INDUSTRIAL CONTROL SYSTEMS AND THEIR ONLINE AVAILABILITY

Oxana Andreeva, Sergey Gordeychik, Gleb Gritsai, Olga Kochetova,
Evgeniya Potseluevskaya, Sergey I. Sidorov, Alexander A. Timorin

Table of Contents

1 Introduction

1.1 Overview

Industrial control systems (ICS) surround us: they are used across multiple sectors including electricity, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods). Smart cities, smart houses, smart cars, and medical equipment – all of these are driven by ICS.

The number of ICS components available over the Internet increases every year, and the expansion of the Internet makes ICS easy prey for attackers. Taking into account that, initially, many ICS solutions and protocols were designed for isolated environments, their new online availability can make it possible for a malicious user to cause impact on the infrastructure behind the ICS, due to its lack of Internet-ready security controls. Moreover, some components are vulnerable themselves. The first information about vulnerabilities in ICS components became available in 1997, when only two vulnerabilities were published. Since then the number of vulnerabilities has significantly increased. Over the past five years, this index has increased from 19 vulnerabilities in 2010 to 189 vulnerabilities in 2015.

Sophisticated attacks on ICS systems are not new anymore. Here, it is worth remembering the 2015 incident in Ivano-Frankivsk, Ukraine, where around a half of the area's houses were left without electricity because of a cyber-attack against the Prykarpattyaoblenergo power company. It was only one of multiple victims of the BlackEnergy1 APT campaign.

Another notable incident in 2015, described in the Verizon Data Breach Digest2, was an attack on the Kemuri Water Company's ICS infrastructure. Intruders infiltrated a water utility's control system and changed the levels of chemicals being used to treat tap water. The intrusion was performed through a vulnerable externally available system, which managed the programmable logic controllers (PLCs) regulating the valves and ducts that controlled the flow of water and chemicals used through the system.

In 2015, there were other reports of ICS-related incidents, such as attacks on a steel mill in Germany and on the Frederic Chopin Airport in Warsaw[3].

This report provides an overview of the current worldwide situation with ICS security, looking at vulnerabilities, and the vulnerable ICS components exposed to the Internet.

1.2 Analysis Approach

This report is dedicated to research about ICS Availability over the Internet. We used a passive approach for analysis. To identify ICS systems in the Shodan and Censys search engines we used a fingerprint knowledgebase containing about 2000 records, allowing us to identify product vendors and versions by banners.

[1] https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/

[2] http://www.verizonenterprise.com/verizon-insights/data-breach-digest/2016/

[3] https://securelist.com/analysis/kaspersky-security-bulletin/72886/kaspersky-security-bulletin-2015-top-security-stories/

2 Main Findings

The main findings of the research are as follows:

- **Numerous ICS components are available via the Internet**. 220,558 ICS components were discovered by the Shodan search engine. They are located on 188,019 hosts in 170 countries. Most of the remotely available hosts with ICS components are located in the United States (30.5%) and Europe. Among European countries Germany has a leading position (13.9%), followed by Spain (5.9%). The available systems are from 133 different vendors. The most widespread ones are Tridium (11.1%), Sierra Wireless (8.1%), and Beck IPC (6.7%).
- **Insecure protocols are widely used by remotely available ICS components**. There are a number of protocols, which are open and insecure by design, such as HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 and many others. They are used on 172,338 different hosts, which correspond to 91.6% of all the externally available ICS devices found. This provides an attacker with additional ways to compromise devices by performing man-in-the-middle attacks.
- **Multiple vulnerable ICS components are externally available.** We found 13,033 vulnerabilities on 11,882 hosts (6.3% of all hosts with externally available components). The most widespread vulnerabilities revealed include: Sunny WebBox Hard-Coded Credentials (CVE-2015-3964), and the critical vulnerabilities CVE-2015-1015 and CVE-2015-0987 in Omron CJ2M PLC. Merging these results with statistics of usage of insecure protocols, we were able to estimate the total number of vulnerable ICS hosts as 172,982 (92%).
- **Multiple industries are affected.** We found at least 17,042 ICS components on 13,698 different hosts in 104 countries. These are likely to belong to large organizations, and the availability of these components on the Internet brings with it significant risks. Among the owners of these components, we were able to identify 1,433 large organizations, including some belonging to the following industries: electricity, aerospace, transportation (including airports), oil and gas, metallurgy, chemical, agriculture, automotive, utilities, drinks and food manufacturing, construction, liquid storage tanks, smart cities, and ICS vendors. There are also research and education entities, government institutions (including police), medical centers, financial organizations, resorts, hotels, museums, libraries, churches and multiple small businesses among the identified owners of remotely available ICS. The number of vulnerable externally available ICS hosts that are likely to belong to large organizations, is 12,483 (91.1%), where 453 hosts (3.3%), including those belonging to energy, transportation, gas, engineering and manufacturing organizations, drink and foods manufacturing organizations contain critical vulnerabilities.

The above results are low estimations based on our findings. The real number of available ICS components associated with significant risks could be much higher.

3 ICS Availability

3.1 Overview

The availability of ICS components on the Internet is a serious security threat, because in most cases components are designed under the assumption that the corresponding networks are physically isolated, so even basic security controls are often not implemented in these devices.

Based on information from the Shodan search engine, our research uncovered a total of **220,558 ICS components** that can be accessed from the Internet, located **on 188,019 hosts in 170 countries**. This section describes the main findings related to these externally available systems.

3.2 Availability by Vendors

The most widespread externally available systems are from vendors such as **Tridium** (24,446 services – 11.1%)**, Sierra Wireless** (17,908 services – 8.1%), and **Beck IPC** (14,837 services – 6.7%). The "other" category consists of 115 vendors, including Advantech, ABB, Nordex, Honeywell, Emerson and General Electric.

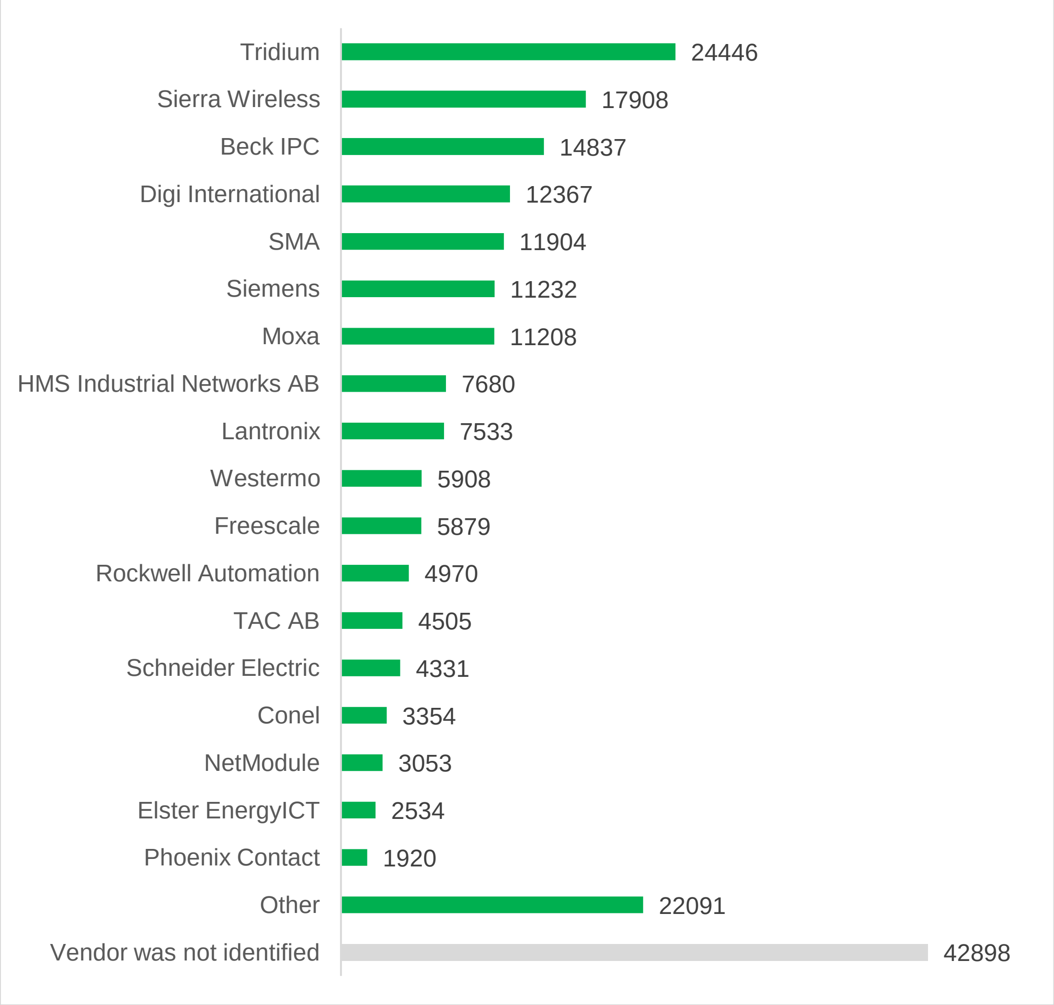

Figure 1. ICS availability by vendor

3.3 Availability of Different ICS Component Types

The most widespread types of available components are **industrial network devices:** 61,335 services – 27.8%, including 41,968 industrial routers and 12,024 industrial gateways, **PLCs** (33,080 services – 14.9%), and **SCADA** (22,624 services – 10.3%). For 18.7% of all remotely available services it was possible to classify them as ICS components (because of protocols or vendors), but the exact types of devices could not be identified using only the passive banner analysis method.

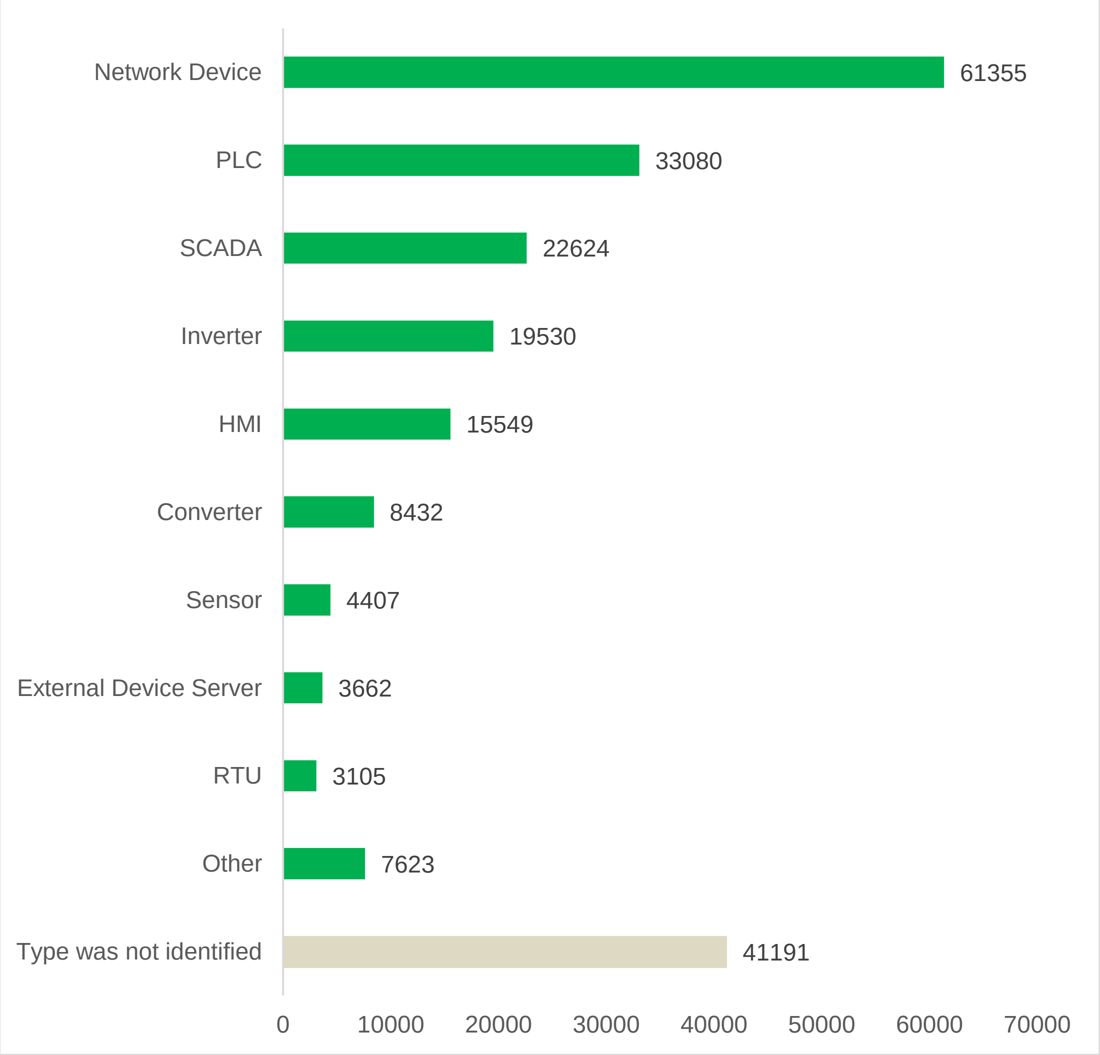

Figure 2. ICS components availability

3.4 Protocols

The ICS components found are available through different protocols. In many cases, several different protocols are used on the same host by the ICS components. The most widespread protocols are: HTTP (116,900 network services available – 53%), Telnet (29,586 services – 13.4%), Niagara Fox (20,622 services available – 9.3%), SNMP (16,752 services – 7.6%), and Modbus (16,233 services – 7.4%).

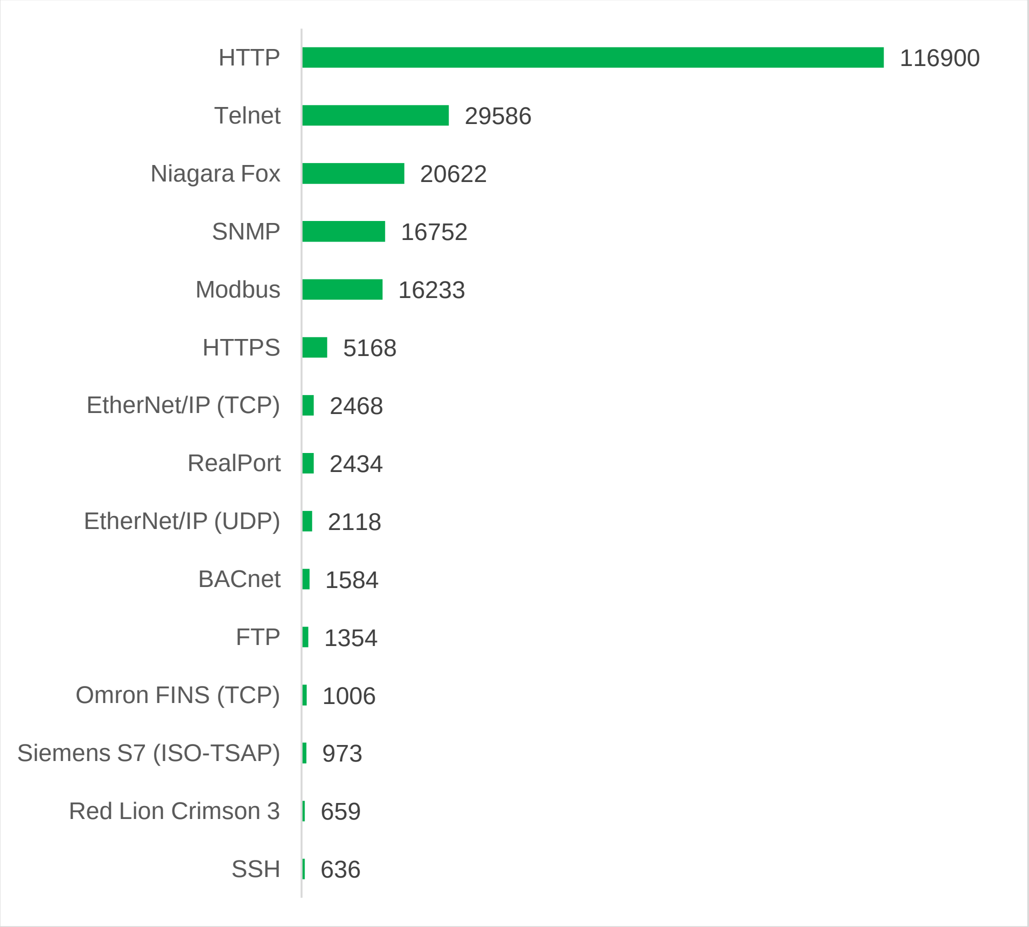

Figure 3. Top 15 protocols used by externally available ICS components

In addition to the fact that the availability of ICS components over the Internet is a security flaw in itself, **most of the protocols used (88.8%) are open and insecure by design**: HTTP, Niagara Fox, Telnet, EtherNet/IP, Modbus, BACnet, FTP, Omron FINS, Siemens S7 and many others. The insecure protocols are used on **172,338 different hosts, which corresponds to 91.6%** of all the externally available ICS devices found. This provides an attacker with additional ways to compromise the devices, using man-in-the-middle attacks.

3.5 Countries and Industries

Most of the remotely available hosts with ICS components (by unique IP addresses) are located in the **United States of America** (57,417 hosts – 30.5%) and Europe. Among the European countries, **Germany** has a leading position (26,142 hosts – 13.9%), followed by Spain (11,264 hosts – 5.9%) and France (10,578 hosts – 5.6%).

