The Cabinet decision on Kaspersky Lab

Reconstruction and analysis

```
// Scan features data by the current tree and return 0/1 (clean/detect).
int32_t tree_scan ()
{
    const Tree* tree = tp_fptr<Tree>();
    set_fptr(&tree->nodes[tree->num_nodes]); // skip the tree

    for (uint32_t node_ind = 1; ; )
    {
        // get current node and the corresponding compiled feature
        const Tree_Node& node = tree->nodes[node_ind - 1];

        const uint32_t prep_data_ind  = kl_get_unaligned_16_le(&node.feat_data_ind);
        const uint32_t node_param     = kl_get_unaligned_32_le(&node.param);
        const uint32_t node_left_ind  = kl_get_unaligned_16_le(&node.left_ind);
        const uint32_t node_right_ind = kl_get_unaligned_16_le(&node.right_ind);

        const Prep_Feat_Data_Ex& feat_data = m_prep_data[prep_data_ind];

        bool go_left = false;
```

Version: 1, 15 November 2018, case number: 2018-0086

Author: Brenno de Winter, De Winter Information Solutions

Consultancy: Hans de Raad, Barbara Bulten

Correction & translation: Transferendi B.V.

Status: FINAL

Table of contents

1. About the reporting

Grounds for the report

On 14 May 2018, the Dutch cabinet instructed the central government to stop using and phasing out Kaspersky Lab's antivirus software. Organisations that fall under the General Security Requirements for Defence Assignments (ABDO) or that fall under vital services and processes are advised to do the same. The advice does not apply to other organizations. The Cabinet also makes it clear that it only concerns the antivirus software, not the other Kaspersky Lab products and services. The Cabinet has three reasons for making this decision:

1. Antivirus software has extensive and in-depth access to a computer. Such access can be misused for espionage and sabotage.
2. As a Russian company, Kaspersky Lab is required by Russian law to cooperate with the government if requested to do so by the Russian intelligence services.
3. The Russian Federation has an offensive cyber program. The latter means that the country is actively engaged in espionage and sabotage with the use of computers.

In a letter to the Dutch Parliament [1] , the Cabinet refers to a precautionary measure based on fear of espionage and sabotage. In this context, the Cabinet writes that it has made its own, more stringent assessment in the context of national security. In essence, the Cabinet's fear is that the anti-virus software of Kaspersky Lab, a company that fights malware, will itself be used as a Trojan horse or malware.

The Netherlands does not have any examples showing that Kaspersky Lab's antivirus software has been abused. No examples are known to other (European) countries or the European Commission either. If public broadcaster KRO-NCRV successfully invokes the Government Information (Public Access) Act (or Wet openbaarheid van bestuur (Wob) in the Netherlands and the Freedom of Information Act (FOIA) in the USA) during a journalistic investigation, further documents become available.

Analysis

Brenno de Winter of De Winter Information Solutions was asked by Kaspersky Lab to make a reconstruction of the cabinet's precautionary measure and to analyse the three observations of the cabinet. In a time of digital operations it is logical and appropriate that the cabinet is alert to the dangers of espionage and sabotage. In terms of content and procedure, this report examines how the cabinet's argumentation came about, to what extent Kaspersky Lab does indeed pose a threat on the basis of this argumentation, and what steps would be necessary to deal with such a threat.

To do that, available documentation, relevant public sources and verification of findings by experts was used. An inspection was also carried out at the Kaspersky Lab Transparency Center in Zurich, Switzerland, where the source code of the antivirus software is available. Within the framework of the investigation, Kaspersky Lab has committed itself to cooperate fully, not to interfere with the content, not to exert pressure on the content and observations, and to agree in advance that the report will be made public regardless of the findings.

[1] Appendix 1, Letter to Parliament from the Minister of Justice and Security of 14 May 2018, reference 2268367.

Additional documentation

The report will also provide attachments with substantiation. The footnotes refer to this substantiation. Where possible, the underlying documents are added to the report or reference is made to a location on the internet to provide as accurate a substantiation as possible.

About Kaspersky Lab

The company Kaspersky Lab was founded in 1997 by, among others, Eugene Kaspersky. He started the company after being attacked by the Cascade virus eight years earlier and becoming interested in fighting malware. The company is active in 200 countries, with 35 offices in 31 countries[2] and provides antivirus software, knowledge and services in the field of information security. The company had a turnover of USD 707.6 million [3] (approximately EUR 624 million [4]) in 2017.

The Benelux office is located in Utrecht under the name Kaspersky Lab B.V.. This is a fully-fledged subsidiary [5] of the parent company Kaspersky Lab Limited [6] in the United Kingdom. Legally speaking, the company is a British company. The head office is in Moscow, Russia. The assembly of the software, the storage of European customer data takes place in Zurich, Switzerland.

Chapter 6 discusses Kaspersky Lab's reputation in the section ‘Relations with the Dutch government’

[2] https://www.kaspersky.nl/about/company - verified on 13 November 2018
[3] Appendix 19 page 514 ff.
[4] Calculated on 11 November 2018 with xe.com
[5] Copy of the Chamber of Commerce of 11 November 2018 - Appendix 18, page 508, 509
[6] https://beta.companieshouse.gov.uk/company/04249748 verified on 11 November 2018

2. Procedure for risk assessment

Comprehensiveness of the dossier

The letter to Parliament contains the considerations that led the Cabinet to the precautionary measure. There was no confidential briefing on this subject. In weighing the precaution, the guiding principle is that the cabinet correctly informed Parliament and did not withhold any information. In the case of a Wob request, the law requires a search for documents[7] (i.e. memos, reports, e-mails, letters, reports, summaries, notes, etc.). The government must make a decision about all documents - including those that are refused. The document lists [8] clearly show which steps have been taken towards the decision on phasing out Kaspersky Lab's software. The Wob request does not show that there is any reason to assume that other considerations, besides the available documents, played a role in the Cabinet's decision. The Cabinet's reasoning can be reconstructed on the basis of the available information and analysed chronologically.

Procedure followed

The letter to Parliament and the documents made public with the Wob request do not show which procedure the Cabinet followed to make a risk assessment and which decision criteria were defined in advance to arrive at a weighted decision. However, a number of steps and decision moments can be derived from the documents in the Wob application:

1. 13 September 2017. The Department of Homeland Security in the United States issues 'Binding Operational Directive 2017-01'[9]. In this, the US government obliges federal government agencies to start stopping the use of Kaspersky Lab products within 90 days.
2. 15 January 2018. The National Coordinator for Counterterrorism and Security (NCTV) prepared an internal risk analysis.
3. 15 January 2018. The CIO-Rijk sends out a request to gain insight into the use of Kaspersky software by at least government parties. He sends this message to the Chief Information Officers (CIOs), Chief Technology Officers (CTOs) and Chief Information Security Officers (CISOs). The request to CISOs is to reply by 19 January 2018.
4. 25 January 2018. Kaspersky Lab has understood through partners that an inquiry is in progress. In a letter,[10] the company offers all assistance with the investigation and points to a penetration test that is available and carried out in the Netherlands. No use is made of this option.
5. In the period 2 February 2018 to 6 May 2018, seven documents will be written by the NCTV to the Committee of United Intelligence Services in the Netherlands (CVIN) and the Security and Intelligence Council (RVI).
6. 14 May 2018. Various announcements of the upcoming decision by the National Cyber Security Centre (NCSC) follow.
7. 14 May 2018. Parliament is informed in a letter.

