Priperem mo Ansa long ol denial-of-service atak

Fas pablis: Septemba 2011
Las apdeit: Maj 2025

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Te Tira Tiaki
Government Communications Security Bureau

National Cyber Security Centre
PART OF THE GCSB

Introdaksen

Pablikesen ya i bin stat tru long Australian Signals Directorate (ASD) we i wok wetem New Zealand's National Cyber Security Centre (NCSC-NZ), Akamai Technologies Ltd mo Cloudflare Pty Ltd, blong rispon long wan rod we i stap kam bigwan long saet blong denial-of-service (DoS) atak insaed long rijen blong yumi. Hemi givim gaed long ol oganaesesen blong oli mekem ol bes praktis we i beis long ol niu tret tradkraf, blong pripea from mo rispon long ol DoS atak.

Mifala i rekomendem se yu ridim advaes ya we i joen wetem ASD's *Internet of Things devices* mo *Secure your Wi-Fi and router* pablikesen. Ol pablikesen ya oli helpem wanwan man blong avoidem blong no mestem blong kontribut long DoS atak we i spolem ol narawan.

DoS atak oli ol saebaatak we oli disaenem blong spolem o putumdaon onlaen seves olsem ol websaet, imel mo Domain Name System (DNS) seves, blong no givim akses long tru yusa. Hemia oli kasem taem oli mekem fulap onlaen seves wetem data, ol koneksen o rikwes blong ovarem seves mo putumdaon ol fangsen blong hem.

DoS atak i rikwaerem wan bigfala namba blong netwok trafik blong save kat sakses. Oli stap kam blong kam bigwan, from wan bigfala namba blong Internet of Things (IoT) divaes we oli agri long hem. Olsem ol IoT bisnes oli rangem yusa eksperiens fastaem ova long saebasekiuriti, ol device we i no safe we hemi ol nomol samting blong haos we i konek long intanet olsem smat TV, ketel, vakium klina mo sekiuriti sistem. Ol divaes ya ol rabis akta oli save spoilem mo krietem wan 'botnet' blong ol divaes we i blong jeneretem netwok trafik, we i save end ap long wan oganaesesen mo kontribiut long infrastrakja we i alawem DoS atak blong i tekem ples.

Ol aktiviti we oli pas oli soem se long wan taem ol saebakriminol oli bin agri blong mekem wan bigfala namba blong IoT divaes, oli save rentem or salem infrastrakja ya long ol saeba kriminol mo hakka, we oli stap kat fulap interes blong mekem DoS atak agensem taget we oli jusum. Long fulap keis, DoS atak oli mekem blong kosem wan oganaesesen prodaktiviti mo faenensol los, o blong kasem atensen blong pablik. Wan eksampol blong aktiviti ya oli diskraebem long ASD's *People's Republic of China-linked actors compromise routers mo IoT divaes blong botnet operesen* advaesori.

Olsem ekonomi blong yumi i stap gohed blong kamap, mo namba blong ol pua sekiua IoT divaes we i konek lo intanet i gro, ol DoS atak bae oli kontinu blong kam bigwan.

Blong stopem o putumdaon wan onlaen seves blong wan oganaesesen, rabis akta oli yusum sam defren rod blong giaman, we i kat:

- daerektem wan bigfala namba blong ol rabis netwok trafik long wan onlaen seves long wan tingting blong kakae evri netwok we i avelebol.
- lidim wan naes netwok trafik long wan onlaen seves long wan tingting blong kakae ol kompiuta proses risos blong olgeta.
- Yusum plante defren kompiuta, IoT divaes mo ol nara intanet-konek divaes blong daerektem netwok trafik long wan onlaen seves we i kam long plante daerekesen mo long wan bigfala skel, wan nomol kaen DoS atak we oli rifea long hem olsem DoS we i brok aot long (DDoS) atak.
- haejakem wan oganaesesen domen rejistresen o DNS seva long wan kraem blong daerektem bakegen ol yusa i go longwe long onlaen oganaesesen seves.

Oganaesesen i no save avoidem blong stap olsem wan taget long DoS atak, be i kat namba blong ol samting we oganaesesen i save mekem blong pripea from mo mekem i go daon namba blong ol impak. Stap pripea from ol DoS atak bifo oli kam hemi gud wei ya nao we yumi wok long hem, from taem yumi no pripea, bae hemi had mo i no efektif blong rispon long taem blong wan DoS atak.

I no mata se ol oganaesesen oli fokas long protektem olgeta wan long ol DoS atak, olgeta i sud tekem step ya tu blong protektem ol onlaen seves mo intanet-konek divaes we ol saeba kriminol oli bin spoilem blong tagetem ol narawan.

Pripea blong ol DoS atak

Long konteks blong wan hae volium blong DoS atak we i stap krosem rijen blong yumi, bifo oli mekem wan rod blong pripea from DoS atak, oganaesesen blong yu i mas feswan asesem bisnes rikao blong save sapos evri wan long ol onlaen seves blong yu i mas kontinu long taem blong ol DoS atak, o sapos eni temporari intarapsen blong seves oli akseptem.

Sapos oganaesesen blong yu i wantem blong kam antap long paoa blong stanap agensem ol DoS atak, yu sud folem mo mekem olting ya, long stret rod mo praktisim, long taem we DoS atak i stap tekem ples.

- Sapos oganaesesen blong yu i stap yusum wan content delivery network (CDN), yu sud mekem ol samting ya bakegen, sapos i gat nid from.
  - Lukluk blong yusum wan CDN we hemi ingkludum fangsen blong protektem ol web seva blong yu long ol defren aplikesen mo netwok leiya atak- sam CDN maet oli gat ol sem fasin olsem pat blong wan web aplikesen faeawol long en.
  - Avoidem ol aneseseri pablik samting we i save soem wan orijinol web seva Internet Protocol (IP) adres mo mekem sua se eni samting we oli soem long pablik oli protektem long ol DoS atak.
  - Avoidem blong yusum wan IP adres blong web seva blong yuwan we ol rabis akta oli save gesem, eksampol, wan IP adres long semak netwok sabnet we i soem long pablik IP adres blong onlaen seves blong yu.
  - Yusum netwok akses kontrol (olsem wan faeawol) blong mekem sua se CDN mo oganaesesen we i gat atoriti manejemen netwok i save aksesem web seva blong yu.
  - Tingting blong yusum ol defren netwok konektiviti, we hemi ingkludum praevet netwok konektiviti, long medel blong web seva blong yu mo CDN provaeda blong yu, sapos yu nidim wan level blong proteksen we i bigwan blong web seva blong yu.
  - Arenjem CDN, orijinol web seva mo klaen HTTP heda blong i mekem i kam gud namba blong storej we oli bin mekem finis.
  - Tingting blong divaedem ol web seva blong mekem se rikwes we i lo i kam long ol risk IP adres blong oli save handelem seperet long rikwes we i kat hae IP adres, sapos yu nidim wan bigfala level blong avalebiliti.
- Talem stret wanem fangsen mo kwaliti blong seves oli aksepetem blong ol yusa we yu akseptem oli save yusum onlaen seves blong yu, hao blong mentenem fangsen ya, mo wanem fangsen oli no nidim long taem blong ol DoS atak.

- Kasem mo yusum wan Cloud-based DoS atak mitigesen seves.
- Lukluk blong katemdaon atak ples blong oganaesesen blong yu:
  - yusum ol nara Onlaen seves (olsem DNS) blong mekem i luk gud seves provaeda we oli save stanap agensem ol DoS atak
  - seperatem ol kritikol onlaen seves (olsem imel) long ol nara onlaen seves we olgeta nao oli makem gud olgeta (olsem ol websaet)
  - mekem sua se DoS atak mitigesen seves i alaoem netwok trafik nomo we i go wetem ol onlaen seves netwok pot.
- Tokbaot wetem seves provaeda blong yu ol ditel blong DoS atak blong olgeta mo hao oli stopem mo ol mitigesen plan, speseli olgeta:
  - paoa we oli kasem blong stap agensem ol DoS atak raon long wol
  - oli bin soem wan histri blong hao oli save handelem tugeta ol DoS atak mo oli andastanem ol DoS atak we oli givim atoroti long olgeta
  - paoa blong stopem plante defren DoS atak witaot yuman involvmen, olsem manuol analaesis blong netwok trafik
  - atak long praes blong seves blong olgeta, olsem se weta kos hemi fiks o no hemi beis long defren amaon blong ol netwok trafik mo kompiuta we oli yusum, mo blong luk sapos yu save setem bil long wan limit
  - stat blong letem yu o ofem ol onlaen seves blong olgeta long taem blong ol DoS atak
  - pri-apruv aksen we i save hapen long taem blong DoS atak
  - arenjmen blong prevensen blong DoS atak wetem ol apstrim provaeda.
- Yusum ol samting blong didektem ol DoS atak, olsem ril-taem monita mo alet avelebol sistem, netwok trafik, kompiuta proses risos, mo ol kos blong hem.
- Priperem wan slo vesen blong websaet blong yu we i nidim smol proses taem mo banwit blong sevem kontinu seves long taem blong ol DoS atak.
- Kasem mo yusum wan onlaen seves we i strong mo i gat wan bigfala banwit, wan kompiuta we i save prosesem ol risos, save faenem ol host lokesen mo i gat klaod beis trafikat klinap blong oli save karemaot ol netwok trafik we oli no wantem- hemia evri taem i yusum tu wan stret CDN blong fandem slo websaet konten mo protektem web orijin seva long netwok trafik we oli no wantem.
- Protektem domen nem blong oganaesesen blong yu taem yu yusum rejista loking, konfemem domen rejistresen kontak ditel mo ol nara ditel oli stret, mo folem sam moa gaed we oli aotlaenem long ASD *Domain Name System sekiuriti blong ol domen ona* pablikesen.
- Mentenem wan apdeit kondak ditel blong seves provaeda blong yu mo serem ol kondak ditel blong oganaesesen blong yu wetem olgeta, mekem se evri kondak i avelebol beis long oganaesesen rikwaemen blong yu, eksampol, 24 haoa long wan dei, 7 dei long wan wik.
- Provaedem oganaesesen blong yu ol aot long ban kondak ditel blong wan ones komunikesen janel long seves provaeda blong yu, blong taem nomol komunikesen janel oli fel.
- Developem, implementem mo mentenem wan saeba sekiuriti insiden rispons plan, we i kavremap ol defren taep blong DoS atak agensem wan long ol onlaen seves we i rikwaemen blong stanap agensem ol DoS atak, mo eksesaesem plan ya evri yia.
- Krietem aplikesen blong protektem ol nomol abius fangsen we oli kakae bigfala kompiuta proses risos o we oli kasem moa faenansol kos (olsem sendem wan SMS mesej).
  - Proteksen i kat tu ret limit mo save konfemem sapos rikwes hemi kam long wan yuman.
  - Ranem tes atak blong DoS ingkludum ol taget blong impropa logik reit long aplikesen we i wok.
  - Mekem broda lod blong tes blong oli aedentifaem mo korektem ol DoS ejen.

Rispon long ol DoS atak

Sapos oganaesesen blong yu i no pripea from ol DoS atak, yu save traem blong mekem sam aksen antap ya long taem blong DoS atak, maet oli no strong mo i tekem taem blong mekem, mekem se paoa blong oganaesesen i slo blong rispon.

Oganaesesen blong yu i sud mekem ol aksen ya long taem blong ol DoS atak, we oli stret mo praktikol.

- Enfosem saeba sekiuriti rispons plan blong yu.
- Askem ol seves provaeda blong yu sapos oli save hariap blong ranem ol risponsif aksen-sapos yu no bin tokbaot fastaem paoa blong olgeta blong rispon, maet bae yu faenemaot se oli no save o no wantem mekem blong rispon, o oli jajem ekstra fi.
- Stopem fangsen blong no-impoten fangsen o karemaot no-impoten konten long ol onlaen seves blong yu we i mekem karen DoS atak i strong, eksampol, putum wan vesen blong websaet blong yu witaot sej fangsen, mo naes konten o bigfala fael.
- Mentenem komunikesen wetem ol kastoma mo seves provaeda, ingkludum ol DoS atak mitigesen seves provaeda, mo gohed blong monitarem avelabiliti blong onlaen seves blong yu.
- Tingting blong jenisim IP adres blong orijin web seva sapos hemi tagetem stret, mo stopem pablik disklosa blong niu IP adres, witaot eni proteksen long ples.
- Ripotem DoS atak long ol stret pati, we i gat tu ASD mo NCSC-NZ olsem wan 'Kondak ditel' seksen long pablikesen ya.

Avoidem blong kontribiut long ol DoS atak

Oganaesesen blong yu i mas stat folem olgeta samting ya blong no kontribiut long DoS atak we i save spolem ol narawan.

- No soemaot ol seves, ol IoT divaes mo ol nara divaes we i konek long intanet we i no nid, we oli disaenem gud o no mentenem gud.
- Wetem gud sekiuriti, mentem mo monitarem seves, IoT divaes mo ol nara divaes we i konek long intanet we oli soemaot long intanet.
  - Sam moa gaed blong ol smol bisnis hemi avelebol long ASD *Internet of Things devices* mo *Secure your Wi-Fi and router* pablikesen.

Sapos oganaesesen i stap ranem wan onlaen seves, yu sud tekem olgeta mesa ya.

- Putum faswan ol riviu protokol we oli aotlanem long United States' Cyber Security mo Infrastructure Security Agency's (CISA) *UDP-Based Amplification Attacks* advaes.
- Lukluk gud wan amplifikesen ejen taem oli aedentifaem mo sekiurem onlaen seves blong yu agensem olgeta.
- Setemap tugeta inbaon mo aotbaon netwok akses kontrol blong limitem akses long ol otoraes onlaen seves mo oganaesesen.
- Blokem ol pablik akses we oli nogat nem blong amplikesen-pron onlaen seves we oli no nidim.
- Tingting blong mekem wan reit limit wok blong daonem ol risal blong abius, sapos yumi blokem o aplaem ol akses kontrol we i no posibol o stret.

Moa infomesen

ASD *Infomesen sekiuriti manuol* hemi wan sekuriti framwok we ol oganaesesen oli save aplae blong protektem ol sistem mo ol data blong olgeta long ol saebatret. Advaes insaed long *Strategies to mitigate cyber security incidents*, folem wetem Essential Eight, oli helpem fremwok ya.

New Zealand Information Security Manual hemi manuol blong New Zealand Government long infomesen asurens mo infomesen sistem sekiuriti. Hemia hemi wan profesonol manuol we oli disaenem blong mitim ol nid blong ol ejensi infomesen sekiuriti eksekutif mo tu ol venda, kontrakta mo konsalten we oli provaedem ol seves i go long ol ejensi.

Sam moa infomesen long plante defren taep blong DoS atak i avelebol long CISA's *DDoS Quick Guide* mo *Understanding and Responding to Distributed Denial-Of-Service Attacks* pablikesen.

Kondak Ditel

Long Australia, sapos yu gat eni kwestin abaot ol gaedlaen ya *raet i go long ASD* o kolem 1300 CYBER1 (1300 292 371).

Long New Zealand, blong ripotem wan saeba sekiuriti insiden imelem incidents@ncsc.govt.nz o visitem NCSC-NZ's Report an incident webpej.

Disklema

Tul insaed long gaed ia hem i jenerol mo man i no mas tekem olsem likol advaes o dipen long hem blong helpem hem long eni taem o imejensi situesen. Long eni impoten mata, yu mas lukaotem stret independen profesenol advaes long saed blong ol situesen blong yuwan.

Commonwealth hem i no akseptem responsabiliti o laeabiliti blong eni damej, lus o ekspens we man i kasem olsem wan risal blong dipen long infomesen we i stap insaed long gaed ia.

Yus blong Coat of Arms

Ditel blong ol kondisen we man i mas folem blong yusum Coat of Arms hem i stap long Department of the Prime Minister and Cabinet websaet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Blong kasem moa infomesen, o blong ripotem wan saeba sekiuriti insiden, kondaktem mifala:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Namba ia hem i avelebol blong yu yusum insaed long Ostrelia nomo.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre