

10(2)(e)

Van: [redacted] BD/NCSC/OP
Aan: [redacted]@ncsc.nl
Cc: [redacted] BD/NCSC/OP
Onderwerp: Pegasus
Datum: woensdag 21 juli 2021 18:42:04

Via cyber veilig nederland werd een tool genoemd waarmee je zou kunnen controleren / detecteren op pegasus infecties. Mogelijk is deze al bekend, mijn vraag zou zijn om IRON te laten onderzoeken of deze tool idd een handelingsperspectief levert, werkt dit ook echt etc. Technisch onderzoek (samen met CTI) voor de komende dagen.

<https://github.com/mvt-project/mvt>

10(2)(e)

Cheer,



Sent with BlackBerry Work
(www.blackberry.com)

10(2)(e) **Van:** [redacted]
Aan: [redacted] BD/NCSC/OP
Cc: [redacted]
 10(2)(g) **Onderwerp:** RE: [NCSC-NL [redacted]] FW: NSO en Pegasus
Datum: donderdag 22 juli 2021 17:07:41

10(2)(e) Hoi [redacted]
 Dank voor het bericht en klinkt goed!
 Ik neem aan dat dit ook met de CISO's gedeeld kan worden?
 Laten we aan de hand van het stuk ook bedenken of we er al iets richting de ambtelijke leiding zou moeten gaan.

10(2)(e) [redacted]
 10(2)(e) **Van:** [redacted] BD/NCSC/OP
Verzonden: donderdag 22 juli 2021 17:00

10(2)(e) **Aan:** [redacted]
CC: [redacted]
 10(2)(g) **Onderwerp:** RE: [NCSC-NL [redacted]] FW: NSO en Pegasus

10(2)(e) Beste [redacted] en [redacted]
 Na overleg met NCTV en veiligheidspartners zijn we er op uitgekomen dat er morgen een gezamenlijke duiding en handelingsperspectief jullie kant op zal komen welke onder de BVAs kan worden gedeeld indien gewenst. Dit zal via de NCTV verlopen.

10(2)(e) Cheers,
 [redacted]
 Sent with BlackBerry Work
 (www.blackberry.com)

10(2)(e) **From:** [redacted] [redacted]@minbzk.nl>
Date: Thursday, 22 Jul 2021, 1:27 PM
To: [redacted] BD/NCSC/OP [redacted]@minjenv.nl>
Cc: [redacted] <[redacted]@minbzk.nl>
 10(2)(g) **Subject:** FW: [NCSC-NL [redacted]] FW: NSO en Pegasus

10(2)(e) Goedemiddag!
 Ik heb [redacted] gevraagd om dit tijdens mijn vakantie over te nemen
 De haakjes die we besproken hebben voor dit onderwerpen zijn ruwweg als volgt:

1. De politieke en bestuurlijke leiding en hun medewerkers worden geraakt en daarmee dus spionage, de veiligheid van het land en de digitale soevereiniteit.
2. Journalisten, activisten en daarmee grondrechten, mensenrechten en democratie
3. De zero day zero click kwetsbaarheden waar sprake van zou zijn, zijn reguliere digitale kwetsbaarheden.

1 en 3 zijn helder belegd denk ik. Voor 2 zit er volgens mij bij BZK een club die daar mee bezig is. Dan houden we contact ook voor het informeren van de bestuurlijke leiding als we daar aanleiding toe zien.

10(2)(e) [redacted]
 Adviseur Informatiebeveiliging en privacy

Directie CIO Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
 Turfmarkt 147 | 2511 DP | Den Haag | 11e etage

Postbus 20011 | 2500 EA | Den Haag

E [redacted]@minbzk.nl

10(2)(e)

T 06 [redacted]

-----Oorspronkelijk bericht-----

Van: cert@ncsc.nl <cert@ncsc.nl>

10(2)(e)

Verzonden: woensdag 21 juli 2021 11:01

Aan: [redacted] [redacted]@minbzk.nl>

10(2)(g)

Onderwerp: [NCSC-NL [redacted]] FW: NSO en Pegasus

-----BEGIN PGP SIGNED MESSAGE-----

10(2)(e)

Beste [redacted]

Bedankt voor uw mail. Hierbij bevestigen wij dat deze in goede orde is ontvangen. Wij doen ons best u zo spoedig mogelijk van een antwoord te voorzien.

Met vriendelijke groet,

Nationaal Cyber Security Centrum

Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl

10(2)(g)

E cert@ncsc.nl

T +31 070 751 55 55 (algemeen)

Bezoekadres:

Turfmarkt 147 | 2511 DP | Den Haag

10(2)(g)

-----BEGIN PGP SIGNATURE-----

Charset: [redacted]

10(2)(g)

-----END PGP SIGNATURE-----

On Wed Jul 21 09:12:53 2021 wrote:

> Ha collega's,

>

> Kunnen jullie deze vraag overnemen? Als NCSC monitoren we, maar

> misschien doorverwijzen naar de dienst, oid?

>

> Dank alvast,

>

10(2)(e)

> [redacted]

>

10(2)(e)

>
>
>
>
> Van: [redacted]
> [redacted]@minbzk.nl>>
> Datum: dinsdag 20 jul. 2021 4:13 PM
> Aan: NCSC Bestuurlijke Ondersteuning
>

10(2)(e)

> [redacted]@ncsc.nl>>
> Kopie: [redacted]
> [redacted]@minocw.nl>>, [redacted]
> [redacted]@minbzk.nl>>
> Onderwerp: NSO en Pegasus
>

> Goedemiddag,
>
> Er gaan nogal wat artikelen over Pegasus en NSO. Waaronder 50.000
> mensen die gemonitord zouden worden en zero-day, zero click
> kwetsbaarheden op IOS. Ik heb ook het idee dat nog veel onduidelijk
> is, zoals uit dit artikel blijkt:
> <https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html>
>
> Hebben jullie al een beter onderscheid tussen feit en fictie en al
> iets van duiding en advies?

10(2)(e)

> [redacted]
> Adviseur Informatiebeveiliging en privacy
>
> Directie CIO Rijk
> Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Turfmarkt 147
> | 2511 DP | Den Haag | 11e etage Postbus 20011 | 2500 EA | Den Haag
>

10(2)(e)

10(2)(e)

> E [redacted]@minbzk.nl
> T 06 [redacted]
>
>
> _____

> Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien
> u niet de geadresseerde bent of dit bericht abusievelijk aan u is
> toegezonden, wordt u verzocht dat aan de afzender te melden en het
> bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor
> schade, van welke aard ook, die verband houdt met risico's verbonden
> aan het elektronisch verzenden van berichten.
> This message may contain information that is not intended for you. If
> you are not the addressee or if this message was sent to you by
> mistake, you are requested to inform the sender and delete the
> message. The State accepts no liability for damage of any kind

het goed is een whitepaper "Veilig gebruik van mobiele dragers" of zoiets) op dit thema als we die hebben. We proberen onze eventuele aanvullingen voor 13:00 terug te geven aan de NCTV.

Alvast bedankt!

Cheers,

10(2)(e)

[redacted]

Van: [redacted] BD/PSD [redacted] <[redacted]@nctv.minjenv.nl>

Verzonden: vrijdag 23 juli 2021 10:23

10(2)(e)

Aan: [redacted] BD/NCSC/Staf <[redacted]@minjenv.nl>; [redacted]
BD/NCSC/OP [redacted] <[redacted]@minjenv.nl>

Onderwerp: FW: Duiding KA Pegasus

Goedemorgen,

Hadden jullie al wat documenten met handelingsperspectief voor de beveiliging van telefoons gevonden om aan de duiding toe te voegen?

Groeten,

10(2)(e)

[redacted]

Van: [redacted] BD/KA <[redacted]@nctv.minjenv.nl>

10(2)(e)

Verzonden: donderdag 22 juli 2021 17:24

Aan: [redacted] BD/PSD [redacted] <[redacted]@nctv.minjenv.nl>

Onderwerp: Duiding KA Pegasus

Ha [redacted]

10(2)(e)

Ik ben net even bij [redacted] langs gelopen en die heeft groen licht gegeven voor het extern verspreiden van de duiding aan BVA's.

In de bijlage hangt de meest recente versie die kan worden gedeeld met CIO Rijk.

Alvast een fijne avond!

10(2)(e)

Met vriendelijke groet,

[redacted]

10(2)(e) **Van:** [redacted]
Aan: [redacted]
Onderwerp: Update Pegasus
Datum: vrijdag 23 juli 2021 13:13:43
Bijlagen: Pegasus-2021-07-23-13-13-43.pdf
 ALLIAN-02-10

Beste collega's,
 Ter info: Zoals gisteren afgesproken heeft [redacted] een duiding inzake Pegasus gedeeld met OIO Rijk, met het verzoek dit verder te verspreiden onder de CIO's en BVA's binnen de rijksoverheid. Onze input is in deze duiding meegenomen. Als handelingsperspectief wordt gewezen op een AIVD- en een NCSC-factsheet. Deze duiding kan ook worden gebruikt als rijksoverheidsorganisaties vragen aan ons stellen. Zie verder eveneens de algemene woordvoeringslijn bijgevoegd.

10(2)(e) Mocht het nodig zijn: Voor BO heb ik vanavond piket [redacted] dit weekend.

Groet [redacted]

Van: [redacted] -BD/NCTV [redacted]

Verzonden: vrijdag 23 juli 2021 14:31

10(2)(e) **Aan:** [redacted]

CC: [redacted] BD/PSD [redacted]

10(2)(e) **Onderwerp:** Duiding Pegasus - verzoek om delen info

Dag [redacted]

Naar aanleiding van de berichtgeving over de Pegasus spionagesoftware in de media, tref je hierbij onze meest recente duiding aan.

Bijgevoegd tref je ook twee links aan met handreikingen van de AIVD en het NCSC voor de beveiliging van mobiele apparaten.

Ons verzoek is of je deze wilt delen met de CIO's van de departementen en de Hoge Colleges van Staat.

Wij blijven de ontwikkelingen rond Pegasus volgen.

10(2)(e) <https://www.ncsc.nl/documenten/fact sheets/2019/juni/04/factsheet-veilig-gebruik-ansamrtphonex-en-tablets>

/Beveiliging_van_mobiele_apparaten_tijdens_de_levenscyclus_v1.1_.pdf

Hartelijke groet

10(2)(e)

tel: +31707515050 | mob: +316 [redacted]

10(2)(e)

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

10(2)(e) Van: [redacted] BD/PSD
 Aan: [redacted] NCSC/OP
 Cc: [redacted] NCSC/OP
 Onderwerp: RE: Duiding KA Pegasus
 Datum: vrijdag 23 juli 2021 14:04:47

Bedankt

Van: [redacted] BD/KA

Verzonden: vrijdag 23 juli 2021 14:04

10(2)(e) Aan: [redacted] BD/NCSC/OP; [redacted] BD/PSD

CC: [redacted] BD/NCSC/Staf

Onderwerp: RE: Betr: RE: Duiding KA Pegasus

Hi [redacted] en [redacted]

10(2)(e) Dank voor de aanvullingen en suggesties. Punt over Israëlische taskforce stond inderdaad ook al in onze geüpdatete versie.

Ik heb je punten verwerkt, de meest recente versie hangt in de bijlage als PDF.

Groet,

10(2)(e)

Van: [redacted] BD/NCSC/OP; [redacted] [redacted]

Verzonden: vrijdag 23 juli 2021 13:34

10(2)(e) Aan: [redacted] BD/PSD; [redacted] [redacted]

CC: [redacted] BD/NCSC/Staf; [redacted] [redacted] BD/KA; [redacted] [redacted]

Onderwerp: RE: Betr: RE: Duiding KA Pegasus

Hi [redacted] en [redacted]

Hierbij onze suggestie voor de duiding en handelingsperspectief. Staat er straks bij de communicatie duidelijk voor wie het bedoeld is?

Rij de een andere suggestie/tevoorzieningen

[redacted]

We kunnen verwijzen naar de volgende factsheet. Eventueel ook in de woordvoeringslijn.

<https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-veilig-gebruik-van-smartphones-en-tablets>

Cheng's,

10(2)(e) Van: [redacted] BD/PSD; [redacted] [redacted]

Verzonden: vrijdag 23 juli 2021 12:56

Aan: [redacted] BD/NCSC/OP; [redacted] [redacted]

Onderwerp: FW: Betr: RE: Duiding KA Pegasus

Hi [redacted]

Kan ik dit factsheet dat [redacted] stuurde gebruiken of heb jij een andere versie en nog eventuele andere documenten?

Gr

Van: [redacted] [redacted] [redacted]

Verzonden: vrijdag 23 juli 2021 11:00

10(2)(e) Aan: [redacted] [redacted]

CC: [redacted] BD/PSD; [redacted] [redacted] [redacted] BD/NCSC/Staf; [redacted] [redacted]

Onderwerp: Betr: RE: Duiding KA Pegasus

Hierbij de NCSC brochure van 2014

[redacted] NCSC-NL; [redacted] [redacted] [redacted] [redacted] [redacted]

Aan: [redacted] BD/PSD; [redacted] [redacted] [redacted] [redacted] [redacted]

Van: [redacted] (NCSC-NL); [redacted] [redacted]

Datum: 23-7-2021 10:57

Cc: [redacted] [redacted]; [redacted] BD/NCSC/Staf; [redacted] [redacted]

Onderwerp: RE: Duiding KA Pegasus

Die willen wij ook graag ontvangen, thanks!!

Cheng's,

10(2)(e)

Ministerie van Justitie en Veiligheid: Ministry of Justice and Security
 Nationaal Cyber Security Centrum | National Cyber Security Centre
 Turfmarkt 147 | 2511 DP | Den Haag
 Postbus 20011 | P.O. Box 20011 | 2500 EA | Den Haag | The Netherlands

T +31 (0) [redacted]

M [redacted]

[redacted]

From: [redacted] BD/PSD; [redacted] [redacted]

Verzonden: vrijdag 23 juli 2021 10:42

To: [redacted] [redacted]

Cc: [redacted] NCSC-NL; [redacted] [redacted] [redacted]

Subject: RE: Duiding KA Pegasus

Thnx!

Zou je jullie woordvoeringslijn ook nog even kunnen doorsturen?

Van: [redacted] [redacted]

Verzonden: vrijdag 23 juli 2021 10:30

Aan: [redacted] BD/PSD; [redacted] [redacted]

CC: [redacted] NCSC/NL; [redacted] [redacted]

Onderwerp: RE: Duiding KA Pegasus

Ha [redacted]

[redacted]

[redacted]

[redacted]

Bij deze de link naar de whitepaper op Rijksportaal. Handigste is om de link in de mail te zetten.

We verwijzen in de whitepaper ook naar een factsheet van NCSC. Ik heb [redacted] hier ook even op getipt.

Hg.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Beveiliging van mobiele apparaten rijks.nl-je-encyclopedie_v1.1.pdf

Van: [redacted] BD/PSD; [redacted] [redacted]

Datum: vrijdag 23 juli 2021 10:24 AM

Aan: [redacted] [redacted]

Onderwerp: FW: Duiding KA Pegasus

Goedemorgen [redacted]

Had jij al wat documenten met handelingsperspectief gevonden die ik aan de duiding voor CIO Rijk kan toevoegen?

Groeten,

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10(2)(e) **Van:** [redacted] BD/PSD
Aan: [redacted] BD/NCSC/OP; [redacted] BD/NCSC/Staf
Onderwerp: RE: Duiding KA Pegasus
Datum: vrijdag 23 juli 2021 11:07:04

De woordvoeringslijn is nog niet afgestemd.
 Afgestemde versie stuur ik, als ik die heb, rond.

