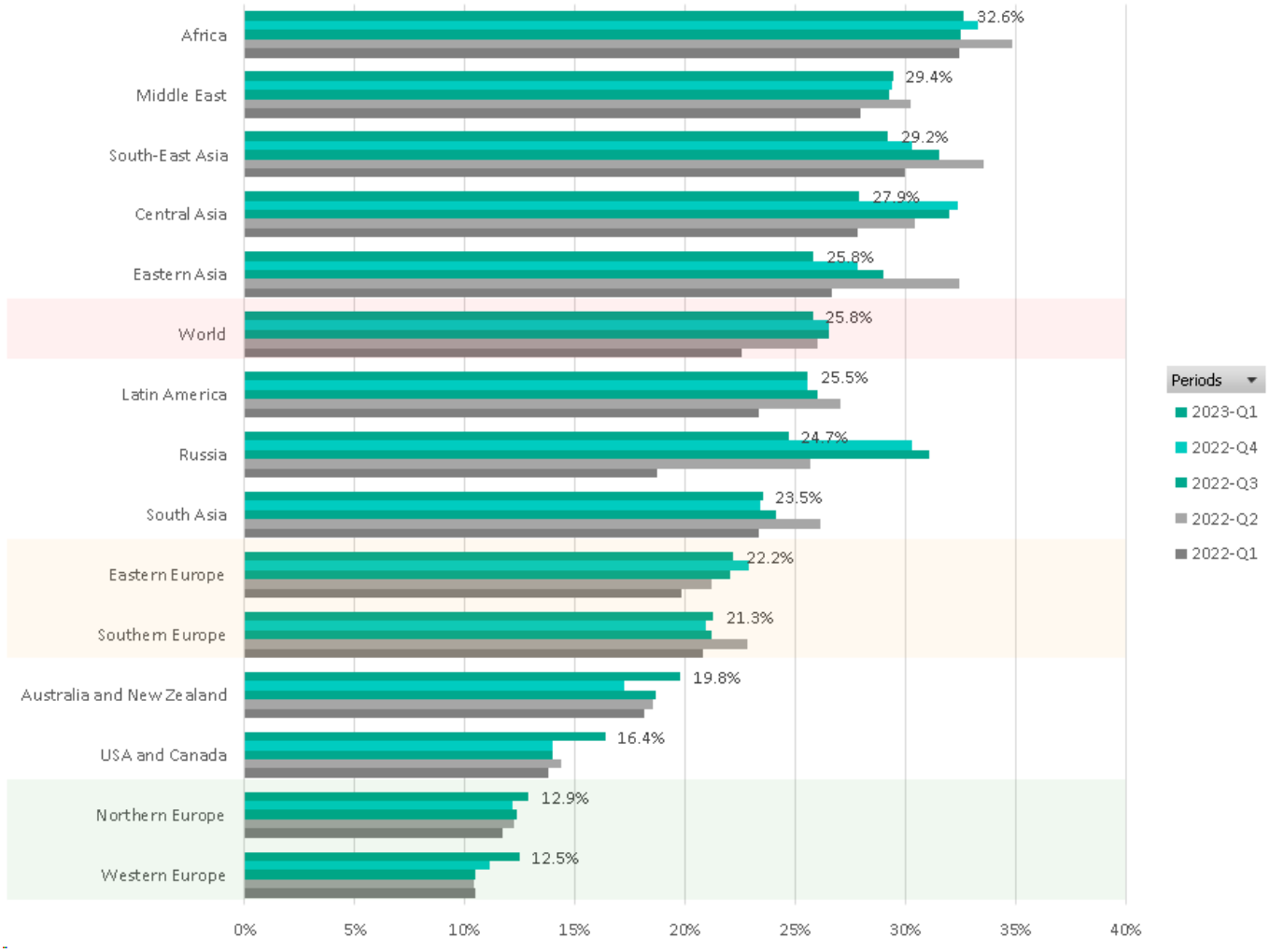
For the purposes of this report, “attacked computers” are those on which Kaspersky security solutions blocked one or more threats during the reporting period (in the diagrams below, a reporting period can be a month, a six-month period or a year, depending on the context). When determining the percentages of machines on which malware infections were prevented, we use the ratio of the number of computers attacked during the reporting period to the total number of computers in our sample from which we received depersonalized information during the reporting period.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

Statistics on attacked OT computers in Europe

Region in the world

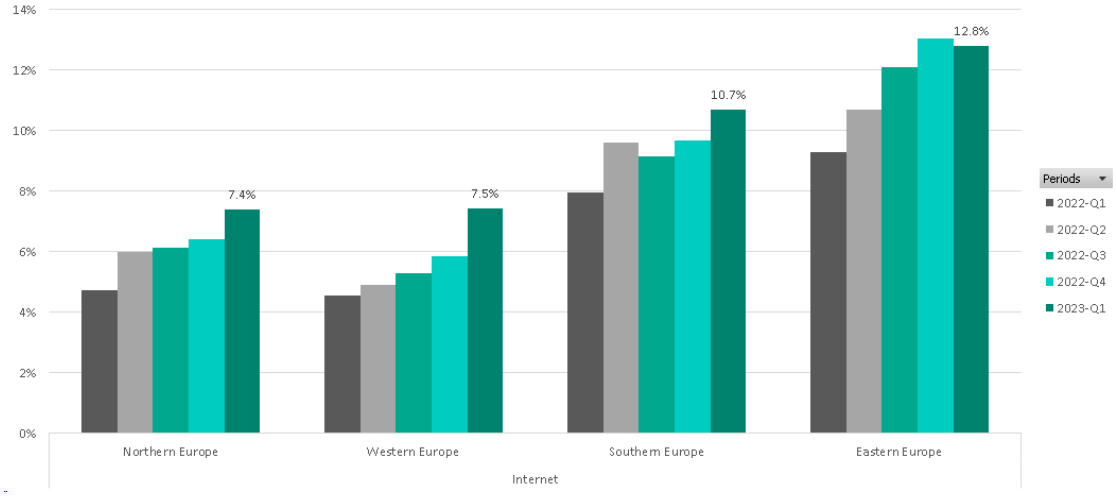
In Q1 2023, European regions had some of the lowest percentages of attacked OT computers worldwide, placing them among the least affected regions. The percentage of attacked OT computers in Europe was less than half the global average.



Percentage of attacked OT computers in the world and by region
Q1 2022 - Q1 2023

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

In Q1 2023, the percentage of attacked OT computers increased by an average of 0.4 p.p. compared to Q4 2022. Eastern Europe was the only region where the percentage decreased (-0.7 p.p.), while Northern (+0.7 p.p), Southern (+0.4 p.p.), and Western (+1.4 p.p) Europe experienced growth.



Percentage of attacked OT computers regions of Europe, Q1 2022 – Q1 2023

Statistics by country

In Q1 2023, countries in each of the European regions displayed mixed attacked OT computer percentage values. Some countries, such as Belarus and Estonia, had significantly lower percentages compared to Q4 2022, while others, like the United Kingdom, Albania, and Belgium, experienced a significant rise.

The percentage of attacked OT computers on which malware was blocked ranged from 6.7% in Luxembourg to 35.3% in Serbia.

☞ *The threat landscape can vary by country because of the following factors:*

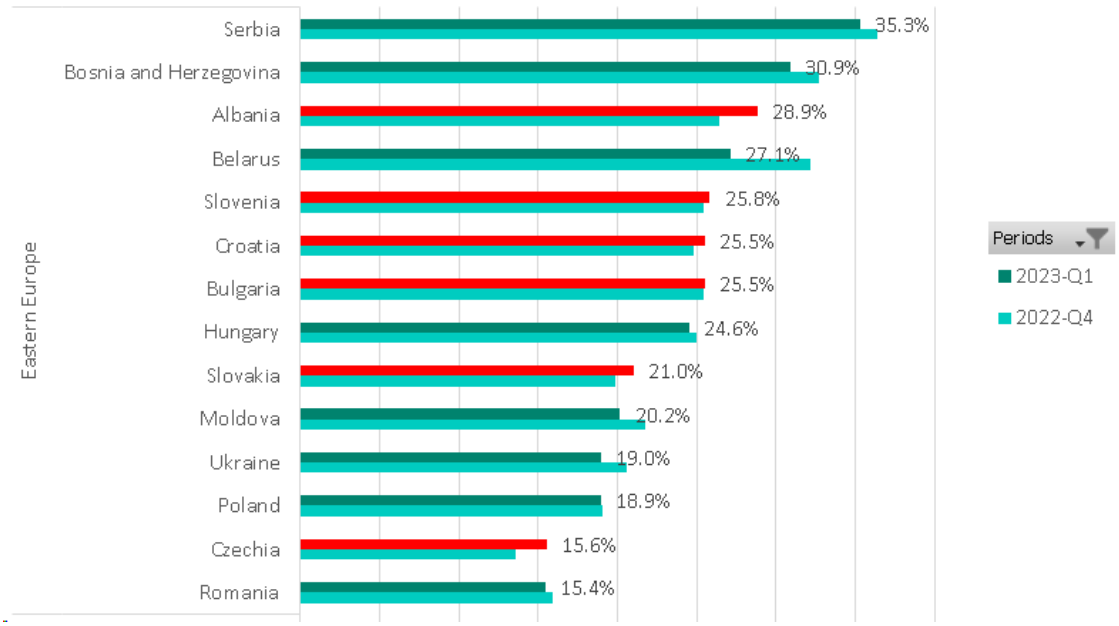
- *differences in the overall security maturity;*
- *differences in business processes, relations within the sector / industry ecosystem, work style habits, and cultural specifics;*
- *current focus of threat actors.*

The most significant increases in the percentage of attacked OT computers, compared to the previous quarter, were observed in the following countries:

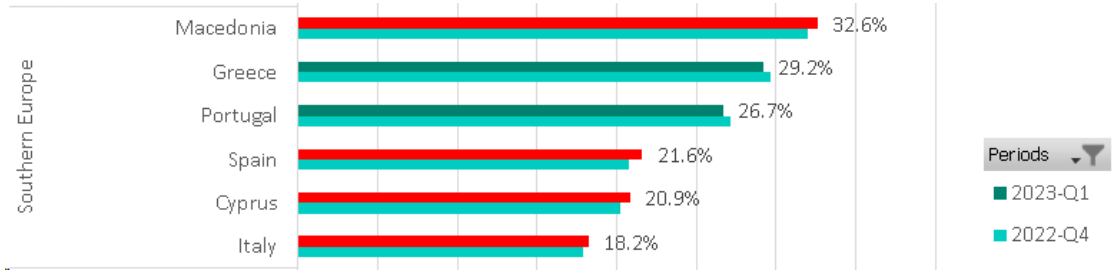
- United Kingdom, +2.5 p.p.
- Albania, +2.4 p.p.;
- Belgium, +2.3 p.p.

On the next four charts, bars are colored red in cases where there was growth in Q1 23 compared to Q4 22.

