Threat landscape for the ICS engineering and integration sector. 2020

ICS reports service

Version: 1.0 (17.03.2021)

The threat landscape for computers in the ICS engineering and integration sector varies depending on a computer's environment, including its geographical location, ability to access external networks and services, and user behavior.

Object of research

For this research we have analyzed cyberthreats blocked on computers used to engineer, configure and maintain industrial control equipment and software on which various software packages for the ICS engineering and integration industry are installed, including human-machine interface (HMI), OPC gateway, engineering, control and data acquisition software.

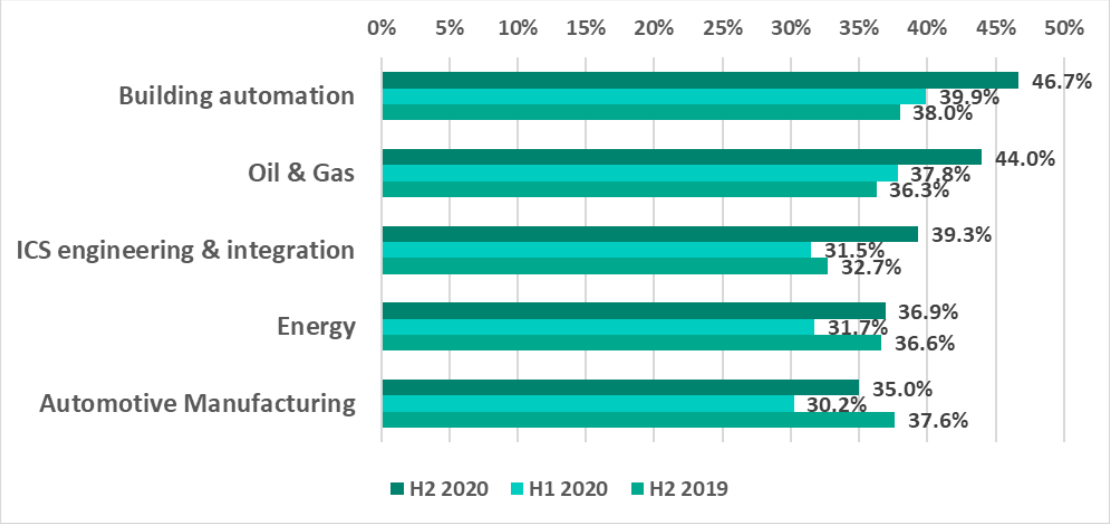
A key aspect in which of the ICS engineering sector is different from other industries is that an ICS engineering computer often has direct and indirect connections to various industrial control systems, some of which may even belong to other industrial enterprises. And while an ICS engineering computer has more access rights and fewer restrictions (such as application control, device control, etc.) than the average ICS computer, it also has a wider attack surface. A typical ICS engineering computer:

- allows the user to install any software;
- provides access to both ICS and corporate networks simultaneously;
- is used to access the internet, email services, network file shares and instant messengers.

At the same time, we noticed that ICS engineering environments normally react to new threats much faster than the average ICS computer environment. In a typical ICS environment, a computer can be repeatedly hit by the same malware (often by the same threat) due to a constant source of infection, which is normally not the case for the environment at an ICS engineering company.

The percentage of computers on which malware was blocked

In H2 2020, Kaspersky products were triggered on 39.3% of computers in the ICS engineering and integration sector. The percentage of computers in the ICS engineering and integration sector on which malware was blocked in H2 2020 (39.3%) was higher than the percentage for H1 2020 (31.5%). The last six months of 2020 also saw an increase in the percentages for several industries, including building automation, automotive manufacturing, energy and oil & gas, though the biggest increase (7.8 p.p.) was in the ICS engineering sector.