10(2)(e) **Van:** [redacted] BD/NCSC/OP
Verzonden: vrijdag 23 juli 2021 11:02
Aan: [redacted] BD/PSD ; [redacted] BD/NCSC/Staf
Onderwerp: RE: Duiding KA Pegasus

10(2)(g) Hij ligt nu bij een dreigingsanalist om te zien of er nog toevoegingen op gedaan kunnen worden, tevens zijn we even aan het graven welke eventuele adviezen kunnen worden toegevoegd vanuit het NCSC. Komt straks naar je toe.
 Is de woordvoeringslijn nu helemaal afgestemd (NP, BZK JenV)? En kunnen wij die ook krijgen?

10(2)(e) Cheers,

[redacted]

10(2)(e) **Van:** [redacted] BD/PSD [redacted] @nctv.minjenv.nl>

Verzonden: vrijdag 23 juli 2021 10:23

10(2)(e) **Aan:** [redacted] BD/NCSC/Staf [redacted] @minjenv.nl> [redacted]
 BD/NCSC/OP [redacted] @minjenv.nl>

Onderwerp: FW: Duiding KA Pegasus

Goedemorgen,

Hadden jullie al wat documenten met handelingsperspectief voor de beveiliging van telefoons gevonden om aan de duiding toe te voegen?

Groeten,

10(2)(e) [redacted]

Van: [redacted] BD/KA [redacted] @nctv.minjenv.nl>

10(2)(e) **Verzonden:** donderdag 22 juli 2021 17:24

Aan: [redacted] BD/PSD <[redacted]@nctv.minjenv.nl>

Onderwerp: Duiding KA Pegasus

10(2)(e) Ha [redacted]

Ik ben net even bij [redacted] langs gelopen en die heeft groen licht gegeven voor het extern verspreiden van de duiding aan BVA's.

In de bijlage hangt de meest recente versie die kan worden gedeeld met CIO Rijk.

Alvast een fijne avond!

10(2)(e) Met vriendelijke groet,

[redacted]

10(2)(e)

[redacted]

10(2)(e) **Van:** [redacted]@minbzk.nl>**Verzonden:** vrijdag 23 juli 2021 10:0910(2)(e) **Aan:** [redacted] BD/NCSC/OP**CC:**10(2)(g) **Onderwerp:** RE: [NCSC-NL [redacted]] FW: NSO en Pegasus

10(2)(e) Hoi [redacted]

Vast bekend, maar deze zag ik nog langskomen:

- <https://www.france24.com/en/europe/20210722-macron-holds-cyber-security-meeting-in-wake-of-allegations-pegasus-spyware-may-have-targeted-him>
- <https://www.theguardian.com/news/2021/jul/22/dalai-lama-inner-circle-listed-pegasus-project-data>

Vragen waar we op kunnen rekenen zijn:

11(1)

[redacted]

[redacted]

[redacted]

[redacted]

10(2)(e) [redacted]

10(2)(e) **Van:** [redacted] - BD/NCSC/OP**Verzonden:** donderdag 22 juli 2021 17:0010(2)(e) **Aan:** [redacted]**CC:** [redacted]10(2)(g) **Onderwerp:** RE: [NCSC-NL [redacted]] FW: NSO en Pegasus

10(2)(e) Beste [redacted] en [redacted]

Na overleg met NCTV en veiligheidspartners zijn we er op uitgekomen dat er morgen een gezamenlijke duiding en handelingsperspectief jullie kant op zal komen welke onder de BVAs kan worden gedeeld indien gewenst. Dit zal via de NCTV verlopen.

Cheers,

10(2)(e) [redacted]

Sent with BlackBerry Work
(www.blackberry.com)

10(2)(e) **From:** [redacted]@minbzk.nl>**Date:** Thursday, 22 Jul 2021, 1:27 PM10(2)(e) **To:** [redacted] - BD/NCSC/OP [redacted]@minjenv.nl>**Cc:** [redacted]@minbzk.nl>10(2)(g) **Subject:** FW: [NCSC-NL [redacted]] FW: NSO en Pegasus

Goedemiddag!

10(2)(e) Ik heb [redacted] gevraagd om dit tijdens mijn vakantie over te nemen

De haakjes die we besproken hebben voor dit onderwerpen zijn ruwweg als volgt:

1. De politieke en bestuurlijke leiding en hun medewerkers worden geraakt en daarmee dus spionage, de veiligheid van het land en de digitale soevereiniteit.
2. Journalisten, activisten en daarmee grondrechten, mensenrechten en democratie
3. De zero day zero click kwetsbaarheden waar sprake van zou zijn, zijn reguliere digitale kwetsbaarheden.

1 en 3 zijn helder belegd denk ik. Voor 2 zit er volgens mij bij BZK een club die daar mee bezig is.

Dan houden we contact ook voor het informeren van de bestuurlijke leiding als we daar aanleiding toe zien.

10(2)(e) [redacted]
Adviseur Informatiebeveiliging en privacy

.....
Directie CIO Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147 | 2511 DP | Den Haag | 11e etage
Postbus 20011 | 2500 EA | Den Haag

10(2)(e) [redacted]@minbzk.nl
T 06 [redacted]

-----Oorspronkelijk bericht-----

Van: cert@ncsc.nl

Verzonden: woensdag 21 juli 2021 11:01

10(2)(e) Aan: [redacted]

10(2)(g) Onderwerp: [NCSC-NL [redacted]] FW: NSO en Pegasus

10(2)(g) -----BEGIN PGP SIGNED MESSAGE-----
[redacted]

10(2)(e) Beste [redacted]

Bedankt voor uw mail. Hierbij bevestigen wij dat deze in goede orde is ontvangen. Wij doen ons best u zo spoedig mogelijk van een antwoord te voorzien.

Met vriendelijke groet,

.....
Nationaal Cyber Security Centrum

Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl

E cert@ncsc.nl

T +31 070 751 55 55 (algemeen)

10(2)(g) [redacted]

.....
Bezoekadres:

Turfmarkt 147 | 2511 DP | Den Haag

10(2)(g) -----BEGIN PGP SIGNATURE-----
[redacted]

Charset: [redacted]

10(2)(g) [redacted]
[redacted]
[redacted]
[redacted]

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

On Wed Jul 21 09:12:53 2021 wrote:

> Ha collega's,
>
> Kunnen jullie deze vraag overnemen? Als NCSC monitoren we, maar
> misschien doorverwijzen naar de dienst, oid?

>
> Dank alvast,
>

10(2)(e) > [Redacted]

>
>
>
>
>
>

10(2)(e) > Van: [Redacted]
> [Redacted]@minbzk. [Redacted]@minbzk.nl>>
> Datum: dinsdag 20 jul. 2021 4:13 PM

10(2)(e) > Aan: NCSC Bestuurlijke Ondersteuning
> [Redacted]@ncsc. [Redacted]
> [Redacted]@ncsc.nl>>

10(2)(e) > Kopie: [Redacted]
> [Redacted]@minocw. [Redacted]@minocw.nl>>, [Redacted]

10(2)(e) > [Redacted]@minbzk.n [Redacted]@minbzk.nl>>

> Onderwerp: NSO en Pegasus

>
> Goedemiddag,

>
> Er gaan nogal wat artikelen over Pegasus en NSO. Waaronder 50.000
> mensen die gemonitord zouden worden en zero-day, zero click
> kwetsbaarheden op IOS. Ik heb ook het idee dat nog veel onduidelijk
> is, zoals uit dit artikel blijkt:
> <https://www.calcalistech.com/ctech/articles/0,7340,L-3912882,00.html>

>
> Hebben jullie al een beter onderscheid tussen feit en fictie en al
> iets van duiding en advies?

10(2)(e) > [Redacted]
> Adviseur Informatiebeveiliging en privacy

>
> Directie CIO Rijk
> Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Turfmarkt 147
10(2)(e) > | 2511 DP | Den Haag | Postbus 20011 | 2500 EA | Den Haag

>

10(2)(e) > E [Redacted]@minbzk.nl

> T 06 [Redacted]

>
>

10(2)(e)

10(2)(g)

Van: @minbzk.nl>
Verzonden: woensdag 28 juli 2021 15:29
Aan:
Onderwerp: Informatie - Duiding Pegasus - 28 juli 2020
Bijlagen: Pegasus Feiten en Duiding KA 23-7.pdf

Dit bericht is verzonden aan de departementale CIO's, departementale CISO's en CISO's Hoge Colleges van Staat

Beste collega's

In de bijlage treft u, naar aanleiding van de berichtgeving over de Pegasus spionagesoftware in de media, de meest recente duiding van de NCTV aan.

Daarnaast kunt u gebruik maken van de handreikingen van de NCSC en de AIVD voor de beveiliging van mobiele apparaten.

Met vriendelijke groet,

10(2)(e)

10(2)(e)

CIO Rijk

Directoraat-generaal Overheidsorganisatie
 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
 Turfmarkt 147 | 2511 DP | Den Haag
 Postbus 20011 | 2500 EA | Den Haag
<http://www.rijksoverheid.nl>

10(2)(e) T +31 (0)70

10(2)(e) M +31 (0)61

10(2)(e) [redacted]@minbzk.nl

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

10(2)(e)

BD/NCSC/Staf

buiten scope

-----Original Message-----

From: Info (NCSC-NL) <info@ncsc.nl>

Sent: maandag 2 augustus 2021 15:23

10(2)(e) To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

Subject: FW: Duiding Pegasus vanuit CIO Rijk

-----Original Message-----

From: [redacted] BD/DII/ICS [redacted]@minjenv.nl>

Sent: maandag 2 augustus 2021 15:04

10(2)(e) To: [redacted]@rijksoverheid.nl>; Info (NCSC-NL) <info@ncsc.nl>

Cc: [redacted] BD/DGM/DRM/KV [redacted]@minjenv.nl>; [redacted]

[redacted]@minbzk.nl>

Subject: RE: Duiding Pegasus vanuit CIO Rijk

10(2)(e)@ [redacted], Dank voor de respons.

@NCSC: kunnen jullie meer duiding geven m.b.t. de vragen over de factsheet? Alvast dank!

- De factsheet 'veilig gebruik van smartphones' is uit 2014. Gezien de snelheid waarmee de techniek verandert geeft dat niet het gevoel dat dit een passend advies is.
- Bovendien mis ik in de factsheet een specifiek handelingsperspectief t.a.v. de Pegasus casus.

Met vriendelijke groet,

10(2)(e) [redacted]

.....
 Ministerie van Justitie en Veiligheid
 Minister van Justitie en Veiligheid
 DI&I
 Turfmarkt 147 | 2511 DP | Den Haag
 Postbus 20301 | 2500 EH | Den Haag

T 06 [redacted]

10(2)(e) [redacted]@minjenv.nl [redacted]@minjenv.nl> www.rijksoverheid.nl/jenv <<http://www.rijksoverheid.nl/jenv>>

Voor een rechtvaardige en veilige samenleving

10(2)(e) Van: [redacted]@rijksoverheid.nl>

Verzonden: maandag 2 augustus 2021 14:59

10(2)(e) Aan: [redacted] BD/DII/ICS [redacted]@minjenv.nl>

CC: [redacted] BD/DGM/DRM/KV [redacted]@minjenv.nl>; [redacted]
[redacted]@minbzk.nl>

Onderwerp: RE: Duiding Pegasus vanuit CIO Rijk

10(2)(e) Hoi [redacted],

Ik heb een aantal collega's gesproken.

Zij gaven aan dat je het best even contact kunt zoeken met het NCTV/NCSC, de opsteller van de factsheet (zie onder aan de factsheet + hieronder).

@ncsc.nl <mailto: [redacted]@ncsc.nl>

T 070 -

Publicatienr:

Ter aanvulling ontving ik nog:

- Gebruik gewone mobiele devices niet voor vertrouwelijk (alleen BIO/BBN1), ze bieden geen effectieve weerstand tegen statelijke actoren; gebruik in plaats daarvan geëvalueerde producten.
- Als je toch mobieltjes wilt blijven gebruiken, dan geeft de factsheet aanvullend advies dat er vooral op gericht is het maximaliseren van de eigen controle en het verkleinen van het aanvalsoppervlak en de window of opportunity voor kwaadwillenden.
- De zwakte van dergelijke producten (smartphones, tablet, citrix, webex, etc) is genoegzaam bekend, de overheid past risicomangement toe met acceptatie van restrisiko's voor haar eigen processen.

10(2)(g) [redacted]

- In samenhang daarmee: hieronder wordt de vraag gesteld: "Hoe kan gecontroleerd worden of een telefoon besmet is?"
- Er valt wellicht te controleren of door Pegasus een telefoon 'besmet' is, andere vormen van 'besmetting' zijn echter ook mogelijk.
- Wat dat betreft is Pegasus gewoon een enkel voorbeeld voor wat in deze schaduwmarkt (en in de op criminaliteit gerichte markt) bij voortduring wordt aangeboden.

Met vriendelijke groet,

10(2)(e) [redacted]

10(2)(e) Van: [redacted]@minjenv.nl [redacted]@minjenv.nl> >

Verzonden: maandag 2 augustus 2021 11:26

Aan: [redacted]@rijksoverheid.nl [redacted]@rijksoverheid.nl> >

10(2)(e) CC: [redacted] BD/DGM/DRM/KV [redacted]@minjenv.nl

[redacted]@minjenv.nl> >; [redacted]@minbzk.nl
[redacted]@minbzk.nl> >

Onderwerp: RE: Duiding Pegasus vanuit CIO Rijk

10(2)(e) Dag []

10(2)(e) De out-of-office van [] stuurt me door naar jou.

N.a.v. de duiding van Pegasus die vorige week is verstuurd, heb ik onderstaande vragen binnengekregen. Kun je die (laten) beantwoorden?

10(2)(e) Alvast hartelijk dank, ook namens []

- Wat is de methode die gebruikt wordt om de spyware op een telefoon te krijgen?
- Hoe kan gecontroleerd worden of een telefoon besmet is?
- De factsheet 'veilig gebruik van smartphones' is uit 2014. Gezien de snelheid waarmee de techniek verandert geeft dat niet het gevoel dat dit een passend advies is.
- Bovendien mis ik in de factsheet een specifiek handelingsperspectief t.a.v. de Pegasus casus.

Met vriendelijke groet,

10(2)(e)

[]

.....
Ministerie van Justitie en Veiligheid
Minister van Justitie en Veiligheid
DI&I
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

T 06 - []

10(2)(e) []@minjenv.nl []@minjenv.nl > www.rijksoverheid.nl/jenv <<http://www.rijksoverheid.nl/jenv>>
.....
Voor een rechtvaardige en veilige samenleving

10(2)(e) Van: [] BD/DII/ICS

Verzonden: maandag 2 augustus 2021 10:58

10(2)(e) Aan: []@minbzk.nl []@minbzk.nl >

CC: [] BD/DGM/DRM/KV []@minjenv.nl

10(2)(e) []@minjenv.nl >

Onderwerp: RE: Duiding Pegasus vanuit CIO Rijk

Dag []

10(2)(e)

N.a.v. de duiding van Pegasus die je vorige week doorstuurde, heb ik onderstaande vragen binnengekregen. Kun

10(2)(e) je die (laten) beantwoorden? Alvast dank, ook namens []

Met vriendelijke groet,

10(2)(e) [redacted]

.....
Ministerie van Justitie en Veiligheid
Minister van Justitie en Veiligheid
DI&I
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

10(2)(e) 06 - [redacted]

10(2)(e) [redacted]@minjenv.nl [redacted]@minjenv.nl> www.rijksoverheid.nl/jenv <<http://www.rijksoverheid.nl/jenv>>

Voor een rechtvaardige en veilige samenleving

10(2)(e) Van: [redacted] BD/DGM/DRM/KV [redacted]@minjenv.nl

[redacted]@minjenv.nl> >

Verzonden: vrijdag 30 juli 2021 09:48

10(2)(e) Aan: [redacted] BD/DII/ICS [redacted]@minjenv.nl [redacted]@minjenv.nl> >; [redacted]

BD/DII/ICS [redacted]@minjenv.nl [redacted]@minjenv.nl> >

CC: [redacted] BD/DGM/DRM/KV [redacted]@minjenv.nl [redacted]@minjenv.nl> >

Onderwerp: RE: Duiding Pegasus vanuit CIO Rijk

10(2)(e) Hallo [redacted] en [redacted],

Goed dat de NCTV deze informatie deelt.

