To: 5.1.2e [5.1.2e]; 5.1.2e [5.1.2e @newnexus.nl]
Cc: 5.1.2e @cyberoperaties.nl[5.1.2e @cyberoperaties.nl]; 5.1.2e [5.1.2e @dictu.nl]; 5.1.2e [5.1.2e @icloud.com]; 5.1.2e @cinqict.nl[5.1.2e @cinqict.nl]; 5.1.2e . (5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e)[5.1.2e @minvws.nl]; 5.1.2e [5.1.2e @minvws.nl]; 5.1.2e [5.1.2e @minvws.nl]; 5.1.2e @minvws.nl[5.1.2e @minvws.nl]
From: 5.1.2e
Sent: Sat 9/12/2020 11:50:29 AM
Subject: Re: CDN/F5 DDOS issue CIBG-C2009 01100 Corona melder - Spike in 5xxerrors (CDN)
Received: Sat 9/12/2020 11:50:34 AM

Hoi,

Nee ik wil een brede review. Dus een post-mortem gaat mogelijk nog met een onderzoek worden opgevolgd. Ik vind het echt wel een ding dat bij een beveiligingsincident security buiten de deur is gehouden. Daarnaast had er mogelijk ook een verdere escalatie moeten zijn als er uiteindelijk een datalek was uitgekomen.

Hartelijke groet,

5.1.2e

Op 12-09-2020 om 13:21 schreef 5.1.2e :

> 5.1.2e
> Goed nieuws indeed.
>
> Jij gaat nog wel even achter een postmortem aan ? En hamert met name op een goede verklaring van de CNAME's te krijgen ?
>
> Want we moeten echt gaan begrijpen waarom ons DNS nodeloos 'stuk' gemaakt werd c.q. verkeerd geconfigureerd was.
>
> Want dat maakte de impact vele malen groter dan nodig was c.q. betekend dat we een onwenselijk/erg groot operationeel risico hebben dat we niet in kaart hebben / geen compenserende maatregelen voor hebben nog.
>
> 5.1.2e
>
> > On 12 Sep 2020, at 11:42, 5.1.2e < 5.1.2e @newnexus.nl> wrote:
> >
> > Allen,
> >
> > Hierbij de statusupdate.
> >
> > De bereikbaarheid/beschikbaarheid is weer binnen de norm.
> >
> > De DDOS is gister rond 20:45 gestopt. Totale duur van 07:06:04.
> > Geen problemen bij GGD en/of appgebruikers.
> > Er zijn aanpassingen doorgevoerd in KPN eigen netwerk en NAWAS.
> > Het verkeer wordt op dit moment uit de NAWAS gehaald.
> >
> > KPN houdt het ticket open en heeft verhoogde dijkbewaking.
> > CIBG checkt op errors zodra het verkeer weer via de reguliere route loopt en schakelt indien nodig met KPN.

Prettig weekend!

Groet 5.1.2e

Van: 5.1.2e <5.1.2e@newnexus.nl>
Datum: vrijdag 11 september 2020 om 17:29
Aan: "5.1.5@cyberoperaties.nl" <5.1.5@cyberoperaties.nl>, 5.1.2e <5.1.2e@dictu.nl>, 5.1.2e <5.1.2e@icloud.com>, "5.1.2e@cinqict.nl" <5.1.2e@cinqict.nl>
CC: "5.1.2e)" <5.1.2e@minvws.nl>, "5.1.2e)" <5.1.2e@minvws.nl>, 5.1.2e <5.1.2e@minvws.nl>, 5.1.2e <5.1.2e@minvws.nl>, "5.1.2e@minvws.nl" <5.1.2e@minvws.nl>
Onderwerp: CDN/F5 DDOS issue CIBG-C2009 01100 Corona melder - Spike in 5xx errors (CDN)

Allen,

- Sinds 13:18 is er een DDos aanval op het CDN netwerk van KPN. Het verkeer verloopt daardoor via NAWAS (DDoS wasstraat), wat resulteert in tragere DNS response.
- GGD ervaart geen problemen door dit issue.
- Gebruikers van de app ervaren pas een foutmelding na 24 uur, op dit moment is er voor de appgebruikers geen issue.

In de call besloten om het op een P2 inciden te houden gezien de geringe impact.
Morgen een call om 11:00 uur om tijdig te checken hoe we ervoor staan. Als het probleem groter is geworden dan moeten we snel
schakelen om eventueel op te schalen naar P1/P0.

Issue wordt door KPN opgepakt en zodra de DDos opgehouden is zal het verkeer weer via de normale route (zonder NAWAS) kunnen
verlopen.

Morgen na de call volgt de volgende update.

Met vriendelijke groet,

5.1.2e

<image001.png>

+31 5.1.2e
5.1.2e@newnexus.nl
www.newnexus.nl