Ministry of Justice and Security
To: Mr. F. Grapperhaus
Postbus 20301
2500 EH Den Haag

Subject	Our reference	Date
Assessment Kaspersky software	N.A.	25 May 2018
Phone	**Contact person**	**E-mail**
+31 6 - 5521 3804	Harco Enting	Harco.Enting@kaspersky.nl

Dear Mr. Grapperhaus,

Kaspersky Lab would be grateful for the opportunity to express its deepest regret at the decision of the Government of The Netherlands to ban the company's antivirus software used by the central government and to advise companies in critical infrastructure to do the same.

Considering Kaspersky Lab's ongoing commitment to protecting citizens and organizations in The Netherlands from cyber threats, regardless of the purpose or origin, our very successful collaboration with the Dutch police and several other non-profit activities*, we are disappointed by the Government's decision. Especially because it was made before Kaspersky Lab could provide any information to address the concerns and to mitigate any possible risks and vulnerabilities.

We would appreciate it if, through your good offices, the Government could kindly share with us more information related to these restrictions, in particular:

- Disclosure of the Government's investigation and risk analysis in order to understand on what facts the final decision was based.
- Which Russian law that could force us to provide the Russian government with critical information, or compel us to execute unethical activities, is being referred to in the letter? How is the application of that law to Kaspersky Lab different to other cybersecurity companies that have a subsidiary in Russia and are also active in The Netherlands?
- Disclosure of the contracts between Kaspersky Lab and the central Government, because the company is not aware of contracts with the central Government.

We would like to emphasize that we have never helped, nor will help, any government with its cyberespionage or offensive cyber efforts; Kaspersky Lab provides technical expertise, forensic analysis, and security-related training to governments and law enforcements around the world to assist with defensive efforts only.

The company recognizes that trust is essential in cybersecurity and that it is not a given – we must repeatedly earn it through an ongoing commitment to transparency and accountability. For such reasons, Kaspersky Lab has launched its Global Transparency Initiative to verify the trustworthiness of its products and business operations. As part of this initiative we will open our first Transparency Center in Switzerland, and move core infrastructure from Russia to Zürich, including customer data storage and processing for most regions, as well as software assembly, including threat detection updates. To ensure full transparency and integrity, Kaspersky Lab is arranging for this activity to be supervised by an independent third party, also based in Switzerland. We would be honoured to have the opportunity to explain this in more depth.

**For our successful collaboration with Dutch police and several other non-profit activities please see Appendix 1*

Thank you for your attention and time. Again, we would be grateful if the Ministry can engage in a dialogue with us. As you may understand, an announcement by the Government of this nature creates a lot of controversy and raises questions among our clients and partners. Therefore, we kindly ask that you provide Kaspersky Lab with more clarity as soon as possible, in order to prevent further damage to our reputation. Our team and I are always available to discuss the matter and to provide detailed answers to any questions or concerns.

Looking forward to hearing from you, I remain,

Yours sincerely,

Harco Enting
General Manager
Kaspersky Lab Benelux

Appendix 1:

1) **Research on Carbanak, the Great Bank Robbery – collaborated with NHTCU and shared info with NCSC and other (GOV-CERTS).**
The Dutch Police seized servers, Kaspersky Lab analyzed them and shared the data reports with the police. Some of the outcomes were more than 300.000 stolen credit card numbers that were found and shared with the credit card organizations, preventing further damage. We shared reports about Carbanak with the NCSC (Dutch GOV-CERT) who then shared it with other (GOV)-Certs so they had all the latest information on how to protect themselves for free. We were also able to share data through our channels to hacked financial institutions in other countries because we have very good contacts there.

2) **Research on Coinvault – joint research with NHTCU.**
NHTCU and Kaspersky Lab worked together on Coinvault. Suspects were arrested and gave a full confession. We got all the keys and were able to help everybody who was once infected with CoinVault ransomware.

3) **Several presentations at SAS** – The Dutch police has presented several times at our yearly Security Analyst Summits including a joint presentation with Jornt van der Wiel about Coinvault.