Het roept bij mij wel een aantal vragen op:

- Wat is de methode die gebruikt wordt om de spyware op een telefoon te krijgen?
- Hoe kan gecontroleerd worden of een telefoon besmet is?
- De factsheet 'veilig gebruik van smartphones' is uit 2014. Gezien de snelheid waarmee de techniek verandert geeft dat niet het gevoel dat dit een passend advies is.
- Bovendien mis ik in de factsheet een specifiek handelingsperspectief t.a.v. de Pegasus casus.

10(2)(e)

Groeten, [redacted]

10(2)(e)

Van: [redacted] BD/DII/ICS [redacted]@minjenv.nl [redacted]@minjenv.nl> >

Verzonden: donderdag 29 juli 2021 18:12

Onderwerp: FW: Duiding Pegasus vanuit CIO Rijk

10(2)(e) Namens [redacted] mail ik jullie het volgende:

Beste mensen,

Op 19 juli kwam de Pegasus-spionagesoftware wereldwijd in het nieuws. CIO Rijk heeft daarbij de bijgevoegde duiding gegeven (departementaal vertrouwelijk). Graag willen we je hierop attenderen. Eventuele vragen n.a.v. deze mail zullen we bundelen en doorzetten naar CIO Rijk ter beantwoording.

Met vriendelijke groet,

10(2)(e) [redacted]

.....
Ministerie van Justitie en Veiligheid
Minister van Justitie en Veiligheid
DI&I
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20301 | 2500 EH | Den Haag
.....

10(2)(e)T 06 - [redacted]

10(2)(e) [redacted]@minjenv.nl [redacted]@minjenv.nl> www.rijksoverheid.nl/jenv <<http://www.rijksoverheid.nl/jenv>>

.....
Voor een rechtvaardige en veilige samenleving

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

$$10(2)(g)$$

Periode: maandag 19-07-2021 – dinsdag 20-07-2021

10(2)(g)

10(2)(e)

buiten scope

buiten scope

* Pegasus

De recente berichtgeving over de Pegasus spyware heeft tot vragen geleid uit onze doelgroepen. Op dit moment krijgt het de nodige aandacht en houden diverse teams de situatie in de gaten.

buiten scope

– Apple Has ‘Major’ iMessage Security Problems, Says Pegasus Spyware Expert

Apple has faith in its iMessage security, despite claims that Israeli spyware agency NSO Group’s tool has repeatedly cracked iPhone security using iOS’ own messaging system. Critics say Apple needs to copy what Facebook and Twitter do with message security.

<https://www.forbes.com/sites/thomasbrewster/2021/07/19/>

/pegasus-spyware-does-apple-have-major-imessage-security-problems/

buiten scope

[Redacted text block]

[Redacted text block]

[Redacted text block]

=====
= TLP:AMBER =
=====

buiten scope

[Redacted text block]

[Redacted text block]

[Redacted text block]

buiten scope

[Redacted text block]

10(2)(g)

Van:

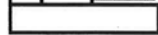
 (NCSC-NL)

Aan:

 ncsc.nl

10(2)(g)

Onderwerp:

 - Tuesday 20-07-2021  - Wednesday 21-07-2021 

--- TLP:AMBER NCSC ONLY / Departementaal Vertrouwelijk / Intern ---
[\(https://first.org/tlp/\)](https://first.org/tlp/)

10(2)(g)





Periode: dinsdag 20-07-2021  - woensdag 21-07-2021 

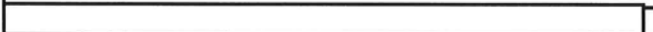
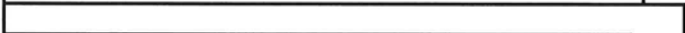
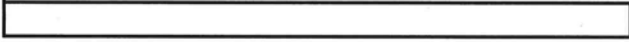
10(2)(g)

 (NCSC-NL)

10(2)(e)

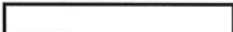
 (NCSC-NL) (NCSC-NL) 

buiten scope








buiten scope










* Pegasus

Diverse teams houden de situatie in de gaten en werken aan het verkrijgen van meer informatie. Er zijn verder geen ontwikkelingen te delen op dit moment.

buiten scope














buiten scope

[REDACTED]

=====
= TLP:AMBER =
=====

buiten scope

[REDACTED]

– Dit is de NSO Group, die ook jouw telefoon kan hacken
Dat er bedrijven zijn die spionagesoftware verkopen, ook aan dubieuze regimes, dat wist onderzoeker Sico van der Meer van instituut Clingendael wel. Toch verbaast hem de omvang waarmee de Pegasus-software van het Israëlische bedrijf NSO Group is gebruikt om journalisten, politici en activisten te volgen.
<https://nos.nl/l/2390114>

[REDACTED]

buiten scope

[REDACTED]

buiten scope

[REDACTED]

10(2)(g)

Van:

□ (NCSC-NL)

Aan:

□ ncsc.nl

10(2)(g)

Onderwerp:

□ - Wednesday 21-07-2021 □ - Thursday 22-07-2021 □

--- TLP:AMBER NCSC ONLY / Departementaal Vertrouwelijk / Intern ---
(<https://first.org/tlp/>)

10(2)(g)

□
□
□

10(2)(g)

Periode: woensdag 21-07-2021 □ – donderdag 22-07-2021 □
□ (NCSC-NL)

10(2)(e)

□ (NCSC-NL)
□ (NCSC-NL)

Beste collega's,

□
□
□

buiten scope

□
□
□

□
□

□
□

□
□
□
□
□
□
□
□
□

buiten scope

□
□
□
□
□
□

□
□
□
□
□
□
□
□



buiten scope

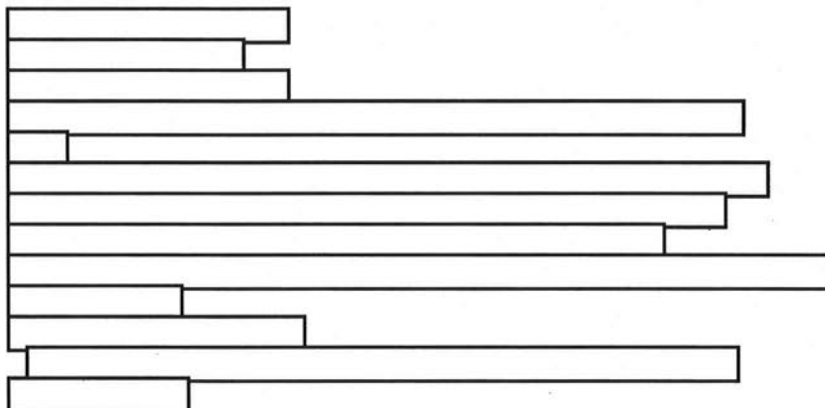


=====

= TLP:AMBER =

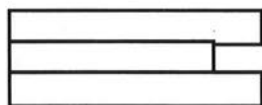
=====

buiten scope

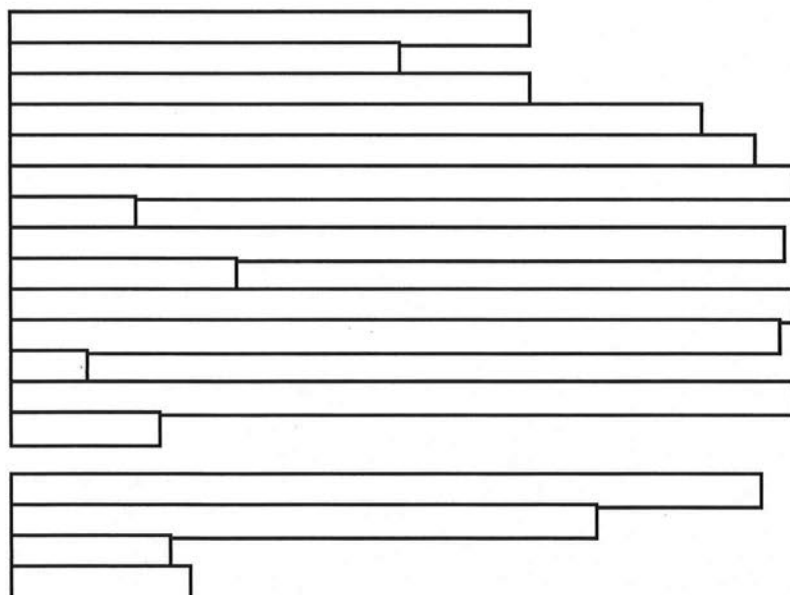


– Pegasus spyware seller: Blame our customers not us for hacking
NSO Group tells BBC News: "The finger-pointing should be at the
customer."

<https://www.bbc.co.uk/news/technology-57922664>



buiten scope



10(2)(g)
10(2)(g)

Van: [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: [redacted] 23-07-2021

-----BEGIN PGP SIGNED MESSAGE-----

[redacted]

- - - TLP:GREEN - - -

(<https://first.org/tlp/>)

Beste NCSC-partner,

10(2)(g)

Hierbij de [redacted] van week 29 in 2021.

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

buiten scope

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

buiten scope

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

* Pegasus spionagesoftware

Het zal veel van onze lezers waarschijnlijk niet zijn ontgaan dat er in internationale media geschreven wordt over spionagesoftware van NSO group. Forbidden Stories en Amnesty International hebben door middel van zelfstandig onderzoek een lijst samengesteld met daarin telefoonnummers van 50.000 mogelijke slachtoffers van hacks met de

spionagesoftware. Amnesty International heeft tevens IOC's beschikbaar gesteld die men kan gebruiken voor het detecteren van compromittatie van een telefoon [8]. Wij verwijzen u verder naar onze beveiligingsrichtlijnen voor beheerders en gebruikers van mobiele apparaten [9].

Verstuurde beveiligingsadviezen

=====

NCSC-2020-1012 [v1.10][M/M] Kwetsbaarheden verholpen in cURL

NCSC-2021-0259 [v1.06][H/H] Kwetsbaarheden verholpen in OpenSSL

NCSC-2021-0592 [v1.01][H/H] Kwetsbaarheden verholpen in Kaseya Virtual System Administrator (VSA)

NCSC-2021-0596 [v1.02][M/H] Kwetsbaarheden verholpen in Node.js

NCSC-2021-0617 [v1.01][M/H] Kwetsbaarheden verholpen in QEMU

NCSC-2021-0621 [v1.00][M/H] Kwetsbaarheid aangetroffen in Microsoft Printer Spooler service

NCSC-2021-0622 [v1.00][M/H] Kwetsbaarheden verholpen in Icinga Web

NCSC-2021-0623 [v1.00][M/H] Kwetsbaarheid verholpen in Cisco ASA

NCSC-2021-0624 [v1.00][H/M] Kwetsbaarheden verholpen in Google Chrome

NCSC-2021-0625 [v1.00][M/H] Kwetsbaarheden verholpen in IBM Tivoli Monitoring

NCSC-2021-0626 [v1.00][M/H] Kwetsbaarheden verholpen in Citrix ADC, Gateway en SDWAN WAN-OP

NCSC-2021-0627 [v1.00][M/H] Kwetsbaarheid verholpen in Juniper Junos OS

NCSC-2021-0628 [v1.00][M/H] Kwetsbaarheden verholpen in de Lexmark Universal Printer Driver

NCSC-2021-0629 [v1.00][M/H] Kwetsbaarheid verholpen in FortiNet producten

NCSC-2021-0630 [v1.00][M/H] Kwetsbaarheden verholpen in Typo3

NCSC-2021-0631 [v1.00][M/H] Kwetsbaarheden verholpen in Aruba AOS-CX switches

NCSC-2021-0632 [v1.00][M/H] Kwetsbaarheid ontdekt in Microsoft Windows

NCSC-2021-0633 [v1.00][M/H] Kwetsbaarheid verholpen in Linux kernel

NCSC-2021-0633 [v1.01][M/H] Kwetsbaarheid verholpen in Linux kernel

NCSC-2021-0634 [v1.00][M/M] Kwetsbaarheden verholpen in Google Chrome

NCSC-2021-0635 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Virtualization-producten

NCSC-2021-0636 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Peoplesoft-producten

NCSC-2021-0637 [v1.00][M/M] Kwetsbaarheden verholpen in Atlassian Jira

NCSC-2021-0638 [v1.00][M/H] Kwetsbaarheid verholpen in Elasticsearch

NCSC-2021-0639 [v1.00][M/M] Kwetsbaarheden verholpen in Adobe Photoshop

NCSC-2021-0640 [v1.00][M/M] Kwetsbaarheid verholpen in Adobe Premiere Pro

NCSC-2021-0641 [v1.00][M/M] Kwetsbaarheden verholpen in Adobe After Effects

NCSC-2021-0642 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle JD Edwards

NCSC-2021-0643 [v1.00][M/M] Kwetsbaarheden verholpen in Adobe Media Encoder

NCSC-2021-0644 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle MySQL

NCSC-2021-0645 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Siebel Suite

NCSC-2021-0646 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Supply Chain Products Suite

NCSC-2021-0647 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Java SE en GraalVM

NCSC-2021-0648 [v1.00][M/H] Kwetsbaarheden verholpen in Oracle Fusion Middleware producten

NCSC-2021-0649 [v1.00][M/H] Kwetsbaarheden verholpen in Apple Mac OS

NCSC-2021-0650 [v1.00][M/H] Kwetsbaarheden verholpen in Apple iOS en

iPadOS

buiten scope

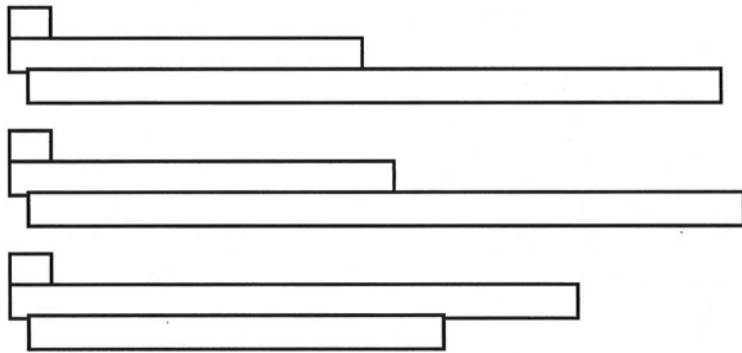
buiten scope

buiten scope

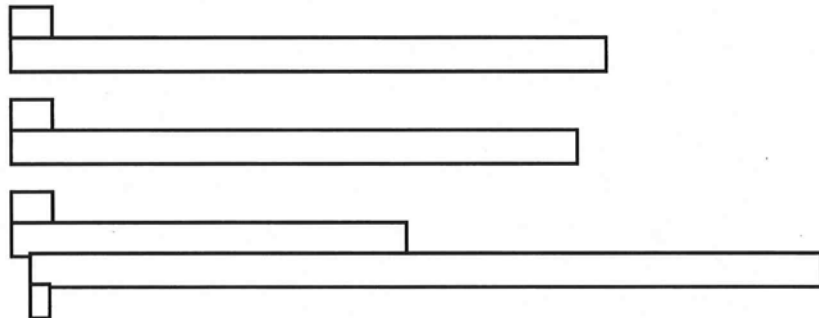


[8]
https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso

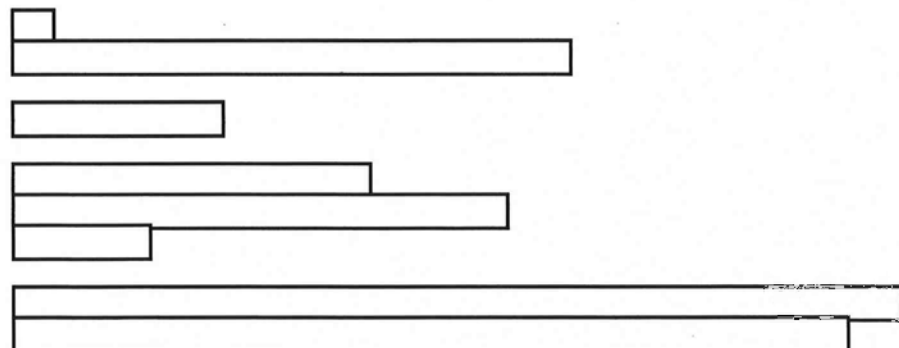
[9]
<https://www.nesc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten>



buiten scope



buiten scope



10(2)(e)

10(2)(g)

Van:**Aan:****Onderwerp:**

[REDACTED]

[REDACTED]@cymru.com

[DNB] [MALWARE] Technical Analysis of the Pegasus Spyware (PDF)

Title: Technical Analysis of the Pegasus Spyware (PDF)

Source: Lookout.com

Date Published: 25 August 2016

Excerpt:

"This report is an in-depth technical look at a targeted espionage attack being actively leveraged against an undetermined number of mobile users around the world. Lookout researchers have done deep analysis on a live iOS sample of the malware, detailed in this report.