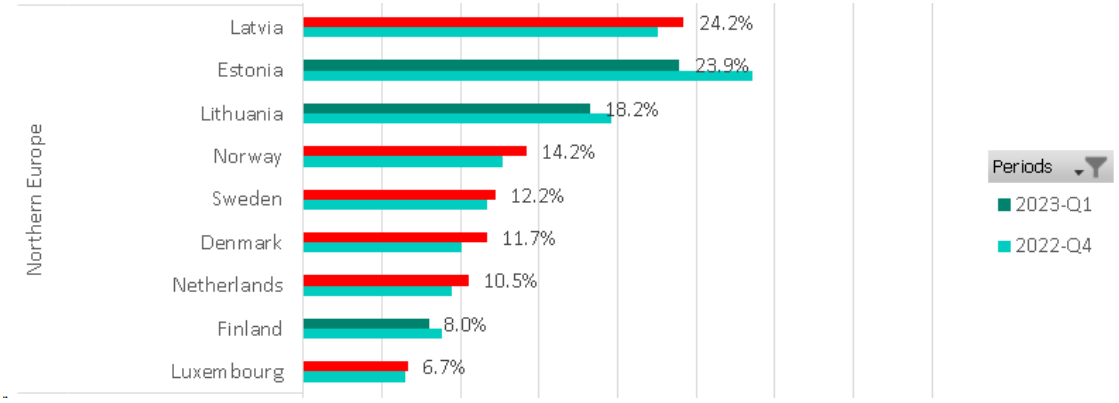
**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers in Eastern Europe by country
Q4 2022 – Q1 2023

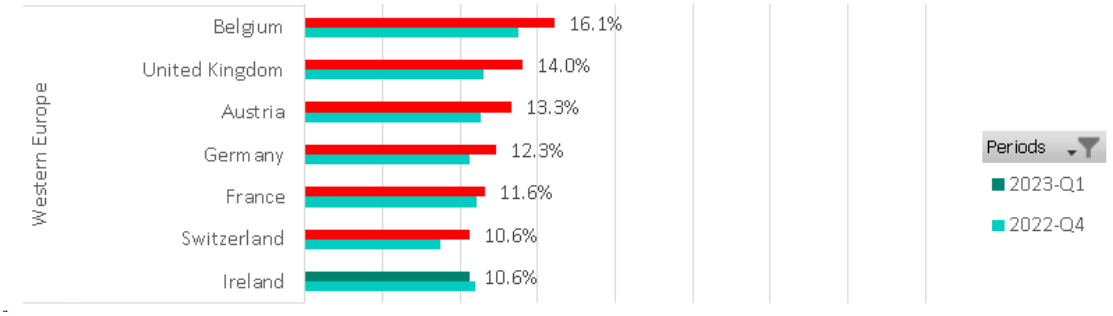


Percentage of attacked OT computers in Southern Europe by country
Q4 2022 – Q1 2023



Percentage of attacked OT computers in Northern Europe by country
Q4 2022 – Q1 2023

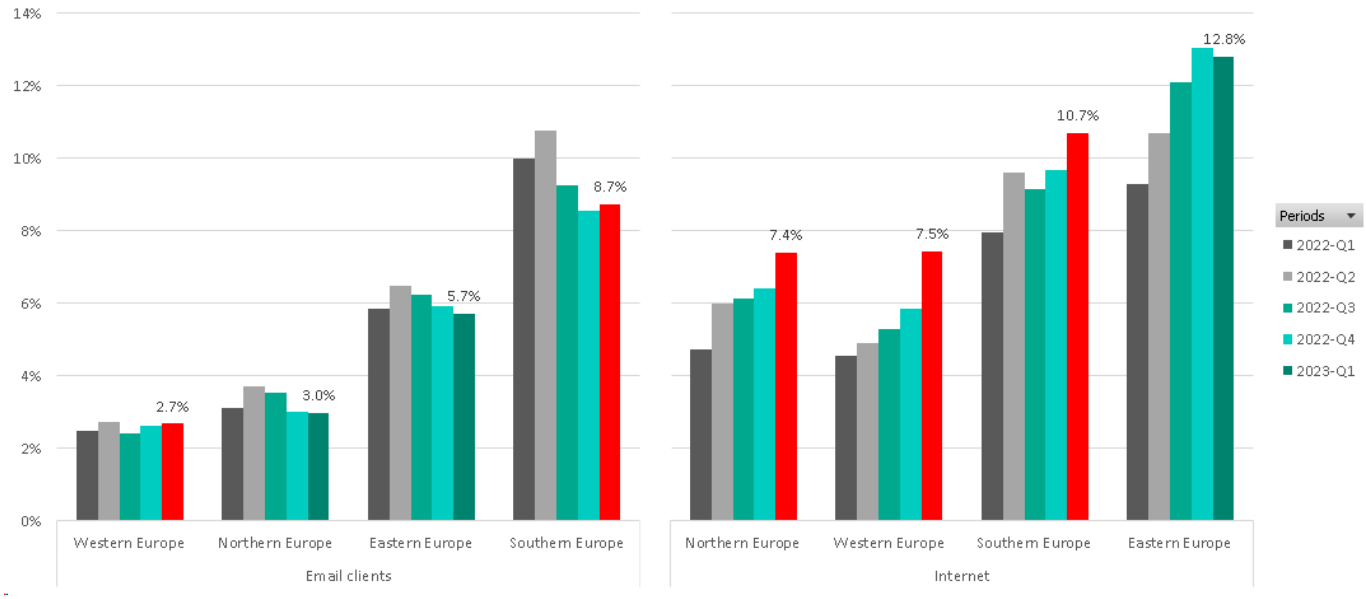
**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers in Western Europe by country Q4 2022 – Q1 2023

Threat sources

In Q1 2023, most European regions continued to exhibit higher percentages of internet threats and lower percentages of threats delivered via email clients compared to Q4 2022. Eastern Europe was the only region where percentages for both threat sources were lower in Q1 2023 than in Q4 2022.



Email clients and Internet sources of threats detected on OT computers in Europe by regions, Q1 2022 - Q1 2023

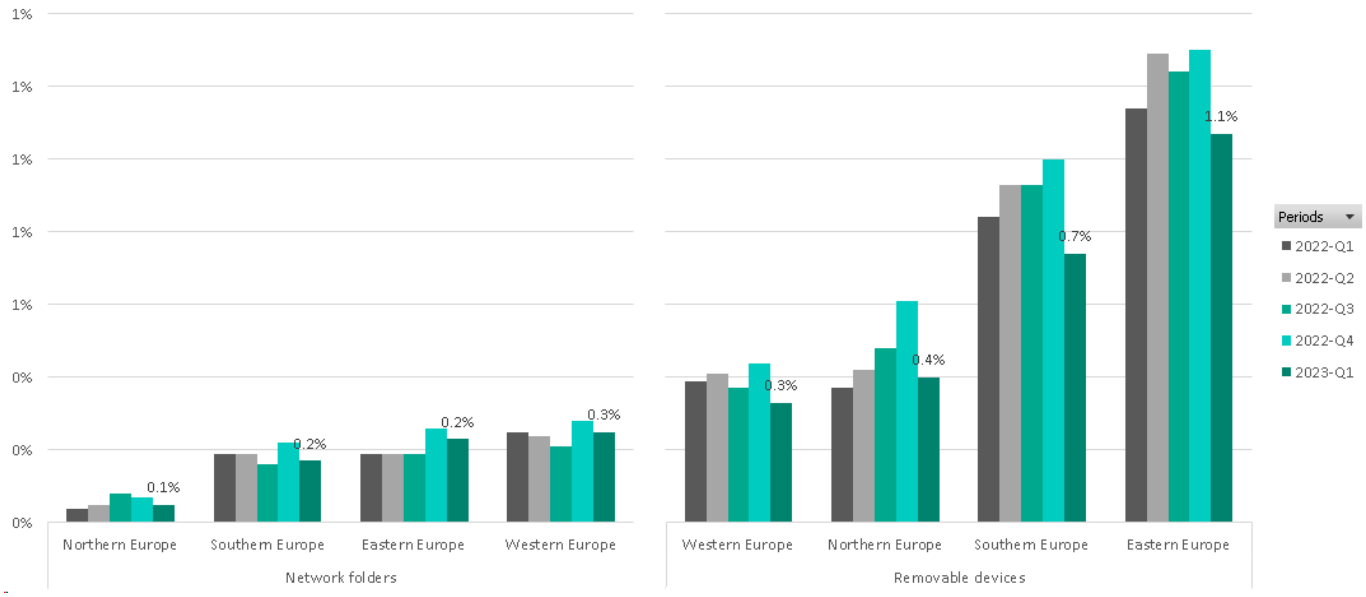
A continuous increase in the percentage of OT computers attacked through the internet from Q1 2022 to Q1 2023, along with a steady decrease in attacks through email clients, maybe a reflection of changes in the tactics employed by threat actors to deliver malware. The traditional method of attaching malware to a phishing email is becoming less effective, prompting threat actors to employ alternative strategies to evade detection. These strategies include encrypting the attachment or providing users with phishing links that deliver the malware via HTTPS when opened.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

The surge in the percentages of internet threats in Northern, Western, and Southern Europe can be attributed to increases in the percentages of denylisted internet resources and malicious scripts and phishing pages (JS and HTML).

The percentage of threats distributed through email clients decreased slightly in all regions except Southern Europe, which bounced back in Q1 2023 after significant decrease since Q2 2022.

The percentage of threats distributed via removable devices decreased by an average of 25.8% compared to Q4 2022. This coincided with a small decrease in the percentage of threats distributed through network folders.



Network folders and removable devices as sources of threats detected on OT computers in Europe by region, Q1 2022 – Q1 2023

Network folders and removable devices are commonly targeted by self-propagating threats such as viruses and worms. However, the modern threat landscape reveals that various types of malware, including spyware, crypto-miners, and ransomware, often incorporate worm-like functionality to facilitate automated lateral movement.

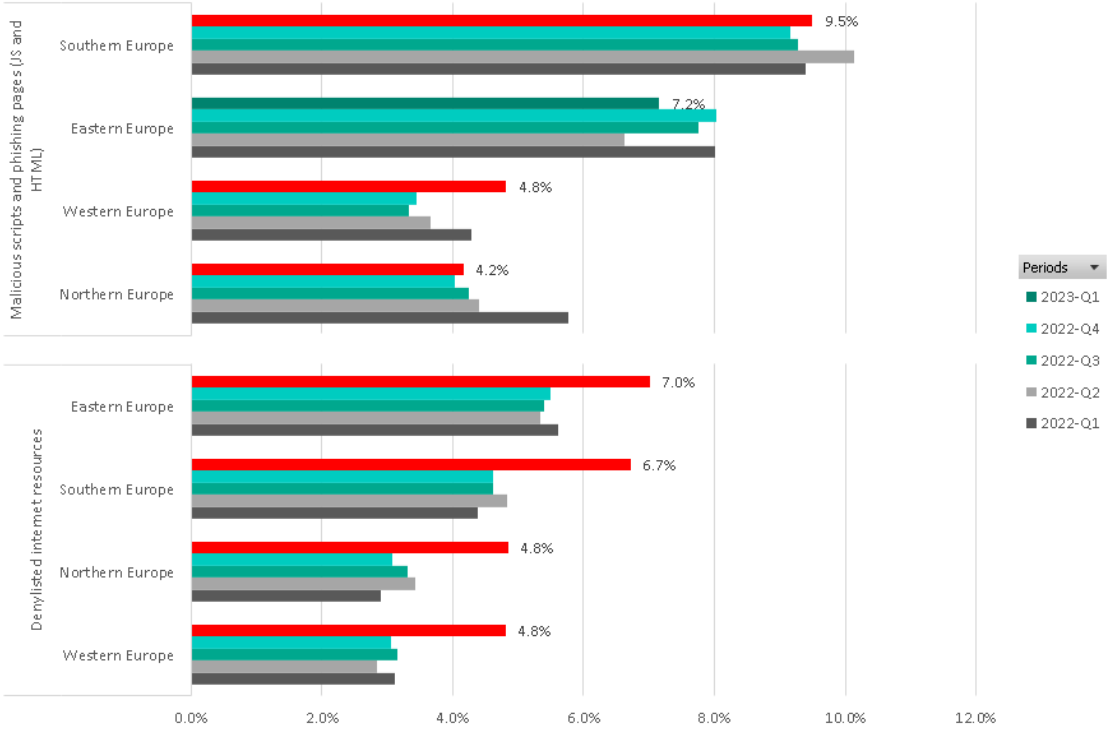
Curiously, a significant number of threats spread through removable media, even without self-propagation capabilities, relying instead on the actions of unsuspecting users. An analysis of data for Q1 2023 indicates that the decrease in the percentage of threats distributed through removable media was primarily driven by changes in user behavior. It is worth noting that worms and viruses still persist, despite the overall decrease in the percentage of threats that attack OT computers through removable media.

Threat types

In Q1 2023, the percentage of malicious scripts and phishing pages bounced back after a steady slowdown since the beginning of 2022 in most regions of Europe. However, this trend did not

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

hold true for Eastern Europe, which experienced a decrease in the percentage of malicious scripts and phishing pages in Q1 2023 after increases in the previous quarters.

