



**Geopolitiek.
Transparantie.
Reactie.**

ONE Conference 2016



Intensieve samenwerking met Nederlandse Politie



Samenwerking leidt tot succesvolle strijd tegen ransomware

AD Nieuws Regio Sport Show Video Koken & Eten

Binnenland Buitenland Politiek Economie Gezond Bizar Wetenschap Auto Tech Wonen

NO MORE RANSOM!

Crypto Sheriff Ransomware: Q&A Prevention Advice Decryption Tools Report a Crime Partners About the Project

NEED HELP unlocking your digital life
without paying your attackers*?

YES **NO**

Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom. However this is not guaranteed and you should never pay!

GOOD NEWS
Prevention is possible. Following simple cyber security advice can help you to avoid becoming a victim of ransomware.

BAD NEWS
Unfortunately, in many cases, once the ransomware has been released into your device there is little you can do unless you have a backup or security software in place.

GOOD NEWS
Nevertheless, it is sometimes possible to help infected users to regain access to their encrypted files or locked systems, without having to pay. We have created a repository of keys and applications that can decrypt data locked by different types of ransomware.

▲ Website van No More Ransom © nomoreransom.org

Nederlands project boekt succes in strijd tegen ransomware

Het Nederlandse project 'No More Ransom' tegen computercriminaliteit heeft in de eerste twee maanden na de lancering al 2500 mensen geholpen. Dat bespaarde de slachtoffers zo'n 1,35 miljoen euro, liet de politie weten.

Redactie 17-10-16 12:31 | Laatst updated op 17-10-16 12:31 | Foto: ANP

Dat niet alleen; ook maken we samen een einde aan Coin Vault

Kaspersky Lab en Nederlandse politie maken eind aan nachtmerrie voor gijzelingssoftware-slachtoffers wereldwijd

EMERCE



Utrecht, 29 oktober – In september arresteerde de Nederlandse politie twee mannen in Nederland op verdenking van betrokkenheid bij de CoinVault en Bitcryptor ransomware-aanvallen. Met deze arrestaties, en door het feit dat het laatste gedeelte van de decryptiesleutels nu beschikbaar is, is het mogelijk om de zaak over de CoinVault-aanvallen ook voor de slachtoffers te sluiten. **Kaspersky Lab** heeft nog eens 14.031 decryptiesleutels toegevoegd aan de database noransom.kaspersky.com. Hierdoor kunnen nu alle slachtoffers van de CoinVault en Bitcryptor gijzelingssoftware hun gecodeerde gegevens herstellen

zonder een enkele bitcoin aan losgeld te betalen aan de cybercriminelen.

Sinds april 2015 zijn er in totaal 14.755 sleutels beschikbaar gesteld aan slachtoffers, zodat zij hun bestanden weer kunnen ontgrendelen met behulp van de door beveiligingsexperts van Kaspersky Lab ontwikkelde tool. Het Landelijk Parket van het Nederlandse Openbaar Ministerie haalde de decryptiesleutels van de CoinVault command & control-servers na de arrestatie van de verdachten in

Coin vault makers gaan de cel in

RTLnieuws OM: makers gijzelsoftware Coinvault de cel in

Nieuws Economie Sport Boulevard Tech Lifestyle EditieNL Uitzendingen

Twee Amersfoortse broers hebben tientallen computers gegijzeld en losgeld geëist van de slachtoffers. Dat geven ze ook toe. Het Openbaar Ministerie vindt dat twee daarom de cel in moeten.

De officier van justitie eiste donderdag een jaar gevangenisstraf, waarvan 9 maanden voorwaardelijk, tegen de 25-jarige Melvin en de 21-jarige Dennis van den B. uit Hoogland bij Amersfoort. Ook zouden ze een taakstraf van 240 uur moeten krijgen.

Bitcoin

De broers stonden donderdag voor de rechter in Rotterdam. In 2014 en 2015 hebben ze volgens justitie zeker 1259 computers besmet, vooral in Nederland. Ze eisten 1 bitcoin losgeld, die in die tijd enkele honderden euro's waard was. Bijna honderd gedupeerden betaalden. "Toen ze begonnen gaf het een kick om malware te maken. Toch werd het al snel een manier om geld te verdienen. Ze hebben niet stilgestaan bij wat ze hebben aangericht bij de mensen", verklaarde de aanklager.

De broers verdienden elk ongeveer 10.000 euro aan de besmettingen. Ze hadden een helpdesk opgezet om slachtoffers te helpen met betalen. "Mensen stuurden noodkreten, maar daar werd kil op geantwoord dat ze maar moesten betalen", aldus justitie. Volgens het OM was het "grootschalig en professioneel" en kunnen sommige gedupeerden nog steeds niet bij hun bestanden.