Citizen Lab's investigation links the software and infrastructure to that of NSO Group which offers a product called Pegasus solution. Pegasus is professionally developed and highly advanced in its use of zero-day vulnerabilities, code obfuscation, and encryption. It uses sophisticated function hooking to subvert OS- and application-layer security in voice/audio calls and apps including Gmail, Facebook, WhatsApp, Facetime, Viber, WeChat, Telegram, Apple's built-in messaging and email apps, and others.

It steals the victim's contact list and GPS location, as well as personal, Wi-Fi, and router passwords stored on the device. The iOS version of the attack uses what we refer to as Trident, an exploit of three related zero-day vulnerabilities in iOS, which Apple patched in iOS 9.3.5, available as of the publishing of this report."

To read the complete article see:

<<https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegasus-technical-analysis.pdf>>

----- next part -----

A non-text attachment was scrubbed...

Name: signature.asc

Type: application/pgp-signature

Size: 204 bytes

Desc: OpenPGP digital signature

URL:

<https://lists.cymru.com/mailman/private/dragon_newsbytes/attachments/20160826/236ddaac/attachment.sig>

<https://www.team-cymru.org/News/dnb.html>

buiten
scope

[REDACTED]

[REDACTED]

[REDACTED]

2.28 Israeli Pegasus spyware allegedly used to hack phones of dozens of Al Jazeera journalists in large-scale attack - report

The personal phones of some 36 Al Jazeera journalists have been hacked by “government operatives” who used a controversial spying tool by Israel’s infamous NSO Group to snoop on them, a report by a Canadian research lab claims. Read Full Article at RT.com

https://www.rt.com/news/510275-pegasus-spyware-aljazeera-hack/?utm_source=rss&utm_medium=rss&utm_campaign=RSS

buiten
scope

[REDACTED]

[REDACTED]



2021-07-20 NSO Group Pegasus spyware

Title	NSO Group Pegasus spyware
TLP	TLP:AMBER
Date	20 Jul 2021
CTI-Specialist	[redacted] (NCSC-NL)
[redacted]	
Version	1.0
Status	CONCEPT
Recipient(s)	

10(2)(e)

10(2)(g)

Summary

Onderzoekers hebben de infrastructuur van Pegasus spyware bekend gemaakt. Deze spyware is ontwikkeld door NSO group en wordt oa gebruikt voor het af luisteren van journalisten. [redacted]

10(2)(g)

Analysis

De infrastructuur is publiek gemaakt door Amnesty International Security Lab middels een Github repo. De repo bevat zowel nieuwe als oude domeinen. Het Fusion Centre van het NCSC verzameld de berichtgeving omtrent dit onderwerp [redacted]

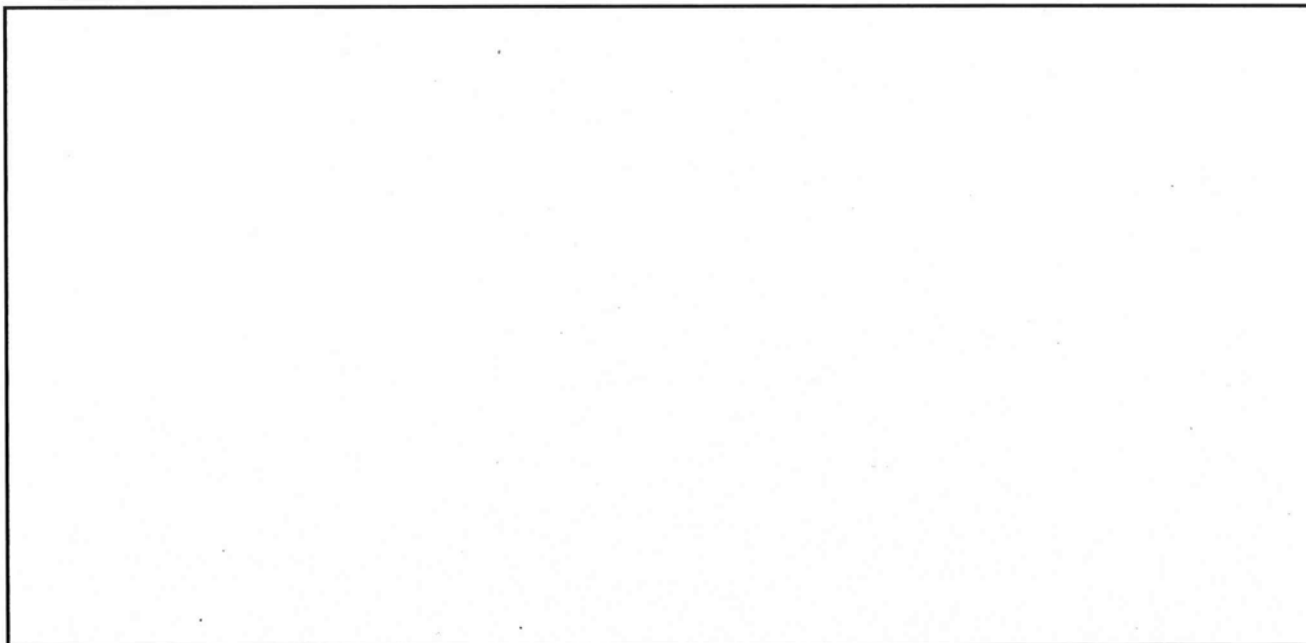
10(2)(g)

Wbni

10(2)(g)

[redacted]

Wbni



10(2)(e) **Van:** [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: FW: situatieschets technische analyse NSO Pegasus malware

10(2)(e) Ter info, [redacted] hielp me even uit de brand toen ik wat weinig tijd had.
 Eerste contact is dus gelegd.

Vriendelijke groet,

10(2)(e) [redacted]

Ask-van-vandaag

10(2)(e) **From:** [redacted] (NCSC-NL)

Sent: dinsdag 20 juli 2021 16:25

10(2)(g) **To:** [redacted]@nctv.minjenv.nl

10(2)(e) **Cc:** [redacted] (NCSC-NL) ; [redacted] (NCSC-NL)

Subject: situatieschets technische analyse NSO Pegasus malware

Beste collega's van bewaken en beveiligen,

Graag geven wij jullie even een korte situatieschets van de NCSC inspanningen rond de Pegasus spyware van NSO. De berichtgeving hierover heeft tot vragen geleid uit onze doelgroepen. Op dit moment krijgt het de nodige aandacht en houden diverse teams binnen het NCSC de situatie in de gaten.

10(2)(g) Amnesty International heeft een aantal indicators of compromise die duiden op een Pegasus besmetting op GitHub geplaatst. De indicatoren om de Pegasus spyware op netwerk niveau te kunnen detecteren is uitgezet binnen het nationaal detectie netwerk (NDN). Hierop is een analyse gedaan binnen alle sensoren bij Rijksoverheid. Hierbij zijn geen netwerksessies gevonden die matchen met het netwerkverkeer van de Pegasus spyware. [redacted]

Wbni [redacted]

[redacted] Dit matcht niet met het verkeer dat je verwacht van de Pegasus spyware. In gewone mensentaal: het is ruis en geen indicator [redacted]

Wbni [redacted]
 Momenteel hebben we nog een vraag uitstaan bij de Telecom ISAC (samenwerkingsverband voor het uitwisselen van dreigingsinformatie tussen partijen in de sector telecom). Mocht daar nog iets uit komen dan zullen we dat zeker delen.

Met vriendelijke groet,

10(2)(e) [redacted]

Van: NCC - NCTV
Aan: [redacted] BD/NCC/ECR; NCC - NCTV; [redacted] BD/PBB; [redacted] BD/PNDV; [redacted]
 [redacted] BD/PNDV; [redacted] BD/KS; [redacted] BD/KA; [redacted] BD/KA;
 [redacted] BD/NCC/ECO; [redacted] BD/NCSC/Stat; [redacted] BD/NCSC/OP; [redacted]
 [redacted] BD/NCC/ECO
Onderwerp: Situationeel beeld Pegasus (NCSC)
Datum: woensdag 21 juli 2021 17:12:53
Bijlagen: TFC-SituationeelbeeldPegasusspyware-210721-1707-163.pdf

Geachte heer/mevrouw,

Zie onderstaande en de bijlage.

Met vriendelijke groet,

Nationaal CrisisCentrum (NCC)

E [redacted]@nctv.minjenv.nl
 T +31 (0)70 [redacted] (algemeen nummer)
 T +31 (0)70 [redacted] (incident nummer)
 F +31 (0)70 [redacted]

-----Oorspronkelijk bericht-----

10(2)(e) Van: [redacted] (NCSC-NL) [redacted]@ncsc.nl>
 Verzonden: woensdag 21 juli 2021 17:08
 10(2)(g) Aan: NCC - NCTV [redacted]@nctv.minjenv.nl>
 Onderwerp: Situationeel beeld Pegasus (NCSC)

Ha collega's,

Zoals afgesproken in de bijlage onze input voor het beeld.

Met vriendelijke groet,

10(2)(e) [redacted]
 Duidingsspecialist

.....
 Nationaal Cyber Security Centrum
 10(2)(e) Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
 [redacted]@ncsc.nl

T +31 070 [redacted] (algemeen)
 10(2)(g) M +31 06 [redacted] (mobiel)

.....
 Bezoekadres:
 Turfmarkt 147 | 2511 DP | Den Haag

Situationeel beeld Pegasus spyware

Bronnen:

- What is Pegasus spyware and how does it hack phones?
- 'Spyware Israëlisch bedrijf ingezet om wereldwijd journalisten te bespioneren'
- Forensic Methodology Report: How to catch NSO Group's Pegasus

Secundaire bronnen, nog niet beoordeeld:

- <https://www.businessinsider.com/nso-group-spyware-iphone-zero-click-icmessage-attacks-2021-7>
- <https://nos.nl/artikel/2389999-vragen-over-rol-israelische-overheid-na-onthulling-over-spijonesoftware>
- <https://securityaffairs.co/wordpress/120291/malware/pegasus-project-nso-pegasus-spywar.html>
- https://www.reddit.com/r/cybersecurity/comments/ong7l4/anybody_here_working_on_the_pegasus_spyware_or/
- <https://www.computerworld.com/article/3625871/iphone-spyware-its-a-dirty-job-but-nso-gonna-do-it.html>
- <https://www.securityweek.com/pegasus-scandal-shows-risk-israels-spy-tech-diplomacy-experts>
- <https://www.theverge.com/2021/7/19/22583523/amazon-web-services-bans-nso-group-pegasus-spyware-infrastructure>
- <https://www.zdnet.com/article/nso-groups-pegasus-spyware-used-against-journalists-political-activists-worldwide-report/>
- <https://www.theguardian.com/news/2021/jul/19/nso-clients-spying-disclosures-prompt-political-rows-across-world>
- <https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china>
- <https://thehackernews.com/2021/07/us-and-global-allies-accuse-china-of.html>
- <https://www.volkskrant.nl/nieuws-achtergrond/indringend-en-gevaarlijk-spijonesoftware-uit-israel-bedreigt-de-democratie-ook-de-nederlandse-bc886331/>
- <https://www.forbes.com/sites/thomasbrewster/2021/07/19/pegasus-spyware-does-apple-have-major-icmessage-security-problems/>
- <https://www.theguardian.com/news/2021/jul/19/nso-clients-spying-disclosures-prompt-political-rows-across-world>
- <https://www.securityweek.com/explainer-target-list-israeli-hack-hire-firm-widens>
- <https://www.trouw.nl/buitenland/regimes-bespioneren-journalisten-en-activisten-met-spyware-die-mobieltjes-overneemt-b3358b9e/>
- <https://www.security.nl/posting/712979/Amazon+Web+Services+schakelt+cloud+accounts+NSO+Group+uit?channel=rss>
- <https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations>
- <https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state>
- <https://nos.nl/artikel/2390074-frankrijk-opent-onderzoek-naar-gebruik-spijonesoftware-door-marokko>
- <https://www.bbc.com/news/technology-57910355>
- <https://www.govinfosecurity.com/spyware-zero-day-hits-show-apple-ecosystems-imperfections-a-17113>

Aanvullende bevindingen uit de Franse media

- Tussen de lijst van 50.000 telefoonnummers zouden de nummers van een staatshoofd zitten, alsmede twee Europese regeringsleiders, (600) politici in onder andere een voormalige Sovjetrepubliek en een Afrikaans land, "prinsen en prinsessen", (65) bedrijfsleiders, en aantal miljardairs, ambassadeurs en generaals. Tevens bevat de lijst ten minste 180 journalisten, meerdere advocaten en 65 mensenrechtenactivisten: « *Projet Pegasus* » : révélations sur un système mondial d'espionnage de téléphones (lemonde.fr) en Tensions diplomatiques autour du logiciel espion Pegasus (lefigaro.fr)
- De lijst zou zich dus niet direct richten op leden van terroristische of criminele organisaties, hoewel dit niet wordt uitgesloten: « *Projet Pegasus* » : comment la société israélienne NSO Group a révolutionné l'espionnage (lemonde.fr)
- Agnes Callamard, SG van *Amnesty International*, stelt dat het gaat om een twintigtal landen die de software gebruiken, in plaats van de eerdergenoemde elf: Tensions diplomatiques autour du logiciel espion Pegasus (lefigaro.fr). Volgens *Le Figaro* zou de NSO de software aan 55 landen verkocht hebben: Tout savoir sur Pegasus, ce logiciel dévoyé pour espionner journalistes et activistes (lefigaro.fr)
- In juni heeft de NSO voor het eerst een rapport gepubliceerd om de transparantie van het bedrijf te verbeteren. Hierin wordt aangegeven dat het de banden met een tiental klanten heeft verbroken naar aanleiding van mogelijk misbruik van de software en mogelijke mensenrechtenschendingen. In dit rapport wordt ook aangegeven dat de NSO niet verantwoordelijk is voor het gebruik van de technologie. Volgens *Le Figaro* kan dit aangeven dat ze op de hoogte waren van het lek/schandaal: Tensions diplomatiques autour du logiciel espion Pegasus (lefigaro.fr)
- In Frankrijk zijn ongeveer 1000 telefoonnummers getarget, met name vanuit de Marokkaanse overheid: Tout savoir sur Pegasus, ce logiciel dévoyé pour espionner journalistes et activistes (lefigaro.fr)
- Veiligheidsdiensten van Marokko zouden onder andere geprobeerd hebben Pegasus te gebruiken om toegang te krijgen tot de telefoon van de burgemeester van Ivry-sur-Seine (een banlieue in Parijs) naar aanleiding van een donatie van €5000,- aan een schoolproject in de Westelijke Sahara: *Projet Pegasus* : l'obsession du Sahara occidental pousse le Maroc à tenter d'espionner le maire d'Ivry-sur-Seine (lemonde.fr).
- Het Franse OM (parquet de Paris) start tevens een onderzoek naar aanleiding van mogelijke spionage van twee journalisten van Mediapart door de Marokkaanse geheime dienst: « *Projet Pegasus* » : comment la société israélienne NSO Group a révolutionné l'espionnage (lemonde.fr) en « *Projet Pegasus* » : Mediapart a été espionné par le Maroc - Page 1 | Mediapart

10(2)(g)

10(2)(e)

Van: [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: RE: Pegasus sample hashes
Bijlagen: image001.png

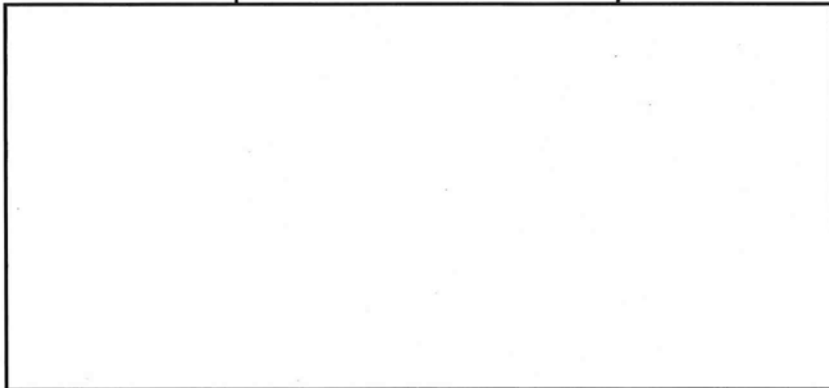
10(2)(e)

Hi [redacted]

10(2)(g)

Ik heb ze even in [redacted], daar komt dit naar boven:

10(2)(g)



10(2)(g)

Het event matched ook met wat hij hieronder in de mail zegt. Aangezien het vooral APKs zijn heeft het weinig zin de IOCs naar de sensoren te pushen. Wellicht iets voor [redacted]? Wil je die zelf doorsturen?