4) **No More Ransom initiative** – Kaspersky Lab established the initiative NMR together with Europol, Dutch police and McAfee in order to prevent balkanization. We believed that by working together and by working with other parties we can allocate resources better and fight cybercrime more efficiently. Highlights:

   a. We worked together on Troldesh / Shade ransomware. We found the server that was seized and there with roughly 250k keys – around 180k keys were usable.
   b. We collaborated on Wildfire / Zyklon / GNL/ Hades/ Serpent ransomware. We found the location of the Wildfire C2 which was then seized. Roughly 5800 keys were captured.
   c. Some statistics about successful decryptions by KL alone:

      Coinvault: 1500
      Wildfire: 1000
      Shade: 2600
      Rakhni (November 2016): 18730
      Rannoh (December 2016): 7000 +

      30830 X 300 = ~9.2 Million Euro saved

5) **ONE Conference** – We did joint presentations with the NHTCU about successful researches at the ONE Conference in 2017 and 2016. We organized KIPS games (gamification) for the conference's participants in the lunch breaks. Also was Eugene Kaspersky invited by NCSC to do the keynote in 2017.

6) **Other researches that are not yet public** - We also worked together with the NHTCU on other cases that are not public (yet). But in general some of the things we do is to provide telemetry, malware analysis, etc.

7) **TKI Urban Energy event** – This event was organized by TKI Urban Energy and targeting decision makers in the energy sector. Maria Garnaeva, security analyst from GReAT, did a presentation about industrial cyber threats in order to inform decision makers in the Dutch energy sector.

8) **Cooperation with TU Delft** – we did several student conferences together with TU Delft to make students aware of their opportunities in the cyber security sector and

Eugene Kaspersky was interviewed during a Cyber Talk by students, which was moderated by Rick Nieman.

9) **Nederlandse orde van Advocaten** – Martijn van Lom did a presentation and took part in a panel discussion about cybercrime , how this affect the legal industry/ law firms and how they can protect themselves against these cyber threats.

10) **Digital Trust Center** – Kaspersky Lab is part of the initiative Digital Trust Center, an initiative by the government to help entrepreneurs and SMB become more resilient against cybercrime.

11) **GeefITdoor** – Martijn van Lom gave ca. 10 guest lectures at schools as part of the national campaign 'GeefITdoor'. This campaign is aimed at inspiring youngsters for an education and career in IT.

12) **Children's book Kasper, Sky and the Green Bear** – We created a children's book in cooperation with Dutch writer Marlies Slegers which is meant for children between 6-9 years old in order to educate them in a playful way about how to stay safe in the online world. We sent the book to all primary schools in The Netherlands for free. We also collaborated with the 'Week of Mediawijsheid', which is a national campaign that promotes media savviness amongst parents, teachers and children and supported our children's book through their channels.

13) **Nederland ICT** – Martijn van Lom plays an active role within the branch association of the ICT sector which stands up for the interests of all organizations within the branch.

14) **Alert Online campaign** – We yearly contribute to the Alert Online campaign which is a governmental initiative to promote security awareness amongst organizations and consumers. Jornt van der Wiel attended a roundtable at Alert Online's kick-off event at KPN. He was also invited for the TekTok talkshow to talk about ransomware. Plus we also organized free of charge KIPS games for companies in close cooperation with our partner SLTN.

15) **Cyber security awareness campaigns of the government** – We have supported the government in their awareness campaign in the past ('Maak het ze niet gemakkelijk') and will do in the future ('Boefproef' & 'Maak het ze niet gemakkelijk').

16) **Support The Hague security delta with launching a testbed** – The Hague Security Delta launched their (international) testbed in 2017 and we supported them with a keynote by Eugene Kaspersky and Martijn van Lom who participated in the panel discussion.

17) **Supporting cyber initiative TIBER** – Kaspersky Lab supported DNB and are currently supporting ECB their TIBER project.