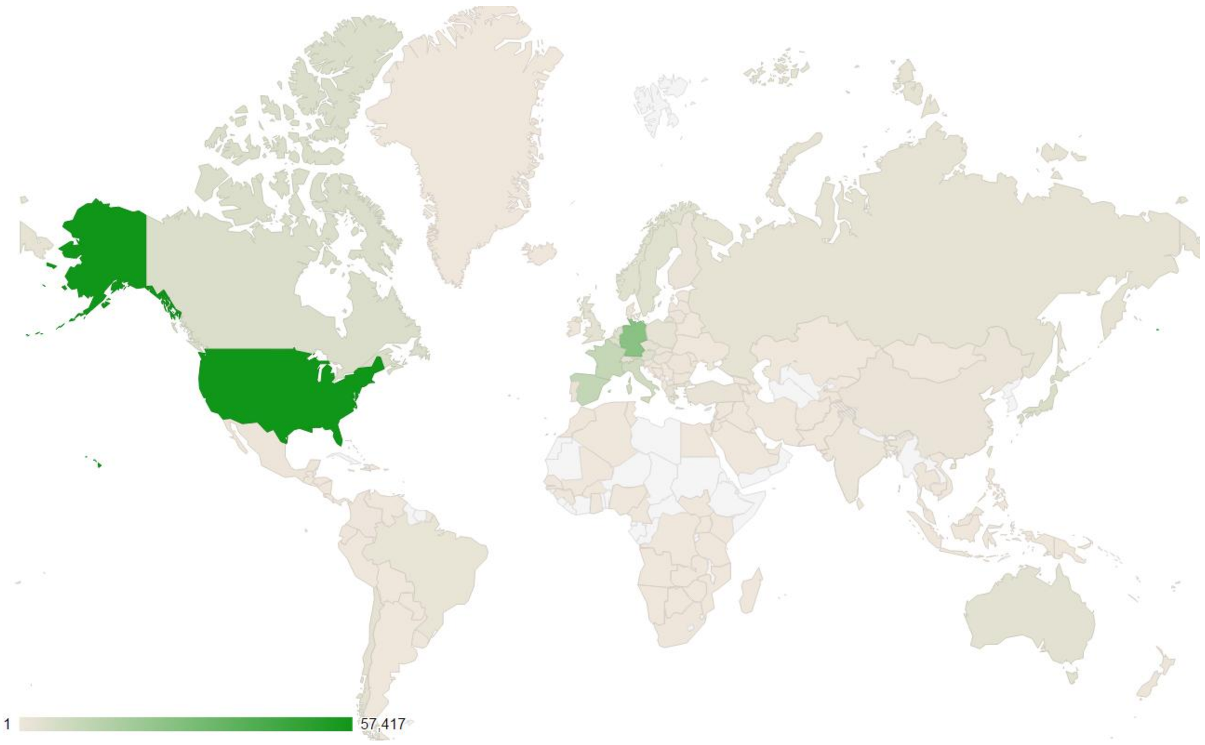

Figure 4. ICS availability by country

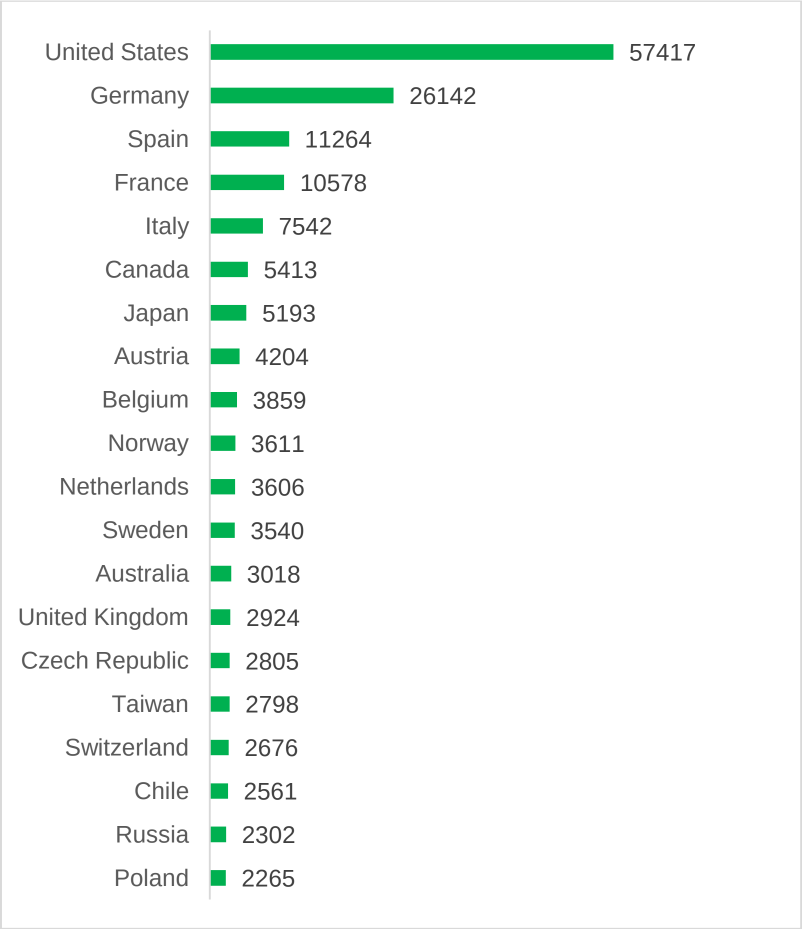

Figure 5. ICS availability by country (Top-20)

Such statistics are probably related to the fact that the United States and European countries are more technologically advanced. Analysis of relative rates for the hosts with identified ICS components to the total number of remotely available hosts in a country (based on Shodan data) shows a different picture: the leading positions are taken by **New Caledonia** (0.547%), **Belgium** (0.475%) and **Norway** (0.458%). In this rating, the USA is in 34th place, and Germany is 21st.