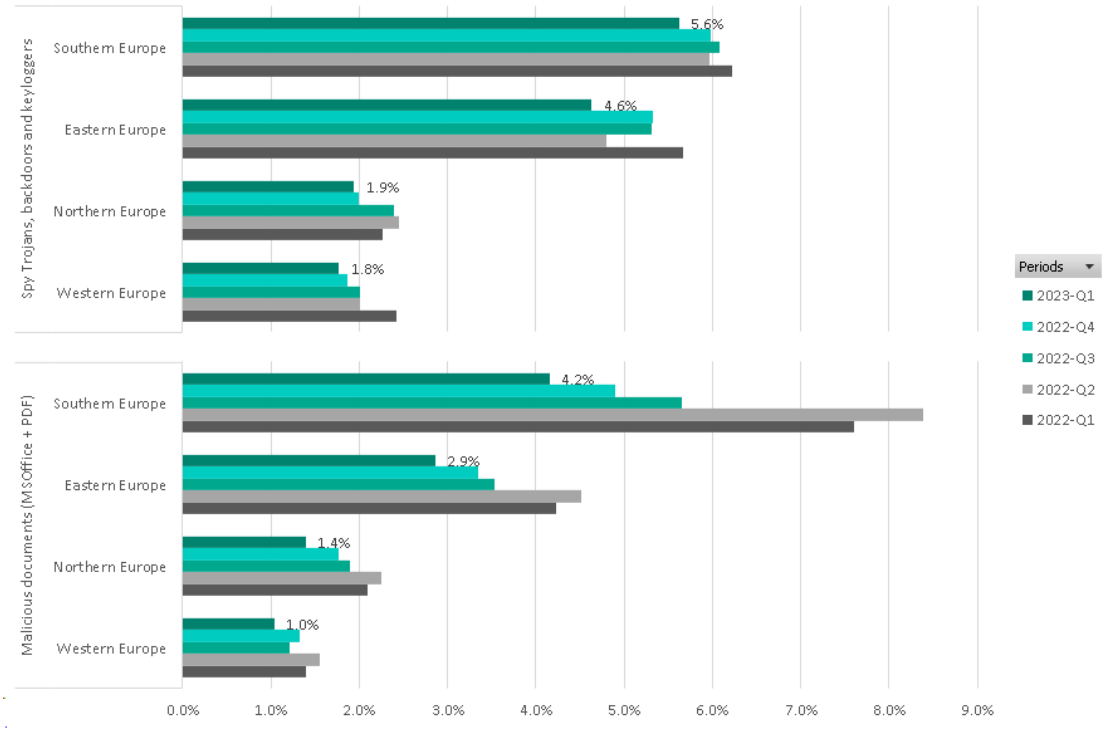


Percentage of attacked OT computers* in regions of Europe by threat type
Q1 2022 – Q4 2023

The percentage of denylisted internet resources surged by +1.8 p.p. on average in Q1 2023 across all European regions. This significant rise can be attributed primarily to the increased detection of malicious notification settings for browsers. These notifications led users to malicious pages or scripts, facilitating the infection process.

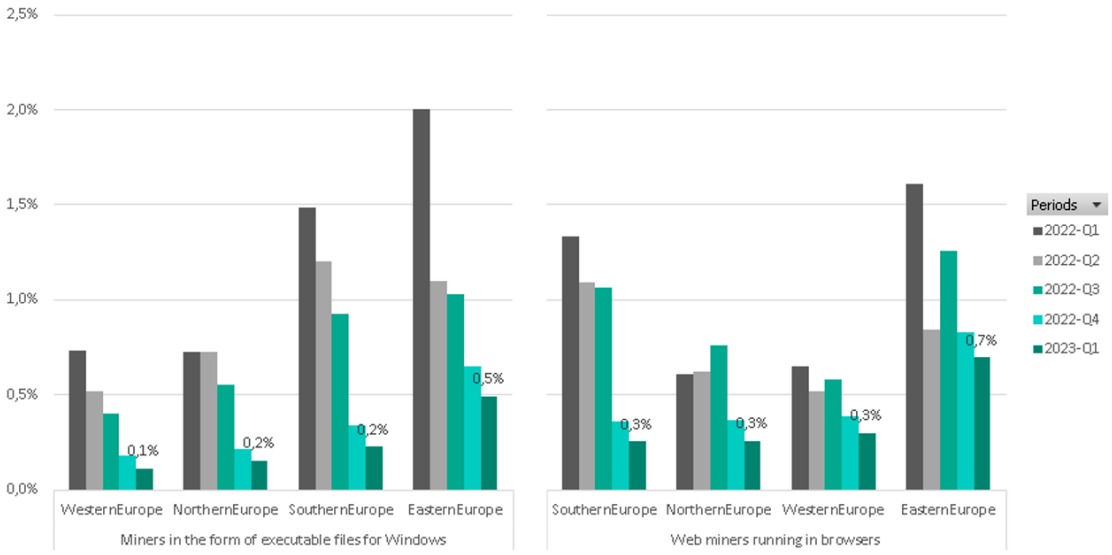
Simultaneously, the percentages of malicious documents and spyware have mostly been slightly decreasing since Q2 2022. This trend suggests that fewer threats were able to reach OT systems due to the detection and blocking of initial-stage infections, such as blocking access to denylisted internet resources and malicious scripts.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers* in regions of Europe by threat type
Q1 2022 – Q1 2023

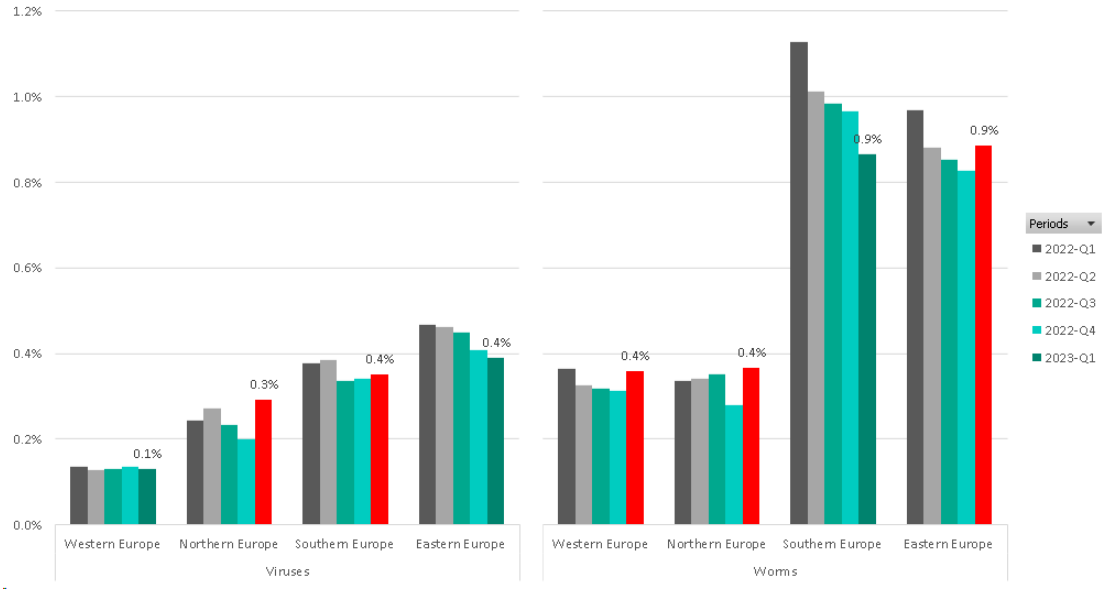
In Q1 2023, all European regions experienced a decrease in crypto-miner attacks on both Windows and browser platforms. This can be attributed to the effectiveness of denylisting internet resources, as it effectively blocks various parts of the crypto-mining infrastructure used by threat actors. By preventing crypto-miners from being downloaded, connecting to servers, and updating, denylisting helps to mitigate the threat of crypto-mining attacks.



Percentage of attacked OT computers* in regions of Europe by threat types
Q1 2022 – Q1 2023

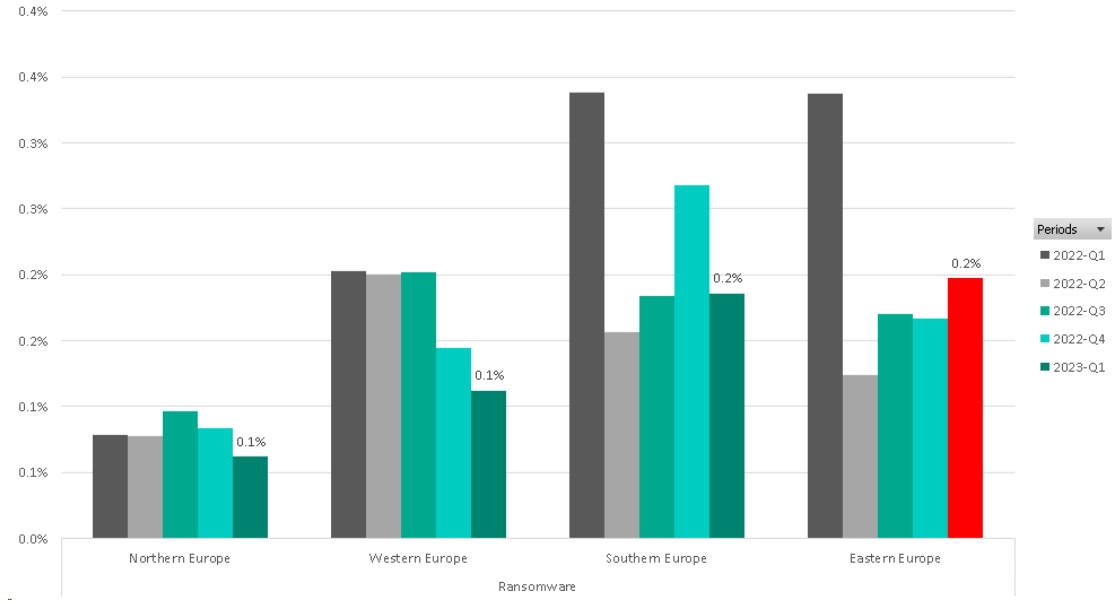
**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

The statistics on viruses and worms in Q1 2023 indicate a slight increase, breaking the downward trend observed in 2022. This suggests a potential shift in the threat landscape, with a resurgence in the prevalence of viruses and worms during this period.



Percentage of attacked OT computers* in regions of Europe by threat type
Q1 2022 – Q1 2023

The percentage of ransomware threats in Europe remained low in Q1 2023. Ransomware tends to be a rare threat because it is usually employed at the final stage of an attack kill chain, which can often be stopped and prevented at earlier stages of the attack. This suggests that security measures and defenses in place in Europe effectively mitigate the risk of ransomware attacks.



Percentage of attacked OT computers* in regions of Europe by threat type
Q1 2022 – Q1 2023

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

In most cases, denylisted internet resources, malicious scripts, and phishing pages are distributed via internet connections used by computers on the OT network. The connections can be proxied either through the company's IT / office communication channels (such as access to the corporate internet proxy or corporate email server, which is often seen being used by ICS engineers to exchange data), or via OT-specific external communication channels. The latter includes both legitimate connections, such as connections to and from remote sites, partner organizations, and contractor/supplier-controlled systems, and connections violating security policies (for example, via mobile modems or dual-homed networks).

If such 'initial' threats are detected on a high percentage of hosts in OT networks, this means that, overall, the security measures in place (in the country/industry) were not sufficient to block these threats before they reached OT-related hosts (where they were ultimately detected and blocked by endpoint protection).

The point above is also supported by statistics on self-propagating threats such as worms, cryptocurrency miners, and viruses. Most worms and viruses are legacy threats that have no active C&C infrastructure, and significant percentages mean that the security measures in place are not sufficient to prevent such threats from spreading via removable media, network shares, exploitation of network services, or account abuse. Such threats re-emerge from time to time. Even if an outbreak was cured, some of the threats could remain in backups (enabling them to cause the next outbreak).

The linear decrease in percentages of threats along the kill chain (from the initial vector to next-stage threats) means that each next stage in an attack is proportional to the previous stage – in other words, the more initial threats are passed to hosts the more next-stage threats will be delivered.

Spyware is a set of multifunctional tools used for unauthorized remote access, as well as exfiltration of confidential information or information used to deliver highly targeted next-stage payloads, including ransomware.

Ransomware is the last stage in the kill chain of many attacks. The theft, loss or leakage of sensitive corporate or technological information, as well as ransom payments, are obvious losses (e.g. financial) that a company could expect from such an incident.

At the same time, the more sophisticated threats could be delivered by threat actors using data leaked by next-stage spyware – such targeted threats could then be used to cause emergency stoppage, blackouts, or physical impact.

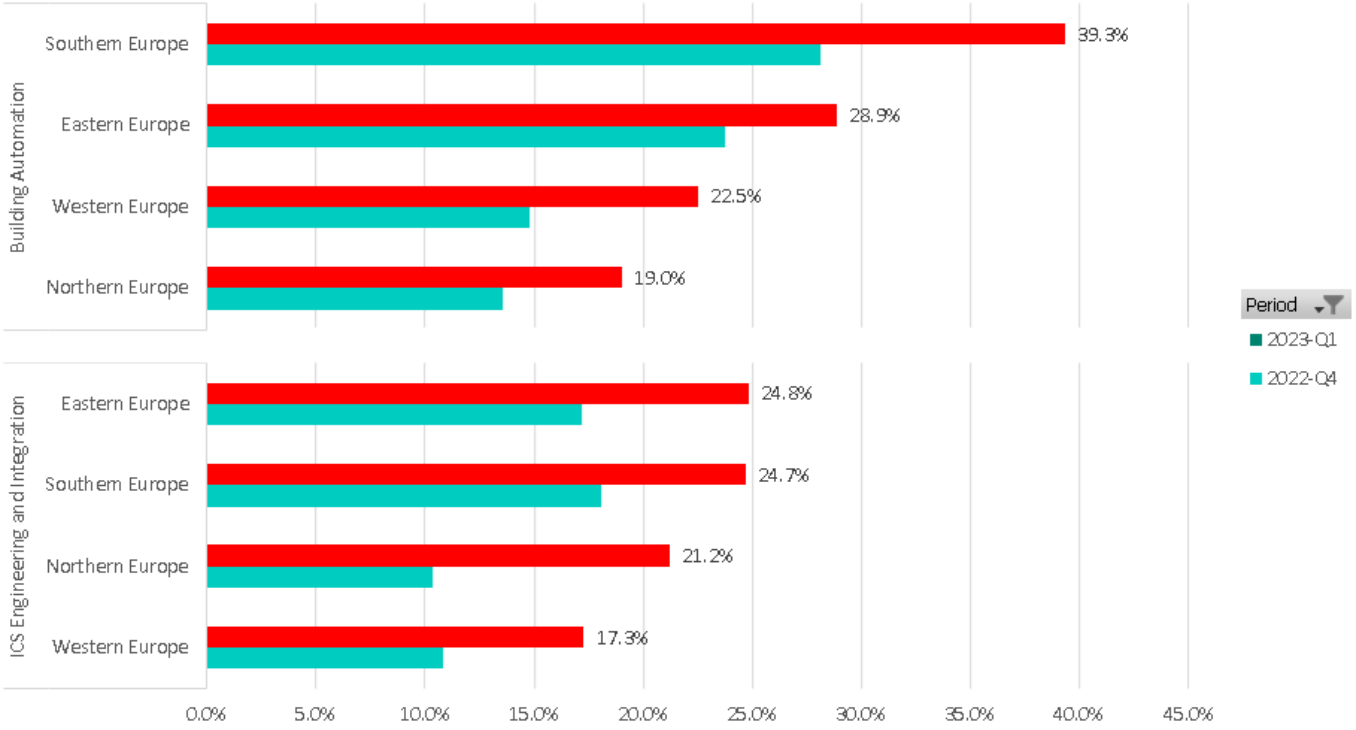
Industries in the region

Overview

In Q1 2023, the percentage of attacked OT computers in European regions varied significantly both across regions and across industries. Southern Europe experienced the most significant change, with a +11.2 p.p. increase in the Building Automation industry. Northern Europe followed closely with a +10.9 p.p. increase in the ICS Engineering industry.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

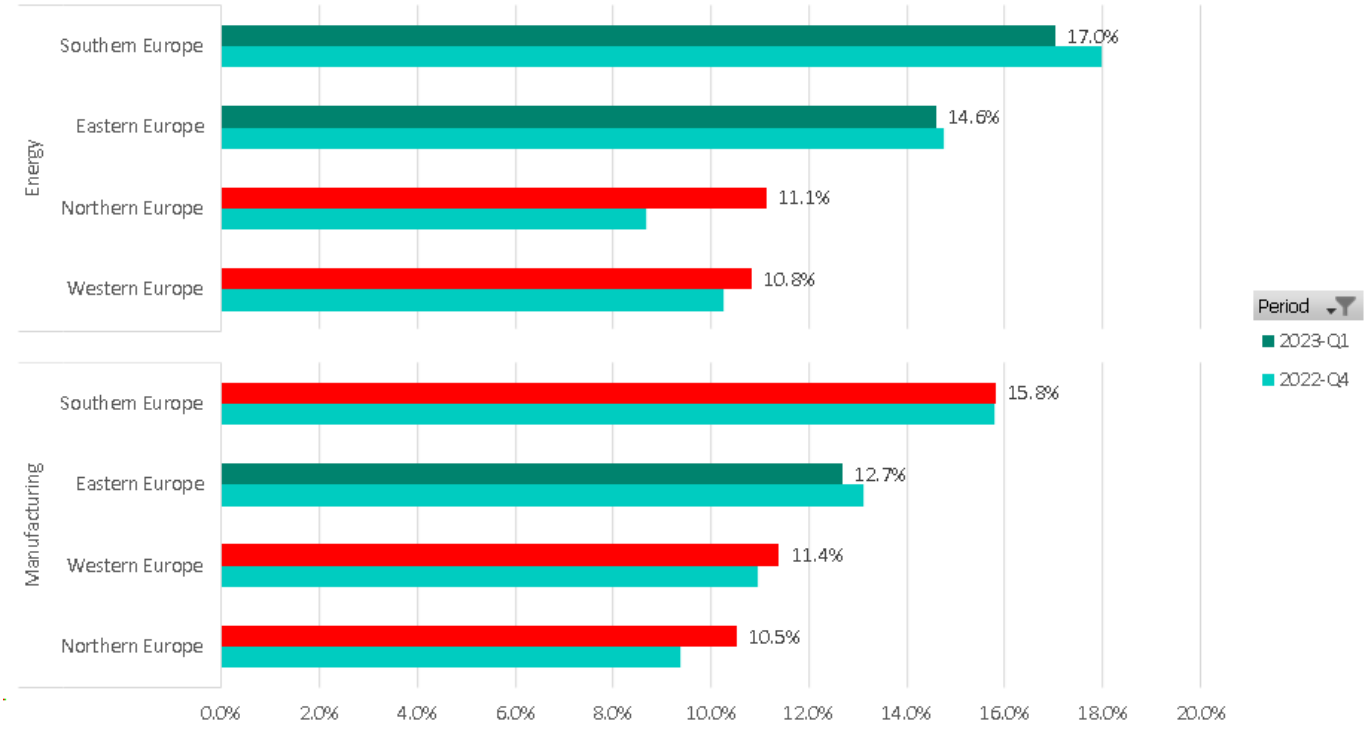
The statistics reveal that the Building Automation and ICS Engineering industries across all regions showed a significant increase in the percentage of attacked OT computers. These industries are particularly susceptible to threats originating from the internet and email clients, primarily due to broad access and extensive network connectivity which are common security issues for computers within these industries.



Percentage of attacked OT computers in Europe by industry and by region
Q4 2022 – Q1 2023

The percentages for the Energy and Manufacturing industries in Europe display a mixed trend. While the Southern and Eastern regions mostly exhibit a slight decline, the Northern and Western regions show a significant growth.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



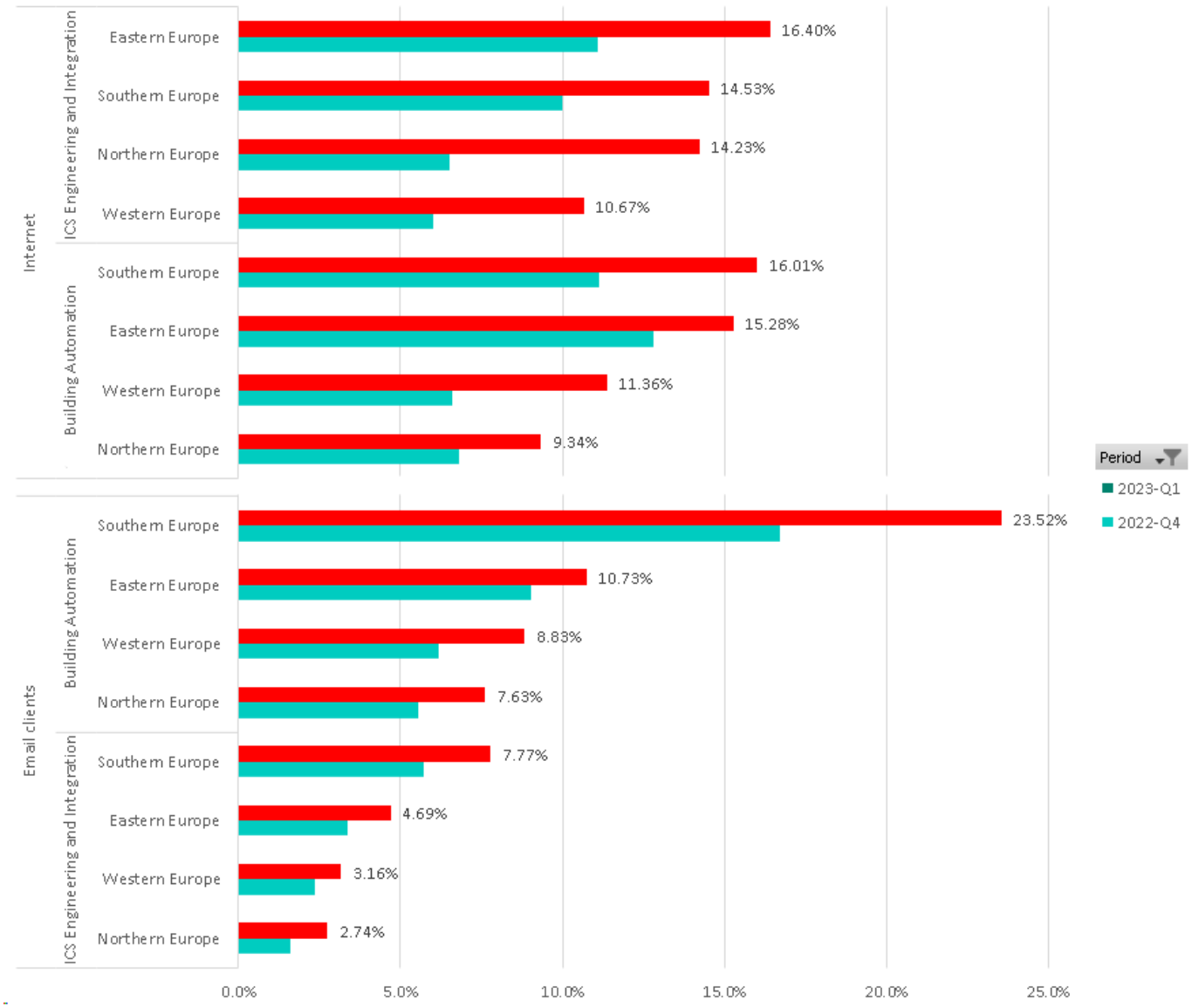
Percentage of attacked OT computers in Europe by industry and by region
Q4 2022 – Q1 2023

It is worth noting that the specific percentage values and details of the changes for each industry in the respective regions would provide a more comprehensive understanding of the trends.

The increase in the percentage of attacks on the Energy and Manufacturing industries in Western Europe during Q1 2023 was primarily driven by internet threats, specifically from denylisted internet resources, malicious scripts, and phishing pages. Similarly, in Northern Europe, the increase in the Energy and Manufacturing industries was also influenced by these types of initial access threats, as well as by spyware in the next attack stages.

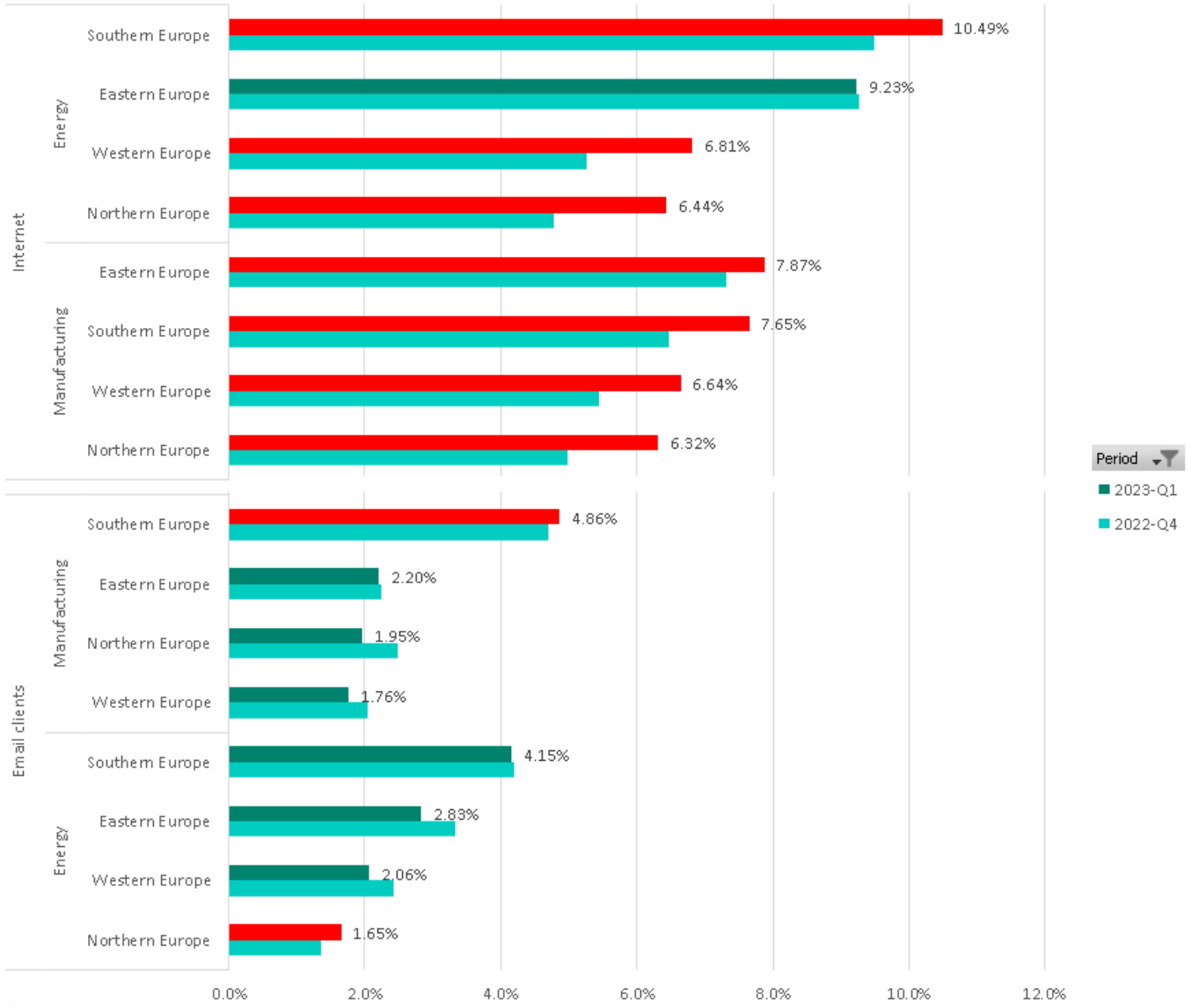
In the case of the Building Automation industry in Southern Europe, the significant change observed in Q1 2023 was predominantly driven by email threats, which increased by +5.5 p.p. compared to Q4 2022. This suggests a higher susceptibility to attacks through email-based vectors in the Southern European region.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers by threat type, industry, and region
Q4 2022 – Q1 2023

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

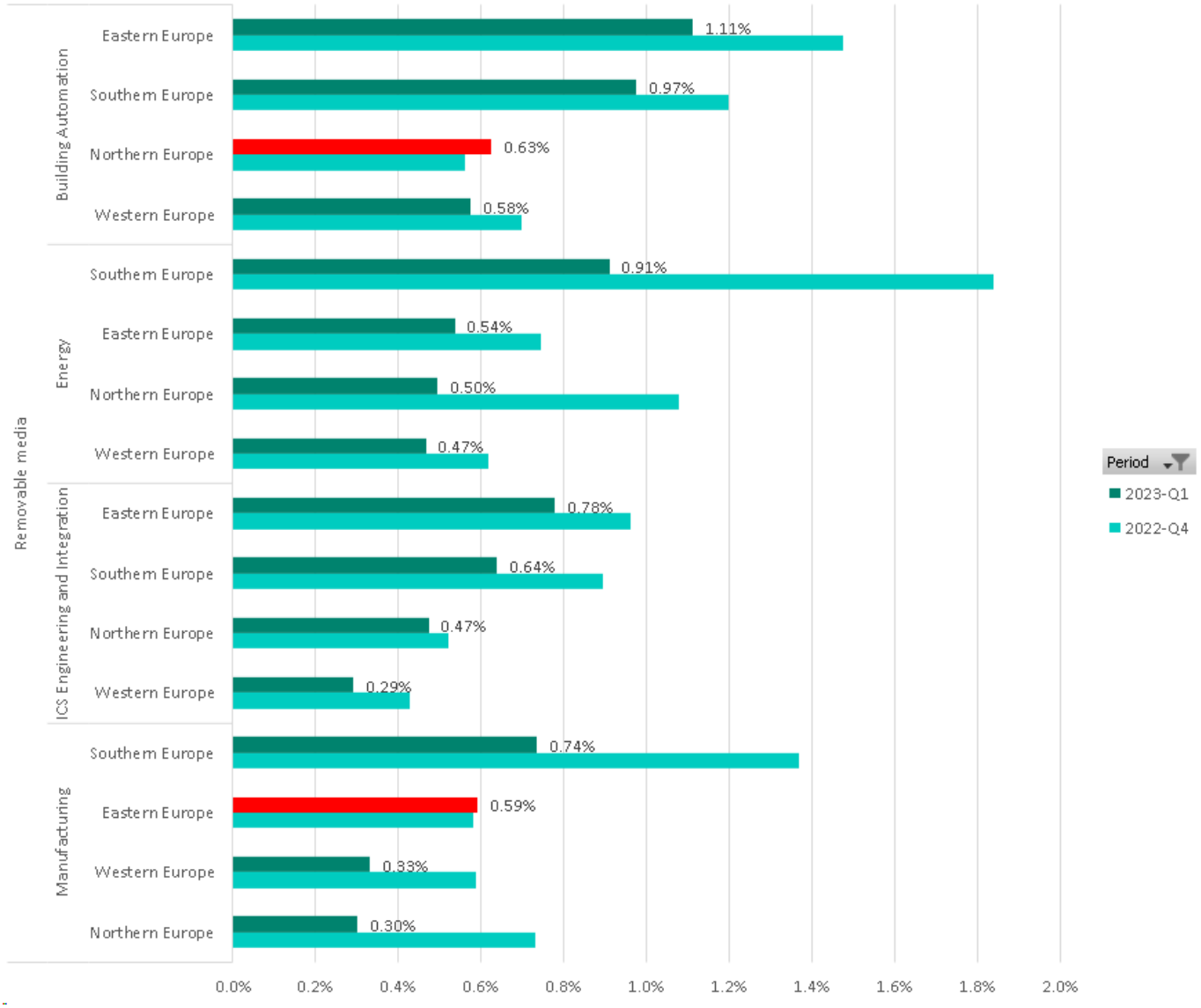


Percentage of attacked OT computers by threat type, industry, and region
Q4 2022 – Q1 2023

The percentage of ICS computers on which malware was detected on removable media and in network folders showed no significant changes in Q1 2023. Values for almost all regions and industries were slightly lower compared to Q4 2022, with the exception of Northern Europe, which had slightly higher values.

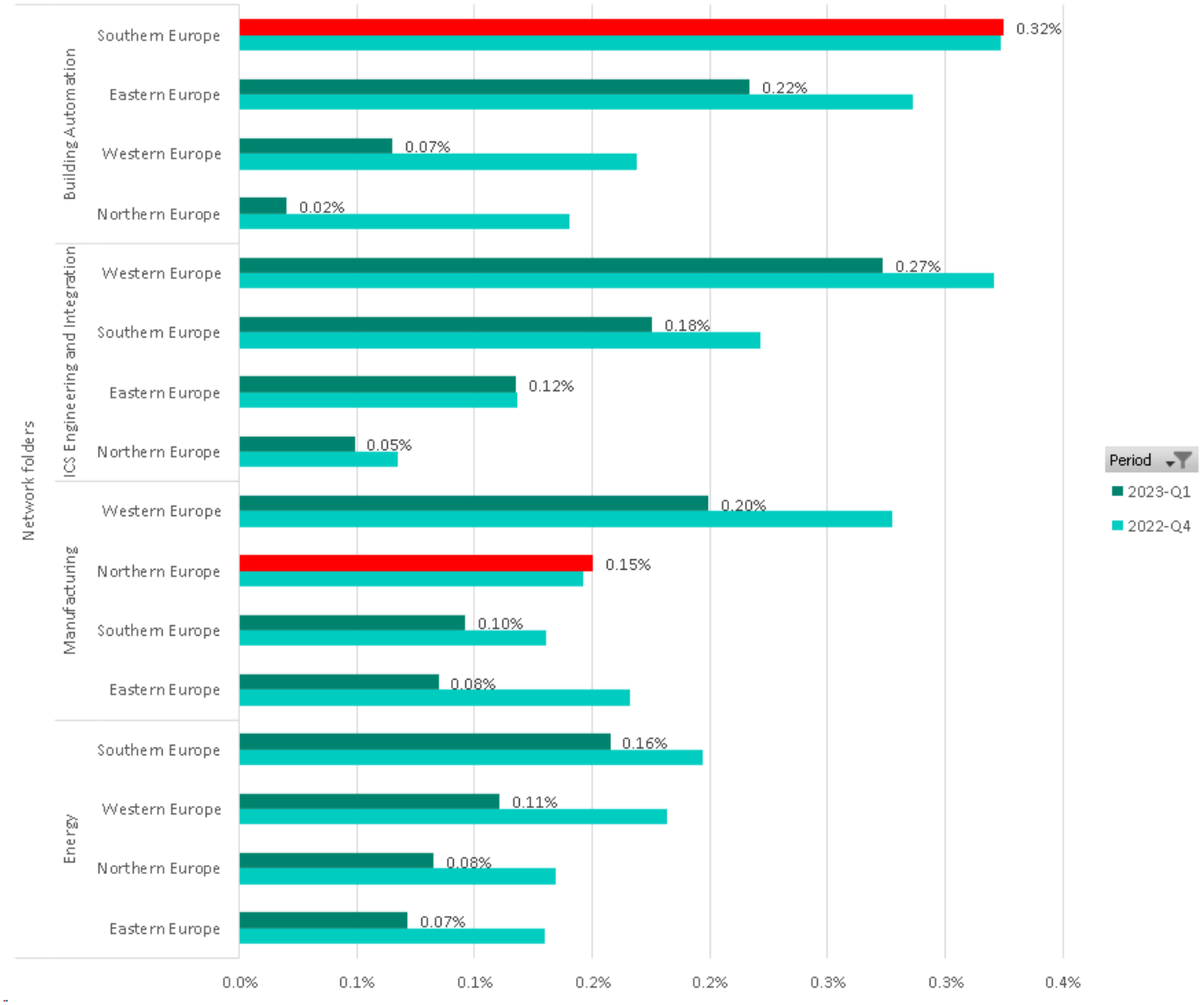
The decrease in the percentage of malware detected on removable media and in network folders is a long-term trend. It reflects efforts to address LAN infections made by companies in developed countries with high security maturity levels. This trend is likely driven by the desire to reduce maintenance costs, as LAN infections not only pose a headache for OT staff but also require significant human and technical resources to address.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers on which malware was blocked on removable media, by industry and by region, Q4 2022 – Q1 2023

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers on which malware on network folders was blocked, by industry and region, Q4 2022 – Q1 2023