[7] A document is very broadly defined in the Government Information (Public Access) Act as 'a written document or other material held by an administrative body that contains information'
[8] Appendices 2, 3 and 4 to this report.
[9] Appendix 10
[10] Appendix 5

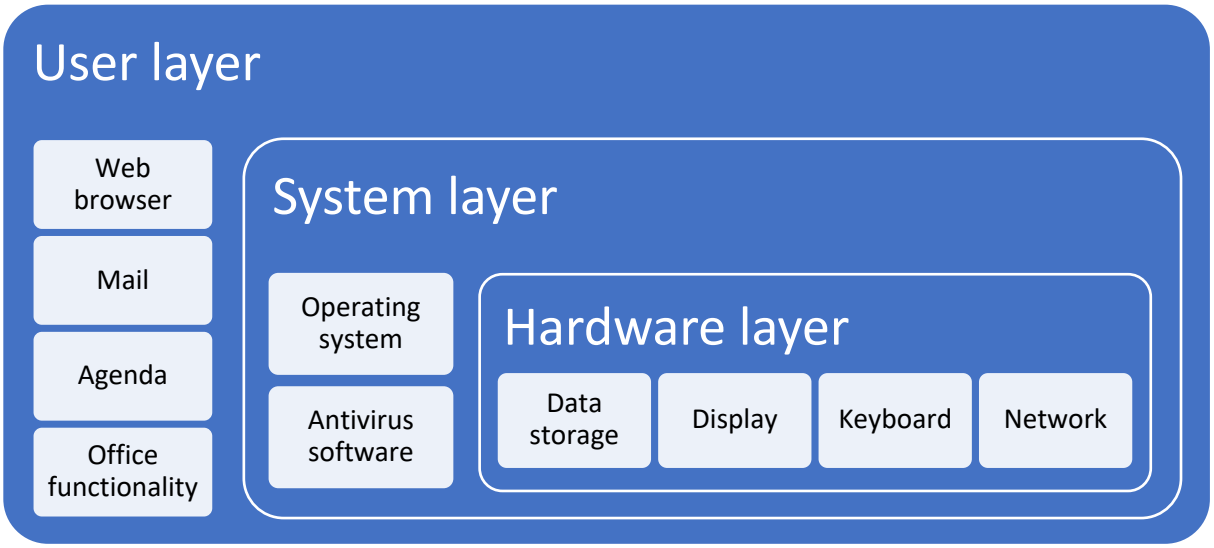
The dossier (Letter to Parliament containing published documents and the list of documents available for the Wob request) lacks a number of items that could be expected for a decision of this magnitude:

1. It is not clear which methodology has been used to weigh the interests between potential risks and measures. The assessment criteria that have been predefined to make a risk appraisal are also missing. This is important to explain the basis for the assessment of risk and to be able to check whether this assessment (in peer review) is shared. It also remains unclear whether products from other suppliers in similar areas of application may involve risks. The government's observations should prompt the identification of more software and hardware with the same or larger risk profile.
2. There is no technically substantiated analysis underlying the risk appraisal. No document focuses on technology. The explanation is therefore limited to the observation that antivirus software 'has extensive and in-depth access to a computer or network'. In the Netherlands, penetration tests were performed on Kaspersky Lab's antivirus software, the results of which were made available to the government[11]. This knowledge was offered, but the file does not show that this information was taken into account.
3. The legal reasoning as to why Kaspersky Lab would pose an increased risk is based solely on the American documents. Nowhere does it appear that an audit into the accuracy of these documents has been carried out in the Netherlands, that the relevance in the Dutch context has been examined or that contact has been made with the authors of these documents. Our own research shows that there is at least a discussion about how Russian legislation should be interpreted.
4. No adversarial hearing, or (insofar as the documents show) an independent peer review, took place. Kaspersky Lab was not given the opportunity to respond to the Cabinet's observations, nor were the observations submitted to a third party for validation.
5. The (urgent) advice does not specify the circumstances or areas of application when Kaspersky Lab's software does or does not pose a risk. The European Commission did investigate [12] the existing application areas in response to questions from the European Parliament. This appears to be the case for antivirus software on systems that are not directly connected to the Internet. 'The risk of data exfiltration therefore would be minimal even if the software was in fact malicious. However, the Commission has no indication for any danger associated with this anti-virus engine', writes European Commissioner Mariya Gabriel.

[11] In Kaspersky's letter (Appendix 5) reference is made to investigations (penetration tests or 'hack tests') carried out by several market parties. One of them is considered to be a critical sector. [911911]
[12] http://www.europarl.europa.eu/doceo/document/P-8-2018-000603-ASW_EN.html - verified on 10 November 2018

3. Observation 1: Danger of software on the system level

The Cabinet's first observation states that antivirus software has extensive and in-depth access to a computer or network. The Cabinet distinguishes two levels: the 'system part' and the 'user part'. To sketch a complete picture of a computer, network component, mobile phone or other device, three layers can be distinguished: the user part, the system part and the active hardware underneath. On each layer, a component of a system (computer, telephone, network device, etc.) functions.



As we descend deeper into the system, the threat of abuse increases and it becomes more difficult to detect malicious code. The downside is that it becomes more difficult to make an attack. To be able to place the threat correctly, we walk through the dangers layer by layer.

User layer

The user layer is the layer where the software functions with which a user communicates. This is, for example, a web browser, word processor, e-mail package and other functionality. Some examples are Apple Mail, Google Chrome, Microsoft Office, Microsoft Outlook, Mozilla Firefox or apps such as Facebook, LinkedIn, Twitter, a weather app, NS Travelplanner Xtra, a news app, Apple/Google Maps, Waze etc. on a smartphone.

Many attacks initially take place at this level. When a user downloads something, visits a malicious site or responds to an e-mail, attackers can quickly deliver malware or exploit a weakness in the software used. Through other weaknesses in a system, an attack on this first level can, as it were, 'upgrade' to a system-level attack through a *privilege escalation*. The software is then, as it were, an administrator of the system.

To prevent this, the operating system limits what software can do. The user will notice this if the system explicitly requests permission to run something as an administrator. In many operating systems and on many phones, the user must give permission for rights, such as access to the address book, saving files or sending text messages. Attackers avoid this by enticing the user to give them system access or by exploiting weaknesses at system level. Many antivirus software aims to recognize and stop this type of harmful, deviant behaviour between user and system levels. To do this effectively, it must operate deeper than the user software.

System layer

Underneath the user layer lies the system layer. The Cabinet states that this layer 'provides extensive and in-depth access to ICT systems'. Here all processing is done that is necessary to control the hardware of one system and to facilitate the software with which the user interacts. This is the place where signals from a touch screen, mouse or keyboard enter, a screen is controlled, the temperature of hardware is monitored, network traffic is controlled, the remaining battery charge is tracked and the storage or retrieval of files is controlled.

To be truly effective as an antivirus software, most vendors focus on this layer. When a file is opened or network traffic passes by, it can immediately scan for malware and, if necessary, intervene in an attack. It also detects unusual and undesirable behaviour on the system at this switching point and intervenes if necessary. Such interventions provide tenability to attacks on the user layer and vice versa to weaknesses in, for example, an operating system. Antivirus software can report any abnormalities found to monitoring systems. This way, the managing organization knows that there is a problem. Examples of operating systems are Android OS, iOS, Linux, Microsoft Windows and MacOS. Examples of vendors of antivirus

WannaCry- & NotPetya-infections

In April, the 'Shadow Brokers' hacker group published a number of attacks based on weaknesses in the Microsoft Windows operating system. The weaknesses are said to come from the US National Security Agency (NSA). A month before the announcement, Microsoft fixed the weaknesses.

Several malware outbreaks followed. Most of them are ransomware. It is striking that after infection via e-mail, for example, the malware abuses the revealed leaks. At that moment, the attack is specifically aimed against the system layer of the software.

During one of the ransomware outbreaks, for example, the British National Health Service is hit. This attack is called 'WannaCry'. Some experts point to North Korea as the distributor.

A few weeks later, an outbreak of a virus that is soon referred to as a variant of the ransomware Petya follows. In this case, the source of the infection appears to be compulsory accounting software in Ukraine. This software also abuses the system-level leak in Windows. The outbreak also affects a container terminal in the port of Rotterdam.