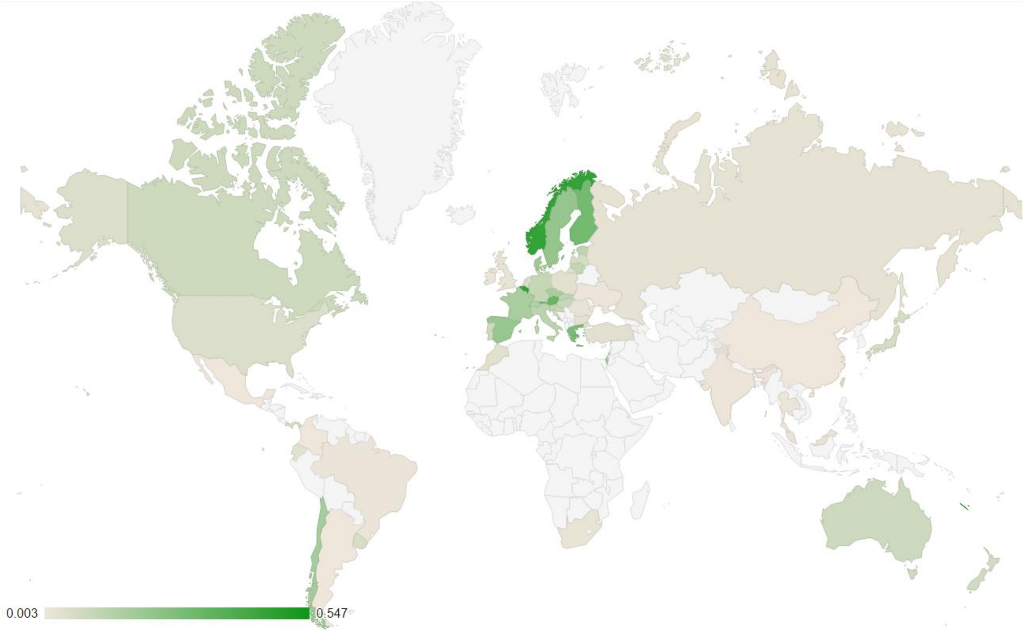

Figure 6. ICS availability by country (rate of available ICS hosts to the total number of available hosts)

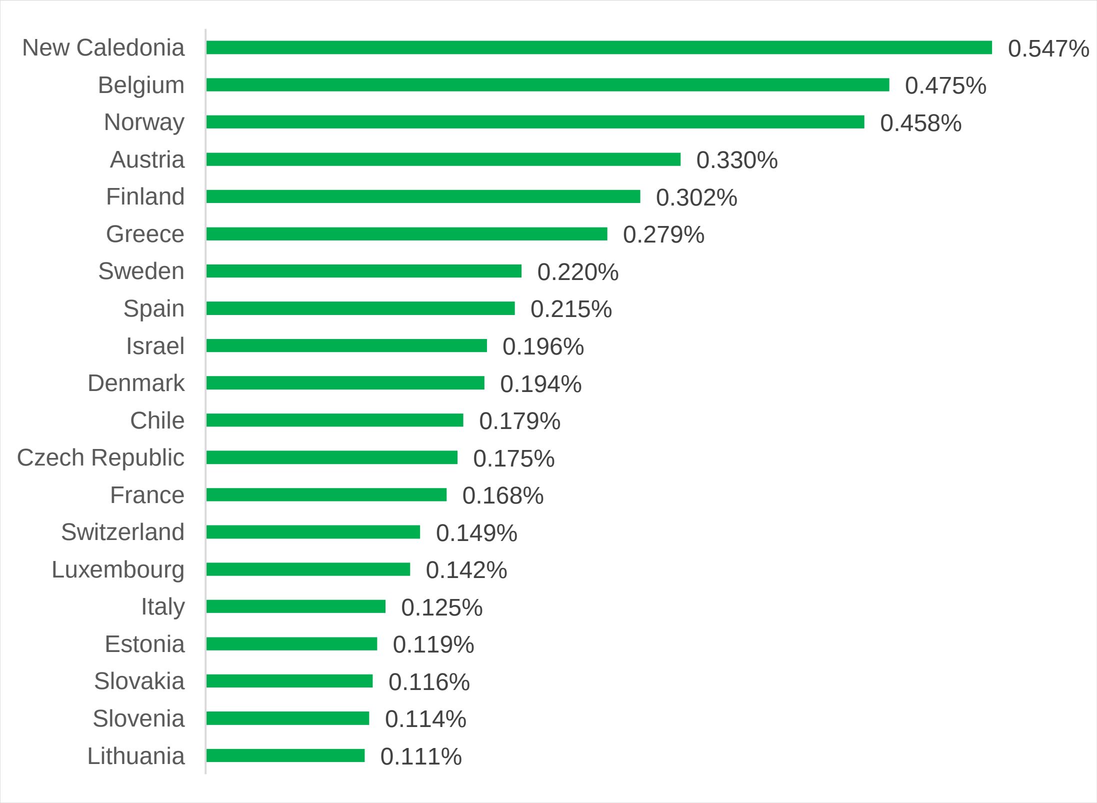

Figure 7. Top-20 ICS availability by country (rate of available ICS hosts to the total number of available hosts)

For most of the remotely available ICS components, it’s uncertain by whom they are used: home users, small and medium businesses, or enterprises. We analyzed WHOIS results for public IP addresses used by ICS, and found:

- At least 87.7% of IP addresses (164,905) are registered to telecom providers (including cellular and satellite networks), so we were unable to identify their real owners.
- At least 3.1% of hosts (5,828) belong to the research and education area: universities, colleges, schools, etc. The available ICS components can be used to support the infrastructure of the corresponding buildings (electricity, air conditioning, etc.). But it’s also likely that these components are test systems used for research purposes.
- Among other users we identified 1,433 large organizations, including those belonging to the following industries: **electricity, aerospace, transportation (including airports), oil and gas, metallurgy, chemical, agriculture, automotive, utilities, drinks and food manufacturing, construction, liquid storage tanks, smart cities, and ICS vendors**.
- There are also government institutions (including police), medical centers, financial organizations, resorts, hotels, museums, libraries, churches and multiple small businesses among the identified owners of remotely available ICS.

To find out how many systems could be used by large organizations (in addition to the ones where owners were identified), we prepared a non-exhaustive list of industrial-grade ICS components that are unlikely to belong to smaller companies due to their specifics and cost, and we added this criterion to our analysis. As a result, we found that **at least 17,042 ICS components on 13,698 different hosts in 104 countries are likely to belong to large organizations**. The availability of these components on the Internet brings with it significant risks. However, **the real number is probably much higher**, because many ICS solutions, not included in the check list, could also be used by large organizations.

The Top three countries with available ICS components likely belonging to enterprises are **the United States of America** (2,994 hosts – 21.9%), **France** (1,331 hosts – 9.7%) and **Italy** (1,100 hosts – 8%).

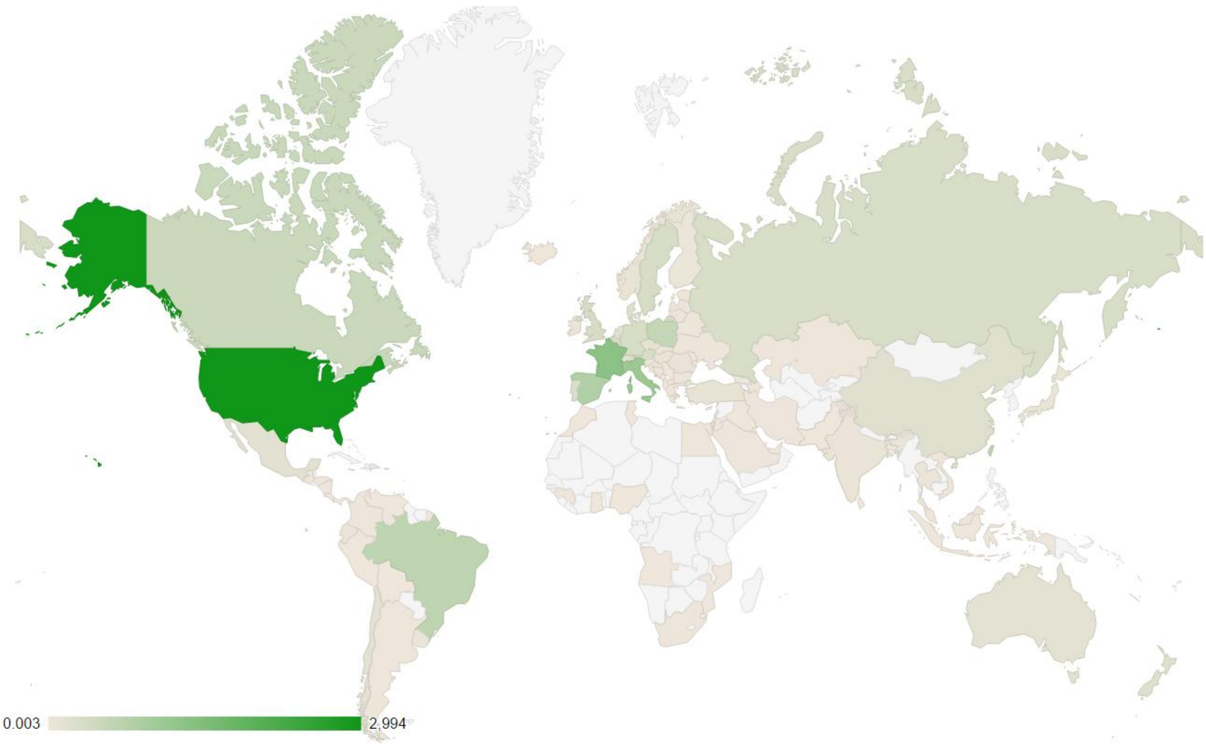

Figure 8. Countries with available enterprise-level ICS components (estimated lower bound)

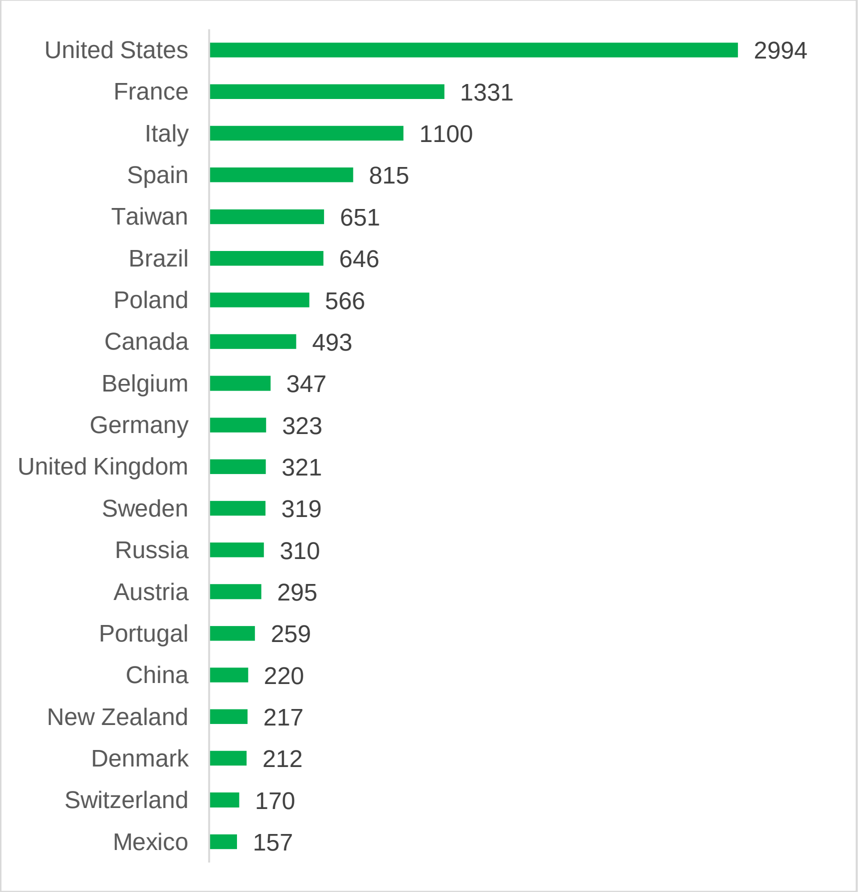

Figure 9. Top 20 countries with available enterprise-level ICS components (estimated lower bound)

The most widespread systems likely belonging to the enterprise segment are from the following vendors **Moxa** (5,057 services – 29.7%), **Siemens** (3,559 – 20.9%), **Rockwell Automation** (2,383 – 13.9%), and **Schneider Electric** (2,107 - 12.4%).