Threats most often used as the initial attack vector

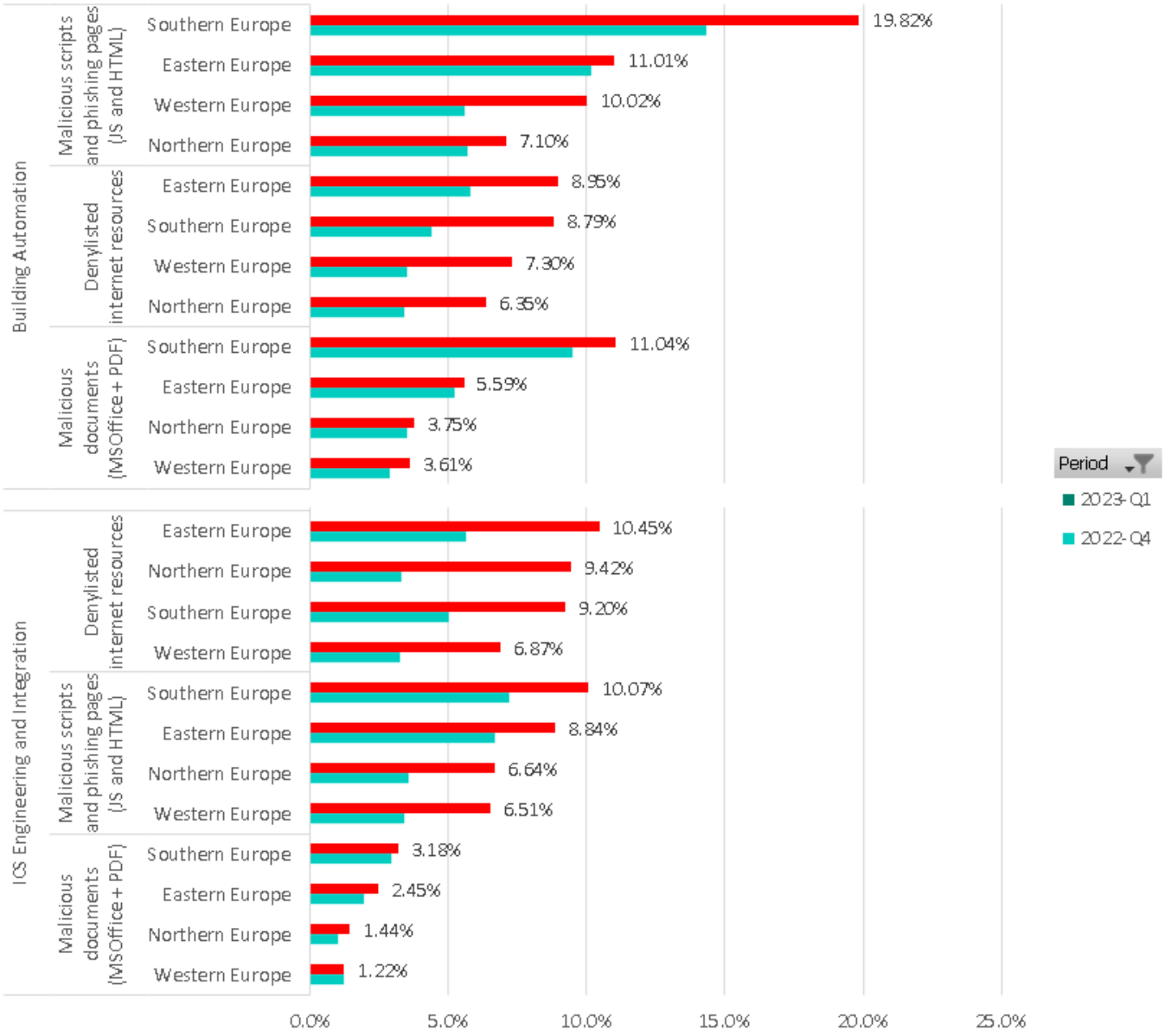
The Building Automation sector, particularly in Southern Europe, has exhibited the highest percentages of OT computers on which threats commonly used as entry points in the kill chain were detected. These threats include denylisted internet resources, malicious scripts, phishing pages, and malicious documents.

The significant percentage figures for malicious scripts and email threats detected on computers in the Building Automation sector in Southern Europe are not coincidental but are indicative of a wave of phishing emails targeting this industry.

Similarly, the high percentages observed for ICS Engineering across Europe in Q1 2023 can be attributed to the increased detection of denylisted internet resources, as well as malicious scripts

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

and phishing pages. These factors highlight the importance of addressing these specific threat sources to enhance the security posture of the ICS Engineering industry.



Percentage of attacked OT computers in Europe by industry, threat type, and region
Q1 23 vs Q4 22

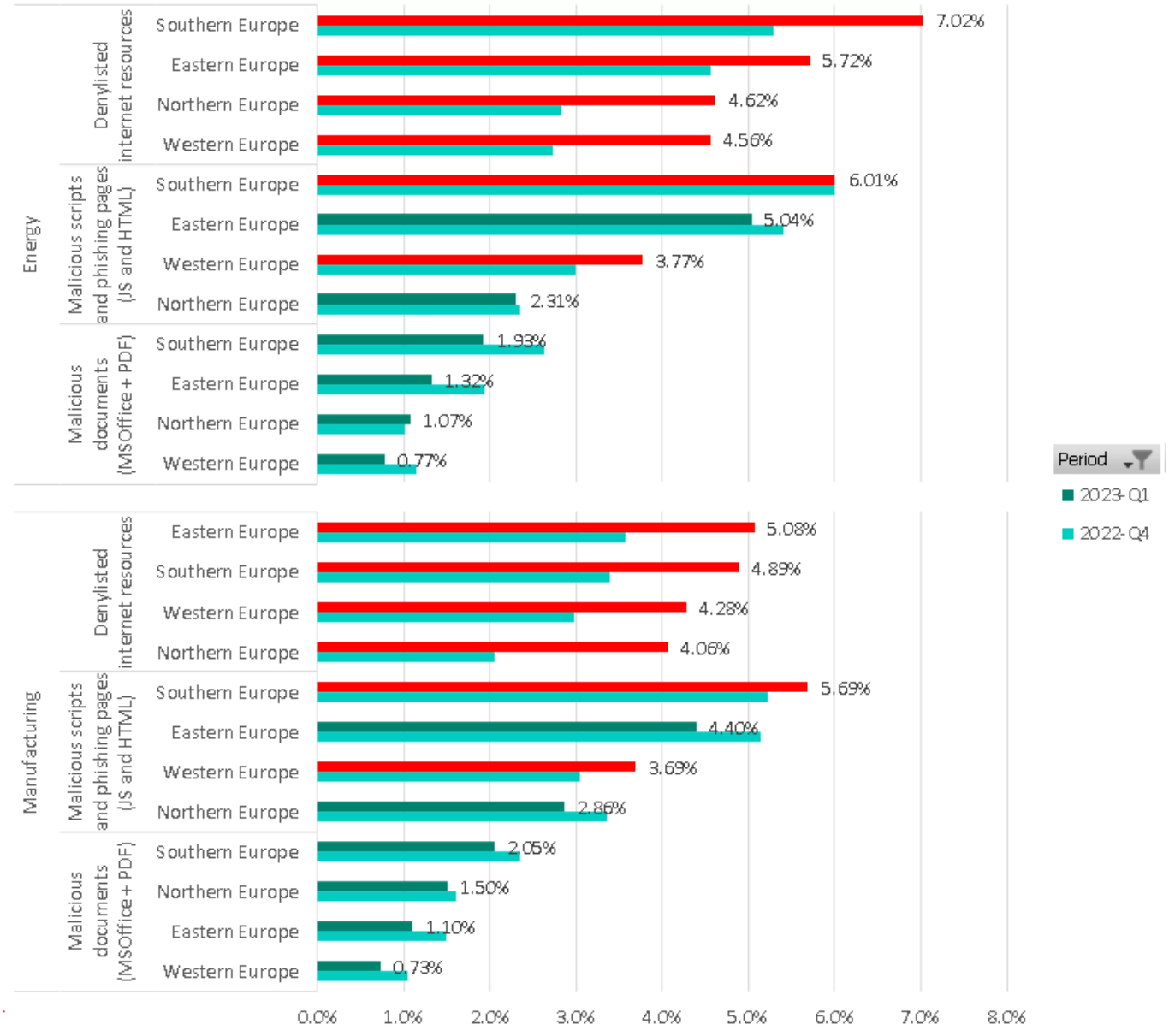
In the Manufacturing and Energy sectors in Europe, we observed a higher percentage of denylisted internet resources and lower percentage of malicious documents and malicious scripts for most of the regions. Our data indicates that in Q1 2023, some threat actors reinvented an old phishing technique that was first seen back in 2010 to target organizations in Europe, including industrial ones.

The technique involves infecting a website with a malicious script that triggers a pop-up window resembling a Microsoft tech support window. The pop-up does not contain any links, but instead

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

presents a phishing message and a local phone number to call. When a user calls the number, a threat actor answers the call and communicates in the local language, manipulating the unsuspecting user to download and install a remote access tool or a piece of multifunctional spyware.

This technique leverages social engineering tactics to deceive users and gain unauthorized access to their systems, posing a serious threat to organizations in the Manufacturing and Energy sectors.



Percentage of attacked OT computers in Europe by industry, threat type, and region Q1 23 vs Q4 22

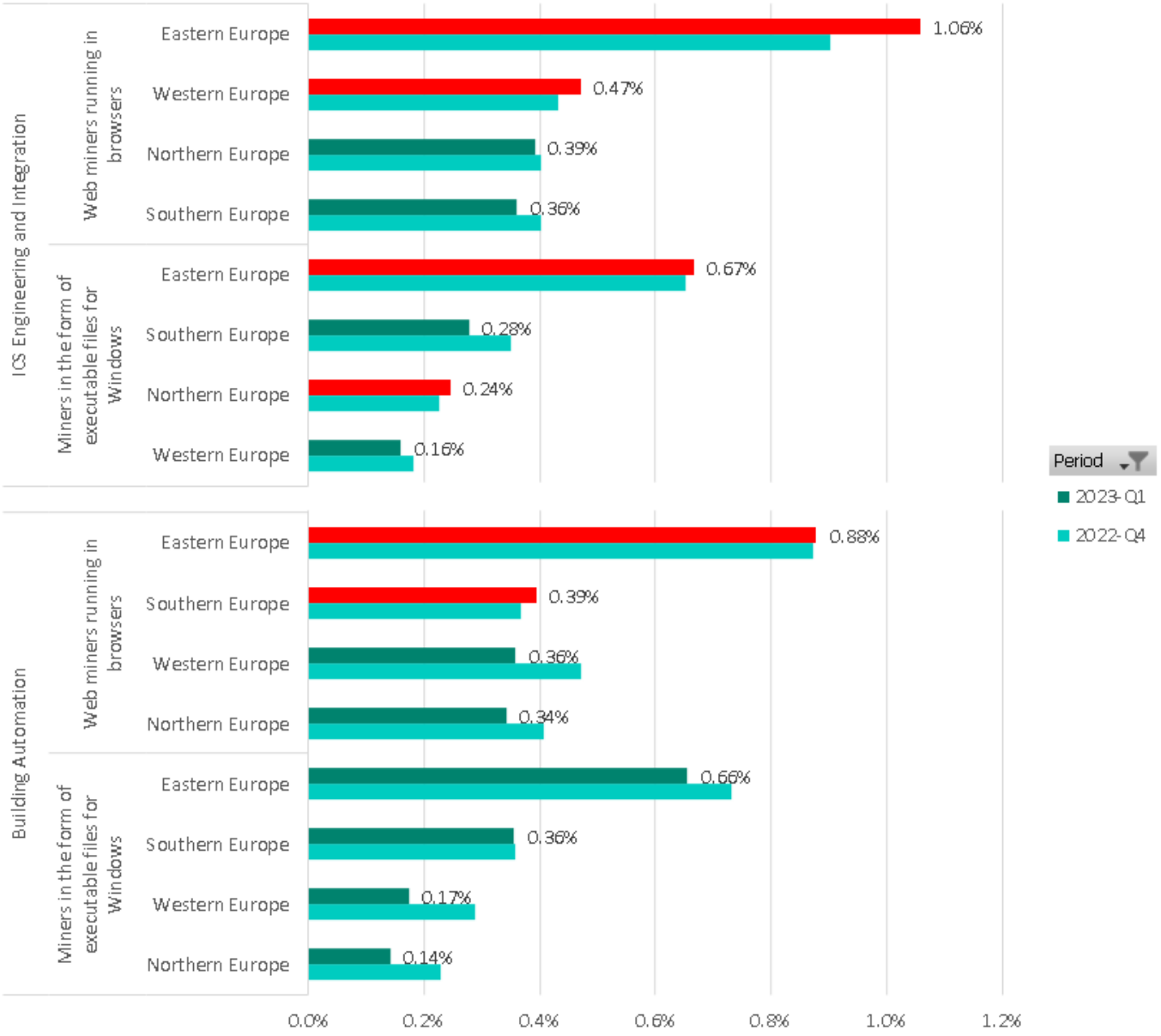
**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

Self-propagating threats: crypto-miners

The percentages for crypto-miners did not significantly change in Q1 2023 compared to Q4 2022, and they have followed a downward trend across all European regions since the beginning of 2022.