Samenwerking op alle niveaus; media en zakelijke partners als KPN



Maak het ze niet te makkelijk

➤ [Veiliginternetten.nl](https://www.veiliginternetten.nl)

Bescherm jezelf tegen cybercrime. Voer updates altijd direct uit; klik niet zomaar op iedere link; gebruik verschillende wachtwoorden; gebruik altijd een virusscanner; maak regelmatig een back-up.



29 maart · 🌐

Martijn van Lom aan tafel bij Koffietijd / 5 Uur Live over de overheidscampagne "maak het internetcriminelen niet te makkelijk".



KOFFIETIJD.NL

Veilig online

Internetcriminaliteit is een van de meest voorkomende misdaden.

14 MEI 2018



Afnemend vertrouwen is een wereldwijde trend

#1 Balkanisering

Groei van het aantal
cyberincidenten +
industriële internet



Noodzaak van
bescherming van
kritieke infrastructuur



Staatsregulering
als oplossing

Balkanisering als natuurlijke reactie



European Union
GDPR, NIS regulation,
local legislation



UK
Investigatory Powers
Bill, 2016



Germany
Surveillance Bill,
2017



China
Cybersecurity Law,
2017



Singapore
Cybersecurity Bill,
2017



Russia
Critical Informational
Infrastructure Bill,
2018

#2 Protectionisme



Stimuleren
van binnenlandse
bedrijven



Handhaving
van samenleving met
buitenlandse bedrijven



Weren
van buitenlandse
bedrijven

#3 Militarisering van cyberspace



Meer dan 30 landen hebben aangekondigd dat ze militaire cyberdivisies hebben



Wetgevende druk op softwareontwikkelaars:

Chinese cybersecurity wet
Singapore cybersecurity wet
Russische executive order,
02/02/2018



NATO artikel 5



Verdediging – is een element van aanval

#4 afbreken van internationale samenwerking





Vertrouwenscrisis
als gevolg van
lekken



Geopolitieke
bevriezing



Inefficiëntie van
internationale
instellingen



Onderontwikkeling
van internationale
wetgeving

tegelijkertijd



Strengere lokale
wet- en regelgeving



Het gaat niet alleen om ons. De wereld verandert. We lopen voor, maar anderen volgen.

“De BOD was niet gebaseerd op
ontrouw, schuld of een andere
overtreding van Kaspersky Lab*

Andere Europese landen wijken af; Duitsland....

Presse



Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Stellungnahme zu Medienberichten über AV-Software

Ort Bonn
Datum 11.10.2017

Het overheidsexpertisecentrum voor Informatietechniek stelt niet met een waarschuwing te komen *‘omdat het geen enkele aanwijzing heeft voor malafide praktijken of kwetsbaarheden’*

BSI keine Belege für ein Fehlverhalten des Unternehmens oder Schwachstellen in der Software vorliegen.

Antiviren-Programmen kommt nach wie vor eine bedeutsame Rolle in der Absicherung von IT-Systemen zu. Um diesen Schutz realisieren zu können, haben AV-Programme in der Regel Vollzugriff auf alle auf dem Rechner gespeicherten Daten.

Ook Frankrijk...

 **France Diplomacy**  
@francediplo_EN Follow

Launch of the [#ParisCall](#) for Trust and Security in Cyberspace : 9 goals to limit hacking and destabilizing activities on the Internet. fdip.fr/Call



LAUNCH OF THE
PARIS
11 • 12 • 2018
CALL
FOR TRUST AND SECURITY
IN CYBERSPACE

 **Eugene Kaspersky** 
@e_kaspersky Following

Proud to be an early supporter of the [#ParisCall](#) for trust and security in cyberspace unveiled today by [@EmmanuelMacron](#) at the [#ParisPeaceForum](#) 🌐 🤝 Say no to balkanization, say yes to cooperation! diplomatie.gouv.fr/en/french-fore ...

Ministry of Foreign Affairs
37, quai d'Orsay - 75007 Paris
"Paris Call for Trust and Security in Cyberspace"

Re: Kaspersky Lab's support for the call

Dear Mr. Jean-Yves Le Drian,

Kaspersky Lab – the company I represent – really appreciates the launch of the 'Paris Call for Trust and Security in Cyberspace' that President Macron and yourself are promoting. For years, my company has been fighting cyberthreats because we believe that everyone – from home computer users through to large corporations and governments – should be able to protect what matters to them most. And for more than a decade I've been advocating an international convention that would guarantee that people's rights are to be protected online.