10(2)(g)

[redacted]

10(2)(e)

Gr, [redacted]

-----Original Message-----

10(2)(e)

From: [redacted]

Sent: donderdag 29 juli 2021 09:48

10(2)(g)

To: [redacted] (NCSC-NL)

Subject: Pegasus sample hashes

10(2)(g)

* PGP Signed by an unverified key: [redacted]

For what its worth, misschien waardevol als toevoeging op bestaand onderzoek. Hashes en context mogen verder intern gedeeld worden indien gewenst. Misschien meer iets voor [redacted].

10(2)(e)

Cheers,

[redacted]

//// Onderstaande mailwisseling geeft aan hoe de hashes zijn vergaard, dus niet bepaald bruikbaar zonder eigen verdieping maar de bron is zeer betrouwbaar, kan de bron alleen niet vrijgeven.

> I've got plenty of older NSO Pegasus samples through 2020, but nothing in 2021 (except for some ZIPs containing pre-2021 samples).

>

>

>

> If anyone can share any more recent samples (or at least hash) along with reason for confidence, would be appreciated.

>

>

>

> Thanks,

>

>

>

> S

////

> Same here! Would be interested in recent samples.

>

> Did anyone test <https://github.com/mvt-project/mvt> ?

>

> Just wondering if this would be a tool worth promoting or not for

10(2)(e) > techies doing IR> gr, Sent from my refrigerator

////

> Hey mate, here's ~2400 hashes I'm pretty sure are NSO based on some pivoting on APK attributes.

>

>

>

> Feel free to share without attribution – unless someone needs to discuss how we found them, in which case feel free to intro.

>

>

>

> Cheers,

>

>

>

> S

////

> sweet!

>

>

>

> so, how did you find them? :)

>

>

>

> Thx no matter what m8

10(2)(e) > Gr,

> Sent from my refrigerator

////

> I took a look at some samples on Twitter and found they matched to some samples we already had tagged as 2018 Chrysaor <https://android-developers.googleblog.com/2017/04/an-investigation-of-chrysaor-malware-on.html> ("Chrysaor" == Pegasus). So confident they are the real deal.

>

>

>

> Found a bunch of stuff to pivot off to find other samples. The most useful is the string "dujmehn" seen in APK defined service / package name. That string has no meaning outside of this malware... and we found ~2400 samples with it. All of them look suspicious enough themselves (some piggyback grayware/adware etc).

>
>
>

> Just nothing 2021 but just found one on VT

10(2)(g)

[redacted] gonna look at it
later.

--

#####

Sent from my refrigerator

#####

10(2)(e)
10(2)(g)

* [redacted] <[redacted]@[redacted].net>

* [redacted] - Unverified

10(2)(e)

Van: [redacted] (NCSC-NL)
 Aan: [redacted] (NCSC-NL)
 Cc: [redacted] (NCSC-NL)
 Onderwerp: RE: MO Pegasus
 Bijlagen: rev-gevli-2021-08-02 MO Pegasus v1.docx

Tnx, hierbij een review van mijn kant. Laat maar horen als je vragen hebt.

Mvg,

10(2)(e)

[redacted]

From: [redacted] (NCSC-NL)

Sent: dinsdag 3 augustus 2021 10:13

10(2)(e)

To: [redacted] (NCSC-NL)

Cc: [redacted] (NCSC-NL)

Subject: FW: MO Pegasus

Hi [redacted]

10(2)(e)

Zie bijlage! Ik zet [redacted] even in de CC voor het geval er aanpassingen nodig zijn.

10(2)(e)

Thanks,

[redacted]

Buiten scope

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10(2)(e)

Van: [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>

Verzonden: vrijdag 30 juli 2021 09:52

Aan: [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>;

[redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>;

[redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>;

[redacted]@betaalvereniging.nl>; [redacted] BD/NCC/ECO <[redacted]@nctv.minjenv.nl>; [redacted]

10(2)(e)

D [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/Staf <[redacted]@minjenv.nl>; [redacted]

BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK

[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted]@minbzk.nl'

[redacted]@minbzk.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK

[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] BD/NCSC/SK

10(2)(e)

[redacted]@minjenv.nl>; [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted]

[redacted]@nctv.minjenv.nl>; [redacted]@minezk.nl' [redacted]@minezk.nl>; [redacted] BD/NCSC/SK

[redacted]@minjenv.nl>

CC: [redacted] BD/KA <[redacted]@nctv.minjenv.nl>; [redacted] BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted]

[redacted] (NCSC-NL) <[redacted]@ncsc.nl>; [redacted] - BD/KA <[redacted]@nctv.minjenv.nl>; [redacted]

10(2)(e)

(NCSC-NL) <[redacted]@ncsc.nl>; [redacted]@ncsc.nl' [redacted]@ncsc.nl>; [redacted]

BD/NCSC/SK <[redacted]@minjenv.nl>; [redacted] (NCSC-NL) <[redacted]@ncsc.nl' [redacted]

[redacted]@ncsc.nl>; [redacted] BD/NCSC/OP <[redacted]@minjenv.nl>; [redacted]

(NCSC-NL)' [redacted]@ncsc.nl>; [redacted] NCSC-NL' [redacted]@ncsc.nl>

Onderwerp: RE: Trendanalyse sessie

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

buiten scope

Ministerie van Justitie en Veiligheid

Ministry of Justice and Security



NCSC Maandmonitor

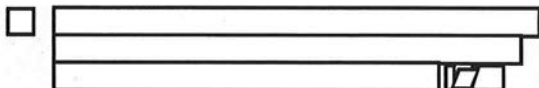
juli 2021

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand juli 2021. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar de bronnen [2] en commentaren van het NCSC opgenomen. Zie de "NCSC Maandmonitor Bijsluiter" voor meer uitleg over dit product en de verspreidingsvoorwaarden.

buiten
scope

buiten
scope

buiten
scope

buiten
scope

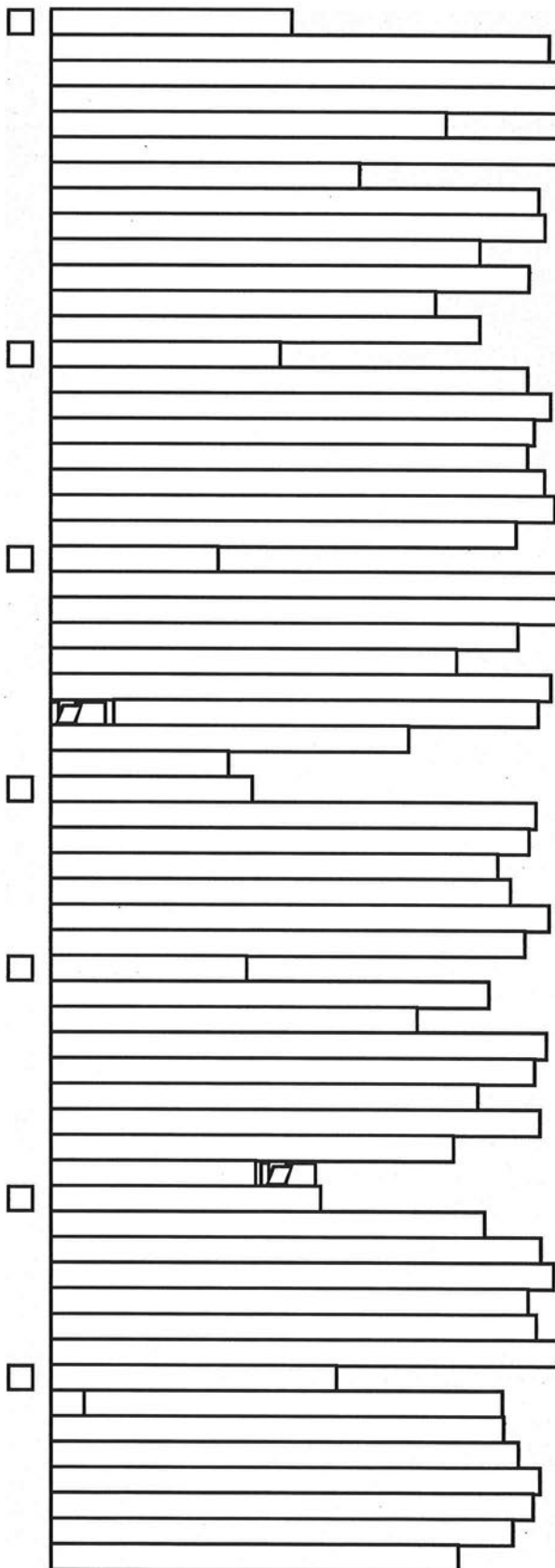
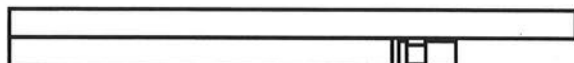
Pegasus-spyware toont dreiging mobiele malware

Op 18 juli publiceerde een consortium van 17 nieuwsorganisaties meerdere artikelen waarin wordt beschreven dat dissidenten, mensenrechtenadvocaten, activisten, journalisten en soms ook politici wereldwijd mogelijk doelwit zijn van spionagesoftware Pegasus. [~20] [~21] Met behulp van deze software, ontwikkeld door de Israëlische NSO Group, kan toegang verkregen worden tot allerlei data van besmette iPhone- en Android-telefoons, zonder dat het slachtoffer zelf enige actie onderneemt: een zogenaamde *zero-click-aanval*. Het consortium noemt een lijst van 50.000 telefoonnummers die mogelijk een doelwit vormen. Hier staan ook politici tussen, waaronder de Franse president Emmanuel Macron en voorzitter van de Europese Raad Charles Michel. De NSO Group zou mogelijk nauwe banden onderhouden met Israëlische veiligheidsdiensten. [~22] Israël heeft naar aanleiding van de onthullingen een taskforce opgezet om te onderzoeken of er beleidswijzigingen nodig zijn met betrekking tot de export van dergelijke software. [~23] [~24] De NSO Group zelf stelt de software enkel aan staten te verkopen ten behoeve van criminaliteits- en terrorismebestrijding.

Het NCSC heeft op dit moment geen aanwijzingen dat de lijst Nederlandse telefoonnummers bevat.

10(2)(g)

- Het is echter niet uit te sluiten dat er ook Nederlandse telefoons gecompromitteerd kunnen worden. Ook Nederland kent vergelijkbare doelwitten zoals bijvoorbeeld journalisten en politici. Besmettingen kunnen worden gedetecteerd door middel van forensisch onderzoek, waarvoor Amnesty International een tool heeft gepubliceerd. [~25]
- De laagdrempeligheid waarmee geavanceerde aanvalscapaciteiten te verwerven zijn is zorgwekkend, zoals ook aangegeven in het CSBN 2021. [~26] De Pegasus-spyware toont de dreiging voor mobiele telefoons. [~27]
- Het NCSC raadt het gebruik van telefoons voor vertrouwelijke gesprekken dan ook af. Gesprekken en berichten kunnen ook inzichtelijk zijn zonder dat de eigen telefoon geïnfecteerd is, bijvoorbeeld wanneer contact verloopt met een telefoon van een gesprekspartner die wel is gecompromitteerd.
- Zie ook de "Handreiking Cybersecuritymaatregelen" voor essentiële veiligheidsadviezen in het algemeen. [~28]

buiten
scopebuiten
scope

10(2)(e) **Van:** [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: RE: MaMo Pegasus

Prima, dank voor het aanpassen!

Groet,

10(2)(e)

[redacted]

10(2)(e) -----Original Message-----

From: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

Sent: donderdag 5 augustus 2021 20:14

10(2)(e) To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

Subject: RE: MaMo Pegasus

10(2)(e) Hi [redacted]

Ik heb je duiding stuk een beetje aangepast. Het volgende stukje heb ik verwijderd:

[redacted]

11(1)

[redacted]

[redacted]

Mocht je vragen hebben, dan hoor ik het graag! Morgen beperkt bereikbaar, want vrij.

10(2)(e) Groet,
[redacted]

10(2)(e) -----Original Message-----

From: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

10(2)(e) Sent: donderdag 5 augustus 2021 14:31

To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

Subject: MaMo Pegasus

10(2)(e) Hi [redacted]

10(2)(g) Bij dezen de laatste versie mbt Pegasus. [redacted]
[redacted] (maar dat weet ik niet zeker), vandaar dat ik deze heb gearceerd. De suggestie om deze toe te voegen komt van [redacted]

Ik hoor het wel mocht je nog vragen/opmerkingen hebben.

Groet,

Van: ToC (NCSC-NL)
Aan: [redacted] (NCSC-NL); [redacted] (NCSC-NL)
Onderwerp: FW: Misbruik van Pegasus spionage software van NSO

Heren,

Dit is naar de telecom-isac verstuurd

Met vriendelijke groet

From: [redacted] (NCSC-NL)

Sent: maandag 19 juli 2021 15:55

To: [redacted]

Subject: Misbruik van Pegasus spionage software van NSO

Beste Telecom-ISAC leden,

In een artikel van The Guardian van 18 juli [1] wordt een datalek beschreven van de firma NSO die spionage-software levert. Het lek maakt duidelijk dat er software gebruikt is, het artikel spreekt van Pegasus software, voor het bespioneren van een groot aantal mensenrechten activisten, journalisten en juristen. [redacted]

[redacted] [2]. [redacted]

[redacted] We denken dat de

Telecomsector het best is staat is om deze waar te nemen. Onze vraag aan jullie is nu dan ook of jullie misbruik waarnemen.

[1] <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>

[2] https://raw.githubusercontent.com/AmnestyTech/investigations/master/2021-07-18_nso/domains.txt

[3] [https://\[redacted\].ncsc.nl/events/view/8112](https://[redacted].ncsc.nl/events/view/8112)

Bij voorbaat dank voor het uitzoeken en de terugkoppeling,

Met groet,

[redacted]
NCSC-NL

10(2)(e) **Van:** [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: FW: [Telecom-isac] Misbruik van Pegasus spionage software van NSO
Bijlagen: image002.png

10(2)(e) Hi [redacted]
 10(2)(e) Volgens mij wilde [redacted] deze terugkoppeling delen met de DC/WeCo. Dus ik zet het even door
 10(2)(e) naar jou.
 10(2)(e) [redacted] en [redacted] kennen de achtergrond en details.
 10(2)(e) Groet, [redacted]
From: [redacted] (NCSC-NL)
 10(2)(e) **Sent:** dinsdag 20 juli 2021 12:16
To: [redacted] (NCSC-NL)
Subject: FW: [Telecom-isac] Misbruik van Pegasus spionage software van NSO
 Zoals besproken
 Met vriendelijke groet,

10(2)(e)

Nationaal Cyber Security Centrum
 Ministerie van Veiligheid en Justitie
 Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl
 Turfmarkt 147 | 2511 DP | Den Haag

10(2)(g) T 070 [redacted] (secretariaat) / 06 [redacted] (mobiel)
 E [redacted]@minjenv.nl

Mijn werkdagen zijn: maandag, dinsdag, donderdag en vrijdag.