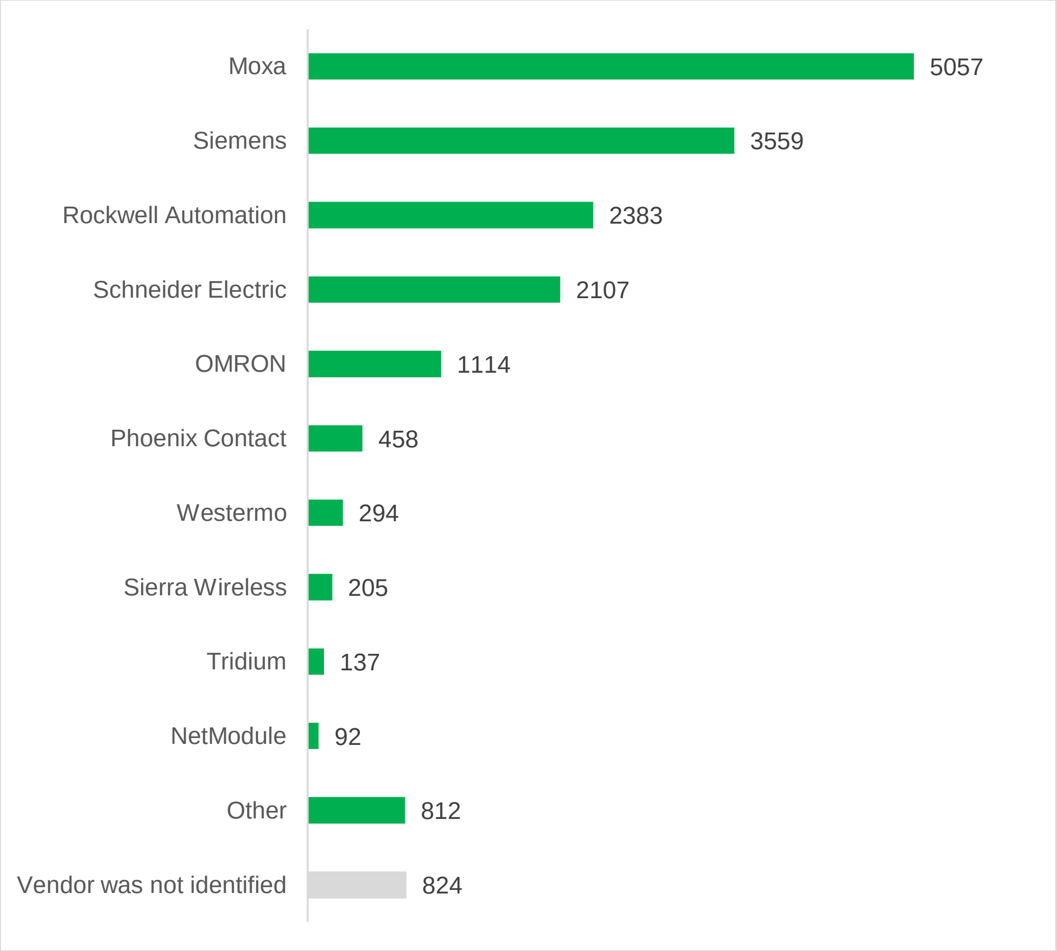

Figure 10. Top Ten ICS vendors in the enterprise segment

3.6 Vulnerable ICS components

Based on information from ICS component banners, we checked these resources for the presence of known vulnerabilities in the corresponding software and hardware versions. In total, **we found 13,033 vulnerabilities on 11,882 hosts, which corresponds to 6.3%** of all hosts with externally available components detected. The most widespread vulnerabilities revealed were:

- Sunny WebBox HardCoded Credentials (CVE-2015-3964) found on 11,904 hosts. This monitoring solution for medium- to large-scale solar power plants has hardcoded passwords, which makes it easier for remote attackers to gain full access to the system.

Vulnerabilities CVE-2015-1015 and CVE-2015-0987 in Omron CJ2M PLC devices were found on 342 devices in total. These devices use a recoverable format for password storage in object files on Compact Flash cards, and the first of the mentioned vulnerabilities makes it easier for local users to obtain sensitive information by reading a file. Meanwhile, the latter vulnerability exploits the fact that the password is transmitted in clear text to unlock the PLC for modification, leaving the password vulnerable to packet sniffing. The CVSS base scores assigned to these vulnerabilities indicate that they are high risk.

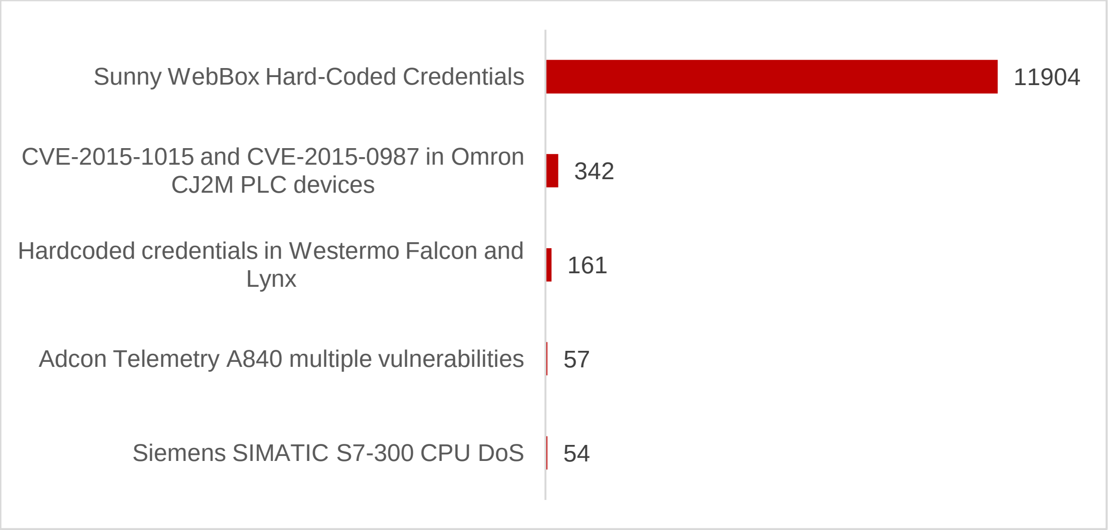

Figure 11. Top-5 vulnerabilities on ICS components

Combining these results with statistics of usage of insecure protocols (as described earlier in section 3.4), we were able to estimate **the total number of externally available vulnerable ICS hosts as 172,982 (92%)**. In most cases (87%) the hosts contain medium risk vulnerabilities. However, 7% of the vulnerable hosts have critical vulnerabilities.