We see a pressing need for an effective mechanism that would ensure the safety of cyberspace. But not only cyberspace! Since the world went digital, we have had to deal not only with the benefits of this process but also the downsides. Our mobile phones, our money, our factories and plants – critical infrastructure – all of it relies on the internet. The line between digital/online and tangible/offline is getting blurred, and that is why international law needs to work in cyberspace the same way it works in other, more conventional areas.

Today I am delighted to say that we are by no means alone in the effort to make the world a safer and more secure place. The Paris Call appeals to the numerous public and private organizations that, to quote the source, will be

n voor Informatie
omdat het
voor malat
n'

Belgische overheid behoudt vertrouwen in Kaspersky-software

datanews



Kristof Van der Stadt
is hoofdredacteur bij Data News

08/11/18 om 22:21 - Bijgewerkt om 22:20
Bron: Datanews

Volgens het CCB kunnen geen enkele objectieve technische informatie of onafhankelijke studies aantonen dat de toepassingen van Kaspersky Lab kwaadaardig zouden zijn of een dreiging zouden betekenen voor de digitale veiligheid van het land. Dit heeft premier Charles Michel gemeld in de Kamer na een vraag van Kamerlid Brecht Vermeulen (N-VA).

Het CCB volgt dus niet het voorbeeld van de Nederlandse evenknie NCSC. Uit vrees voor inmenging van Russische veiligheidsdiensten en onethisch gebruik van de software werd de software in Nederland eerder wél uitgefaseerd. "Het is positief dat onze Belgische regering niet meegaat met de steekvlampolitiek die elders wel de kop opsteekt. Het is logisch dat iedere natie zijn belangen beschermt, maar we moeten hierbij niet naïef zijn. Ook bevriende naties doen aan spionage, denk maar aan de Belgacom-hack uit 2013 of de telefoon van Angela Merkel die door de VS werd afgeluisterd", aldus Brecht Vermeulen.

Kaspersky Lab heeft overigens pas nog zijn kernactiviteiten van Rusland naar Zwitserland verhuisd. Specifiek voor de Benelux zouden bijkomende maatregelen getroffen zijn in de vorm van het Kaspersky Private Security Network. Dat betekent dat de software binnen de Benelux beheerd blijft en dat de informatie rond dreigingsanalyse binnen de grenzen van de Europese Unie blijft.



Waarom Kaspersky Lab?



Wereldwijde geopolitieke turbulentie



Interne politieke situatie in de VS



Concurrenten als free-riders



Combinatie van bovengenoemde



We blijven detecteren en beschermen, wat er ook gebeurt



Wij beschikken over de beste technologieën in de industrie, die beschermen tegen de meest geavanceerde aanvallen. Dat vinden sommige stakeholders niet altijd even prettig.



Onze aanpak

Twee beschuldigingen



Mogelijkheid van een
backdoor



Mogelijkheid van
onwettige toegang tot
data voor geheime
diensten

Meervoudige aanpak op verschillende niveaus

Global Transparency Initiative – Transparency Centers



Onafhankelijke code en update review (Symantec en McAfee geweigerd)



Engineering practices externe audit & certificering



Bug bounty programma



Redesign van R&D infrastructuur



R&D re-design

Verzamelen
van data
+
data
verwerking

Vanaf 2018 voor Europa,
met meer landen om te
volgen

Transparency
Center

Bouw
conveyor
+
Ondertekenen
van
certificaten

Global Transparency Initiative: Kaspersky Lab verplaatst kerninfrastructuur naar Zwitserland



Global Transparency Centre Zurich

Foto invoegen opening GTC



Deze ontwikkelingen zien we als een kans. Transparantie moet een industriestandaard worden.

14 NOVEMBER 2018


WOB-verzoek uitkomsten worden nu onafhankelijk getoetst....



Rijksoverheid

Besluit op Wob-verzoek inzake antivirussoftware van Kaspersky

De minister van Justitie en Veiligheid heeft op 11 oktober 2018 een beslissing genomen naar aanleiding van een verzoek op basis van de Wet openbaarheid van bestuur. Het verzoek betreft de openbaarmaking van informatie over antivirussoftware van Kaspersky.

 [Download 'Besluit op Wob-verzoek inzake antivirussoftware van Kaspersky'](#)

PDF document | 12 pagina's | 448 kB

Wob-verzoek | 11-10-2018

Onze boodschap

#1

Het gaat niet alleen om ons. De wereld verandert.

#2

De wereld digitaal veiliger maken, hoeft niet bij iedereen vrienden te maken

#3

**Transparantie moet industriestandaard worden.
Anderen zullen volgen...**

STAY TUNED!



Vragen?

Martijn van Lom, dank voor uw aandacht