Root Cause Analysis

Vedrørende netværksnedbrud på iODC core netværk.

Tirsdag d. 26/09-2017 kl 02:20 opstod der afbrydelse mellem vores kantrouter og vores CPE.
Denne afbrydelse blev straks opdaget af overvågningstjenesten samt CPE OMC, i samme øjeblik som afbrydelsen fandt sted, hvorefter fejlretningen øjeblikkeligt blev iværksat.
Der var først etableret forbindelse mellem vores kantrouter og CPE kl 03:16, dog kun frem til tirsdag d. 26/09-2017 kl 20:45, hvor forbindelsen igen blev afbrudt, og fejlretningen blev genoptaget.

Kronologisk tidslinie over hændelser

02:20 – Tirsdag d. 26/09-2017
Første afbrydelse til CPE sker. Der fejlsøges minutiøst på netværket, og genetablering sker igen ca 1 time efter. Leverandør (CPE), kontaktes med mistanke om DDoS-angreb direkte på vores linknet IP adresser. CPE OMC bedes udstede nye linknet IP adresser. Alle berørte kunder modtager e-mail advisering.

20:25 – Tirsdag d. 26/10-2017.
Anden afbrydelse til CPE sker. Der fejlsøges igen minutiøst på netværket, og det bliver vanskeligere at opretholde en stabil netværksforbindelse fra iODC kantrouter til CPE. Linietekniker fra iODC fortsætter med skadesbegrænsning og fejlsøgning på kantroutningsudstyr, da dette udstyr har konstant 100% CPU kontrol forbrug.

00:00 – Onsdag d. 27/09-2017
Linietekniker fra iODC, begynder at udskifte kantroutningsudstyr, da dette udstyr anses for defekt.

00:30 – Onsdag d. 27/09-2017
Med nyt kantroutningsudstyr bliver netværket stabiliseret, dog kun kortvarigt, og pakketab til vores netværk sker igen, samtidigt med at nyt kantroutningsudstyr stiger i CPU kontrol forbrug.
Linieteknikere fra både IODC og CPE iværksætter en dybere undersøgelse af routningsprotokoller, faste netværksruter og andet, for at finde fejlen, der får iODC kantroutningsudstyr til at tabe forbindelse til CPE. Dette arbejde fortsættes frem til kl 05.00.

05:00 – Onsdag d. 27/09-2017
Det fastslås at iODC kantroutningsudstyr, samt CPE kantroutningsudstyr er ramt af DDoS-angreb, direkte på linknet IP adresser. Det besluttes, at iODC akut skifter netværksroutning via nye indlagte fiberforbindelser fra CPE. CPE instrureres i, at nullroute alle IP adresser der rammes med mere end 8/Gbit volumetriske angreb, og CPE sender intern mail, om hasteudstedelse af nye linknet IP adresser til iODC.

iODC ApS
Arn. Nielsens Blv. 62B-C
2650 Hvidovre

Telefon: +45 70 27 05 05
E-Mail: support@iodc.dk
Web: https://www.iodc.dk

05:00 – Onsdag d. 27/09-2015.
Linietekniker fra iODC fortsætter minutiøst at opretholde netværkforbindelser til CPE via nyetableret fiber. DDoS-angreb fortsættes nu mod vores kunde-netværk, da det ingen effekt længere har, at DDoS angribe tidligere linknet IP adresser. Alle kunder i iODC regi, e-mail adviseres om DDoS og netværkssituationen. Dette arbejde foregår frem til torsdag d. 28/09-2015. CPE kontaktes i tidsrummet onsdag d. 27/09-2017 fra 08.00 til 17.00, syv gange telefonisk, med henblik på, at få oprettet nye linknet IP adresser, således at iODC kan genetablere stabil drift og netværk beskyttet i mod de konstante DDoS angreb.

09:00 – Torsdag d. 28/09-2017
DDoS angreb er stadigvæk eksisterende, og der er på dette tidspunk nullroutet 46 IP adresser, da disse har oversteget vores volumetriske kapacitet til CPE. iODC har på dette tidspunkt endnu ikke blevet tildelt linknet IP adresser af CPE, hvorfor iODC eskalerer vigtigheden af dette til CPE administrerende direktør.

15:25 – Torsdag d. 28/09-2017
CPE udleverer nye linknet IP adresser, og linietekniker fra iODC skifter omgående netværksrute over iODC fiberinstallationer i Amsterdam. DDoS angreb begynder i samme øjeblik, at blive mitigeret af iODC anti-DDoS soft- og hardware på iODC Amsterdam lokation.

16:30 – Torsdag d. 28/09-2017
Netværkssituationen er normaliseret, og linietekniker fra iODC påbegynder udredning af de mange hundrede DDoS angreb.

23:30 – Torsdag d. 28/09-2017
Alle kunder email adviseres om genoptaget netværksdrift.

Linieteknikere og metoder

Linieteknikere fra IODC:
Kan ikke offentliggøres.

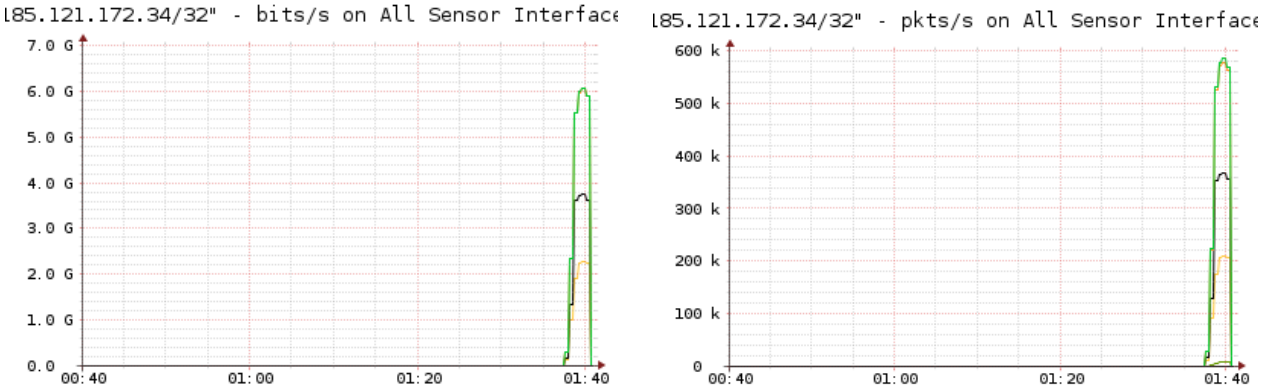
Linieteknikere fra CPE:
Kan ikke offentliggøres.

Metoder anvendt for fejlsøgning og fejlretning:
Junos TCP dump.
Wireshark.
PRTG packet capture.

Det fundne og Root Cause

A) Det er under udredningen blevet fastlagt, at der tirsdag d. 26/10-2017 er blevet benyttet en såkaldt ”flood” metode over HTTPS protokollen, mod en af iODCs’ kunder, på ganske få Mbits, som ikke var tilstrækkeligt beskyttet i vores netværk. Dette angreb blev overset af iODC, da der i samme tidsrum blev udført store volumetriske angreb mod andre IP adresser i iODC regi, for at sløre dette HTTPS flood angreb.

På grund af overstående var det muligt for angriberne at omgås IODC’s DDoS beskyttede netværk, at sende mellem 15.000 og 80.000 netværkspakker i sekundet (PPS), direkte ind til IODCs’ kantroutningsudstyr, under dække af meget store volumetriske DDoS angreb.



HTTPS TCP protokollen, var ikke tilstrækkeligt beskyttet af vores Anti-DDoS systemer.
HTTPS TCP protokollen, foruden ICMP protokollen, er den mest benyttede protokol på internettet, og det har derfor været vigtigt for iODC, ikke at have for striks politik hvad angår denne protokol.
iODC kantroutningsudstyr har ikke været tilstrækkelig med CPU kapacitet, hvorfor denne protokol under et flood, fik kantroutningsudstyr til at bryde ned på CPU kontrol niveau.