The United States, the United Kingdom and Denmark designated Russia as the culprit. Kaspersky Lab investigated the malware and concluded that it is a different virus and calls it NotPetya. This can be found in appendix 14 on page 304.

software on this layer are Avast, AVG, Avira, Bitdefender, Dr. Web, ESET, F-Secure, G-Data, Kaspersky Lab, McAfee, Microsoft, Nano Security, Qihoo 360, Symantec, VirusBlokAda, Webroot and so on.

If you manage to install malware on the system layer, you can influence both the operating system and software on the user layer. Access to the system layer does not automatically mean 'extensive and in-depth access to ICT systems', as the cabinet states. At most, access to one specific system. In the event of a successful attack, there is access to the mobile phone or workstation in question, but not automatically to surrounding systems in a network. They would have to be compromised one by one.

The way of thinking indicated by the cabinet is based on a single layer of security. However, the standard [13] for government services - there are similar standards for other organisations - is to limit the risks of escalation between systems in sensitive environments by segmenting networks. Networks must be managed and controlled to protect information in systems and applications[14]. One step is to divide[15] networks into separate pieces (e.g. via VLANs). Thus, a major attack, such as a virus outbreak (or ransomware), manual hacker intrusion or other intentionally malicious action, is limited to the smaller segment. Therefore, there must be continuous monitoring on the network[16]. All traffic entering or leaving the network and the data moving within the network segment itself is thus monitored. This monitoring is done using Security Information and Event Management (SIEM) systems where all events in a network environment are controlled and monitored[17]. In addition, wider access to a single system does not automatically mean wider access to documents, for example.

Documents are usually always stored in a Document Management System (DMS) and a user only gets access to a temporary copy of a document. This access is - with normal and properly designed systems - limited to the rights of a specific user, so that a system may not access more documents than the user can access at that moment.

[13] The standard for the central government is the 'Baseline Information Security of the civil service' - Appendix 11
[14] BIR 2017, 13.1.1 – 1 (page 230 of the Appendices)
[15] BIR 2017, 13.1.3 – 1 (page 230 of the Appendices)
[16] BIR 2017, 13.1.2 – 1 (page 230 of the Appendices)
[17] BIR 2017, 12.4.1 (pagina 228 of the Appendices)

Hardware layer

The hardware functions even deeper in a system. This is the deepest level of an ICT system. Herein lies literally the control over everything that is technically executed in commands. This control goes so far that even a command from the system layer can be ignored, wrong results can be returned or it is possible to secretly send every action to a third party. The hardware also contains software, which we call firmware. Examples of suppliers of hardware for computers, mobile phones, security devices and network devices are: Acer, Apple, Aruba, Asus, Cisco, Dell, HP, Huawei, Lenovo, LG, Medion, Motorola, Netgear, Nokia, Samsung, Sony, Synology or WatchGuard.

Hidden firmware functionality in the car

A well-known example of hidden software in hardware is the emissions scandal involving various (mainly German) diesel car manufacturers. In the on-board computer there was functionality at company level to detect an official emission test and then let the engine function differently. The emissions on the road were ten to forty times higher than what the tests showed.

Detection at this level is difficult. The cheat software only activates under certain operational conditions. The case was only triggered when there was a suspicion that something was wrong and was being purposefully and intensively tested on public roads. When the results of that specific investigation come out, there will be a commotion.

Whereas with software it is possible, with some effort, to find out exactly what the software does, in the case of firmware in hardware this is difficult or sometimes even impossible. The logic may be hidden in the physical circuits of chips. Even if the blueprints of the hardware are available, without thorough and continuous supervision of the manufacturing process it is difficult to test whether exactly that hardware is built. Anyone who can hide malicious code in the hardware is able to spy or sabotage very effectively.

An attacker who can modify or add firmware is master of it all. For espionage purposes, an attack at this level is extra effective and subtle precisely because it is so difficult to detect and mitigate. After all, the hardware behaves quite normally. However, carrying out such an attack is also more difficult. The attacker must introduce a vulnerability in the design of the physical hardware or in a firmware update. Such an update may still be noticeable in the distribution of that firmware. In such a case, the user (for example an ICT administrator, or a laptop owner) must be tempted to have new firmware installed himself. In some cases, anti-virus software can detect such an attack. Many producers of operating systems have also taken measures to make such an installation difficult or to limit the impact of such a hardware hack on the system level. Awkward recent examples of this in central processing units (CPUs, the core of any computer system) are the vulnerabilities that upon discovery were named Spectre and Meltdown[18]. The names reflect how big the impact is and how difficult it is to combat the risks.

The 'God' mode with Intel processors

In December 2017, two security researchers showed how they could exploit an error in the Intel Management Engine. Because of the wide access to every aspect of the computer (files, network and hardware) they called it the 'God' mode. The hardware appears to be a hidden back door for those who can find the leak.

It is awkward that the security researchers also conclude that the problem goes back to chips that have been on the market since 2007.

No single supplier

By only looking at a supplier of antivirus software, the cabinet ignores many other risks for espionage and sabotage. A much broader view of access to systems and the systems themselves should be taken. A back door does not even need to be built intentionally. This can be caused by errors in the software or hardware. Those who fear the operations of a hostile intelligence service cannot ignore this risk. We should not only consider antivirus software, but also operating systems and hardware as a risk. In this case, by not looking more broadly at adjacent security domains, an overly concise, incorrect and, above all, incomplete picture is created. This gives rise to an image of selective argumentation in which only the Kaspersky Lab case is examined.

Measures against spying and sabotage of a product

Back doors in espionage or sabotage software occur in two ways. The first is a platform that can be used unintentionally for abuse due to errors in the software. A weakness, for example, gives access to files or login data. Especially unknown leaks, so-called zero days, are then instrumental. There is often no defence against the attack, because it is not yet known, analysed (and shared) within the security community of which Kaspersky Lab is part. The second is the deliberate construction of vulnerabilities in software, or a broader infrastructure to carry out attacks (espionage and sabotage). This last form is difficult to detect, because then the software supplier is in on the conspiracy. To discover it more insight into the software is needed. The name for this attack methodology is called an Advanced Persistent Threat (APT).

[18] https://meltdownattack.com/ - verified on 8 November 2018

A number of measures are possible to limit backdoor espionage and sabotage in purchased software:

1. Research into the supplier of a software product or service. Has it previously been involved in espionage? Or is the supplier involved in detecting and combating attacks? Because many external parties play a role in the systems of organisations, trust in a player plays a major role. Whether an antivirus vendor is trustworthy may be tested, for example, on the basis of the following questions:
    a. Are there many weaknesses in the product? When software weaknesses are found, they are publicly announced in a standard way via a Common Vulnerability Exposure (CVE). This makes it possible to follow what the problems with the software are, which attacks are possible due to the vulnerability and therefore also how serious this is. Almost all frequently used software products are included in this list. But the number of reports per product in combination with the seriousness of the reported incidents makes it clear per product to what extent an increased risk of abuse of the software is possible.
    b. Are there known and conscious limitations in the protective effect of the software? Is there malware that is deliberately not detected or stopped?
    c. Has it been known previously that the company - other than placing a legally required eavesdropping device - is used to perform espionage tasks?
2. Performance of penetration tests - also called hack testing. In such an investigation, the software is attacked in many different ways and a search is done for known (and often unknown) leaks. If there are many findings, this may be an indication that the quality of the software is inadequate. The problem with this form of inspection is that a black box is used, which prevents the tester from understanding or testing all relevant scenarios or situations. It remains a snapshot of the system, where only the input (what you put in as a tester) and the output (the results you see) are measured.
3. Performing a code review. When creating useful software, developers write programming code, which is readable text we call source code. This is converted into executable system code, which a computer understands (this step is called compiling). The quality of the software is shown by an inspection of the source code. At this point weaknesses can be searched for, including (unintentional) back doors. This form of verification provides high level confidence, the supplier literally reveals all his secrets. At the same time, access at this level gives malicious parties the opportunity to keep identified weaknesses to themselves and later abuse them. A supplier must be certain of its business in order to provide this level of transparency.