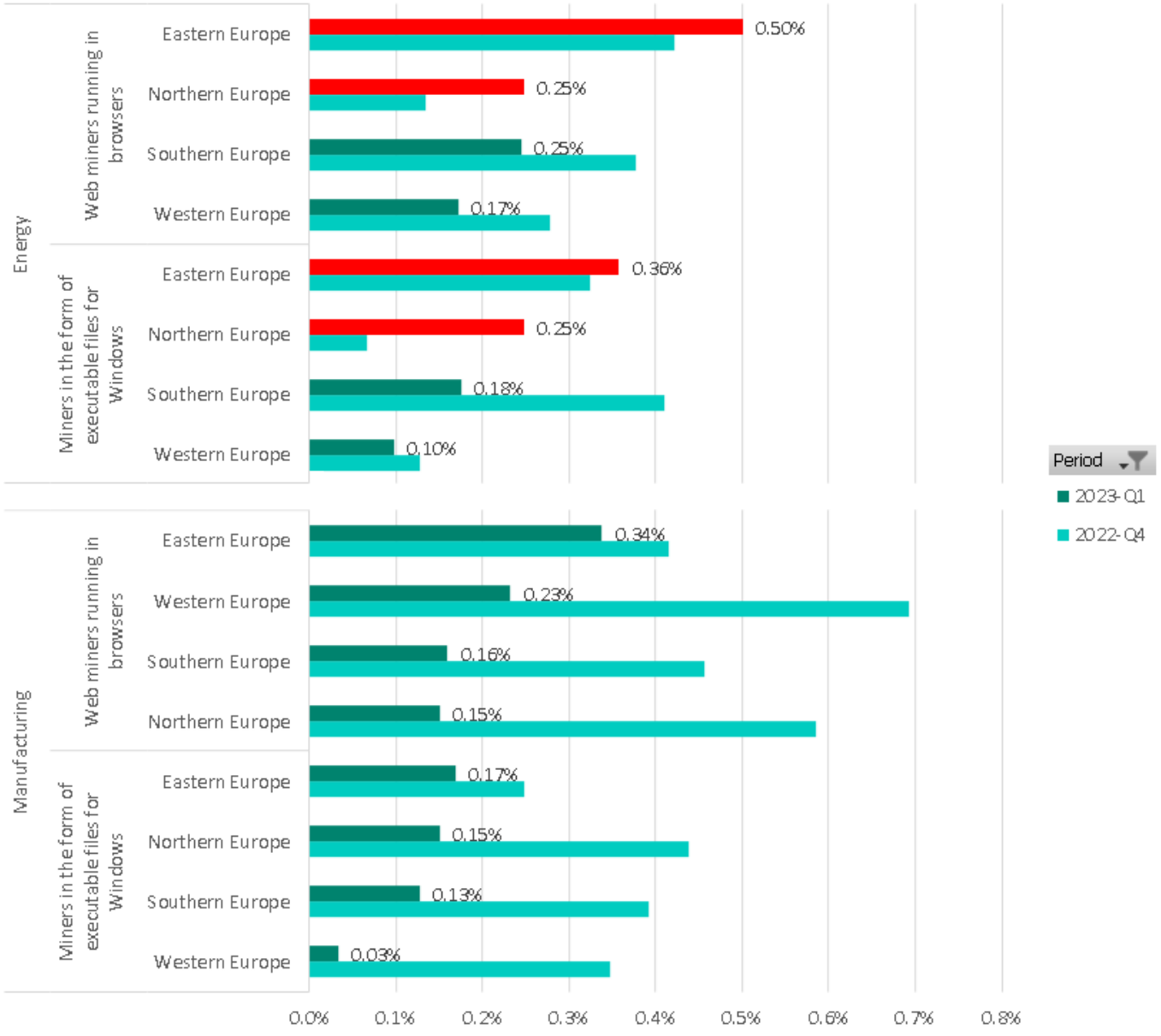
Modern crypto-miners are designed as modular malware, typically comprising the miner itself as the final payload, a backdoor for unauthorized access, and a network worm component. The network worm may incorporate various exploits, functionality for brute-forcing passwords, and even tools like Mimikatz to steal and abuse user account credentials.

The modular nature of these crypto-miners allows threat actors to adapt and evolve their tactics, making this malware more sophisticated and harder to detect. However, the overall trend in Q1 2023 indicates a decrease in the prevalence of crypto-miners in Europe.



**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

Percentage of attacked OT computers in Europe by industry, threat type, and region, Q1 23 vs Q4 22

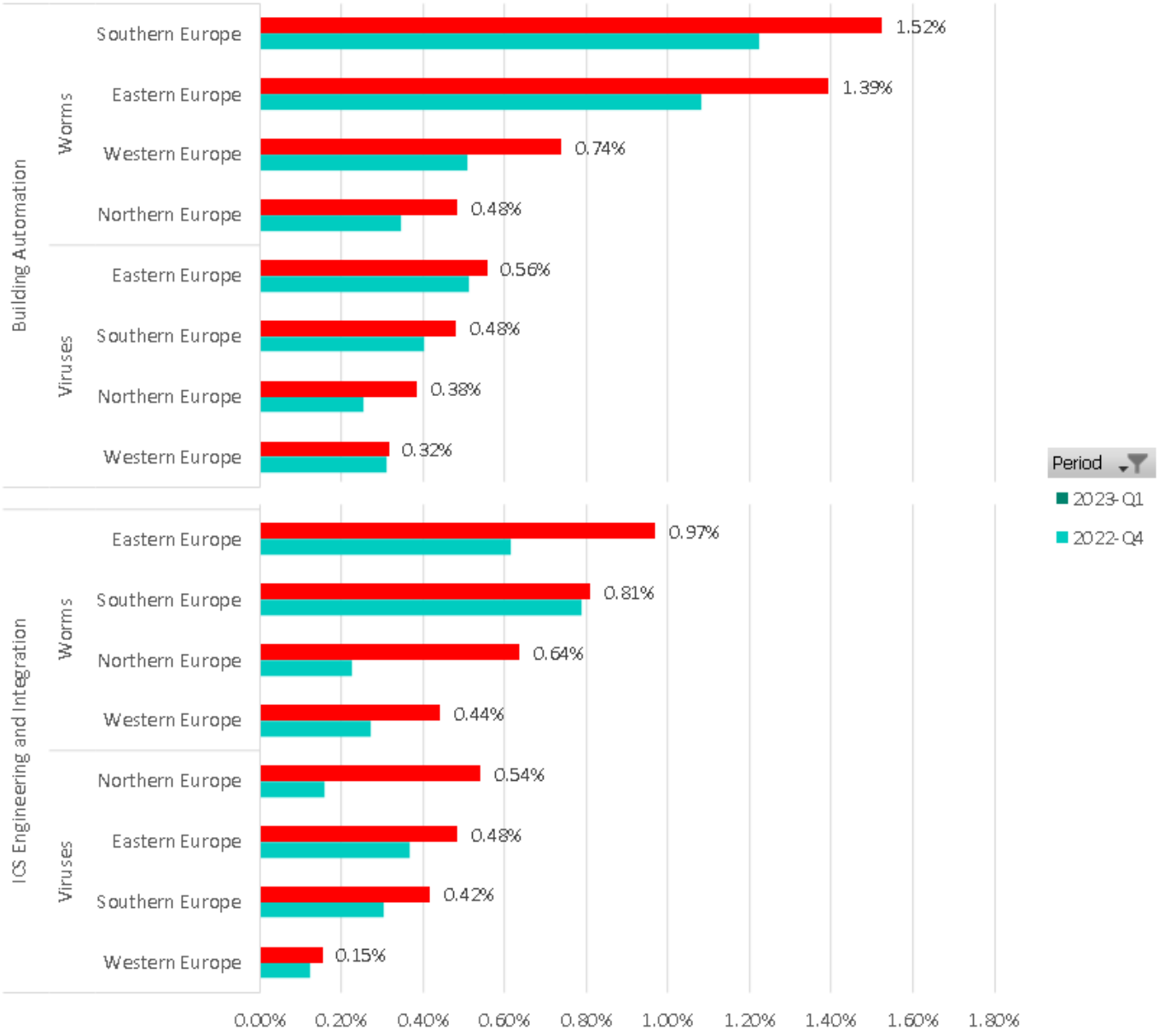


Percentage of attacked OT computers in Europe by industry, threat type, and region, Q1 23 vs Q4 22

Self-propagating threats: viruses and worms

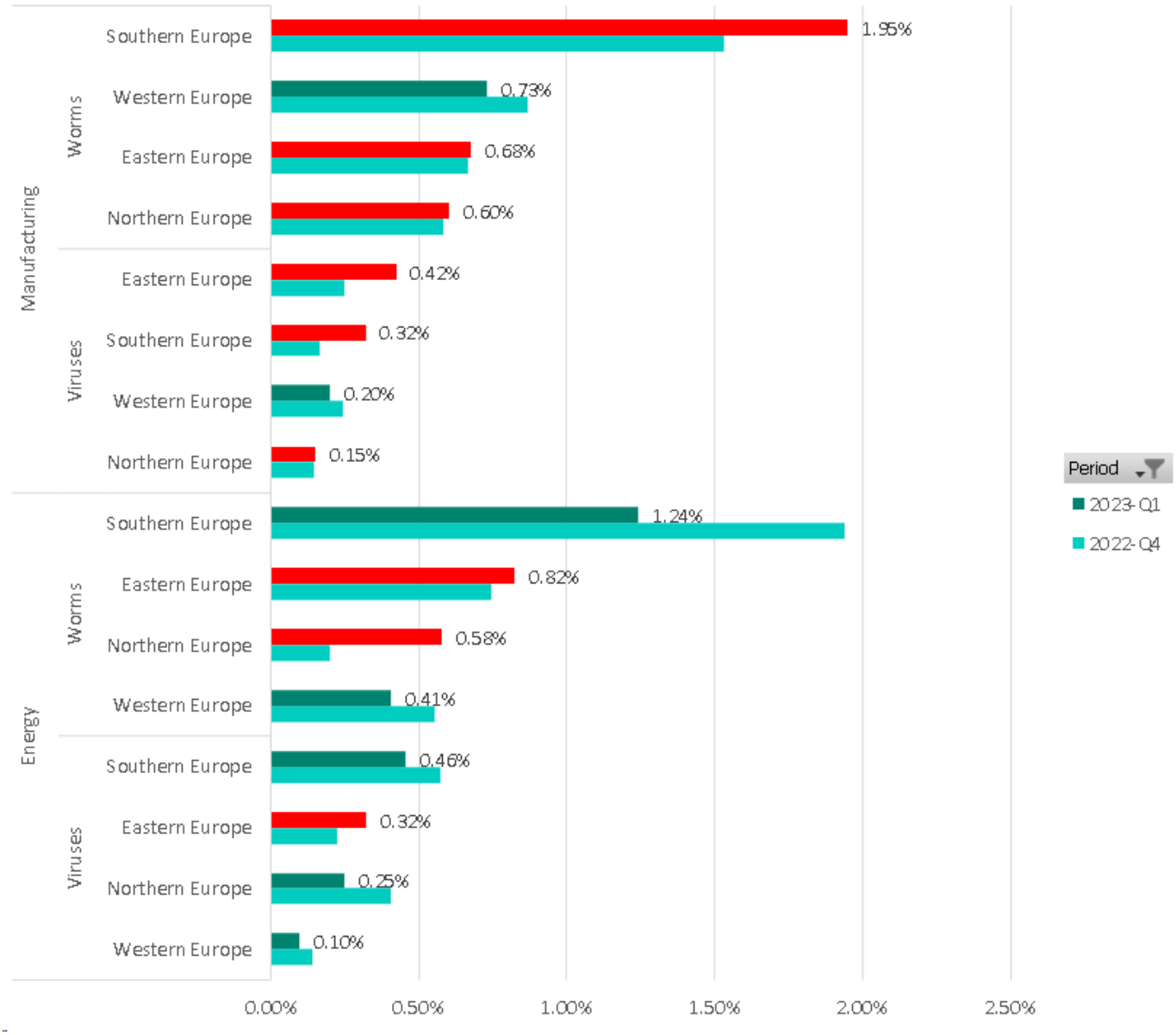
The recent increases in the percentages for worms and viruses in the Building Automation and ICS Engineering sectors can be considered a temporary fluctuation. The overall trend for these sectors has been downward, indicating a decrease in the prevalence of worms and viruses. It is important to focus on the long-term trend rather than short-term fluctuations to gain a more accurate understanding of the threat landscape in these sectors.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