10(2)(e) **From:** [redacted] (NCSC-NL) <[redacted]@ncsc.nl>
Sent: dinsdag 20 juli 2021 12:03
 10(2)(e) **To:** [redacted] (NCSC-NL) [redacted]@ncsc.nl>
Subject: FW: [Telecom-isac] Misbruik van Pegasus spionage software van NSO
 Zoals besproken.

10(2)(e) **From:** [redacted] <[redacted]@[redacted]>
 10(2)(g) **Sent:** dinsdag 20 juli 2021 11:58
 10(2)(e) **To:** [redacted] (NCSC-NL) [redacted]@ncsc.nl>
Subject: Re: [Telecom-isac] Misbruik van Pegasus spionage software van NSO

10(2)(e) Beste [redacted],
 Wij hebben je mail in goede orde ontvangen. Via deze mail wil ik je formeel informeren dat wij
 niet in kunnen gaan op je verzoek, omdat er ons inziens geen juridische grondslag is om deze
 informatie te verzamelen en over te dragen aan het NCSC.
 Met vriendelijke groet,

10(2)(e)

10(1)(c)

10(2)(e)
 Wbni

T: +31 6 [redacted]
 E: [redacted]@[redacted]



Wbni

[redacted]
[redacted]
[redacted]
Al

10(2)(e) +
10(2)(g)

From: [redacted] (NCSC-NL) via Telecom-isac <[redacted]@ncsc.nl>

Date: Monday, 19 July 2021 at 15:55

10(2)(g)

To: [redacted]@ncsc.nl [redacted]@ncsc.nl>

Subject: [Telecom-isac] Misbruik van Pegasus spionage software van NSO

Beste Telecom-ISAC leden,

In een artikel van The Guardian van 18 juli [1] wordt een datalek beschreven van de firma NSO die spionage-software levert. Het lek maakt duidelijk dat er software gebruikt is, het artikel spreekt van Pegasus software, voor het bespioneren van een groot aantal mensenrechten activisten, journalisten en juristen. Naar aanleiding van dit lek zijn er een groot aantal netwerk indicatoren in de vorm van domeinnamen publiek bekend geworden [2]. [redacted]

10(2)(g)

De indicatoren hebben vooral betrekking op mobiele apparatuur. We denken dat de Telecomsector het best is staat is om deze waar te nemen. Onze vraag aan jullie is nu dan ook of jullie misbruik waarnemen.

[1] [MailScanner has detected a possible fraud attempt from](#)

["eur01.safelinks.protection.outlook.com" claiming to be](#)

<https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>

[2] [MailScanner has detected a possible fraud attempt from](#)

["eur01.safelinks.protection.outlook.com" claiming to be](#)

https://raw.githubusercontent.com/AmnestyTech/investigations/master/2021-07-18_nso/domains.txt

[3] [MailScanner has detected a possible fraud attempt from](#)

["eur01.safelinks.protection.outlook.com" claiming to be](#)

10(2)(g)

[redacted]

Bij voorbaat dank voor het uitzoeken en de terugkoppeling,

Met groet,

10(2)(e)

[redacted]

NCSC-NL

10(2)(e) **Van:** [redacted] (NCSC-NL)
Wbni **Aan:** [redacted] (NCSC-NL); [redacted] (NCSC-NL)
Onderwerp: RE: Reactie [redacted]

10(2)(e) Thanks, [redacted] Ik reageer zo nog even inhoudelijk. Hier alvast de beloofde Github link:
https://github.com/AmnestyTech/investigations/tree/master/2021-07-18_nso

10(2)(e) mvg, [redacted]

From: [redacted] (NCSC-NL)

10(2)(e) **Sent:** dinsdag 20 juli 2021 2:58

To: [redacted] (NCSC-NL) ; [redacted] (NCSC-NL)

Wbni **Subject:** Reactie [redacted]

Goedemiddag,

Zie bijlage, ik maak nog een apart document met een paar standaard vragen en daar meer info bij.

10(2)(e) Vriendelijke groet,

[redacted]

.....
Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie
Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl

10(2)(e) T 070 [redacted] (algemeen)

10(2)(e) M 06- [redacted]
E [redacted]@ncsc.nl

.....
Bezoekadres:
Turfmarkt 147 | 2511 DP | Den Haag

10(2)(e) **Van:** [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
Onderwerp: RE: vraag mbt Pegasus software op mobiele apparaten

Top! En dank!

Ministerie van Justitie en Veiligheid | Ministry of Justice and Security
Nationaal Cyber Security Centrum | National Cyber Security Centre
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | P.O. Box 20011 | 2500 EA | Den Haag | The Netherlands

10(2)(e) T +31 6 [redacted]
M [redacted]@ncsc.nl

10(2)(g) [redacted]

10(2)(e) -----Original Message-----
From: [redacted] (NCSC-NL) [redacted]@ncsc.nl>
Sent: dinsdag 20 juli 2021 15:25
10(2)(e) To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>
Subject: FW: vraag mbt Pegasus software op mobiele apparaten

10(2)(e) Hey [redacted]

Voorgesteld antwoord, ben je akkoord?:

10(2)(e) [redacted]

[redacted]

[redacted]
[redacted]
[redacted]
11(1) [redacted]

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

10(2)(e) Vriendelijke groet,
[redacted]

10(2)(g) -----Original Message-----
From: [redacted] (NCSC-NL) [redacted]@ncsc.nl>
10(2)(e) Sent: dinsdag 20 juli 2021 14:12
To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>
Subject: FW: vraag mbt Pegasus software op mobiele apparaten

10(2)(e) -----Original Message-----
From: [redacted]
Sent: dinsdag 20 juli 2021 12:58
To: [redacted] (NCSC-NL) [redacted]@ncsc.nl>

10(2)(e)

Cc: [redacted]

Subject: vraag mbt Pegasus software op mobiele apparaten

Goedemiddag,

Wbni

Naar aanleiding van de nieuwsberichten met betrekking tot Pegasus software op mobiele devices is ook bij de [redacted] enige ongerustheid gerezen of wij een mogelijk doelwit zouden kunnen zijn, en of er manieren zijn om deze software te detecteren en/of te blokkeren.

Wij zijn benieuwd of er vanuit NCSC inmiddels adviezen zijn of komen met betrekking tot deze software. Zijn er indicators of compromise die wij zouden kunnen checken? Is er überhaupt reden tot bezorgdheid in dit stadium?

Met vriendelijke groet,

10(2)(e)

[redacted]

[redacted] | afdeling IT-Diensten

Wbni

[redacted]

[redacted]

10(2)(e)

Van: [redacted] BD/NCSC/Staf
Aan: NCSC Bestuurlijke Ondersteuning
Onderwerp: FW: Pegasus: bespreking follow-up
Datum: donderdag 22 juli 2021 17:18:28
Bijlagen: Pegasus Feiten en Duiding KA 21-7.pdf

Ter info

Van: [redacted] BD/PSD

Verzonden: donderdag 22 juli 2021 17:10

Aan: [redacted]; [redacted]@minbzk.nl'; [redacted]
 [redacted]@minbuza.nl'; [redacted] BD/PSD; [redacted]
 BD/PBB; [redacted] BD/PNDV; [redacted]@mindef.nl'; [redacted] BD/NCSC/Staf;
 [redacted] BD/NCSC/OP; [redacted]@minbzk.nl'; [redacted] BD/KA
CC: [redacted] BD/PSD; - BD/NCTV; [redacted] BD/PNDV;
 [redacted] BD/DCOM/WS&O

10(2)(e)

Onderwerp: RE: Pegasus: bespreking follow-up

Beste collega's,

Veel dank voor het nuttige overleg zojuist. We spraken de volgende actiepunten af:

10(2)(g)

1. NCTV [redacted]
 [redacted] CIO Rijk, [redacted]
2. AIVD/NCSC [redacted]
 [redacted]
3. AIVD/BZ [redacted]
4. NCTV [redacted] NatPol [redacted]
5. AIVD [redacted] MIVD

10(2)(e)

Aanspreekpunt bij de NCTV voor deze casus is vanaf nu [redacted]
 [redacted]@nctv.minjenv.nl), tel 06 [redacted]

Hoop voldoende duidelijk zo.

10(2)(e)

Met vriendelijke groet,

[redacted]

10(2)(e)

Van: [redacted] BD/PSD

Verzonden: woensdag 21 juli 2021 18:03

Aan: [redacted]@politie.nl>; [redacted]
 [redacted]@minbzk.nl) [redacted]@minbzk.nl>; [redacted]@mindef.nl'
 [redacted]@mindef.nl>; [redacted]@minbuza.nl)
 [redacted]@minbuza.nl>; [redacted]@minbuza.nl)
 [redacted]@minbuza.nl>; [redacted] BD/PSD
 [redacted]@nctv.minjenv.nl>; [redacted] BD/PBB
 [redacted]@nctv.minjenv.nl>; [redacted] BD/PNDV
 [redacted]@nctv.minjenv.nl>; [redacted] BD/PNDV [redacted]@nctv.minjenv.nl>
CC: [redacted] BD/PSD [redacted]@nctv.minjenv.nl>;
 BD/NCTV [redacted]@nctv.minjenv.nl>; [redacted] BD/PNDV
 [redacted]@nctv.minjenv.nl>

10(2)(e)

Onderwerp: Pegasus: bespreking follow-up

Urgentie: Hoog

Beste collega's,

De publiciteit rond de 'Pegasus-casus' [redacted] is voor de NCTV aanleiding op korte termijn bijeen te komen met de direct betrokken departementale partners, om wenselijke/haalbare opvolging te bezien. Na deze mail volgt een Outlook-verzoek voor **morgen (do 22 juli) om 15:30u**, bij de [redacted]. Hopelijk kan iedereen, ondanks deze last-minute aankondiging aanwezig zijn. Bij verhindering gelieve voor vervanging te zorgen.

Bij voorbaat dank en tot morgen.

Met vriendelijke groet,

[redacted]

10(2)(e)

10(2)(e)

.....
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 16950 | 2500 BZ | Den Haag
.....

10(2)(e)

T 070
M 06
.....
@nctv.minjenv.nl
.....

10(2)(e)

Van: [redacted] (NCSC-NL)
Aan: [redacted]
Onderwerp: Pegasus

10(2)(g)

-----BEGIN PGP SIGNED MESSAGE-----

10(2)(e)

[redacted]
Dear sir/madam,

My name is [redacted] and I work as an coordinator at the National Cyber Security Center in the Netherlands (NCSC-NL). In regards to the Amnesty and Guardian publications related to NSO and Pegasus spyware, we are trying to make an estimate on impact for the Netherlands and its citizens and have some questions you might be able to help us with. We noticed you have published some tooling in order to detect if a phone has been compromised. Would you be able to share some of the malware samples you might have found so we can perform our own tests and investigations? We are also wondering if you have any indication of compromised Dutch phones. Do you have a list of possible compromised phonenumbers that you would be willing and able to share with us?

Thanks allot for your help in advance!

Kind regards,

10(2)(e)

[redacted]

.....

.....

Ministerie van Justitie en Veiligheid | Ministry of Justice and Security
Nationaal Cyber Security Centrum | National Cyber Security Centre
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | P.O. Box 20011 | 2500 EA | Den Haag | The Netherlands

.....

10(2)(e)

.....
T +31 6 [redacted]
M [redacted]@ncsc.nl

10(2)(g)

[redacted]

-----BEGIN PGP SIGNATURE-----

10(2)(g)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10(2)(e)

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

-----END PGP SIGNATURE-----

10(2)(g)

10(2)(e)

10(2)(e)

10(2)(e)

$$10(2)(g)$$

10(2)(e)

-----END PGP SIGNATURE-----

10(2)(e) **Van:** [REDACTED] (NCSC-NL)
Aan: [REDACTED]
Onderwerp: Pegasus related questions

-----BEGIN PGP SIGNED MESSAGE-----

10(2)(g)

[REDACTED]

Dear [REDACTED],

10(2)(e)

My name is [REDACTED] and I work as an coordinator at the National Cyber Security Center in the Netherlands (NCSC-NL, part of the ministry of Justice and Security). I received your contact via [REDACTED] in the Netherlands. In regards to the Amnesty and Guardian publications related to NSO and Pegasus spyware, we are trying to make an estimate on impact for the Netherlands and its citizens and have some questions you hopefully might be able to help us with. We noticed you have published some tooling in order to detect if a phone has been compromised. Would you be able to share some of the malware samples you might have found during your research so we can perform our own tests and investigations?

10(2)(e)

We are also wondering if you have any indication of compromised Dutch phones. Or do you have a list of possible compromised Dutch phonenumbers that you

would be willing and able to share with us?

Thanks allot for your help in advance!

Kind regards,

10(2)(e)

[REDACTED]

.....
.....
Ministerie van Justitie en Veiligheid | Ministry of Justice and Security
Nationaal Cyber Security Centrum | National Cyber Security Centre
Turfmarkt 147 | 2511 DP | Den Haag
Postbus 20011 | P.O. Box 20011 | 2500 EA | Den Haag | The Netherlands
.....

10(2)(e)

T +31 6 [REDACTED]

M [REDACTED]@ncsc.nl

10(2)(g)

[REDACTED]

10(2)(g)

-----BEGIN PGP SIGNATURE-----

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10(2)(e)

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

-----END PGP SIGNATURE-----

Van: [redacted] BD/PSD
Aan: [redacted] @minbzk.nl"; [redacted] BD/PSD; [redacted] BD/PBB; [redacted] BD/PNDV; [redacted] @mindef [redacted] BD/NCSC/Stat; [redacted] BD/NCSC/OP; [redacted] @minbzk.nl; [redacted] BD/KA
Cc: [redacted] BD/PSD; [redacted] - BD/NCTV; [redacted] BD/PNDV; [redacted] BD/DCOM/WS&O
Onderwerp: RE: Pegasus: bespreking follow-up
Datum: donderdag 22 juli 2021 17:09:35
Bijlagen: Pegasus Feiten en Duiding KA 21-7.pdf

Beste collega's,

Veel dank voor het nuttige overleg zojuist. We spraken de volgende actiepunten af:

1. NCTV [redacted] CIO Rijk, [redacted]
2. AIVD/NCSC [redacted]
3. AIVD/BZ [redacted]
4. NCTV [redacted] NatPol [redacted]
5. AIVD [redacted] MIVD

Aanspreekpunt bij de NCTV voor deze casus is vanaf nu [redacted]

[redacted] @nctv.minjenv.nl), tel 06 [redacted]

Hoop voldoende duidelijk zo.

Met vriendelijke groet,

[redacted]

Van: [redacted] BD/PSD

Verzonden: woensdag 21 juli 2021 18:03

Aan: [redacted] @minbzk.nl);

[redacted] @mindef.nl"; [redacted] @minbuza.nl); [redacted] BD/PSD; [redacted]

BD/PBB; [redacted] BD/PNDV; [redacted] BD/PNDV

CC: [redacted] BD/PSD; [redacted] - BD/NCTV; [redacted] BD/PNDV

Onderwerp: Pegasus: bespreking follow-up

Urgentie: Hoog

Beste collega's,

De publiciteit rond de 'Pegasus-casus' [redacted] is voor de NCTV aanleiding op korte termijn bijeen te komen met de direct betrokken departementale partners, om wenselijke/haalbare opvolging te bezien. Na deze mail volgt een Outlook-verzoek voor **morgen (do 22 juli) om 15:30u**, bij de [redacted]. Hopelijk kan iedereen, ondanks deze last-minute aankondiging aanwezig zijn. Bij verhindering gelieve voor vervanging te zorgen.

Bij voorbaat dank en tot morgen.

Met vriendelijke groet,

[redacted]

.....
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid
 Turfmarkt 147 | 2511 DP | Den Haag
 Postbus 16950 | 2500 BZ | Den Haag

T 070

M 06

[redacted] @nctv.minjenv.nl

10(2)(e)
10(2)(g) **Van:** [redacted]
Aan: [redacted] (NCSC-NL)
Onderwerp: Thanks for your submission (Pegasus in the Netherlands) [Ticket [redacted]]

10(2)(g) Your request [redacted] has been received and will be reviewed by our Security Lab staff. Please note that we are having a high number of requests right now, so we may have some delay in our answer.

10(2)(g) Regards,
[redacted]

10(2)(e) **Van:** [redacted] (NCSC-NL)
 10(2)(e) **Aan:** NCSC Bestuurlijke Ondersteuning
Cc: [redacted] BD/NCSC/OP
Onderwerp: FW: Wob-verzoeken Pegasus - graag reactie vóór 13-08 16.00 uur
Datum: vrijdag 6 augustus 2021 16:29:50
Bijlagen: image001.png

10(2)(e) Hi collega's BO, [redacted]
 Ik heb het volgende contact gehad:

10(2)(e) [redacted] belde mij met vragen. Dit met [redacted] besproken, hij heeft vervolgens deze man telefonisch te woord gestaan en het volgende besproken (copy/paste van de chat) :

10(2)(e)

2:34 PM

10(2)(e) +

10(2)(g)

[redacted] wil graag weten of wij a) beschikking hebben over de pegasus checker app van amnesty en b) iets kunnen zeggen over de betrouwbaarheid daarvan. Die tool staat op de github van amnesty, wij hebben daar zelf niet naar gekeken vzwiw maar hij kan natuurlijk altijd even zelf de broncode checken :wink:

11(1)

2:44 PM

yep ik bel m zo terug!

10(2)(e)

3:13 PM

ok ik heb m teruggebeld

aangegeven dat wij geen indicatie hebben dat er nederlandse nummers in de lijst zouden staan, dat wij indicatoren hebben gedeeld met het NDN netwerk en dat hier ook niks uit is gekomen

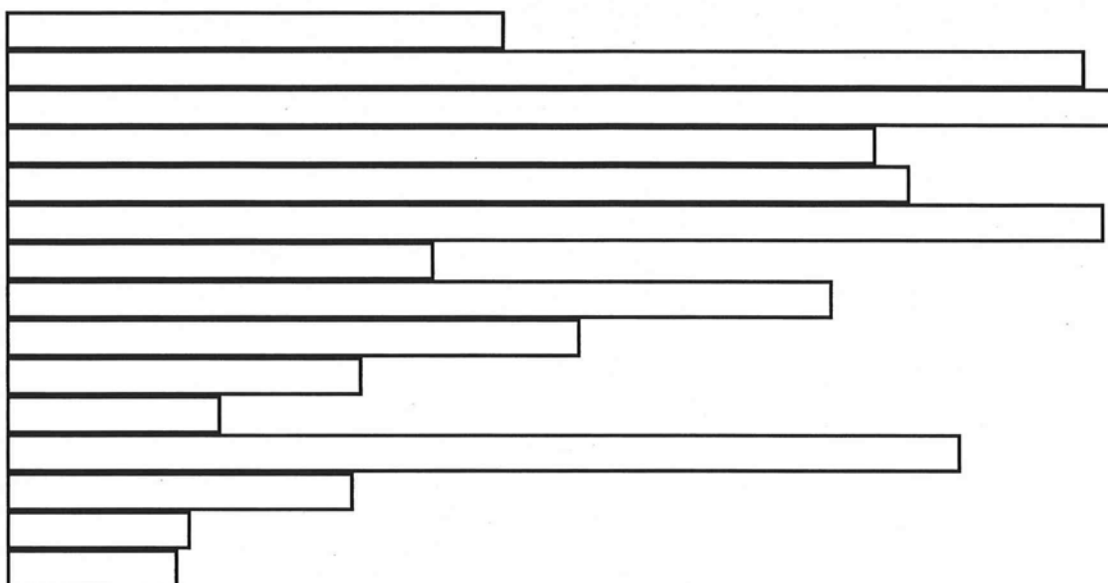
Verder zou alles in tickets moeten staan.

Grt

10(2)(e)

buiten scope

Buiten scope



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

Ministerie van Justitie en Veiligheid

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

Ministry of Justice and Security

10(2)(e)

Van: [redacted] BD/NCSC/Staf
Aan: [redacted] BD/NCSC/Staf
Onderwerp: Dagstart 25/7
Datum: maandag 26 juli 2021 09:37:28

Dagstart 25/7

- [redacted]

Buiten scope

[redacted]

[redacted]
[redacted]

-. Pegasus. Lijkt afgerond. NCTV en Diensten in the lead.

Buiten scope

[redacted]
[redacted]
[redacted]

[redacted]
[redacted]

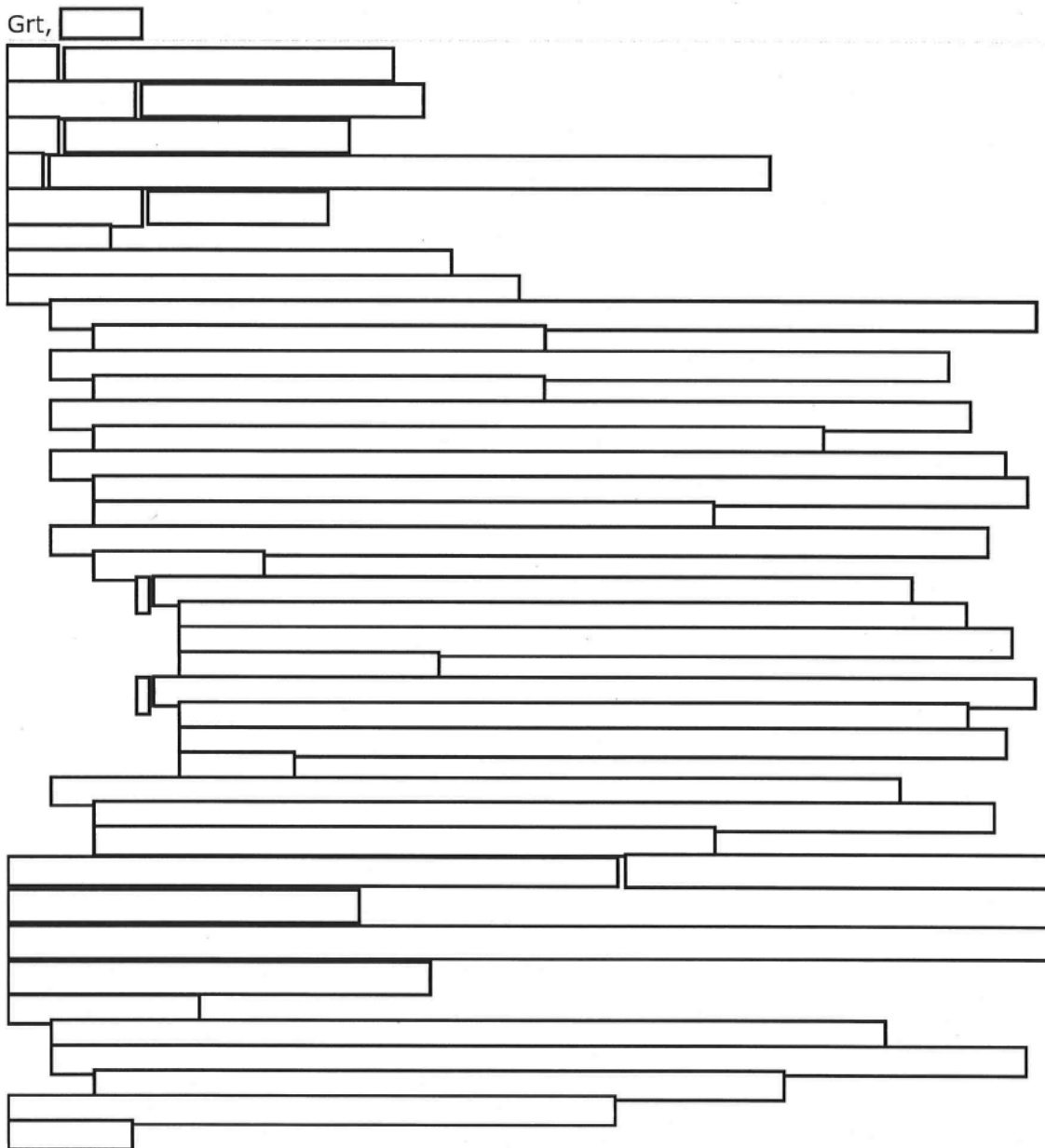
10(2)(e)

Van:
Aan: [REDACTED] BD/NCSC/Staf
Cc:
Onderwerp: FW: TERTS 27072021
Datum: dinsdag 27 juli 2021 09:22:06
Bijlagen: Duidingsoverzicht 27 juli 2021.pdf
 TERTS 26072021.msg

Ter aanvulling: in het definitieve duidingsoverzicht staat nog e.e.a opgenomen in relatie tot de Pegasus-casus (artikel in duidingsoverzicht: Hoge ambtenaren in 2019 al getroffen door Pegasus-spyware).

Ter achtergrond bij deze casus stuur ik je daarvoor nog even de terts-voorbereiding van gisteren mee, waarin ik daarover e.e.a opnam.

10(2)(e)



Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's

Van: (NCSC-NL)
 Aan: (NCSC-NL)
 Onderwerp: [DSC] Ernstige kwetsbaarheden in Apple iOS verholpen

* PGP Signed by an expired key: 26-8-2016 at 10:14:29

Beste NCSC-partner,

Apple heeft gisteren versie 9.3.5 van iOS uitgebracht [0]. In deze versie worden 3 ernstige kwetsbaarheden verholpen die tot nu toe nog niet bekend waren.

De kwetsbaarheden zijn aan het licht gekomen toen een mensenrechtenactivist een opvallend SMS-bericht liet onderzoeken door Lookout [1] en Citizen Lab [2]. Uit deze onderzoeken is gebleken dat het hier waarschijnlijk om een gerichte aanval gaat waarbij kwetsbaarheden worden gebruikt om middels speciaal gemaakte spyware toegang te verkrijgen tot bijvoorbeeld gegevens van messengerdiensten als WhatsApp en Telegram en voor het af luisteren van telefoongesprekken. Door misbruik te maken van de kwetsbaarheden kan een aanvaller echter volledige controle over een Apple-apparaat verkrijgen.

Het NCSC heeft een beveiligingsadvies uitgebracht [3] en adviseert de betreffende update zo snel mogelijk door te voeren. Voor zover bekend worden de kwetsbaarheden zeer beperkt misbruikt. Om deze reden hebben wij de kans op misbruik in ons beveiligingsadvies op dit moment ingeschaald op 'medium'. Zodra er aanvullende informatie beschikbaar is zullen wij dit beveiligingsadvies bijwerken.

[0] <https://support.apple.com/en-us/111207107>

[1] <https://blog.lookout.com/blog/2016/08-25/trident-pegasus/>

[2]

<https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

[3]

<https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2016-0771+1.00+Kwetsbaarheden+verholpen+in+Apple+iOS.html>

Met vriendelijke groet,

.....
 Nationaal Cyber Security Centrum
 Postbus 117 | 2501 CC | Den Haag | www.ncsc.nl

.....
 T 070 751 5555

E @ncsc.nl

.....
 Turfmarkt 147 | 2511 DP | Den Haag

* NCSC-NL 2016 general information < @ncsc.nl>

* 0x0F45D2F4 - Expired(L)

DSC mailing list

10(2)(e)

Van:

[REDACTED] (NCSC-NL) [REDACTED]

Aan:

[REDACTED] (NCSC-NL)

10(2)(g)

Onderwerp:

[OPS] CTI/DA > 2021-07-20 NSO Group Pegasus spyware

Bijlagen:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

10(2)(g)

10(2)(e)



[REDACTED] (NCSC-NL) created a page

☐ 2021-07-20 NSO Group Pegasus spyware

10(2)(e)

10(2)(g)

Title	NSO Group Pegasus spyware
TLP	TLP:AMBER_
Date	☐ 20 Jul 2021
CTI-Specialist	☐ [REDACTED] (NCSC-NL)
	[REDACTED]
Version	1.0
Status	CONCEPT
Recipient(s)	

Summary

Onderzoekers hebben de infrastructuur van Pegasus spyware bekend gemaakt. Deze spyware is ontwikkeld door NSO group en wordt oa gebruikt voor het afluisteren van journalisten.

Analysis

De infrastructuur is publiek gemaakt door Amnesty International Security Lab middels een Github repo. De repo bevat zowel nieuwe als oude domeinen.

[REDACTED]

[REDACTED]

--

10(2)(e)
10(2)(g) **Van:** [redacted] (NCSC-NL)
Aan: [redacted] (NCSC-NL)
10(2)(e) **Cc:** [redacted] (NCSC-NL); [redacted] (NCSC-NL)
Onderwerp: NSO pegasus lijst

10(2)(g) Beste collega's van [redacted],
Hebben jullie de lijst met 50000 telefoon nummers en indien ja kunnen jullie de nederlandse
nummers met ons delen?