    Not every supplier is open to studying the source code. Others allow only a limited part of the source code to be tested. This last step is not very useful, because the part where no inspection has taken place can still hold a back door. It is therefore important to be sure that the tested source code is actually the one used to make the final product that is active on your organisation's computers/telephones.

    Performing an inspection on the source code of used software is an important (or indispensable) step for sensitive environments. It is a form of due diligence that ensures that there is a higher degree of certainty about the operation of the

software. For various products that are used, for example, for the protection of departmental confidential documents, the AIVD has the option of testing the quality and granting approval[19].

4. Continuous in-depth monitoring of the supplier's operational processes. By looking at the processes, systems and measures on the side of the service provider, it becomes clear whether what happens with data in daily practice corresponds to the "paper reality" of, for example, ISO, certificates and other, periodically verified quality labels.

[19] https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/goedgekeurde-producten - verified on 10 November 2018

4. Observation 2: Mandatory legal cooperation

The second observation of the Cabinet is that Kaspersky Lab is obliged under Russian law to cooperate in an operation of the Russian intelligence services. "Kaspersky Lab is a Russian company with its headquarters in Russia and is therefore subject to Russian legislation," writes the Cabinet in its Letter to Parliament. That is incorrect. Kaspersky Lab is a British company, whose head office is indeed in Russia[20].

The Wob request shows that the reports[21] on which this decision is based are based on documentation that formed the basis of the American 'Binding Operational Directive 2017-01'. The documents explain why there is a fear of espionage and sabotage via Kaspersky Lab's software. The documents do not show why Kaspersky Lab is different from another antivirus or software supplier from the Russian Federation. Nor does it show why Kaspersky Lab is classified differently from a supplier of other software on this system layer (or hardware layer), which is also subject to Russian legislation without a company having its primary establishment in the Russian Federation.

In the American decision, the report of the American professor specializing in Russian law Peter B. Maggs[22] plays a key role. He states - simply put - that a company that stores and transports personal data in Russia is a provider of a communication service. Therefore, the company is obliged to cooperate with intelligence services of the Russian Federation. The problem with this is the obligation based on privacy legislation to store data of Russian citizens in Russia. As a result, the provision of a telecommunications service is soon becoming a reality. A company such as Kaspersky Lab would be obliged to cooperate with requests from the Russian intelligence services when carrying out operations and tapping or providing data stored in the Russian Federation.

The Maggs report is not undisputed. Kaspersky Lab claims that it is not subjected to the tap obligation of telecommunication service providers. Regardless of who is right, it can be concluded that there is discussion about these legal obligations. In the explanation of the Dutch decision, no clear explanation was given of the position that the Cabinet has chosen in this respect. This should lead to further investigation or adversarial proceedings. This report explicitly does not address the question of who is right in this discussion.

What has been explicitly looked at is the historical reputation and behaviour of Kaspersky Lab and the question of whether the origins of the company demonstrably lead to an increased risk of being used as a means of espionage and sabotage. Should a Dutch, American, Chinese company with similar services in the Russian Federation comply with the same legislation? Is Kaspersky Lab different from these companies? To clarify this, contact was sought with Professor Maggs[23]. He states that other companies with similar services in the Russian Federation are also subject to the same obligations as Kaspersky Lab:

[20] See the heading 'About Kaspersky Lab' in the chapter 'About the reporting'
[21] Appendices 7, 8 and 9
[22] Appendix 7, page 95 and following
[23] Appendix 13, page 204

" Kaspersky Labs is obliged to comply because it is storing information in Russia and moving information across Russia. A non-Russian company doing the same activities in Russia would also have to comply with the same laws, just as the delivery trucks in Moscow of a Dutch company would have to comply with Russian traffic laws."

It is important to note that Kaspersky Lab stores data of Russian users in the Russian Federation. This obligation also applies to all companies active on the Russian market:

"Indeed, as I understand it -- I have studied the matter carefully -- Russia is pushing to force companies doing business in Russia to store data on Russian citizens on servers in Russia. The policy is sort of the opposite of the EU data privacy protection laws that try to keep data on EU citizens safe in the EU. Russia wants to keep the data accessible in Russia."

The problem of supposed mandatory cooperation with Russian intelligence services does not apply only to Kaspersky Lab. Every market party that establishes relationships with Russian citizens and has an office in Russia has to deal with this legislation. The number of parties at risk is therefore considerable. For example, all the larger suppliers of operating systems for both computers and mobile phones, but also telecommunications services, appear to have an office in Moscow. This is not different for the larger antivirus suppliers. There are many more companies that can be forced to contribute to the (counter)espionage operations of the Russian intelligence services.

In this broad interpretation of the legislation, there are many different software suppliers that pose exactly the same risks to the Dutch central government and sensitive sectors as Kaspersky Lab. It is unclear why, then, the assessment of Kaspersky Lab's case did not look at suppliers that yield an apparently comparable risk profile.

No unique legislation

Legislation in the Russian Federation is not an isolated case. Since the end of June 2017, China has also had provisions in the legislation[24] requiring companies and individuals to assist intelligence and security services. The focus is clearly on the offensive[25]. The United States has the Foreign Intelligence Surveillance Act[26] with all kinds of amendments (for example the Patriot Act) that makes cooperation compulsory. The Netherlands also has an obligation to cooperate in espionage, to reverse encryption or to place a facility on the basis of the provisions of the Intelligence and Security Services Act 2017[27]. Of course, this does not

[24] and the cooperation is among others in articles 11, 12 and 15 and the law also contains penal provisions. - verified on 10 November 2018

[25] https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense - verfied on 10 November 2018

[26] For example: https://www.law.cornell.edu/uscode/text/50/chapter-36 - verified on 10 November 2018

[27] https://wetten.overheid.nl/BWBR0039896/2017-09-01 - For example, Articles 45(9), 52 and 57 - verified on 10 November 2018

immediately hold a licence for Russian parties, but it does create some need for nuance in the applicability of this specific argument.

Incidentally, the National Coordinator for Counterterrorism and Security (NCTV) also refers to the problem of 2018[28] compulsory cooperation with intelligence services in the 2018 Cyber Security Assessment Netherlands and states that several countries are involved:

> *"Dependence on (foreign) parties increases vulnerability to espionage, disruption and sabotage. In specific countries, foreign parties may be required by law to cooperate in supporting operations such as espionage or preparations for sabotage."*

Professor Maggs confirms that the problem is wider in scope:

> *"Pretty much every country reserves the right to spy on other countries' communications. Of course there may be diplomatic repercussions, as in the case of the alleged bugging of Angela Merkel's cell phone.''*

Russian legislation in general does not differ significantly from various other countries.

[28] Appendix 14, page 310

5. Observation 3: Cyber operations against the Netherlands and its interests

The third and final observation by the Cabinet that led to the precautionary measure is that Russia carries out operations against the Netherlands and Dutch interests. Little is needed to establish that operations are indeed being carried out against the Netherlands and Dutch interests. In the Cyber Security Assessment Netherlands 2018, the NCTV points out that states pose the greatest threat:

> *"States carry out digital attacks on other countries, organisations or individuals for primarily geopolitical motives. Their aim is to acquire strategic information (espionage), influence public opinion or democratic processes (influence) or disturbance of vital systems (disruption) or even their destruction (sabotage). Several digital attacks by states have been observed in the past year. These had an impact on national security.''*

In its annual report for 2017, the AIVD points to the special position of the Netherlands as a hub, member of the UN Security Council in 2018, NATO and the EU[29]. Digital espionage is a increasing problem, in which there are various actors:

> *"Digital espionage with an economic motive remains a source of concern and the AIVD acknowledges a slight increase in economic espionage in Europe compared to last year. Several states are guilty of this. In 2017, we identified digital espionage at various European multinationals and research institutes in the energy, high-tech and chemical sectors. This includes various organisations that have intensive cooperation relationships with the Netherlands or have branches in the Netherlands. Terabytes of confidential data representing substantial economic value were stolen from these digital intrusions.'*

The AIVD draws attention in particular to the efforts of Russia and China as state actors attacking our country. Offensive capabilities are part of a broader arms race. Following Edward Snowden's revelations, it has become clear that extensive national programmes are active in proactively and offensively carrying out attacks, introducing backdoors into software (or, when discovered, concealing them) and that customised malware is distributed.