Percentage of attacked OT computers in Europe by industry, threat type, and region, Q1 23 vs Q4 22

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

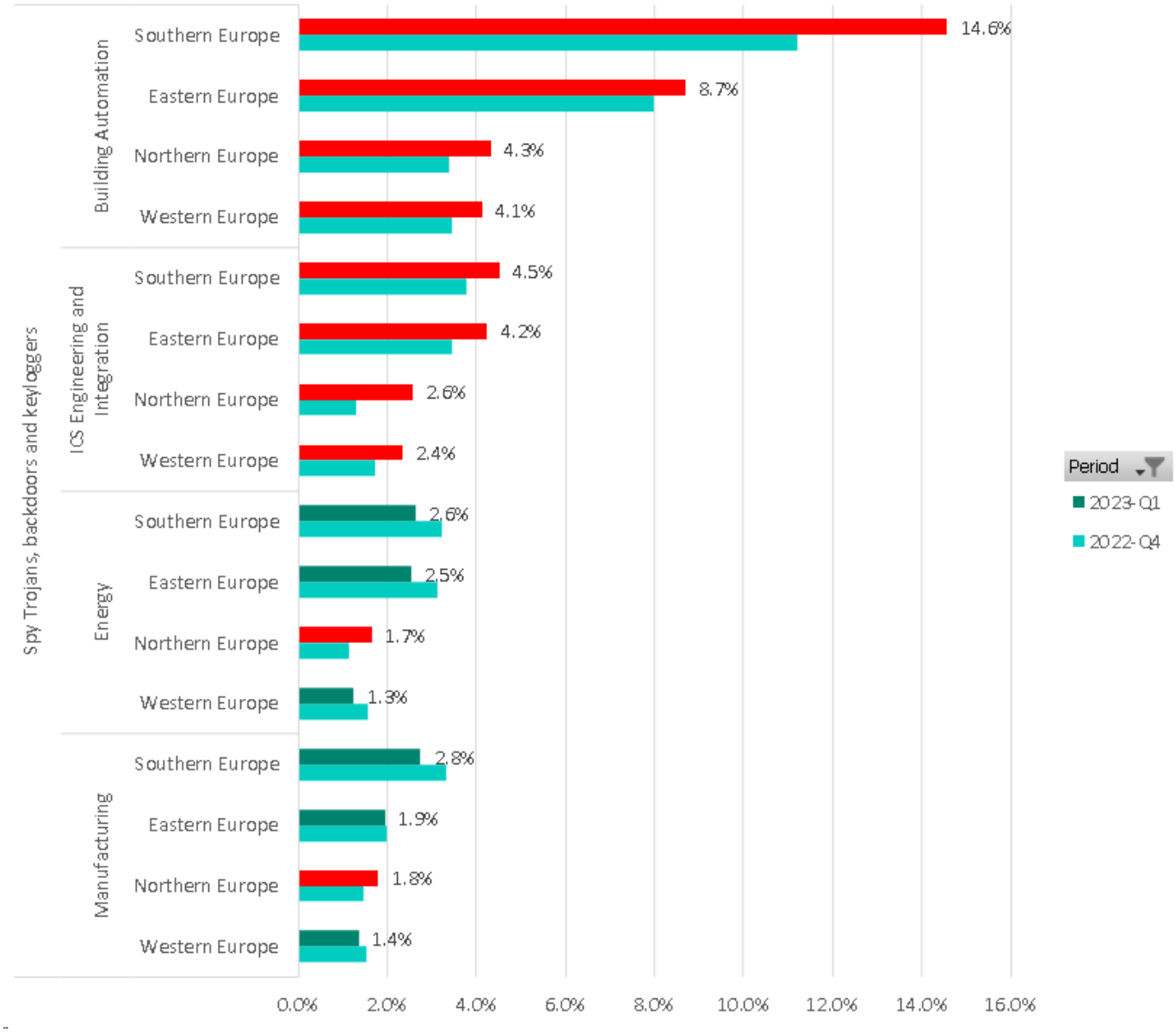


Percentage of attacked OT computers in Europe by industry, threat type, and region, Q1 23 vs Q4 22

Next-stage threat types

For next-stage threat types, the highest percentages of attacked OT computers were observed in the Building Automation sector. Across Europe, there was an average increase of +1.4 p.p., with the Southern region experiencing a significant increase of +3.4 p.p. in Q1 2023 compared to Q4 2022. Additionally, the high percentages of malicious scripts detected in the Building Automation sector, particularly in Southern Europe, are an indication of an ongoing wave of phishing campaigns delivered via email.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*



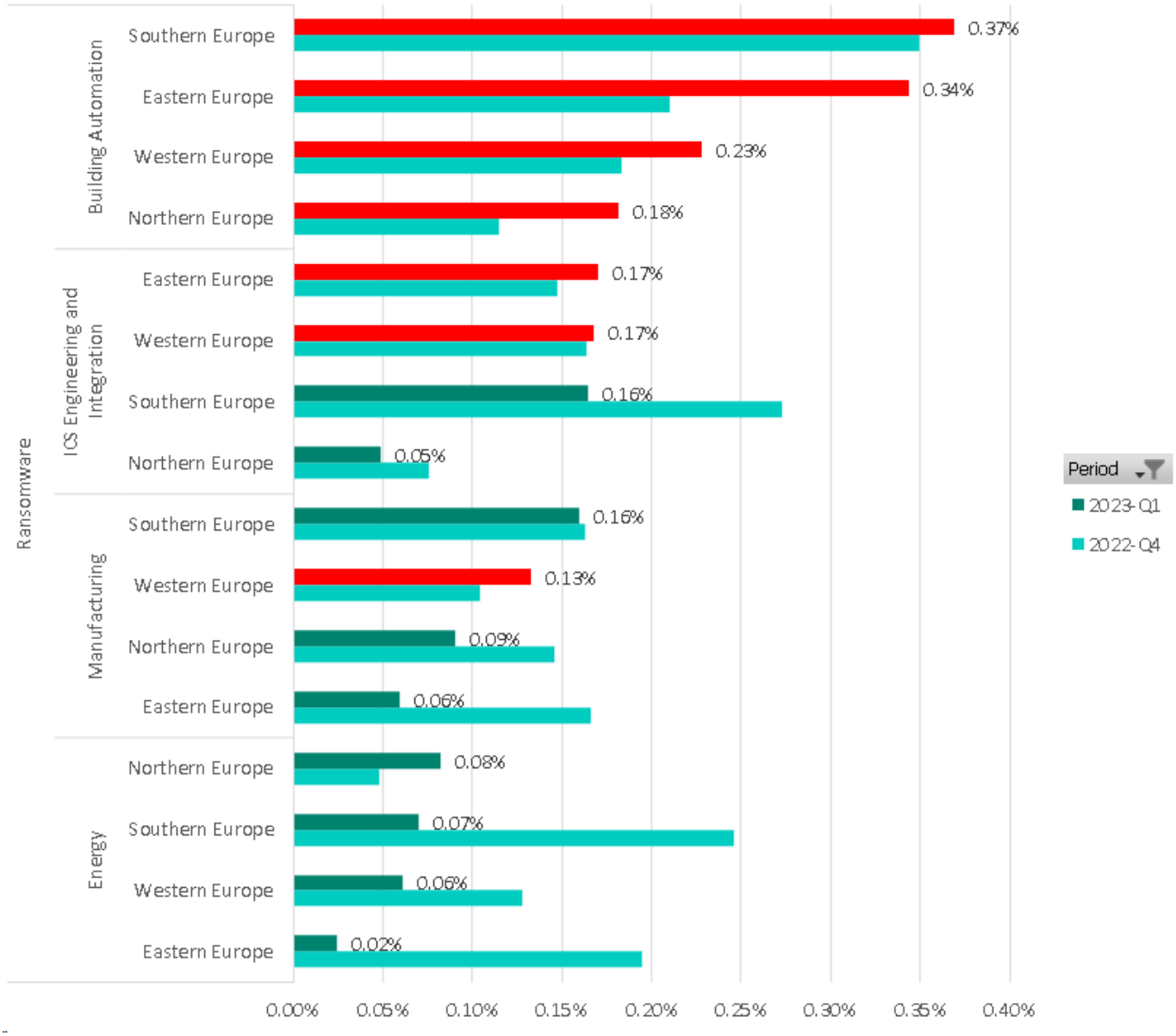
Percentage of OT computers in Europe attacked by spyware, by industry and region, Q1 23 vs Q4 22

It is important to keep in mind that the low numbers for spyware and ransomware in the statistics can indicate successful security measures related to blocking previous stages of attacks or threat actors' shift in focus towards other targets.

However, the situation can change rapidly, especially considering the ongoing phishing attacks targeting the Building Automation and ICS Engineering sectors in Europe. If these phishing campaigns are successful, it could potentially lead to the compromise of related organizations in other industries and regions. Supply-chain attacks are a common occurrence, often facilitated by threat actors skilled in business email compromise techniques, with stolen data being easily sold on illicit online markets.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

While some correlation may be found in the statistics between spyware and ransomware, it is not necessarily strong. In some cases, spyware is used as a means of delivering ransomware, especially in espionage campaigns, rather than as the final stage.



Percentage of OT computers in Europe attacked by ransomware, by industry and region, Q1 23 vs Q4 22

Conclusions

To prevent threats that are commonly used as the initial attack vector in a kill chain, such as denylisted internet resources, phishing emails, malicious scripts, phishing pages, and malicious documents, it is important to strengthen security and organizational measures. Here are some recommended steps to consider:

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

- Raise OT staff's awareness of phishing threats and provide training on identifying and mitigating them. This can include educating employees about common phishing techniques, emphasizing the importance of not clicking on suspicious links or opening attachments from unknown sources, and promoting best practices for secure email communication.
- Strengthen spam and phishing protection measures by implementing robust email filtering systems that can identify and block malicious emails. This can involve using advanced anti-spam and anti-phishing solutions, implementing email authentication protocols such as SPF, DKIM, and DMARC, and regularly updating spam filter rules to adapt to emerging threats.
- Take measures to prevent ad-hoc internet connections from the OT network. This can include implementing strict access control policies, network segmentation, and firewall rules to restrict unauthorized internet access from OT devices. It is important to ensure that only necessary and authorized connections are allowed, and any uncontrolled or ad-hoc connections are blocked.
- Ensure that all endpoint computers on the OT network are protected with a dedicated endpoint protection solution. The solution should be properly configured as recommended by the vendor and should have real-time scanning, behavior monitoring, and blocking known malicious files enabled. Regularly update antimalware databases to ensure detection of the latest threats and protection against them.

By implementing these measures, organizations can strengthen their defenses against the initial attack vectors used in the kill chain and reduce the risk of successful attacks on their OT systems.

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*

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

**Note that the resulting percentages should not be summed up because in many cases threats of two or more types may have been blocked on a single computer during the given reporting period*