kaspersky

Policy Newsletter Kaspersky

First semester 2020

Foreword

Do you remember what you were doing on March 10 this year? I do! I had my last business trip in Europe before the Corona lockdown. On that day, I had a complete different view of the world than I have today. On that day, many questions I answered totally different compared to today. I could not imagine the many drastic but necessary and sensible restrictions to control the Corona pandemic. I had different ideas about good routines. For example, whether it makes sense to meet a previously unknown person for the first time in business via video meeting. Or, whether remote learning is possible at schools? We have very challenging months behind and ahead of us. We must continue to change and learn. Moreover, courageously push ahead with digitalization. This is what the Corona crisis has taught me, besides the fact to be on guard. This is especially the case when it comes to cybersecurity. With this first edition of our newsletter we would like to contribute to this. I would be delighted if you could pick up one or two impulses while reading it and we could start a conversation. I look forward to your feedback.

Jochen Michels
Head of Public Affairs
Europe, Kaspersky

GTI: Kaspersky launches Cyber Capacity Building Program to further secure ICT ecosystem

Kaspersky's Global Transparency Initiative (GTI) is evolving even further. Already announced initiatives – such as the relocation of European users' data to Zurich; the opening of Transparency Centers in several countries to allow source code review; the confirmation of Kaspersky's reliable and secure engineering practices through the independent SOC 2 audit by one of the 'Big Four' firms and the ISO27001 certification for Kaspersky's data services – have already earmarked the GTI as an unique initiative to increase transparency and trust in cybersecurity. However, in May, Kaspersky further advanced its Global Transparency Initiative in multiple ways. In particular, we launched:

Cyber Capacity Building Program

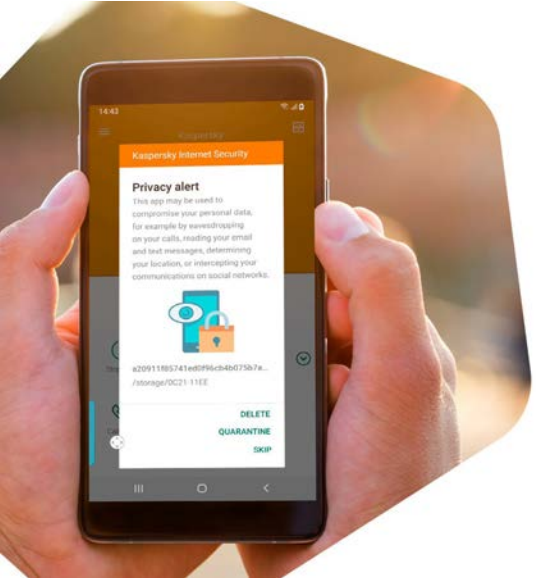
A dedicated training program for product security evaluation to help businesses, government organizations and academic institutions develop skills for assessing their supply chain cyber-resilience. As part of global supply chains and/or critical infrastructure networks, different components of the IT infrastructure can be compromised, causing harm to public security as well as economic and social wellbeing. Luckily, there are ways in which organizations can evaluate and ensure the security and integrity of these elements. To assist in this, Kaspersky developed a Cyber Capacity Building Program that will be available in both online and offline formats in English, and which will be provided free of charge. The training will offer an introduction to product security evaluation and threat modeling, as well as source code review and vulnerability management. To take part, please click here.

Virtual availability of our Transparency Centers

With the reality of global self-isolation and social distancing, we need to make sure key services are not limited by physical access. To ensure this, we launched remote access to services of our Transparency Centers, by providing a 'blue-piste' assessment option – which is the best option for getting acquainted with both the company's engineering practices and unparalleled data protection standards. Request a tour here.

Ethical principles for the Responsible Vulnerability Disclosure

With this, we are laying out how we work with researchers and the security community to better manage product security. These principles, inspired by our experience and guidelines provided by FIRST, are aimed at enhancing transparency and efficiency in vulnerability handling and mitigating harm and risks to users. Learn our principles here.


