To: (10)(2e) (10)(2e)@icloud.com]; (10)(2e)@kpn.com[(10)(2e)@kpn.com]; (10)(2e) (10)(2e)@minvws.nl]; (10)(2e)@kpn.com[(10)(2e)@kpn.com]; (10)(2e)[(10)(2e)@minvws.nl]
Cc: (10)(2e)[(10)(2e)@webweaving.org]; (10)(2e)[(10)(2e)@egeniq.com]; (10)(2e)[(10)(2e)@dictu.nl]; (10)(2e) (10)(2e)[(10)(2e)@minvws.nl]
From: (10)(2e) (10)(2e) (10)(2e)
Sent: Fri 8/14/2020 7:08:16 AM
Subject: RE: SHOWSTOPPER (Re: Load tests - good and bad news)
Received: Fri 8/14/2020 7:08:17 AM

Hi (10)(2e)

Als eerste graag de mail in eerste instantie richten aan (10)(2e) hij is voor jouw het vaste aanspreekpunt.

Ik begrijp van hem dat er om 10 uur een call om dit probleem te bespreken. Zorg jij ervoor dat de juiste personen aanschuiven in deze meeting?.. (10)(2e) heeft de meeting request namelijk nog niet geaccepteerd.

Groet, (10)(2e)

Van: (10)(2e) <(10)(2e)@icloud.com>
Verzonden: vrijdag 14 augustus 2020 08:50
Aan: (10)(2e) (10)(2e) (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e)@kpn.com; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e)@kpn.com
CC: (10)(2e) <(10)(2e)@webweaving.org>; (10)(2e) <(10)(2e)@egeniq.com>; (10)(2e) (10)(2e) <(10)(2e)@dictu.nl>
Onderwerp: Fwd: SHOWSTOPPER (Re: Load tests - good and bad news)

Beste (10)(2e) en (10)(2e)

Er is vanuit ons toch wel een aanzienlijk zorg wat er gebeurt bij een aanval op de servers.
De kans is eigenlijk wel bijna 100% dat men dat zal proberen zodra we live zijn.

De inschatting is dat zonder maatregelen het toch onderuit gaat.

Daarnaast begrijp ik dat het CDN 'shared' is. En dat dus ook andere klanten van het CDN daar dan de gevolgen van ondervinden.

Kunnen jullie jullie licht nog een keer op laten schijnen en iets meer informatie verschaffen welke andere maatregel er zijn om dit te ondervangen?

Groet,
(10)(2e)
Begin doorgestuurd bericht:

Van: (10)(2e) <(10)(2e)@webweaving.org>
Datum: 13 augustus 2020 om 15:54:10 CEST
Aan: (10)(2e) <(10)(2e)@(10)(2e).com>
Kopie: (10)(2e) <(10)(2e)@dictu.nl>, (10)(2e) (10)(2e) <(10)(2e)@icloud.com>, (10)(2e) (10)(2e) <(10)(2e)@minvws.nl>, (10)(2e)@kpn.com, (10)(2e)@kpn.com, (10)(2e)@kpn.com
Onderwerp: Antw: SHOWSTOPPER (Re: Load tests - good and bad news)

Dit gaat specifiek over de /register en de /postkeys -- en het risico van het uitputten van de GGD keyspace.

De CDN wereld is onbeperkt - en dat ook geen punt.

(10)(2e)

On 13 Aug 2020, at 15:51, (10)(2e) <(10)(2e)@(10)(2e).com> wrote:

Even een vraag: gaat dit om CDN of om upload?
Op 13-08-2020 om 15:39 schreef (10)(2e)

@(10)(2e) dank voor het zeer duidelijke antwoord.

@(10)(2e) kan jij dit oppakken - want deze aanname is vanaf dag één een nogal cruciaal uitgangspunt geweest.

En omdat het key-submit (by design) gevoelig is voor scriptkiddies - een serieus impediment voor go-production.

Dus we moeten zien hoe we dat gaan oplossen - misschien iets met een absolute bandwidth Mngt (e.g. 1Mbit) threshhold that raised the alarm with the SOC - en then the usual attack mitigation followup.

Met vriendelijke groet,

(10)(2e)

On 13 Aug 2020, at 15:31, (10)(2e) @kpn.com wrote:

Beste(10)(2e) (10)(2e)

Vanmorgen bespraken we tijdens de dagstart het punt al even aangaande onderstaande melding betreffende monitoring en throtteling.

Wat betreft de monitoring is het voor ons niet mogelijk om reactieve meldingen uit te sturen. Dit is technisch een probleem omdat er voor de Corona App standaard voor is gekozen om de loadbalancer op shared infra te laten draaien. Dit platform is niet ingeregeld om op klant niveau alarmen af te vangen en deze te verwerken waarmee we bij het 2e punt komen. Er is geen proces aanwezig om deze alarmen mee af te vangen. Met dedicated apparatuur is natuurlijk technisch meer mogelijk dan de huidige setup maar het onderliggende proces van alarmen/monitoring/notificaties is er niet op loadbalancer niveau.

Aangaande monitoring en throtteling bij Donor: voor Donor zijn zaken ingeregeld via het Koppelvlak. Dit voorziet in functies als het beperken van aantallen connecties, berichtgroottes en dergelijke. Binnen de Corona Melder omgeving maken we geen gebruikt van het Koppelvlak dus is deze functie niet voor handen.

Dit leidt meteen tot de vraag wat er aan mogelijkheden resteert, mede vanuit het huidige contract. Vanuit mijn oogpunt zal invulling toch vanuit de applicatie moeten komen of zal er additionele functionaliteit moeten worden betrokken zoals bijvoorbeeld het huidige Koppelvlak biedt.

Met vriendelijke groet,

<image002.png><image004.jpg>

(10)(2e)
(10)(2e)
(10)(2e) (10)(2e)
(10)(2e) @kpn.com

CO CM IT KIS KPN BV
Purmerend - Wielingenstraat

<image006.jpg><image008.jpg>

<image009.jpg>

From: (10)(2e) < (10)(2e) @kpn.com>
Sent: Wednesday, 12 August 2020 11:42
To: (10)(2e) < (10)(2e) @kpn.com>; (10)(2e) < (10)(2e) @kpn.com>
Subject: FW: Load tests - good and bad news

Ter aanvulling

Van: (10)(2e) <(10)(2e) @minvws.nl>
Verzonden: woensdag 12 augustus 2020 11:00
Aan: (10)(2e) < (10)(2e) @kpn.com>
Onderwerp: RE: Load tests - good and bad news

Advies vanuit (10)(2e) is trouwens om naar de Donor omgeving te kijken als voorbeeld.
Daar is het goed ingedeeld wat alarmen betreft.

Is er een collega die (10)(2e) vervangt, (10)(2e) heeft een vraag als iemand naar het covid kavel wil connecten, moeten we dan nog steeds IP's whitelisten of hoeft dat niet meer sinds die 2FA portal?

Met vriendelijke groet,

(10)(2e)

Van: (10)(2e) @kpn.com < (10)(2e) @kpn.com>
Verzonden: woensdag 12 augustus 2020 10:46
Aan: (10)(2e) <(10)(2e) @minvws.nl>
Onderwerp: RE: Load tests - good and bad news

Laat ik naar kijken (10)(2e).

(10)(2e) is er op woensdagen niet, dus zal morgen worden.

Groeten
(10)(2e)

Van: (10)(2e) <(10)(2e) @minvws.nl>
Verzonden: woensdag 12 augustus 2020 09:30
Aan: (10)(2e) < (10)(2e) @kpn.com>
Onderwerp: FW: Load tests - good and bad news

Hi (10)(2e)

Kan jij hier naar kijken, mocht dit nog niet bekend zijn?

Met vriendelijke groet,

(10)(2e)

Van: (10)(2e) <(10)(2e)@webweaving.org>
Verzonden: woensdag 12 augustus 2020 08:20
Aan: (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) <(10)(2e)@minvws.nl>; (10)(2e) (10)(2e) <(10)(2e)@icloud.com>; (10)(2e) (10)(2e) <(10)(2e)@dictu.nl>; (10)(2e) <(10)(2e)@(10)(2e)>; (10)(2e) <(10)(2e)@(10)(2e).nl>; (10)(2e) <(10)(2e)@silk.co>; drs. (10)(2e). (10)(2e) <(10)(2e)@dictu.nl>; (10)(2e) <(10)(2e)@dictu.nl>; (10)(2e) (10)(2e). (10)(2e) <(10)(2e)@dictu.nl>; (10)(2e) <(10)(2e)@vng.nl>
Onderwerp: Load tests - good and bad news

Gisteren de load tests gedaan.

GOEDE nieuws - systeem kan 10x meer register/post's handelen dan nodig - in een erg onrealistisch scenario (10k positive tests/dag door de GGD afgehandeld binnen kantooruren/werkdagen waarbij alle Nederlanders een mobieltje hebben).

Het **SLECHTE** Nieuws is dat er totaal geen alarmen afgaan bij dit soort loads - en dat ze nauwelijks te zien waren / niet opvielen. En dat er op dit nog moment geen surge, load/peak of ander soortige detectie is, nog enige throttling.

En dat het (dus nu) triviaal is voor een script kiddie om de huidige GGD keyspace in een paar uur volledig uit te putten.

Dus dat moet ASAP ingeregeld gaan worden op de BigIP/F5. En er moet monitoring op gaan komen met de gebruikelijke ingress filters & triage stappen.

Aangezien we deze pentests als project zelf, in huis, gedaan hebben - is hier geen extern/objectief rapport van.

Ik neem aan dat iemand van MinVWS dat gaat maken ?

Met vriendelijke groet,

(10)(2e)

--

(10)(2e)

(10)(2e)

(10)(2g)