In January 2018[30] it became known that employees of the Joint Sigint Cyber Unit (JCSU)[31] had broken into the networks of the Russian hacker group Cozy Bear, also known as APT29,

[29] Appendix 15, page 374, 375

[30] https://www.volkskrant.nl/nieuws-achtergrond/hackers-aivd-leverden-cruciaal-bewijs-over-russische-inmenging-in-amerikaanse-verkiezingen~b32c6077/ - verified on 9 November 2018

[31] The Joint Sigint Cyber Unit is a joint venture between the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD)

in 2014. They note that this group is affiliated to a Russian intelligence service. Especially, Kaspersky Lab was the first to issue a warning for this group.

The seriousness of the threat posed by offensive programmes should not be underestimated. Especially for suppliers of all kinds of software, including antivirus software and operating systems, the pressure to cooperate with these operations is growing. The most worrying aspect of this is not the deployment in individual operations, but the active creation of a permanent infrastructure to enable operations[32].

[32] https://www.theverge.com/2018/9/3/17815196/five-eyes-encryption-backdoors-us-uk-australia-nz-canada - verified on 12 November 2018

6. Kaspersky Lab Risk level

Providing insight into the risk of espionage and sabotage in antivirus software is quite possible in the Kaspersky Lab case. There is a lot of information about the company and it is possible to perform audits. This makes it possible to sketch a realistic image of the company's activities.

Relationship with the Dutch government

Kaspersky Lab is no stranger to the Dutch government. At the time of the Cabinet's decision, the company supports the National Police in various investigations. They have done this more often in the past, as in the case of the Carbanak[33] attacks, where various financial institutions were broken into. The attacks constituted the largest digital bank robbery in history and prompted Europol to urgently summon European banks together and have Kaspersky Lab explain the situation.

In ransomware attacks, there has been an intensive collaboration with the police to find keys for deciphering encrypted files, so that victims can recover their files without paying a ransom. A well-known example is a Coinvault malware. Kaspersky Lab initiated the No More Ransom initiative together with the police, Europol and antivirus supplier McAfee. This allowed at least 30,000 people to decipher their computers after an infection with ransomware. In 2016, founder Eugene Kaspersky was prominently present as a keynote speaker at the NCSC One Conference. At the same conference in 2016 and 2017, Kaspersky Lab will give joint presentations with Team High Tech Crime of the National Police Unit.

The organisation also participates in various awareness campaigns, such as Alert Online[34] and 'Do not make it too easy'. In short, the company works closely with the Dutch government in various areas when it comes to security.

There is no evidence that Kaspersky Lab's software is actually used to perform espionage or sabotage. When communicating the decision, the Minister writes[35] in the Letter to Parliament that there are no concrete cases of abuse known in the Netherlands. The Binding Operational Directive (abbreviated to BOD) in the United States lacks evidence that Kaspersky Lab has a problem with the products or would do something wrong. In the civil proceedings between Kaspersky Lab and the US government, the judge also writes in his[36] judgment: “The BOD was not based on a determination that Kaspersky Lab was disloyal or guilty of any wrongdoing”. Belgian Prime Minister Charles Michel states[37] that his Centre for Cybersecurity 'does not have objective technical information and independent studies that show that the applications of Kaspersky Lab are malicious or pose a threat'. The German Federal Office for Security in Information Technology, the government's centre of

[33] https://en.wikipedia.org/wiki/Carbanak -

[34] https://www.alertonline.nl/overzicht-partners - verified on 13 November 2018

[35] Appendix 1, page 3 first paragraph

[36] Appendix 12, page 258

[37] https://www.tijd.be/nieuws/archief/Belgie-bant-Russische-antivirussoftware-niet/10064355 - verified on 10 November 2018

expertise,[38] does not propose to issue a warning 'because it has no evidence of malicious practices or software vulnerabilities'. In response to questions from the European Parliament, the[39] European Commission writes 'no indication of any danger'. The Swiss Federal Steering Body also claims not to have any evidence that Kaspersky Lab has been involved in any attack[40].

Malware is malware policy

Kaspersky Lab pursues a policy based on the principle that 'malware is malware' regardless of its creator. It denies cooperation in espionage operations in any country. The company, therefore, does not hesitate to expose malware [41] where its origin is very likely Russian and where military objects from[42] NATO countries are the target or where, for example, the White House is a target[43]. Based on their knowledge of which actors pose a continuous threat to the Netherlands[44], the company also points out an Advanced Persistant Threat (APT). It looks at all players, regardless of their origin.

During the outbreak of the NotPetya virus, which the American government asserts as originating from the Russian government, Kaspersky Lab analyses the malware[45]. The virus proved to originate from accounting software in Ukraine and also affects Dutch interests. A container terminal in the port of Rotterdam had to close down. The virus fighter warns that paying is pointless because the makers cannot undo the damage. The company argues why this is not a Petya virus and therefore calls it NotPetya, which is why it was given that name. The consequence of the 'malware is malware' policy is that malware of Western origin is also exposed, as happened, for example, with the well-known Stuxnet malware[46]. The target here was the Iranian nuclear programme, in which both Israel and the United States were reportedly involved in the attack.

Quality indicators

Kaspersky Lab scores high among authoritative research institutions. In August[47] for example, the company was found to achieve the maximum scores (6 out of 6) for the detection of malware, performance, and usability. This applies to both the personal and the business editions of the test of AV Tests. The same applies to the test of AV Comparatives of

---

38 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/BSI_Stellungnahme_Kapersky_11102017.html - verified on 10 November 2018

39 http://www.europarl.europa.eu/doceo/document/P-8-2018-000603-ASW_EN.html - verified on 10 November 2018

40 https://www.nzz.ch/schweiz/westliche-regierungen-werfen-der-russischen-it-firma-kaspersky-lab-spionage-vor-sie-eroeffnet-im-november-in-zuerich-ein-neues-transparenzzentrum-ld.1430956

41 https://securelist.com/sofacy-apt-hits-high-profile-targets-with-updated-toolset/72924/ - verified on 10 November 2018

42 https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ - verified op 10 November 2018

43 https://securelist.com/the-cozyduke-apt/69731/ - verified on 10 November 2018

44 https://securelist.com/threats-in-the-netherlands/88185/ - verified on 10 November 2018

45 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ - verified on 10 November 2018

46 https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet - verified on 10 November 2018

47 https://www.av-test.org/en/antivirus/home-windows/windows-10/august-2018/kaspersky-lab-internet-security-19-183111/ - verified on 10 November 2018

malware found on the Internet[48]. In the test of how effective suppliers are in removing malicious software, the company scores the only 99 out of 100 points[49]. Kaspersky Lab is thus demonstrably one of the leaders in detecting malware and leading in its removal. Research agency IDC indicates[50] that it does not doubt the quality. Based on publicly available studies, there is no reason to doubt the quality of Kaspersky Lab's software.