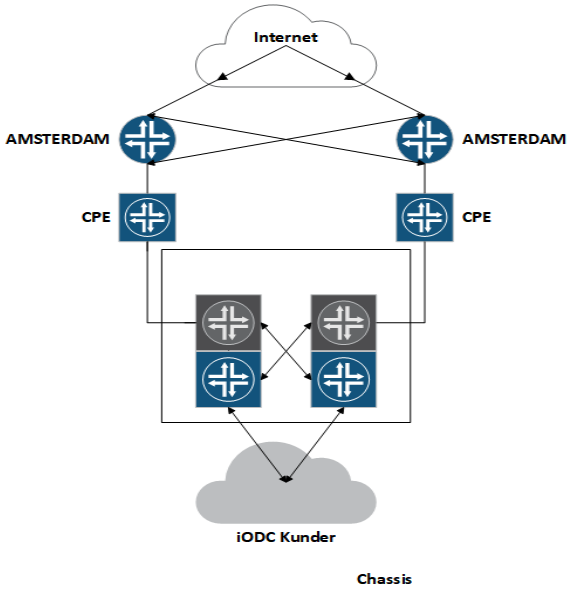
B) Sekundært blev iODC linknet IP adresser opsnappet, da iODC overgik til direkte netværksroutning med CPE. Dette bekræftes af både iODC og CPE linieteknikere tidligt i forløbet.
Desværre, til stor gene for iODC, var CPE ikke i stand til at efterkomme iODCs’ gentagene, og mange opfordringer til at få udleveret nye linknet IP adresser, hvilket resulterede i, at iODC samt CPE OMC var nødsaget til, at manuelt styre og håndtere alle aspekter af netværksforbindelser i mere end 1½ døgn.

Udbedrende handlinger foretaget

1) Kantroutningsudstyr i iODC regi blev nedtaget og udskiftet med nyt.
2) Alle IP adresser i iODC regi, der blev volumetrisk angrebet med mere end 8/Gbits blev manuelt nullroutet.
3) Der blev foretaget et skifte af linknet IP adresser mellem iODC og CPE.
4) Alle TCP og UDP pakker under angreb blev logget og gennemgået løbende for at begrænse og stoppe skade.

Fremadrettede handlinger der foretages

A) Alle netværksforbindelser til- og fra iODC netværk omlægges til fuld redundant 20Gbit fiberlinier, natten mellem lørdag d. 07/10-2017 og søndag d. 08/10-2017 i tidsrummet 01.00 til 06.00.
B) Alle kantroutere i iODC netværk udskiftes til nye, kraftigere og 10Gbit kompatible kantroutere, natten mellem lørdag d. 07/10-2017 og søndag d. 08/10-2017 i tidsrummet 01.00 til 06.00.
C) Alt netværk fra første layer2 switch i iODCs' netværk, og helt frem til iODCs' 2 x 400Gbit POP i Amsterdam, fremføres fuldt redundant, modsat tidligere nul-redundans.

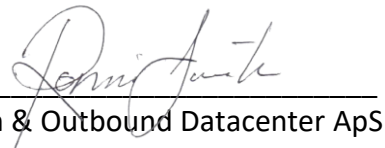


D) HTTPS TCP og HTTP TCP protokollen skærpes og optimeres i iODCs' Anti-DDoS software og hardware, placeret i Amsterdam POPs.
E) ICMP TCP og UDP forbydes i yderligere 2 hop, til og fra iODC netværk, således at linknet IP adresser ikke kan opsnappes uanset fejl begået pr automatik, eller manuelt.
F) iODC advarselssystem rekonstrureres til, at blive et såkaldt early-warning, proaktivt system der ved hjælp af regler og systemiske mekanismer, skal give iODC varsling om anormalitet til- og fra netværket.
G) Switche i 2. lag udskiftes til nyere Brocade switche, samt fremføres disse vha, LACP til vores 3. lag kantswitche. Hermed tages alle enkelte punkter for fejl (single points of failures), ud af kredsløb. Dato for dette er endnu ukendt, men vil ske i Q4 2017.
H) Særlig kundeportal oprettes for kunder med adgang til iODC Anti-DDoS systemer, således at kunder selv kan opstiller særlige regler for trafik, beskyttelse og netværksruter.
I) Alle kunder modtager fremadrettet automatisk e-mail advisering, når/hvis disse bliver udsat for DDoS angreb, uanset varighed, volumen og applikation angrebet, samt når angrebet er slut.
J) 2 IP adresser med dansk oprindelse, overgives til Dansk Politi, sammen med alt logningsmateriale.

////// INTET FØLGER //////

iODC ApS
Arn. Nielsens Blv. 62B-C
2650 Hvidovre
Telefon: +45 70 27 05 05
E-Mail: support@iodc.dk
Web: https://www.iodc.dk

Hvidovre d. 07/10-2017



In & Outbound Datacenter ApS
Arnold Nielsens Boulevard 62B-C
2650 Hvidovre