14:43
Kaspersky
Kaspersky Internet Security
Privacy alert
This app may be used to compromise your personal data, for example by eavesdropping on your calls, reading your email and text messages, determining your location, or intercepting your communications on social networks.
DELETE
QUARANTINE
SKIP

Domestic violence: stalkerware, a growing cyberthreat

Stalkerwares » ou « spousewares » : behind these terms lies a recent but growing threat. In short, these refer to tracking software that makes it possible to follow a person's private life by accessing their personal information: contacts, call logs, photos, videos, SMS messages and even physical location. As things stand, they can be bought legally and installed by anyone with physical access to your phone, and can even be hidden behind the download of an otherwise innocuous program. The threat is that victims did not give consent, which leads to stalkerware spying on victims without their knowledge. And even if the surveillance and hacking takes place online, the consequences are often very real for the victims, as this software can be used by individuals with abusive behaviour, such as in the case of domestic violence or harassment.

In response to the increasing use of such spywares that so far are still legal, Kaspersky and nine partner organisations from different countries - Avira, the Electronic Frontier Foundation, the European Network for Working with Perpetrators of Domestic Violence (WWP EN), DATA CyberDefense, Malwarebytes, the National Network Against Domestic Violence (NNEDV), NortonLifeLock, Operation: Safe Escape and WEISSER RING - launched the « **Coalition contre les stalkerwares** » (www.stopstalkerware.org) in November 2019.

COALITION AGAINST STALKERWARE

The founding members, originating from the cybersecurity community and non-profit organizations working on domestic violence, started with creating a standard definition for stalkerware and reaching a consensus on detection criteria, which has made it possible for the IT security industry to start working on the practical aspects of the issue. The Coalition's objectives today include:

- improving detection and mitigation of stalkerware,
- increasing technical capacity of survivors and advocacy organizations, and
- raising awareness.

+32%

Increase in the number of users of Kaspersky solutions facing stalkerware in 2019, with the number of attacks doubling during the second half of the year.[1]

A global phenomenon

Russia, Brazil, India and the United States are the most affected countries in the world. In Europe, Germany, Italy and France are the three countries where stalkerware is most used.

70 %

of women who have experienced cyber stalking have also experienced at least one form of physical or/and sexual violence from an intimate partner, according to research from the European Institute for Gender Equality.

Given the social importance of the subject, the regular appearance of new forms of stalkerware, and the complexity of the problem in real-life situations (such as that if spyware is detected, its removal by the victim can lead to physical violence), the Coalition against Stalkerware is currently calling for an even broader cooperation. 11 new members, many of them originating from the European Union, joined the Coalition in May 2020. At local level, Kaspersky is also collaborating with other key entities such as the French Ministry of the Interior in order to provide technical training to those involved in the fight against domestic violence.

« According to the study[2] conducted by the Center Hubertine Auclert in France on cyberviolence in intimate relationships, 21% of victims have experienced the use of stalkerware by their abusive partner, while 69% of victims have the feeling that their personal information on their smartphone has been accessed by their partner in a hidden way. Overall, stalkerware is an important source of danger and distress for victims. The Coalition is a great opportunity to bring together the expertise of the IT security sector and of NGOs specialized on violence against women. This synergy on an international level will be fruitful to create together the best solutions for victims' protection »

Clémence Pajot, Director of the Centre Hubertine Auclert

The mission of the Centre is to promote equality and combat violence against women in the Paris region.

[1] https://securelist.com/the-state-of-stalkerware-in-2019/93634/
[2] https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018

COVID-19 crisis: what impact on the cybersecurity of organizations and individuals?

3 questions to Marco Preuss, senior security researcher within the Global Research & Analysis Team (GReAT) of Kaspersky.

Has there been an increase in cyber attacks during containment?
Containment has rapidly become a race for large 'cyber figures' given without sufficient explanation, where the real reason is product advertising. In May for example, one publisher noted "an increase of more than 30,000% in attacks". Where would the human capacity for such an increase come from, when the whole world is being confined and activities are being degraded? With equal capacities, would this mean that in normal times attackers operate at a voluntarily slow? No, the means that enable computer attacks have not increased tenfold, and the motivations behind them are stable. Our data show that there has been no overall increase in the number of malicious code detections between the January-May 2020 period and the same period in 2019 worldwide. On the other hand, the attention surrounding the subject COVID-19 has been well exploited to carry out cyber-attacks: in particular, the appearance of this subject increased by 43% in phishing attempts between January and March. Cybercriminals have also proposed trapped videoconferencing applications, false certificates, notifications of failed parcel deliveries, or even false dismissals by email. Our solutions have also seen a 25% increase in the detection of Internet-based threats between January and April 2020. We could be tempted to justify this phenomenon by an increase in the number of attacks exploiting these vectors. However, an increase in the number of detections may also be simply a consequence of greater digital usage during containment, and does not necessarily mean that there have been more attacks, or that they have been more successful.

Free protection for 2,000 healthcare organizations during the pandemic

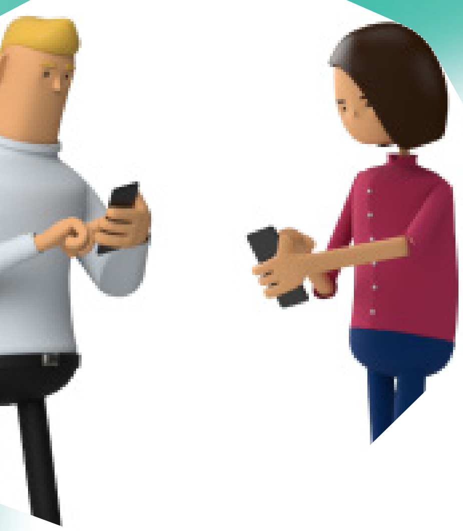
In solidarity in the fight against COVID-19, Kaspersky has provided full 6-month licenses free of charge to public and private health facilities wishing to enhance their security. More than 1,500 hospitals and healthcare organizations worldwide have benefited from this offer and priority support.

The situation has led to massive recourse to teleworking. What lessons can be learned from this period of large-scale experimentation?

Teleworking resources (VPNs, collaborative or videoconferencing platforms, laptops, etc.) had to be quickly exposed or distributed outside the usual perimeters of control. In the rush, security measures may have been neglected. However, an attack on the availability of these resources (e.g. denial of network services or ransom, for example) would profoundly disrupt any activity in this already disrupted situation. IT tools are essential to any organization, and support a survival challenge in such a crisis. Organization managers must therefore agree to devote security resources and efforts commensurate with the stakes, before a crisis occurs: in the case of an exceptional situation, I like to be sure that I would not have to face the unexpected on paper mode, without employees, with an IT disaster as a handicap. The second lesson is that modern digital means of work are meant to be collaborative and distributed by construction - so much the better; but that their safe exploitation in teleworking requires the adoption of the defence-in-depth paradigm. All too often, security is still based on a limited and controlled perimeter (the company, its network and premises), which protects from the "rest". It must be considered that any IT resource (including data and workstations) can be exposed individually, anywhere, and must therefore be protected independently. This requires, in particular, the ability to maintain the remote workstation in secure conditions. Many other lessons can be learned, but I choose this last point of vigilance: various solutions marketed under the name of cloud may appear to be the answer to all the digital challenges highlighted by this crisis. They must be subject to at least as much security effort as the legacy solutions. In addition, they introduce a third party dependency that is difficult to mitigate, which can become a major vulnerability in the event of a crisis, as well as additional difficulties in controlling data. The use of such solutions can also lead to a further reduction in the company's own IT capacity, which is essential for managing exceptional situations.

In the absence of an increase in the number of cyber attacks, has there been any development in this area during a pandemic?

As early as January, targeted campaigns with malicious messages have targeted government organisations in Asia and Europe. Most of the malicious material we discovered in this context included statistics on the spread of the virus, as well as minutes of international meetings. However, the intrusion techniques used by these actors did not change during the pandemic. Other advanced actors released malicious mobile applications under the guise of infection tracking tools, sometimes usurping official national tools, such as "Aarogya Setu" in India. We also found that health sector organizations, including international ones, had been particularly targeted earlier this year. The latter were probably targeted for intelligence purposes on health crisis management, to anticipate international policies. With computer intrusion now an assumed component of many intelligence devices, and coronavirus a major concern, this was to be expected. We have also identified a few cases of targeted ransom attacks that have exploited known vulnerabilities affecting VPN access gateways. It is possible that these devices were particularly targeted during the pandemic, because attackers wanted to take advantage of their hasty exposure, and because affected targets are likely to be more likely to pay ransom in a crisis situation. Finally, we also observed a significant increase (80%) in the number of network denial of service attempts in Q1 2020, compared to the same quarter in 2019. These attempts were mainly aimed at educational and public resources, such as the organization of Paris hospitals (APHP) in France. In short, it should be remembered that no crisis situation justifies a truce for the attackers, and that on the contrary, any event provoking attention will be exploited. In order to reduce uncertainty and avoid over-incidents, there is no choice but to adopt a permanent defence-in-depth posture for its IT resources, or even to prepare business continuity measures that provide for the unavailability of these resources.



Securing e-voting to support the development of e-democracy

Online elections have obvious advantages: they allow the organizer to reduce costs and the voter to save time by avoiding queues or traffic jams. Nevertheless, Internet voting requires significant investment to ensure that it is implemented with strong security safeguards in place. It has therefore often been difficult to justify the need to introduce this option.

However, the current requirement for social distancing makes society more digital in multiple ways. As such, there is also an increased interest in electronic voting within local and regional authorities - which are already experimenting with it through participatory budgets - but also and above all for the boards of directors and general assemblies of companies, associations, trade unions and political parties. We are convinced that this trend will accelerate, and that self-isolation measures at the global level will eventually change people's attitude towards distance voting.

Kaspersky is contributing to this transition by offering its new remote voting platform based on cyber security. The Polys project (www.polys.me) consists of a turnkey online voting system based on blockchain technology and, even more importantly, a decentralized architecture across multiple nodes that can be stored with a trusted third party in the cloud or on-premise, based on the organiser's choice. As a latest addition to our offering, we now also provide secure physical voting machines and ballot boxes connected to the blockchain. Our mission is clear: to ensure the integrity and inviolability of electronic voting.

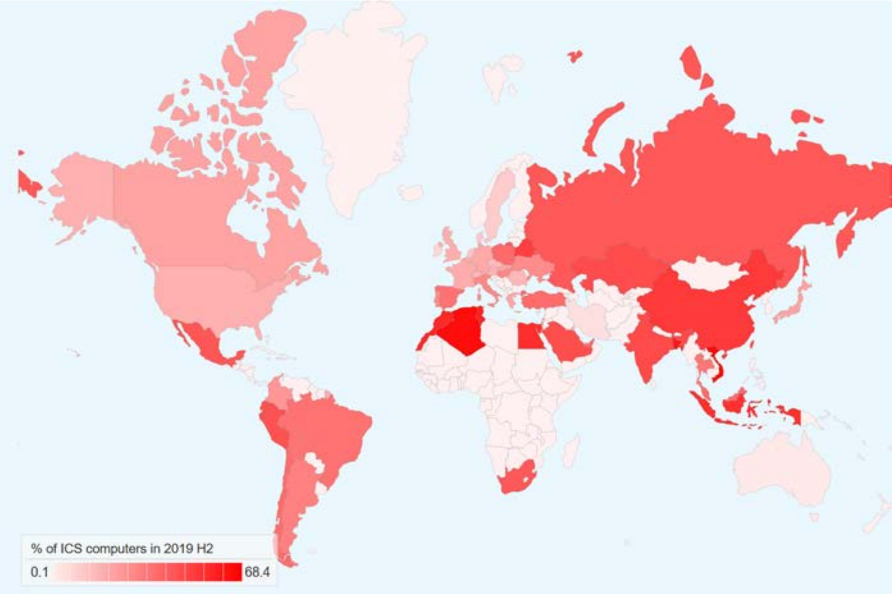
Cybersecurity of critical industrial systems: nearly twice as many vulnerabilities identified in one year

New research by Kaspersky's ICS CERT on threats to industrial control systems (ICS) identified 103 new vulnerabilities in 2019 that could be exploited by cyberattacks - almost double of the 61 reported in 2018. Of these, 33 were still not fixed by manufacturers at the end of the first quarter of 2020.

But the threat is real: **in 2019, malicious objects were blocked on nearly one out of every two ICS systems** (46.4%) participating in the Kaspersky Security Network, be they automation software, industrial control systems or Internet of Things (IoT). It is interesting to note that generic threats also target specialized industrial systems: ransomware (Wannacry - again, GandCrab...) was blocked on 1% of the ICS systems protected by Kaspersky, representing the most potentially devastating threat, particularly in Southeast Asia and Northern Europe.

The energy sector is among the most affected worldwide: 36.6% of ICS systems in the Power & Energy sector have been targeted by an attack, and 36.3% in the Oil & Gas sector. Other critical infrastructures and essential services – such as water treatment, health and food processing – are at the top of the list in terms of detection of vulnerabilities. These trends, unfortunately not very surprising, confirm the importance of regular security audits and active monitoring (threat intelligence) to protect against traditional cybercriminals as well as advanced persistent threats.

To learn more: https://ics-cert.kaspersky.com/



Geographical distribution of attacks* on industrial automation systems, H2 2019

* percentage of ICS computers on which malicious objects were blocked

Kaspersky’s first EU policy webinar inspires lively debate among diverse stakeholders

Technology that works for people: Why the right level of cybersecurity is crucial for digitalization” - this was the question discussed on the 9th of June by high-profile speakers from the EU and Member States at the first Kaspersky Webinar on the challenges and requirements for European cybersecurity policy. And it seems that we hit the mark with the topic and the speakers: more than 100 participants took part in this interesting exchange of ideas.

One aspect quickly became clear: digitization opens up great opportunities and there is no alternative. But cyber-vulnerability has increased over recent years, and this trend has been accelerating recently with the lockdown situation due to the pandemic, as remote working and greater use of the internet opens up new opportunities for cybercriminals.

This situation also implies a need for a long-term reflection effort: **Luisa Franchina**, President of the Italian Association for Critical Infrastructure, is calling on European stakeholders to engage in broader thinking about business continuity and crisis management. According to her, trust, transparency and common security standards should serve as the basis of a more secure digital space.

Axel Voss, a very experienced Member of European Parliament, stressed that policy fragmentation across the EU is a disadvantage. He argued that the Union will have to clarify the legislation of the digital single market to be able to react faster in a more effective way, to tackle upcoming cybersecurity challenges, and achieve cyber-resilience. For this, he recommended a transnational dialogue involving all cybersecurity stakeholders, arguing that “*acting in a united way is the only way*”.

For his part, MP **Eric Bothorel**, Member of the French National Assembly, highlighted a massive ‘digital shift’ that has increased exposure to cyberattacks, citing the fact that over eight million French people are turning towards remote working. He emphasised that it’s hard enough to manage the digital transition, but at the same time the resulting increase in cyber risks have to be managed as well.

Cyber-immunity might be the solution to this problem. According to our CEO **Eugene Kaspersky**, current risk management methods are not sufficient to protect ever more complex infrastructure. Subsequently, we need to redesign the architecture of all systems toward security-by-design. In his words, “*security should become the DNA of systems: it is the only way to make them truly unhackable*”.

Finally, **Jakub Boratyński**, Acting Director for Cybersecurity at the European Commission, observed that at policy level the challenge is to identify the right mix of incentives to keep cybersecurity risks at an acceptable level. Further EU regulation should also assign responsibilities to actors – from states to security vendors and IT users – in a proportionate way.

Stay tuned for our further pan-European policy webinars!

If you wish to receive this newsletter (or no longer receive it), send us a message at kaspersky@political-intelligence.com

Kaspersky Europe

@Kaspersky_Gov @Kaspersky Kaspersky