Over the past five years (from 4 November 2013 to 4 November 2018) nineteen leaks have been found in Kaspersky Lab's software, with an average severity of 5.8 on a scale of 1 to 10. This is relatively low given the size of more than 2 million lines of source code. Again, there is no significant deviation from other market parties. There are a few parties that have had fewer bugs, but that on average score higher in seriousness. There are also reputable parties that have had more faults and score higher. This picture provides no reason to doubt the software of Kaspersky Lab.

Bug bounty

The company offers rewards for finding weaknesses in the software. For major bugs, rewards of up to 100,000 dollars (over 89,013 euro[51]) are offered[52].

Penetration test

Kaspersky Lab's software has undergone at least one known penetration test in the Netherlands and has properly passed it. The test was performed by telecom company KPN in cooperation with one of the largest security companies in the world. In the letter prior to the Cabinet's decision, Kaspersky Lab pointed this out[53].

Audit of source code

Kaspersky Lab opened three Transparency Centers where the company provides insight into the products, the operation of services and source code of the software. The first center is located in Zurich, Switzerland. This allows users to perform an in-depth audit of the source code of the programs. This enables independent research into the risk of espionage and sabotage and into the quality and effectiveness of the software. The company not only offers the possibility to have the current software version tested but also upcoming (security) updates and new versions. Before an organisation allows new software into its own environment, it is therefore made possible to test the reliability of the software in advance.

As part of this report, Brenno de Winter paid a verification visit to the Transparency Center in Zurich, Switzerland, on 12 November 2018. The source code of the antivirus software was tested there. A random check was carried out to determine whether the source code actually converts to exactly the same code that runs on the reference computer. No

[48] https://www.av-comparatives.org/tests/real-world-protection-test-august-2018-factsheet/ - verified on 10 November 2018
[49] https://www.av-comparatives.org/tests/malware-removal-test-2018/ - verified on 10 November 2018
[50] https://www.linkedin.com/pulse/until-theres-some-evidence-dont-kick-out-kaspersky-dominic-trott/ - verified on 12 November 2018
[51] Calculated on 13 November 2018 via xe.com
[52] https://www.kaspersky.com/blog/bug-bounty-boost-2018/21477/ - verified 13 November 2018
[53] Appendix 5 page 56

differences were found, so it is plausible to assume that the company really makes all source code transparent. It was also found that no changes to the source code can be introduced during an audit. The source code is well documented. For example, it is clear which employee has implemented which changes and there is good version management. This also guarantees that updates can be tested quickly. The source code is written in the C++ programming language and looks neat and clean. This makes it possible to have an audit.

The company transfers the installation of the software to Switzerland, as well as the storage of personal data of at least residents of the European Union, Switzerland and the United Kingdom after Brexit. This means that no data is stored in the Russian Federation. With this, Kaspersky Lab effectively implements the General Data Protection Regulation (GDPR). Switzerland has a high level of data protection that closely resembles the GDPR. Kaspersky Lab, therefore, complies with both Swiss and EU regulations for the protection of personal data.

To really appraise the measure taken by the Dutch cabinet, Kaspersky Lab for this study provided access to the source code. The value of such access stands or falls with the question of whether access has been provided to all source code. If a small part cannot be inspected, there would also be the possibility to build in a back door. Using a sample, modules of the source code were converted into executable software and compared to a version running on a separate computer. In summary, Kaspersky Lab provides insight into the source code, allows verifications and thus provides openness with which auditors can test for risks. As of November 2018, this will give the business community and governments the opportunity to test the quality themselves or to have experts do this.

Another question is whether it is possible for the Netherlands to test the content of the software qualitatively now that the Transparency Center has been opened. This question can be answered in the affirmative. The General Intelligence and Security Service (AIVD) has the National Communications Security Agency (NBV) at its disposal. They have sufficient in-house expertise to carry out such a test, have quality criteria that products must meet and carry out such tests regularly. Testing complex products gives this service the right expertise in searching for backdoors in software. NBV will do this not only for classified information[54] for the Netherlands but also for, among others, the European Space Agency, the EU and NATO[55]. Currently, no operating system or antivirus package has been approved. This is remarkable because the cabinet states in the measure about such software that precisely this has profound and broad access to networks and systems. Anyone who experiences this in this way must opt for a high level of security for systems in vital sectors and the central government and must, therefore, enforce controls.

[54] Depending on the inspection, this ranges from departmental confidential information to data that have the designation 'state secret very confidential'.
[55] Appendix 15, page 377

7. Kaspersky Security Network

The user must give permission to upload malware samples.

The fight against malware is an ongoing arms race. Every day new malware appears and attackers adapt existing malware. They respond to new detection possibilities, weaknesses in operating systems or user applications. The aim is to actively exploit these vulnerabilities for theft, espionage or sabotage. Kaspersky Lab daily detects approximately 360,000 malicious malware samples[56]. Antivirus software often detects strange behaviour or unidentified malware. Various suppliers offer the possibility to automatically send this malware to the company for further analysis. This enables antivirus companies to respond more quickly to current threats and to turn knowledge into rules for the software so that new malware can be recognised and stopped more quickly. As a rule, this information is shared with other parties in order to be able to jointly take more effective action and avoid duplication of effort. Kaspersky Lab also has such a service: the Kaspersky Security Network (KSN). Anyone who wants to use this service must give explicit permission for it when installing it or at any later time. Participation can also be terminated at any time in time.

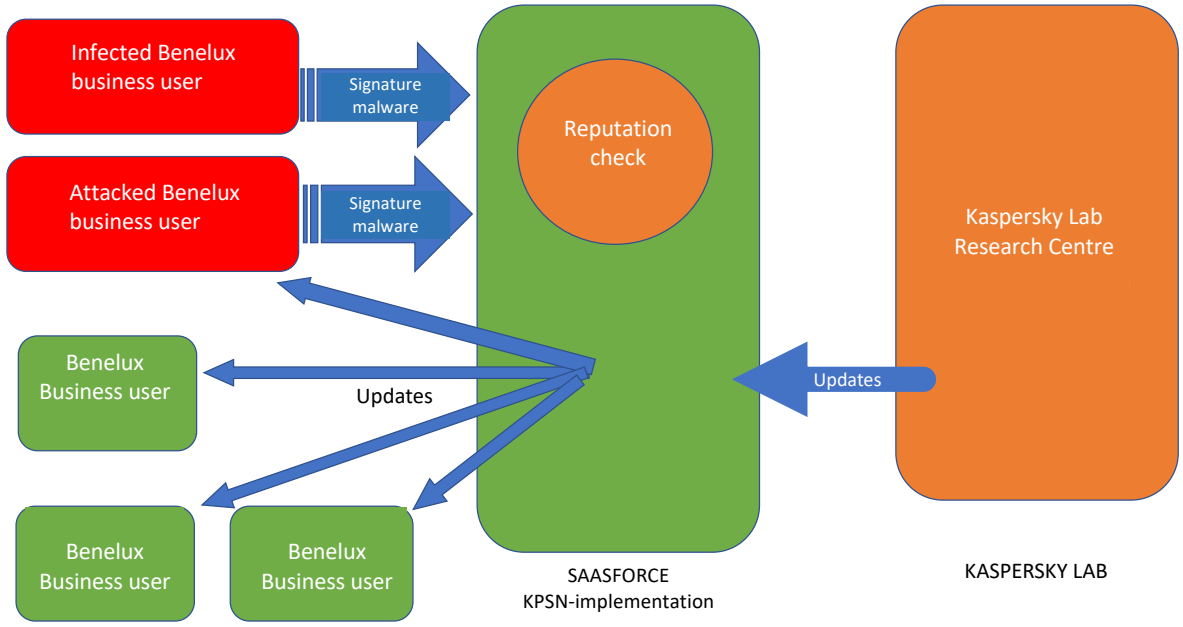
With the KSN, the service activates when the antivirus software detects unusual behaviour or malware. At that moment, the system searches for the piece of software it believes to be malware. It sends a digital signature of the malware (but not the malware itself). The KSN indicates whether the malware is known. If this is not the case, the antivirus software sends the malware to the KSN for investigation. The document containing the malware is not sent. However, the type of document (program, word processing file, etc.) is included.