10(2)(e) Met vriendelijke groet

[redacted]

10(2)(g)

 $10(2)(g)$

10(2)(g)

10(2)(g)

10(2)(g)

10(2)(g)

 $10(2)(g)$

10(2)(e)

Van: [redacted] (NCSC-NL)
 Aan: [redacted] (NCSC-NL)
 Onderwerp: Pegasus: hoofdpunten uit de Franse media

- Tussen de lijst van 50.000 telefoonnummers zouden de nummers van een staatshoofd zitten, alsmede twee Europese regeringsleiders, (600) politici in onder andere een voormalige Sovjetrepubliek en een Afrikaans land, prinsen en prinsessen, (65) bedrijfsleiders, en aantal miljardairs, ambassadeurs en generaals. Tevens bevat de lijst ten minste 180 journalisten, meerdere advocaten en 65 mensenrechtenactivisten: « [Projet Pegasus](#) » : [révélations sur un système mondial d'espionnage de téléphones \(lemonde.fr\)](#) en [Tensions diplomatiques autour du logiciel espion Pegasus \(lefigaro.fr\)](#)
- De lijst zou zich dus minder richten op leden van terroristische of criminele organisaties, hoewel dit niet wordt uitgesloten: « [Projet Pegasus](#) » : [comment la société israélienne NSO Group a révolutionné l'espionnage \(lemonde.fr\)](#)
- Agnes Callamard, SG van *Amnesty International*, stelt dat het gaat om een twintigtal landen die de software gebruiken, in plaats van de eerdergenoemde elf: [Tensions diplomatiques autour du logiciel espion Pegasus \(lefigaro.fr\)](#). Volgens *Le Figaro* zou de NSO de software aan 55 landen verkocht hebben: [Tout savoir sur Pegasus, ce logiciel dévoyé pour espionner journalistes et activistes \(lefigaro.fr\)](#)
- In Juni heeft de NSO voor het eerst een rapport gepubliceerd om de transparantie van het bedrijf te verbeteren. Hierin wordt aangegeven dat het de banden met een tiental klanten heeft verbroken naar aanleiding van mogelijk misbruik van de software en mogelijke mensenrechtenschendingen. In dit rapport wordt ook aangegeven dat de NSO niet verantwoordelijk is voor het gebruik van de technologie. Volgens *Le Figaro* kan dit aangeven dat ze op de hoogte waren van het lek/schandaal: [Tensions diplomatiques autour du logiciel espion Pegasus \(lefigaro.fr\)](#)
- In Frankrijk zijn ongeveer 1000 telefoonnummers getarget, met name vanuit de Marokkaanse overheid: [Tout savoir sur Pegasus, ce logiciel dévoyé pour espionner journalistes et activistes \(lefigaro.fr\)](#)
- Veiligheidsdiensten van Marokko zouden onder andere geprobeerd hebben Pegasus te gebruiken om toegang te krijgen tot de telefoon van de burgemeester van Ivry-sur-Seine (een banlieue in Parijs) naar aanleiding van een donatie van €5000,- aan een schoolproject in de Westelijke Sahara: [Projet Pegasus : l'obsession du Sahara occidental pousse le Maroc à tenter d'espionner le maire d'Ivry-sur-Seine \(lemonde.fr\)](#).
- Het Franse OM (parquet de Paris) start een onderzoek naar aanleiding van mogelijke spionage van twee journalisten van Mediapart door de Marokkaanse geheime dienst : « [Projet Pegasus](#) » : [comment la société israélienne NSO Group a révolutionné l'espionnage \(lemonde.fr\)](#) en « [Projet Pegasus](#) » : [Mediapart a été espionné par le Maroc - Page 1 | Mediapart](#)

10(2)(e)

Van: [redacted] BD/NCSC/OP
Aan: [redacted] @ncsc.nl"
Cc: [redacted] BD/NCSC/OP
Onderwerp: Pegasus software
Datum: donderdag 22 juli 2021 17:45:57

10(2)(g)

10(2)(e)

11(1)

[redacted]:

<https://mobile.twitter.com/vxunderground/status/1418207502974525441?s=21>

11(1)

[redacted]

Cheers,

10(2)(e)

[redacted]

Sent with BlackBerry Work
(www.blackberry.com)

10(2)
(g)

[redacted] is vermoedelijk Pegasus smartphones

backdoor NSO

10(2)(g)

Buiten
scope

10(2)(g)

Buiten scope

10(2)(g)

9/2/2021

FD

[redacted] is vermoedelijk Pegasus smartphones backdoor NSO

10(2)(g)

Buiten scope

History

Wed, 11 Jul 2018 19:26:21 +0200 **NCSC-NL <cert@ncsc.nl> - Ticket created**

10(2)(e)

CC: [redacted] (NCSC-NL)" [redacted] @ncsc.nl>, [redacted] (NCSC-NL)" [redacted] @ncsc.nl>

Subject: [redacted] is vermoedelijk Pegasus smartphones backdoor NSO

Date: Wed, 11 Jul 2018 17:26:16 +0000

10(2)(g)

To: [redacted] (NCSC-NL)" [redacted] @ncsc.nl>

From: "Cert (NCSC-NL)" <cert@ncsc.nl>

[hxxps://twitter.com/dangoodin001/status/1017087816440770561](https://twitter.com/dangoodin001/status/1017087816440770561)

With kind regards,
NCSC

.....
National Cyber Security Centre
P.O. box 117 | 2501 CC | The Hague | The Netherlands | www.ncsc.nl

.....
E cert@ncsc.nl
T +31 70 751 55 55 (general)

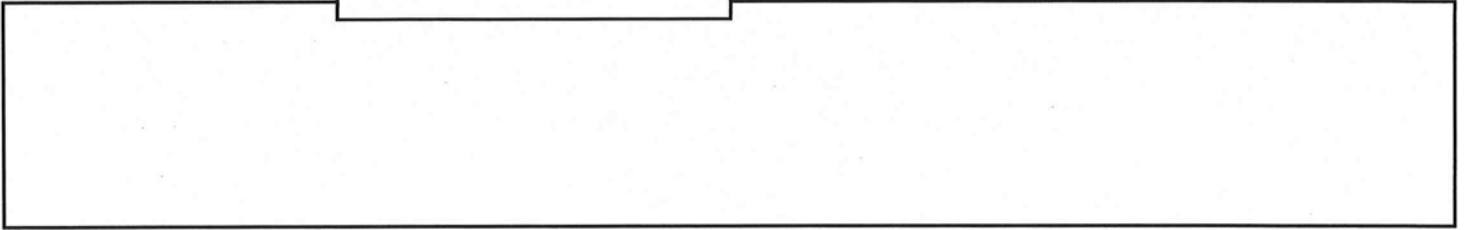
10(2)(g)

.....
Visitor address:
Turfmarkt 147 | 2511 DP | The Hague | The Netherlands

10(2)(g)

9/2/2021

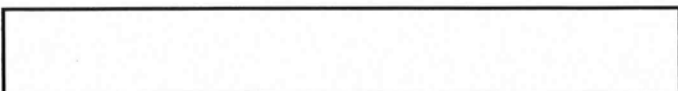
[REDACTED] is vermoedelijk Pegasus smartphones backdoor NSO



10(2)(g)

Buiten scope

10(2)(g)

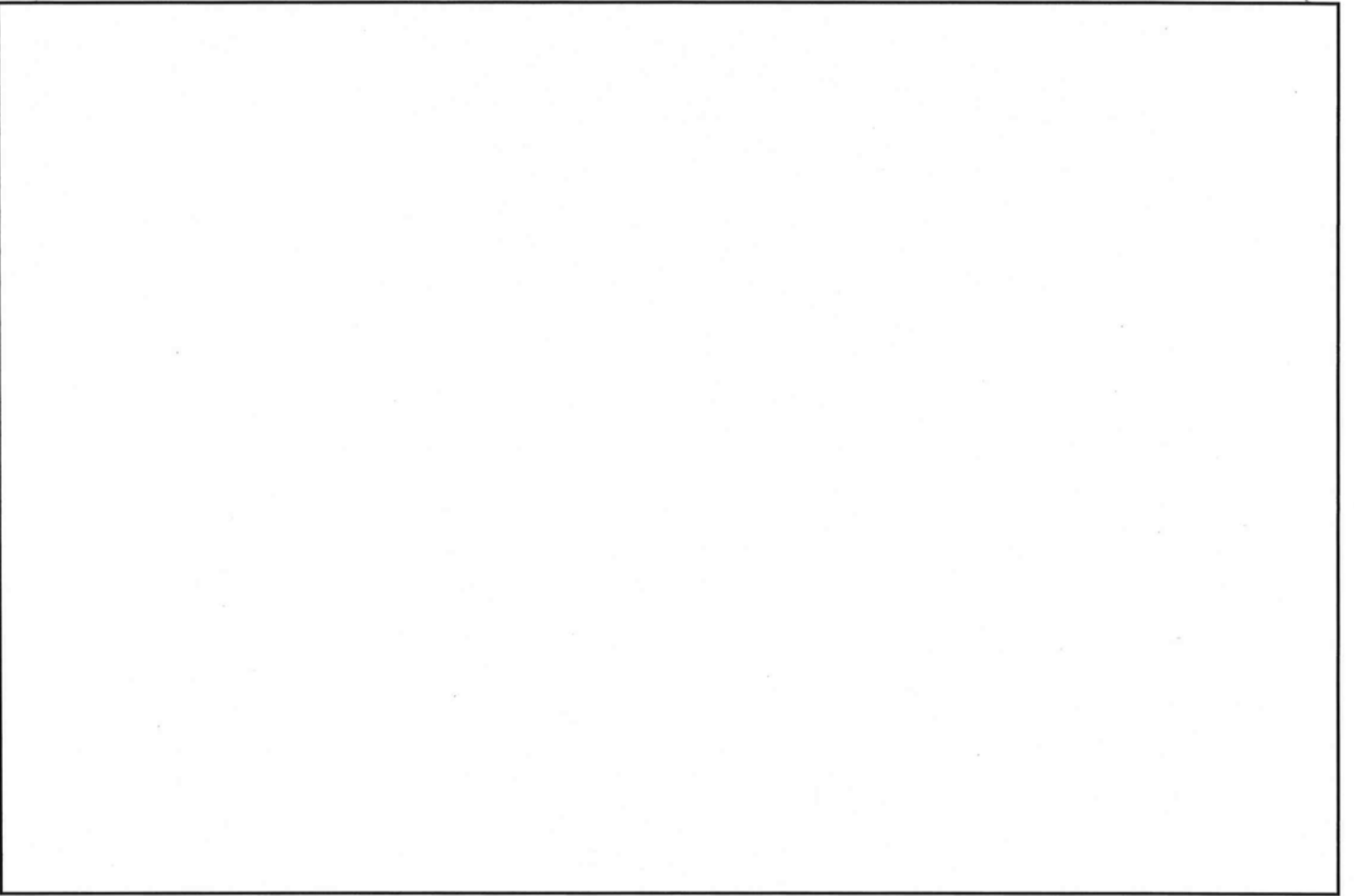


9/2/2021
10(2)(g)

[redacted] voo [redacted] meer details bekend geworden over WhatsApp hack door NSO Group

FJ

[redacted] voor [redacted]: meer details bekend geworden over
WhatsApp hack door NSO Group



10(2)(g)

10(2)(g)

[redacted]

9/2/2021

10(2)(g) [redacted] voor [redacted] meer details bekend geworden over WhatsApp hack door NSO Group

10(2)(g) Thu, 31 Oct 2019 20:59:23 +0100 [redacted] Ticket created

10(2)(e) CC: [redacted]@lists.ncsc.nl" [redacted]@lists.ncsc.nl>, "Cert (NCSC-NL)"
<cert@ncsc.nl>

10(2)(g) Subject: voor [redacted] meer details bekend geworden over WhatsApp hack door NSO Group

Date: Thu, 31 Oct 2019 19:59:20 +0000

10(2)(g) To: "NCC - NCTV" <[redacted]@nctv.minjenv.nl>

10(2)(e) From: [redacted] (NCSC-NL)" [redacted]@ncsc.nl>

Hai,

10(2)(g) Hieronder een berichtje voor [redacted] met duiding vanuit het NCSC.

Groet,

10(2)(e) [redacted]

Meer details bekend geworden over WhatsApp hack door NSO Group (verschillende media)

Facebook (eigenaar WhatsApp) heeft eerder deze week de NSO Group aangeklaagd. Uit de aanklacht en een gepubliceerd onderzoek van The Citizen Lab blijkt dat de NSO Group misbruik heeft gemaakt van een kwetsbaarheid in de communicatiemethoden van WhatsApp. The Citizen Lab geeft aan meer dan honderd slachtoffers te hebben geïdentificeerd, voornamelijk mensenrechtenactivisten en journalisten over de hele wereld.

<https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/>

<http://feeds.reuters.com/~r/reuters/technologyNews/~3/1jFiRjxtVRI/exclusive-whatsapp-hacked-to-spy-on-top-government-officials-at-u-s-allies-sources-idUSKBN1XA27H>

<https://www.aljazeera.com/news/2019/10/india-seeks-answers-whatsapp-cyberespionage-191031160608817.html>

<https://www.bbc.com/news/technology-50249859>

Duiding NCSC:

Eerder dit jaar heeft de minister kamervragen beantwoord[1] over dezelfde NSO Group die een andere kwetsbaarheid van WhatsApp had misbruikt om een Engelse advocaat af te luisteren [2]. Deze advocaat stond verschillende dissidenten bij die eerder door de NSO Group waren aangevallen, uit Saudi Arabië, Mexico en anderen.

11(1)

[redacted] De klanten van NSO Group zijn voornamelijk overheden die zich actief willen richten op haar dissidenten.

Er zijn geen aanwijzingen dat er Nederlandse belangen geraakt zijn door deze aanval.

[1] <https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/24/antwoorden-kamervragen-over-het-bericht-whatsapp-rushes-to-fix-security-flaw-exposed-in-hacking-of-lawyer-s-phone>

[2] <https://www.nytimes.com/2019/05/13/technology/nso-group-whatsapp-spying.html>

10(2)(g)

Buiten scope

10(2)(g)

9/2/2021

buiten scope

10(2)(g)

[REDACTED]

RE: Contact details pegasus phonelist

FT

[REDACTED]

RE: Contact details pegasus phonelist

[REDACTED]

[REDACTED]

9/2/2021

10(2)(g)

RE: Contact details pegasus phonelist

FT

10(2)(e)

Wed, 21 Jul 2021 16:34:48 +0200

@ssi.gouv.fr> - Ticket created

10(2)(e)

CC: [redacted] (NCSC-NL)" <[redacted]@ncsc.nl>, "Cert (NCSC-NL)" <cert@ncsc.nl>

Subject: RE: Contact details pegasus phonelist

Date: Wed, 21 Jul 2021 14:33:55 +0000

10(2)(g)

To: "IoC (NCSC-NL)" <[redacted]@ncsc.nl>

10(2)(e)

From: [redacted] <[redacted]@ssi.gouv.fr>

10(2)(e)

Dear [redacted] Dear friends at NCSC-NL,

Thank you for reaching out.

10(2)(a)

I have notified my colleagues of your interest for this document, so we might be able to come back to you if we somehow manage to obtain it in the future.

Have a good afternoon,

10(2)(e)

--



10(2)(g)

ANSSI - Agence Nationale de la Sécurité des Systèmes d'Information

51 boulevard de la Tour Maubourg, 75700 Paris, France

10(2)(g)

Tel: +33 [redacted]

PGP: [redacted]

10(2)(g)

De : IoC (NCSC-NL) <[redacted]@ncsc.nl>

Envoyé : mercredi 21 juillet 2021 13:37

10(2)(e)

À [redacted] <[redacted]@ssi.gouv.fr>

10(2)(g)

9/2/2021

10(2)(g)

RE: Contact details pegasus phonelist

FT

10(2)(g) **Cc :** [redacted] (NCSC-NL) <[redacted]@ncsc.nl>; Cert (NCSC-NL) <cert@ncsc.nl>
Objet : Contact details pegasus phonelist

-----BEGIN PGP SIGNED MESSAGE-----

10(2)(g)

[redacted]

10(2)(e)

Dear [redacted]

As agreed by our phone call I will sent you my contact details, as we both
start our holidays by the end of this wee I also cc-ed our IOC and CERT
mailbox.

10(2)(a)

[redacted]
[redacted] to the cert@ncsc.nl (mailto:cert@ncsc.nl) and [redacted]@ncsc.nl
[redacted]@ncsc.nl
mailboxes.

10(2)(e)

Best regards

[redacted]

CTI-Specialist NCSC-NL

-----BEGIN PGP SIGNATURE-----

10(2)(g)

[redacted]

10(2)(g)

[redacted]

10(2)(g)

10(2)(g)
buiten
scope

[REDACTED] **[PEGASUS]**

Buiten scope

[REDACTED]

[REDACTED]

[REDACTED]

9/2/2021

10(2)(g)

[REDACTED] [PEGASUS]

FU

10(2)(g)

Wed, 21 Jul 2021 18:17:27 +0200

[REDACTED] Ticket created

Subject: [PEGASUS]

10(2)(e)

From: [REDACTED]@ncsc.nl

To: cert@ncsc.nl

Date: Wed, 21 Jul 2021 18:17:27 +0200

10(2)(g) Wed, 21 Jul 2021 18:22:25 +0200

[REDACTED] Comments added

10(2)(g)

[REDACTED] t.b.v. overzicht omtrent Pegasus.

10(2)(a)

Contact met Cert-FR

[REDACTED] [CTI]

10(2)(e)

10(2)(g)

Vraag Rijks CIO Office om advies en duiding

Wbni

Vraag [REDACTED] om duiding en IOC's [ASK/FC]

10(2)(g)

Bijdrage [REDACTED] 20 juli 2021 (Duiding NCTV)

10(2)(g)

Wed, 21 Jul 2021 18:52:00 +0200

[REDACTED] Pegasus added

Wed, 21 Jul 2021 21:30:36 +0200

[REDACTED] ANP App alert Terrorisme:

10(2)(g)

Dubai-prinses Latifa op lijst met mogelijke doelwitten Pegasus added

10(2)(g)

Thu, 22 Jul 2021 22:18:09 +0200

[REDACTED] Pegasus software added

10(2)(g)