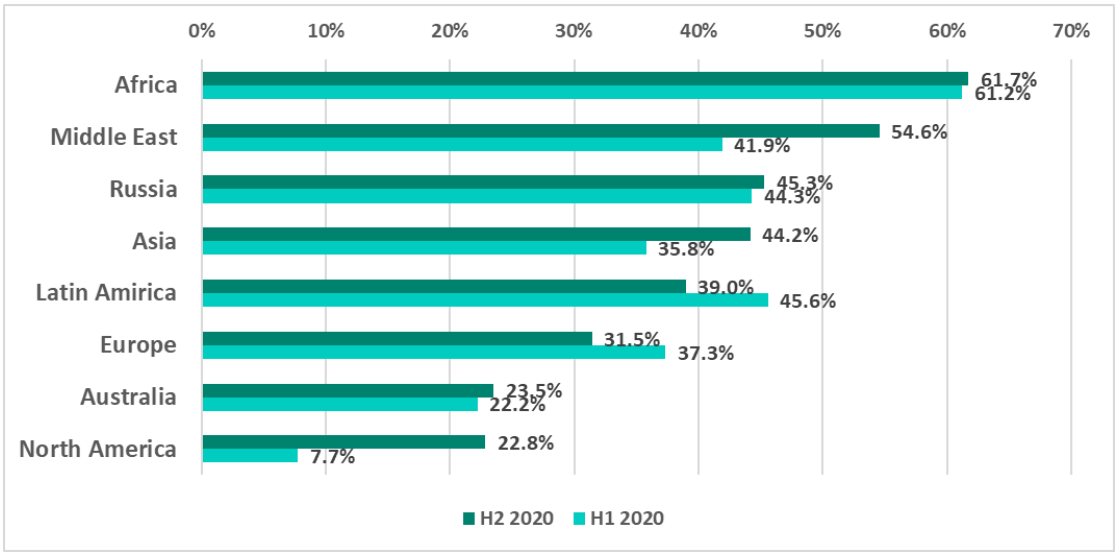


Percentage of ICS computers on which malware was blocked by industry
H2 2019 – H2 2020

The threat landscape for computers in the ICS engineering and integration sector varies depending on a computer's environment, including its geographical location, ability to access external networks and services, and user behavior.

Geography

In Latin America, the Middle East, Asia and North America the percentage of ICS computers in ICS engineering environments that had malware blocked on them in H2 2020 was higher than the percentage for H1 2020. This was in contrast to Africa, Russia and Europe where the percentage for H2 2020 was lower than that for H1 2020.



Top regions by percentage of computers in the ICS engineering sector on which malware was blocked, H1-H2 2020

The North America region demonstrated the highest percentage increase (15.1 p.p.) in H2 2020 (22.8%), mainly associated with an increase in the number of web-miners blocked. The second region showing a significant percentage increase (12.7 p.p.) in H2 2020 (54.6%) compared to H1 2020 (41.9%) was the Middle East. The increase in the Middle East region was mostly due to an outbreak of Fast-Load AutoLISP modules that spread within infected AutoCAD projects and other self-propagating worms that spread via USB.

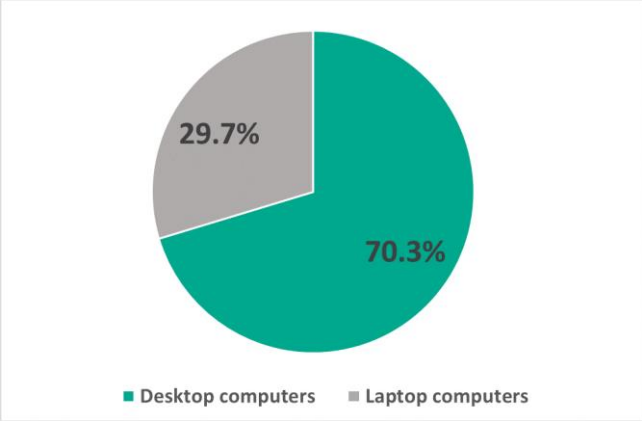
ICS engineering companies in southern and eastern regions of Europe mainly encountered phishing emails that were used to deliver spyware and cryptominers, which are usually capable of spreading inside a network either automatically or manually. These worms use various techniques for network propagation, like credentials abuse, exploitation of vulnerabilities (SMB, MS SQL, RDP, etc.) and brute forcing credentials.

Environment

The environment of a computer in the ICS engineering and integration sector significantly affects the computer's threat landscape. For instance, an isolated computer is likely to be less vulnerable to attacks than a computer that has access to the internet or that is used outside a secured network perimeter (e.g., laptops).

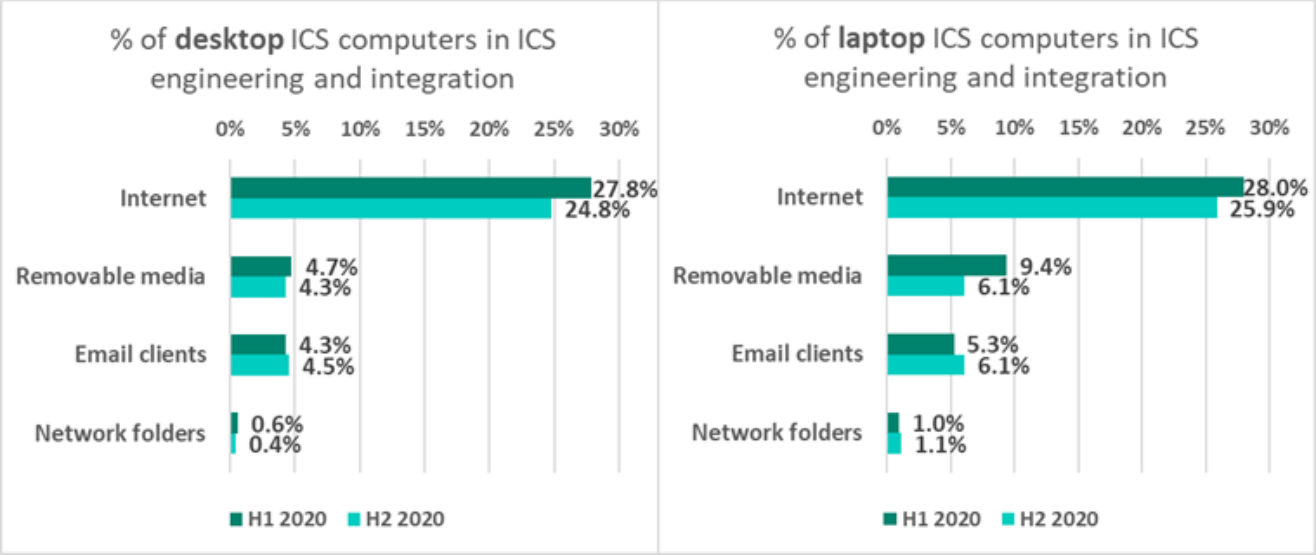
Laptops vs. desktops

Our dataset shows the proportion of laptop (29.7%) and desktop (70.3%) computers used in ICS engineering and integration.



Proportion of laptop and desktop computers in the ICS engineering sector, H2 2020

Compared with desktop computers, laptop computers used in the ICS engineering sector show a higher rate of threats delivered with internet content, removable media devices, email clients and network folders.

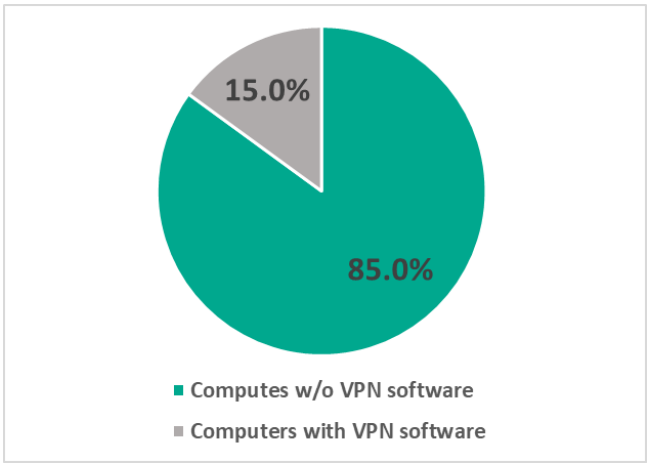


Threat sources by percentage of computers in the ICS engineering sector on which malware was blocked, desktop computers vs. laptops, H1-H2 2020

This means that a laptop used in the ICS engineering sector usually has less protection (more vulnerable to attack) than a desktop, and at the same time laptops usually have the same permissions as secured desktops in an ICS environment.

VPN software

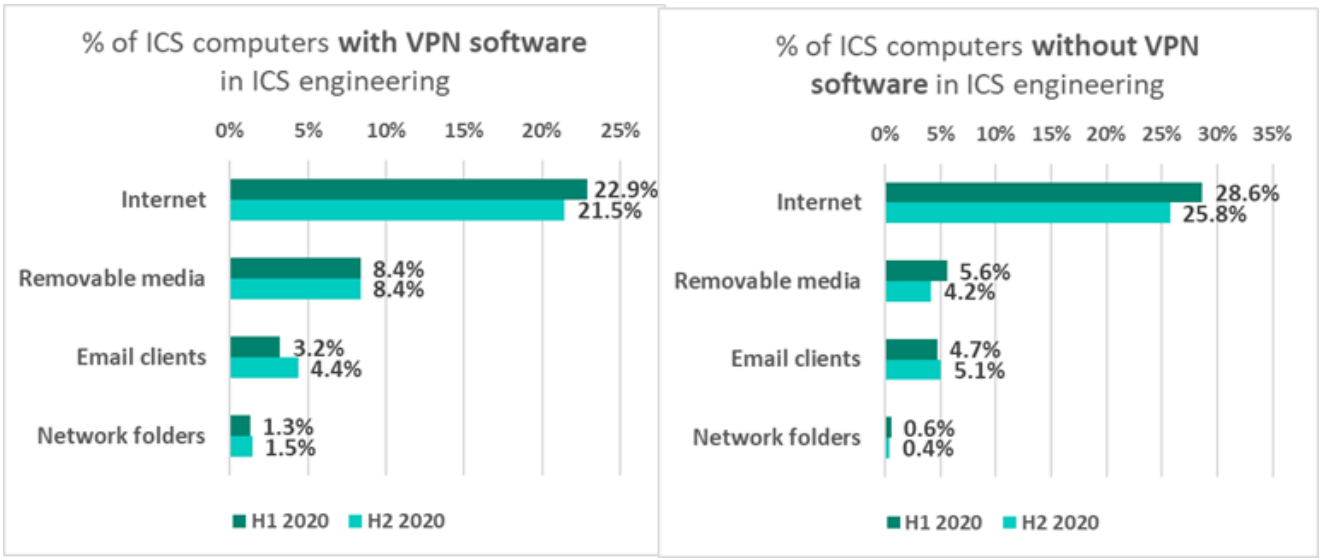
Both laptop and desktop computers used in ICS engineering and integration can be broken down into groups of computers that use VPN software (15%) and those that don't (85%), and analyzed further.



Proportion of computers in the ICS engineering and integration sector with and without VPN software, H2 2020

Computers in the ICS engineering sector that use VPN software clearly have a smaller attack surface and, in particular, encounter fewer of the internet threats that are usually delivered along with the content of web services. That's probably because those using VPN software tend to be more security conscious or the configuration of their VPN tunnel is designed to route all the traffic through the tunnel, which may have network security measures in place to filter out dangerous content.

At the same time, computers with VPN software show a higher percentage of threats delivered via removable media and network folders.

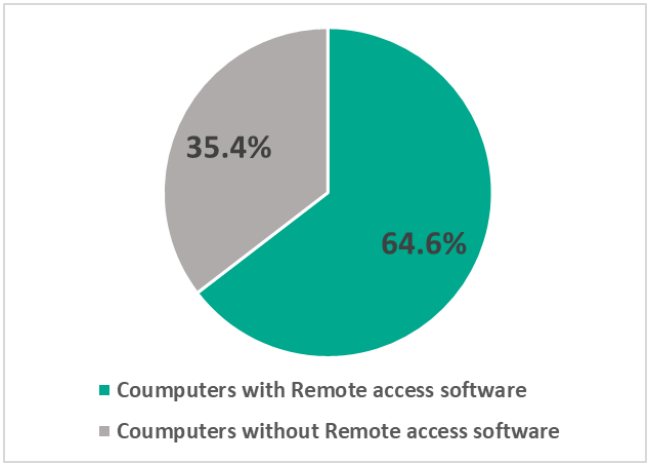


Threat sources by percentage of ICS computers with and without VPN software in the ICS engineering sector on which malware was blocked, H1-H2 2020

From time to time, the various viruses and worms that have been spreading for a decade between computers in ICS environments via USB devices or network folders hit the computers of ICS engineers. Such threats were blocked more often on computers with VPN software.

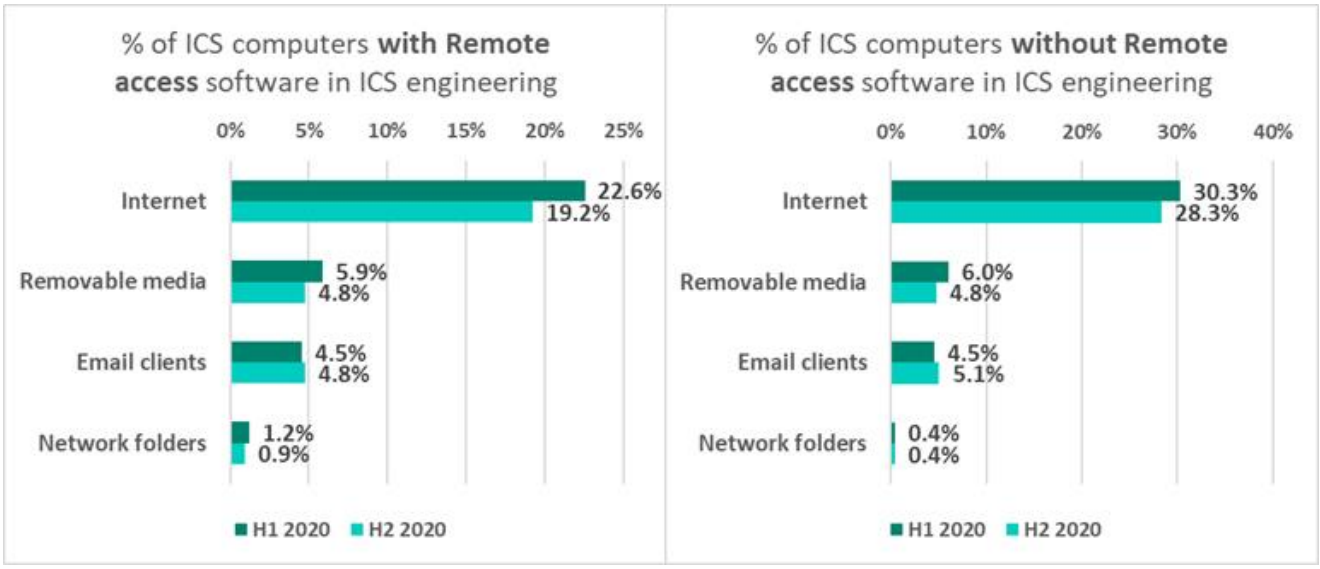
Remote access software

In addition to analyzing computers with and without VPN software, we also analyzed groups of computers with and without remote access software (64.6% and 35.4% respectively).



Proportion of computers in ICS engineering and integration with and without remote access software, H2 2020

Both groups (computers in the ICS engineering sector with and without remote access software) have a fairly similar threat landscape except for threats delivered with internet content – the percentage for this type of threat is significantly lower for computers on which remote access software has been used.



Threat sources by percentage of ICS computers with and without remote access software in the ICS engineering sector on which malware was blocked, H1-H2 2020

Some computers that use remote access software evidently also use VPN software, meanwhile using internet less frequently than computers without remote access software.

Although computers using remote access software show a lower percentage of internet threats, we encounter many cases of attacks on network services such as SMB, MS SQL and RDP. The majority of these attacks are due to worm outbreaks in a subnet (physical or virtual). Those worms use Mimikatz and spread over the network by abusing stolen credentials, exploiting an RCE vulnerability or by successfully running brute-force attacks on a network service.

The full report is available on Kaspersky Threat Intelligence.
For more information please contact ics-cert@kaspersky.com

Recommendations

The following measures are necessary to ensure adequate protection of ICS systems:

- Ensure that ICS engineering computers and especially laptops are well protected from network attacks, web-based threats and phishing campaigns, including targeted attacks. To achieve this, consider using modern threat detection technologies – both at the network perimeter and on all endpoints inside and outside the perimeter.
- Install all OS and application software updates in a timely fashion, with particular emphasis on security updates, or apply workaround protection measures when installing updates is not an option.
- Regularly train employees to recognize suspicious behavior by a computer or application, as well as fraudulent emails and instant messages.
- If possible, restrict the use of any unnecessary but dangerous and/or vulnerable software that widens the attack surface, including remote access software, office solutions, PowerShell, Windows Script Host, etc.
- Monitor the execution of files in the organization and use application control with Default Deny to limit the use of applications to only those apps that are allowed.
- Restrict the use of USB devices to only those that are trusted and encrypted. The implementation of such restrictions should be monitored. Many modern host protection tools include the necessary functionality.
- Use different accounts for different users. Manage the rights of user and service accounts in such a way as to prevent an infection from spreading across the enterprise if an account is compromised. Log and monitor the use of administrator functions.
- Restrict the rights of users on their systems, as well as corporate service access rights, leaving the minimal set of rights required for specific employees to perform their work.
- Maximize granular access control. Limit the use of privileged accounts. When possible, admins should use accounts with local administration privileges or with administration rights to specific services and avoid using accounts with domain administration rights.
- Audit the use of privileged accounts and regularly review access rights.
- Use group policies that require users to change their passwords on a regular basis. Introduce password strength requirements.
- Configure the OS to always show file extensions for all file types in order to see files with double extensions (a tactic used to trick users).

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