A number of measures protect users and organisations against possible theft of documents or espionage via antivirus software:

1. Transparency Center. The source code can be checked at the Transparency Center. The ongoing audit by one of the 'Big Four' companies tests whether the antivirus software only sends something to the KSN if the user has chosen to do so.
2. Procedural audits. One of the 'Big Four' companies conducts an audit of the procedural aspects of the KSN. This provides insight into whether the company actually handles the data as they claim.
3. Awareness and instructions to users. Compulsory training[57] of users trains people to deal properly and correctly with the tools provided to them and to make an informed choice whether or not to use this functionality.
4. Most importantly, Kaspersky Lab has created a new guarantee for business users in the Benelux. A copy of the security information from Kaspersky Lab is stored at the

[56] Figures for 2017 - https://www.kaspersky.com/about/press-releases/2017_kaspersky-lab-detects-360000-new-malicious-files-daily - verified on 9 november 2018
[57] Appendix 11 BIR 2017 - 6.2 page 213 and 7.2.2/7.2.3 page 215

Dutch company SaaSForce [58]. However, no data subsequently flow to Kaspersky Lab, as a result of which it is procedurally excluded that this technology can be misused outside the EU for espionage. This is the Kaspersky Private Security (KPSN).



The KPSN solution exists as a concept for some time. KPN has implemented such a solution in the Netherlands. Even before the discussion about espionage and sabotage, it was possible that the central government would also install this solution in the national data centres. It is, therefore, possible for the government to prevent the flow of information under its own control.

Thinking about the use of functionality, such as the Kaspersky Security Network, is necessary. In 2017, the Wall Street Journal[59] revealed that an intelligence service had successfully broken into Kaspersky Lab. After viewing the software, the newspaper stated that the intelligence service claimed that it is possible for Russian intelligence services to search for documents. Kaspersky Lab was said to be a 'tool for espionage'. The company investigated the break-in as early as June 2015[60] and issues a report in response to the reports[61].

When Kaspersky Lab investigated the Wall Street Journal's claim, it discovered something significant: It discovered a computer that reported a lot of malware. It sits in an illegal version of Microsoft Office, loose malware and even source code of the Equation Group malware. A zip file contains several malware files and four classified Word documents. The malware concerns new variations of the Equation Group malware. The samples were sent to

[58] https://saasforce.eu/benelux-klanten-van-kaspersky-lab-profiteren-van-unieke-real-time-bescherming-zonder-dat-data-de-eu-verlaten/ - verified 11 November 2018
[59] https://www.wsj.com/articles/russian-hackers-scanned-networks-world-wide-for-secret-u-s-data-1507743874 - verified on 11 november 2018
[60] https://securelist.com/the-mystery-of-duqu-2-0-a-sophisticated-cyberespionage-actor-returns/70504/ - verified on 12 november 2018

the KSN. In one of the classified Word documents, the antivirus software recognised the source code of the malware. Based on the source code, the unique samples analysts from Kaspersky Lab suggested that the Kaspersky user may be a creator of malware. The suspicion arose that the NSA employee referred to in the article had taken his work home with him. The analysts also suspected that the person's own computer has been hacked because there is a backdoor (malware) in the illegal Microsoft Office version. Kaspersky Lab suspects Russian hackers of this hack. For a longer period of time, the antivirus software on this computer was not used, which could have infected the computer.

Such a scenario cannot occur in the situation of the SaasForce Benelux. Kaspersky Lab does not receive forwarded information about malware. The company cannot access the files, Russian legislation has no influence on the SaasForce in the Netherlands and Belgium. This security layer makes the scenario that a Russian intelligence service forces Kaspersky Lab to cooperate successfully in a spying or sabotage operation very unlikely.

8. Implications of the Cabinet Decision

The cabinet's precautionary measure has adverse implications for the Dutch government, the business community, citizens and, of course, the company Kaspersky Lab. Kaspersky Lab puts a lot of energy into contributing free of charge to the fight against cybercrime. A proper working relationship has been established with the Dutch police. The Cabinet's measure obstructed this cooperation. From conversations with Kaspersky Lab, it is clear that at least three major criminal cases are affected. One case had just started, another case concerned an ongoing investigation and a third one was temporarily put on hold. In these cases, Kaspersky Lab's expertise can no longer be used. Expertise of comparable quality may be found, but such expertise is usually expensive. After the example of Kaspersky Lab, the question is how attractive it is for companies to offer services to a relatively small country like the Netherlands.

As early as March 2014, in the Cyber Security Assessment Netherlands, the National Cyber Security Center (NCSC) referred explicitly [62] to the vulnerability of our country to espionage via a targeted, advanced and sustained attack, known as an Advanced Persistent Threat: "The Netherlands, with its open society and extensive technical and scientific knowledge and economic position, is an attractive target for espionage. Moreover, it can take months and sometimes even years before an Advanced Persistent Threat (APT) is discovered". An important expertise of Kaspersky Lab is the intensive research into such APTs. Precisely this kind of time-critical information, knowledge, and support is important in incidents, in the fight against espionage and sabotage and for securing the knowledge necessary for our digital ambitions.

Currently the reality after the cabinet decision is that contacts between Dutch governments and Kaspersky Lab (and in the future possibly also other global companies) are more complicated. This means, for example, in the event of major outbreaks of malware, offensive espionage and sabotage actions in the direction of the Netherlands, that Kaspersky Lab warns, but that there is no effective cooperation. In case of larger global incidents, there is suddenly a great deal of demand for scarce knowledge and expertise. A bad working relationship does not help. When the NotPetya malware broke out, Kaspersky Lab, among others, was able to provide information quickly and accurately. The consequence of this incident, which disrupted a container terminal in the port of Rotterdam, is enormous. Apart from the disruption of the business community, the damage, based on conservative estimates of NotPetya alone[63], is more than a billion dollars[64].

One of the partnerships between the government (mainly the police) and Kaspersky Lab and McAfee is the No More Ransomware initiative. This initiative is a collaborative effort to crack ransomware cryptography in such a way that citizens and businesses can recover their encrypted files without paying a ransom fee.

---

[62] Appendix 17, page 446 and 447.

[63] Maritime company Maersk between € 200 and € 300 million - Appendix 14, page 334, Nuance Communications € 92 million U.S. dollars, pharmaceutical company Merck € 135 million - https://www.security.nl/posting/552421/Nuance+Communications+schat+schade+NotPetya+op+92+miljoen+dollar – verified 10 November 2018

[64] Company reporting Cyber Reason: https://www.cybereason.com/hubfs/Content%20PDFs/Paying-the-Price-of-Destructive-Cyber-Attacks.pdf?t=1541798173918 – verified 10 November 2018

To do this properly, high-quality expertise in both malware and cryptography is required. This knowledge is limited and not sufficiently available to the Dutch government. Now that the working relationship between the government and Kaspersky Lab has come to a standstill, this means that victims of digital attacks have a smaller chance of recovering their files.

For Kaspersky Lab, the decision is harmful. Although the government writes in the precautionary measure that there is no incident at hand, an image arises that there is 'something wrong' with the company. It is an idea of 'where there is smoke, there is fire'. For a company that focuses on protection against malware, espionage, and sabotage, it is precisely the accusation that it is used specifically for such purposes - even though no example of this is known - that is harmful. The procedure wherein there has been no form of rebuttal or wherein there has been a signal that some form of consultation has taken place, may evoke an impression that it is 'so bad that there must be something very big'. That image arises not in the least due to the extensive communication of the precautionary measure, for example through a letter to Parliament and a television performance by the Minister of Justice and Security at *Pauw*.