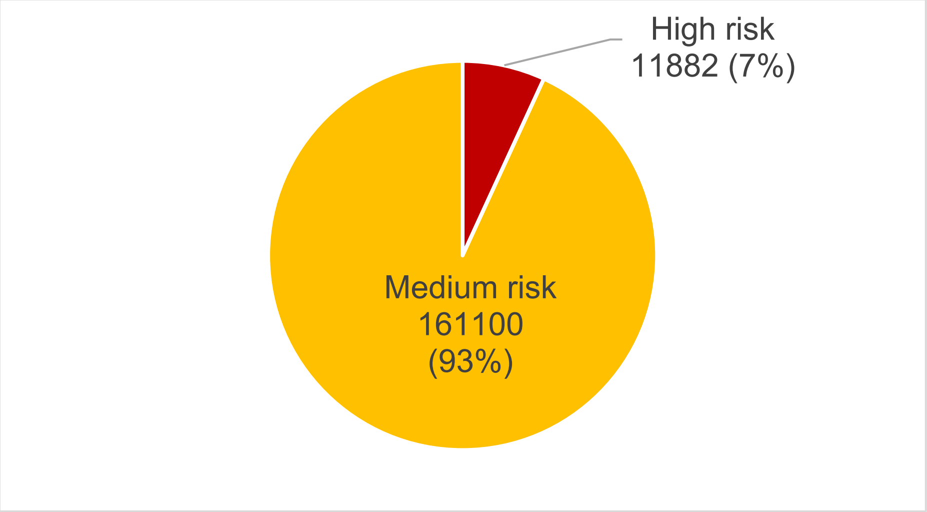

Figure 12. Statistics of vulnerable hosts (by maximum vulnerability severity level per host)

As to the hosts belonging to large organizations (as identified previously in section 3.5), 12,425 of them (90.7%) use insecure protocols. On 453 hosts (3.3%) we found other types of vulnerabilities. **The total number of externally available vulnerable ICS hosts that are likely to belong to large organizations, is 12,483 (91.1%)**.

453 hosts, including hosts belonging to energy, transportation, gas, engineering and manufacturing organizations, contain critical vulnerabilities. 96% of vulnerable hosts contain medium-risk vulnerabilities. Among these hosts there are some belonging to the energy, oil and gas, transportation, aerospace, agriculture, automotive, smart cities, drinks and food manufacturing industries.

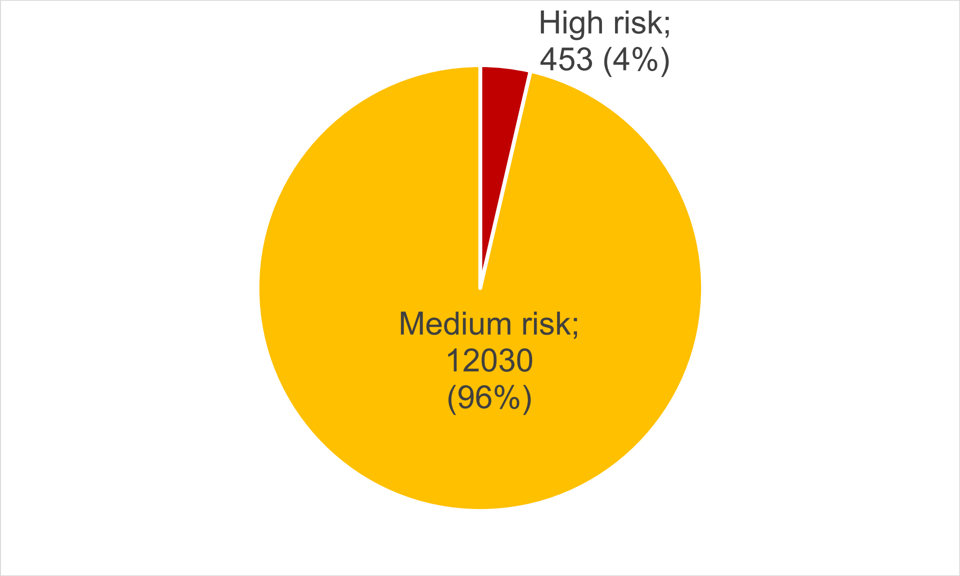

Figure 13. Statistics of vulnerable enterprise hosts (by maximum vulnerability severity level per host)

We also detected external hosts with medium-risk vulnerabilities within the network ranges belonging to ICS vendors. It's notable that the vendors' own solutions were not the only ones available in the networks of ICS vendors.

It's worth mentioning that the above results are only low estimations, and the real number of available ICS components associated with significant risks could be much higher. Besides, vulnerability risk levels were assessed based on CVSS v2 and CVSS v3 base scores, which are general estimations. However, in ICS environments, even when vulnerabilities are not classified as critical, if they are exploited they could have a serious impact on the infrastructure (depending on the system peculiarities). For example, successful exploitation of the Siemens S7 protocol security flaws (estimated as having medium-risk) could lead to the unauthorized reflashing of Siemens PLCs. These are similar to the devices targeted by the Stuxnet worm, and a total denial of service could be possible, hampering corresponding technological processes.

4 Conclusion

The cybersecurity of ICS is closely tied with the physical safety of populations. Yet, the security of ICS is often not given the treatment it deserves. Small and medium businesses, as well as individuals, are completely reliant on vendors when it comes to the security of the Internet of Things. Consumers do not go beyond the simple basic steps from device manuals, obtaining ready-to-work and easily accessible, but also vulnerable devices. On the other hand, in the enterprise and government sectors, companies understand the high risks associated with the incorrect configuration of an ICS environment. However, because of that, system owners often consider ICS devices as “black-boxes”, and dread making changes in their environments, including the enhancement of cybersecurity measures.

The findings of this research are an additional reminder that the “Security through Obscurity” principle cannot serve as a good basis to achieve effective protection from modern attacks. The security of industrial control systems should not be jeopardised in favor of safety, especially because, here, security and safetyare inextricably connected.

Contact us at: intelligence@kaspersky.com (Kaspersky Security Intelligence Service)

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy