

Jean-Pierre Aerts – Product Management Grégory Degueldre – Networks



Before we start...









Name + Organization

We speak:





DDoS attacks



Europees Parlement doelwit cyberaanval na stemming over Rusland



Check Point' SOFTWARE TECHNOLOGIES LTD

65 procent van de Belgische ziekenhuizen kreeg reeds met cyberaanvallen te maken

Cyberaanvallen op ziekenhuizen nemen wereldwijd met 45 procent toe

Zamenten. 19 januari 2021. Chack. Point Bassauch (CDP) molt enn tentam van dit in het aantal menddelijk opbrassmollen op coppograntaties in de stjedepen hete manden. Ziekenbuizen bijfen ansterkholijke desiellen in zijn voor cybercinteelen, omdat ze in het commendatien om de nacental versterfellenorszermat. Ist ar felskreibische bestellen zerhoe.

belangrijkste feiten op een rijtj

- De toename (+45%) van wereldwijde cyberaanvallen op de zorgsector is het dubbele van de toename (+22%) van cyberaanvallen op alle
- Het gemiddelde aantal vekelijkse aanvallen in de zorgsector bedroeg in november 626 per organisatie, vergeleken met 430 in de
- De primaire ransomware-variant die wordt gebruikt bij de cybersamvallen is Ryuk, gevolgd door Sodinokibi.

Dreiging twee keer zo groot als in andere sectore

De sections van ophesamenten op de coprection una tree lever op oper als de terrams un operamenten op als antéries actions in dezeides periods in antiere sactions una et grafiet van een treesmen ser 22°. So exprephenamente gap an van promorriume to betales fact hat altrovers van code op attant en DOS-bassvalles Bastorniare blijd de meest verdommend derejdig te zijn en voerst in vergrejking met andere induziriels excelorer nur de belangstjore malvare-bedriging voer organisatels in de zogspector.

One Demission, Manager Data Intelligence III Cheef Part, Erit in Yvin earth optivamenters on at mentioping procratication priori and private and a second private processor of the private priority of the private private private private private private priority of the demander of the private pri



DDoS-aanvallen steeds vaker onderdeel

NaWas Tapdienst Kenniscentrum Over de NBIP Nieuws

van bredere aanval

De trend die we sinds Q4, 2021 zien, een daling van DDOS-aanvallen, is het tweede kwartaal van 2022 doorgezet. Goed nieuws zou u zeggen. Niet bepaald, er zijn namelijk weel meer DDOS-aanvallen gemeten die langer dan 4. uur duren. NaWas/NBIP deeft net als voorgaande jaren de DDOS-infographic met daarin de belangriikste trends en cijfere op het gebiel van DDOS-aanvallen.

Op basis van de meest recente cijfers zien we dat de duur van DDoS-aanvallen toeneem: Begin 2022 waren er door NaWas nog 6 aanvallen geregistreerd die langer dan 4 uur duurden. In het afgelopen kwartaal zijn er 18 aanvallen met dezelfde duur vastgesteld. Deze verdrievoudiging is een ontwikkeling die we nauwlettend in de gaten bouden

Afname totale hoeveelheid DDoS-aanvallen

In vergetijking met O2, 2022 (666) ziene we ne omfanme in het aantal DDOS-aanvallen. In digelopsen koestaal negistreerden we izd. DDOS-aanvallen. Vorig jaar zegaen we in het laatste kovertaal ook al dimenen om vervolgens daarna weer toe te nement. Helaas ich en we op basis van eerdere ontwiktelicingen dat het en antala aanvallen dus uiterindelijk weer zal toensmen. De 'vakantieperiode' van junit /m augustus is meestal een periode waarin erminder DDOS-aanvallen Dastevinden.

DDoS-aanvallen om andere aanvallen te maskeren

Over het hele kwartaal gezian, zijn er geen nieuwe methoden of opvallende aarwallen geweest. Wet jiers we een lichte stijfigin id ne malsdellijn in te zesten 'Utge Pfood'. Hiernaast zien we dat DDoS valeer gebruikt wordt als middel om Extortion Ransomware aarwallen effectiever te maksom om bedrijven te chanteren. Feit is dat met de meeste aanvallen filmandeel gewin is gemoeld. Maar DDoS aarwallen worden ook gebruikt om andere aarwallen, bijvoorbeeld op applicaties en databases in de systemen te masferen. Samenvattend: DDoS aanvallen zijn lastiger, krachtiger, meer frequent en steeks valser onderdeeld van een breder ingezette aanval geworden.

Ddos-aanval op Belnet haalt 200 organisaties offline

moensdag, 5 mei 2021

Een ddos-aanval heeft gisteren ongeveer 200 organisaties, waaronder universiteiten, overheidsdiensten en onderzoeksinstellingen getroffen. Zij werden in meer of mindere mate afgesloten van het internet.

De websites van de Vlaamse overheid bleven gelukkig gespaard. VLAIO is op zoek naar een IT-veiligheidsexpert. Iets voor jou? Ontdek deze job via www.vlaio.be/vacatures.



External Cloud Scrubbing Center

- External scrubbing center since May 2021
- Already activated a few times
- Renewed in 2022





Internal Scrubbing Center - Out of Path



Status?

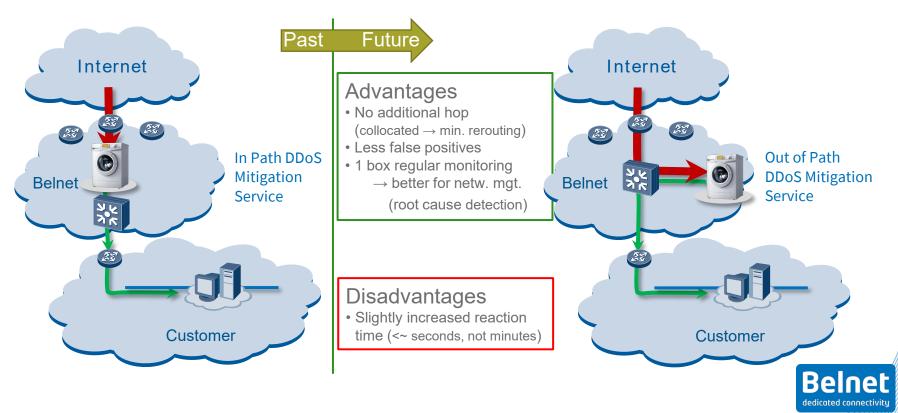
- RFP is finished
- Solution is defined
- Hardware & Software ordered
- Migrations and Onboarding planned early 2023





Inline – Out of Path Architecture





DDoS 2.0



Key Features new DDoS solution

- Protection against volumetric (L3-L4) DDoS attacks.
- Attack detections by constant monitoring of traffic flows.
- Mitigation done "in path" by Belnet routers.
- More complex attack mitigated to Belnet scrubbing centres in Brussels.





DDoS 2.0



Key Features new DDoS solution

- Very low delay of traffic redirection.
- Time-to-mitigate in a few seconds.
- No extra device "in path" during peace-time.
- Alarms sent when mitigation is triggered.
- Reporting of the mitigation after the attack.
- Historic of attacks being kept for 1 year.





DDoS 2.0 in a nutshell

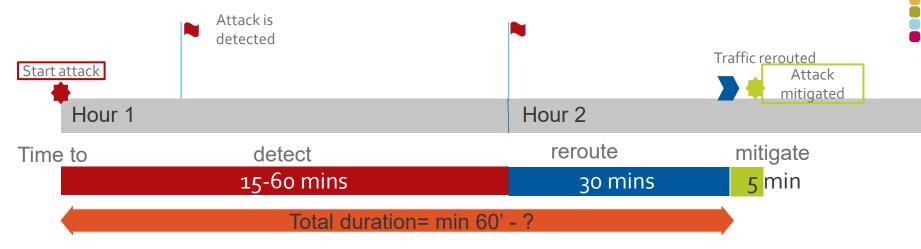
- Internal and external scrubbing center combined for an increased capacity.
- When under attack, little to no impact for end users.
- External scrubbing with some F7 protection.
- Real-time alerts.
- Full reporting after an attack.
- Self-Service dashboard optional.

.





Without new DDoS solution in place



With new DDoS solution in place





DDoS 2.0- Pricing

- Current pricing cannot be maintained.
- New pricing is not confirmed yet.
- Un-protected customers under attack will pay exceptional DDoS interventions in the future.