Also harmful is the communication by the NCSC "Recommendation to vital [sector]: stop using Kaspersky Lab antivirus software"[65] without any nuancing in the message. It is precisely the NCSC that is the central point from which a lot of advice comes. The central government and the vital sectors have direct contact with the NCSC and direct, non-public channels are available. By publicising this advice - which would not have any general effect -, the government gives the impression that it disguisedly issued a general advice. This image is reinforced by pointing out legal consequences in the line of communication[66].

In communication, the Cabinet states that other organisations must make their own considerations. Many governmental organisations and companies are unable to properly carry out such a complex risk analysis. The fear that intelligence services may have more knowledge which may be made public in this way does not help. When weighing threats such as 'espionage' and 'sabotage', any self-respecting organisation will see itself as a potential target. This combination of factors means that the scope of the precautionary measure is received much more broadly than just the central government and vital sectors.

In addition to the previous point, the measure is harmful to Kaspersky Lab in the long-term. The measure formally concerns only the antivirus software. But this is found in many products. For example, the CIO Rijk will send a fifteen page list[67] to parties in order to ask them which Kaspersky Lab products are in use. The list consists of partners who have incorporated Kaspersky Lab's solution into their solution. With this advice, the Cabinet also partly affects these stakeholders. By taking that step, it is not inconceivable that some stakeholders may cancel a partnership with Kaspersky Lab for that reason. This is once again harmful to the company.

[65] https://www.ncsc.nl/actueel/nieuwsberichten/advies-aan-vitaal-stop-met-antivirussoftware-kaspersky-lab.html - verified 10 November 2018 and Appendix 18 page 506
[66] Appendix 6 page 70, consideration 21 and 22
[67] Appendix 5 pages 37 to 51

10. Conclusions and recommendations

The documents from the FOIA-request and the letter from the Cabinet show that the US documents are defining for the measure. The European situation is unlike the American. For example, EU legislation exists, such as the General Data Protection Regulation (GDPR). In the Netherlands, standard frameworks, such as Baseline Information Security for the Government Agency, determine how organisations organise security. Meanwhile, the Security of Network and Information Systems Act requires standards to be adhered to. From the reconstruction and analysis of the decision-making process, an image of selective argumentation emerges. It is unclear which methodology was used for risk analysis. There are also no predefined assessment criteria for antivirus software.

Sometimes facts are displayed incorrectly. "Kaspersky Lab is a Russian company with its headquarters in Russia and therefore falls under Russian legislation", the cabinet writes, for example, to Parliament. That is incorrect. Kaspersky Lab is a British company, with its headquarters in Russia

The image of selective argumentation is reinforced by:

- not considering differences between our country and the situation in the US;
- not considering standards frameworks;
- not considering quality audits of Kaspersky Lab that have been proactively offered;
- not considering information from Belgium, Germany, Switzerland, and the European Commission;
- lack of technical guidance on antivirus software;
- lack of own assessment around the Russian legislative framework;
- the absence of circumstances when the risk is present or not;
- Not holding adversarial proceedings.

The Cabinet states that it has no knowledge of espionage or sabotage in which Kaspersky Lab is involved in any way. The Cabinet's three observations are based on generalities that do not adequately reflect the Kaspersky Lab situation:

1. The fact that antivirus software is deeply embedded in a system does not automatically mean that there is extensive access for espionage and sabotage. Obligatory control measures at government and corporate level and the extensive testing of Kaspersky Lab's software and procedures of all kinds make the risks highly manageable.
2. The Russian legislative framework for intelligence and security services explicitly applies not only to the Kaspersky Lab operating under a British holding company. Every software maker at the system level (antivirus and operating systems) with branches in the Russian Federation has this problem. There are other countries, such as China, the United States, and the Netherlands, where espionage legislation may ask companies for cooperation. The legislation is therefore not very unique.
3. The Russian Federation carries out espionage and sabotage operations. From annual reports issued by intelligence services, it appears that many countries are working on this. It is precisely Kaspersky Lab that qualifies as an effective jammer for many operations, regardless of the origin of the attack and without any hesitation in exposing Russian operations. The company uses a 'malware is malware' policy regardless of origin

With the introduction of the Transparency Center in Zurich, Kaspersky Lab is taking an effective step in its tenability to espionage and sabotage. Being able to test the source code makes risks manageable. Kaspersky Lab has an audit carried out by a Big Four company. The theoretical possibility therefore proves to be practice. This is an effective step in hindering the execution of espionage and sabotage via the Kaspersky Lab software. By transferring the processing of data for European customers and the software installation to Switzerland, it becomes more difficult for the Russian Federation to abuse Kaspersky Lab software. In summary: The measure is effective.

The publicity on the Kaspersky Lab break-in by an intelligence service and the accusation that classified documents ended up at the company has had an impact on Kaspersky Lab. It is questionable whether it is sufficient to point out that participation in the Kaspersky Security Network is always voluntary, the antivirus software did exactly what it had to do: detect malware and send and detect samples from the back door in Microsoft Office. The Kaspersky Private Security Network (KPSN) solution, as also applied with SaasForce for the Benelux, prevents data from going to Kaspersky Lab. But the story about the suspected NSA employee does not justify the conclusion that data may be stolen via the KSN. The use of the antivirus software by intelligence services for espionage and sabotage with the KPSN is difficult to imagine. Meanwhile, it remains possible to detect new malware in seconds. The measure is effective.

The decision around Kaspersky Lab is harmful to all parties. The (free) high-quality expertise offered on malware assistance in three criminal cases has come to a standstill. With a scarcity of good knowledge, that is a bad thing. Kaspersky Lab has proven its ability to deliver information quickly, decisively and accurately in the event of major malware incidents. The disturbed relationship of trust makes it difficult for Kaspersky Lab to advise the Netherlands. Stopping the cooperation between the government and Kaspersky Lab means that victims of ransom viruses have less chance of recovering their data. For Kaspersky Lab, the measure and the communication about it are downright harmful. By asserting that the software is a tool for espionage and sabotage, the image that the malware fighter provides malware himself is wrongly created.

On 13 September 2017, the American government decided to ban the software of Kaspersky Lab. On 15 May 2018, the Netherlands takes the same decision on the basis of the American case. That is eight months and two days later. Is this careful or slow bureaucratic decision-making? This is a relevant question for the cabinet if it wants to deal decisively with the serious threat of espionage and sabotage.

The proposition that software has broad and deep access at system level raises the question in the Dutch situation whether the vital sectors sufficiently comply with the applicable standards. The measures in these standards protect against the risks of excessively broad access to information and proper detection of incidents.

The CIO Rijk had to find out which Kaspersky Lab software is in use. This raises the question of whether there is sufficient insight into the software used. Is the government aware in the right place of which software is in use (and therefore what risks are involved)? Software at

the system level includes hardware, which is also found in network components. Is it clear what risks are involved? Similar questions are also justified for the use of cloud service providers in the vital sectors because a lot of data comes together in these sectors and it is often unclear to which countries this data goes.

The general reasoning in the Cabinet's precautionary measure justifies the fear for other companies that they will be completely excluded even without any adversity and that a public warning will be issued about the company. After all, the quality of products, contributions to safety in the Netherlands and guarantees in the European and Dutch regulatory framework do not matter.

The Netherlands has strong ambitions in the field of innovation and information security. This sets the bar high to make tough decisions with great care and motivation. Kaspersky Lab takes the fears of espionage and sabotage seriously. The Transparency Center is an effective way to address concerns based on both facts and emotion. It can actually be tested. The Benelux-specific solution with SaasForce adds an extra layer of security to Kaspersky Lab's software. The company proves repeatedly and continuously that software and procedures - in terms of security - are on the right track. It, therefore, has a head start on many suppliers. Yet that is not unusual in itself, because testable quality should be the norm when purchasing the software. All in all, reconsidering the decision taken would be just and in everyone's interest.