Mekim yu yet redi na wei bilong kam bek taim yu kisim ol denial-of-service attack

Nambawan taim ol pablisim: September 2011
Lastaim ol mekim senis: March 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

Introduction (Tok Go Pas)

Australian Signals Directorate (ASD) wok klostu wantaim National Cyber Security Centre (NCSC-NZ) bilong New Zealand, Akamai Technologies Ltd na Cloudflare Pty Ltd long kamapim dispela pablikesin long givim helpim, taim ol luksave olsem planti moa denial-of-service (DoS) attack wok long kamap long region bilong yumi. Dispela em helpim ol organisation wantaim ol best practice mitigation, o rot, we ol yusim contemporary threat tradecraft, long redim ol yet na ken kam bek taim ol kisim ol DoS attack.

Mipela tok strong long ridim dispela advice, o toksave, wantaim ol dispela pablikesin *Internet of Things devices* na *Secure your Wi-Fi and router* bilong ASD. Ol dispela pablikesin em helpim ol manmeri long luksave na abrusim ol rot bilong helpim ol DoS attack we em ken bringim birua long ol arapela manmeri.

Ol DoS attack em ol cyberattack, o birua, ol kamapim long brukim o bagarapim ol online service olsem ol website, email na Domain Name System (DNS) service, long stopim ol trupela user long yusim ol service. Dispela em save kamap taim ol pulmapim ol online service na salim planti data, ol connection o request na dispela ken brukim o bagarapim wok bilong ol dispela service.

Ol DoS attack mas yusim bikpela network traffic tru long kamapim dispela birua. Ol dispela attack, o birua, wok long kamap moa nau, na em bikos gat planti moa ol Internet of Things (IoT) device em ol ken kalap go insait na yusim long ol dispela kain attack. Na bikos ol IoT manufacturer save putim user experience go pas long cybersecurity, ol dispela device em ol samting yu save yusim long haus bilong yu olgeta taim na save connect long internet olsem ol smart TV, kettle, vacuum cleaner na security system. Ol dispela device em ol malicious actor, o birua manmeri, ken stap long narapela hap na kalap go insait long ol na kamapim 'botnet' wantaim ol dispela device na yusim long salim dispela bikpela network traffic, na dispela em min olsem ol household na ol organisation ken helpim ol dispela DoS attack tasol ol no luksave olsem dispela samting wok long kamap.

Ol kain activity olsem kamap nau soim olsem taim ol dispela malicious actor kalap go insait long planti ol IoT device, ol ken traim salim dispela infrastructure long ol cybercriminal na ol hacktivist, husait gat bikpela tingting long mekim DoS attack long wanem target ol laik. Long planti bilong ol dispela case, ol DoS attack kamap long traim bringim hevi long organisational productivity na kamapim financial loss, or long bringim public attention long cause bilong ol. Wanpela kain activity olsem em ol toktok long em insait long dispela advisory bilong ASD *People's Republic of China-linked actors compromise routers and IoT devices for botnet operations*.

Taim economy bilong yumi wok long kamap moa digital na planti moa bilong ol dispela IoT device wok long connect go long internet, ol DOS attack wok long kamap planti moa.

Long brukim o bagarapim ol online service bilong wanpela organisation, ol malicious actor o birua bai yusim ol kain samting olsem:

- salim bikpela namba bilong network traffic go long ol online service long traim kisim olgeta network bandwidth
- salim network traffic go long ol online service long traim kisim olgeta computer processing resource
- yusim planti computer, IoT device o ol arapela device em connect wantaim internet long salim planti kain network traffic long ol online service em ken kam long planti hap na em bikpela moa, dispela kain DoS attack em ol kolim distributed DoS (DDoS) attack
- stilim domain registration o DNS server long traim senisim rot bilong ol trupela user go long ol arapela hap na no long online service bilong organisation.

Ol organisation bai no inap long pasim ol yet long kamap target bilong DoS attack, tasol gat ol rot organisation ken bihainim long redim ol yet na traim rausim hevi bilong ol dispela attack. Long redim yu yet pastaim long ol DoS attack kamap em gutpela rot tru bilong bihainim, em bikos em hat tru long kam bek taim DoS attack wok long kamap.

Ol organisation save lukluk pastaim long banisim ol yet long ol DoS attack, na tu ol mas mekim wok long strongim ol online service bilong ol na ol device save connect long internet long traim stopim ol malicious actor long yusim ol dispela samting long bagarapim ol arapela organisation.

Redim yu yet long ol DoS attack

Long taim we ol DoS attack wok long kamap planti taim moa long region bilong yumi, bipo long mekim ol samting long redim yu yet long ol DoS attack, organisation bilong yu mas pastaim tru sekim ol business requirement bilong em long luksave sapos ol online service bai sanap yet taim DoS attack kamap, o sapos ol temporary service bai orait.

Sapos organisation bilong yu laik strongim em yet long ol DoS attack, yu mas wok hat long mekim ol dispela samting, sapos em inap long mekim, bipo long ol DoS attack kamap.

- Sapos organisation bilong yu save yusim wanpela content delivery network (CDN), yu mas mekim ol dispela samting tu, sapos yu inap long mekim, long strongim yu yet.
  - Lukluk gut long CDN yu yusim olsem em ken banisim origin web server bilong yu long ol kainkain application na network layer attack – sampela CDN gat dispela ol samting wantaim web application firewall em insait long em.
  - Noken mekim bikpela toksave long Internet Protocol (IP) address bilong origin web server bilong yu, na tu yu mas banisim yu yet gut long ol DoS attack sapos ol birua painim aut IP address bilong yu.
  - Noken yusim wanpela IP address long origin web server bilong yu we ol malicious actor ken painim, kain olsem, wanpela IP address em stap long wankain network subnet olsem ol IP address bilong ol online service bilong yu we em isi long painim.
  - Yusim ol network access control (kain olsem wanpela firewall) long larim CDN na ol authorised management network bilong organisation bilong yu tasol kalap go insait long origin web server bilong yu.
  - Tingting long yusim ol kainkain strongpela network connectivity, em kain olsem ol private network connectivity, long origin web server bilong yu go long CDN provider bilong yu, sapos yu laik gat strongpela banis long origin web server bilong yu.
  - Strongim CDN, origin web server na ol client HTTP header bilong yu taim yu lukluk gut long hamas caching ol mekim.

  - Tingting long mekim ol partition, o brukim, origin web server bilong yu we em ken lukluk long ol lower risk IP address long wanpela hap na lukluk long ol higher risk IP address long arapela hap, sapos yu laik strongim origin web server bilong yu.

- Mekim klia long wanem kain functionality na quality bilong service em ol trupela user bilong ol online service bilong yu bai hamamas wantaim, rot bilong strongim dispela functionality, na wanem ol functionality em ol no nidim taim DoS attack kamap.
- Kisim na yusim wanpela cloud-based DoS attack mitigation service.
- Tingting long strongim organisation bilong yu long ol attack sapos yu:
  - givim ol foundational online service (kain olsem DNS) long ol service provider husait save gut long ol dispela service na ken sanap strong taim ol DoS attack kamap
  - mekim partitioning, o brukim, ol critical online service (kain olsem email) long ol arapela online service em ol birua bai traim long bagarapim (kain olsem ol website)
  - lukluk gut olsem ol DoS attack mitigation service bilong yu em larim network traffic em kam long ol network port bilong online service bilong yu tasol.
- Toktok wantaim ol service provider bilong yu long ol DoS attack prevention na mitigation strategy, o rot, ol save bihainim olsem:
  - ol samting ol gat pinis em ken mekim ol sanap strong taim ol DoS attack kam long olgeta hap long world
  - ol ken soim olsem taim ol DoS attack kamap bipo ol inap stopim na ol gat ol comprehensive authorised DoS attack testing tu
  - ol gat wei bilong luksave na sanap strong taim planti ol DoS attack kam we ol no nidim ol manmeri long mekim samting, kain olsem ol analysis bilong network traffic
  - rot bilong mekim ol price long service bilong ol, kain olsem sapos cost em wankain tasol o em save senis taim gat senis long hamas network traffic na ol computer processing resource yu yusim, na sapos yu ken mekim billing limit
  - wanem taim stret bai ol toksave long yu o tanim off ol online service taim DoS attack kamap
  - ol action yu tok orait long em bipo taim em ol bai mekim taim DoS attack kamap
  - ol prevention arrangement ol gat wantaim ol upstream provider taim DoS attack kamap
- Mekim ol samting long luksave long ol DoS attack, kain olsem real-time monitoring na ol alert bilong system availability, network traffic, computer processing resource, na ol cost em kam wantaim ol dispela samting.
- Redim wanpela static version bilong website bilong yu em bai no nidim planti processing na bandwidth long helpim service bilong yu stap yet taim DoS attack kamap.
- Kisim na yusim ol strongpela online service wantaim bikpela bandwidth, planti computer processing resource, em stap long kainkain ol hosting location na cloud-based traffic scrubbing long pasim ol network traffic em no gutpela – dispela em save yusim ol gutpela CDN long holim ol static website content na banisim origin web server bilong yu long ol network traffic yu no laikim.
- Banisim ol domain name bilong organisation bilong yu wantaim registrar locking, stretim gut ol domain registration contact details na ol arapela details, bihainim ol guidance, o helpim, em stap long *Domain Name System security for domain owners* pablikesin bilong ASD.
- Sekim olsem ol contact details bilong ol service provider bilong yu em stret na toksave long ol tu long contact details bilong organisation bilong yu, na tu ol contact mas stap taim ol laik givim toksave long wanem taim long dei em organisation makim, kain olsem 24 aua long wanpela dei, sevenpela dei long wanpela wik.
- Givim ol out-of-band contact details bilong organisation bilong yu we em yusim gutpela rot bilong communication long ol service provider, taim ol normal rot bilong communication em bagarap.

- Kamapim, mekim na lukautim wanpela cybersecurity incident response plan, em karamapim ol samting olsem kainkain ol DoS attack em ol online service bilong yu bai mas sanap strong tai mem kamap, na traim ol exercise bilong bihainim dispela plan olsem wanpela taim long olgeta yia.
- Mekim ol application long banisim ol functionality em ol birua save yusim planti taim na em save yusim planti computer processing resource o em save mekim yu baim planti moni (kain olsem long salim ol SMS message).
  - Ol kain banis em olsem rate limiting na sekim gut olsem request em kam long ol manmeri tru.
  - Mekim ol DoS attack testing olsem yu lukluk long improper logic flow long application functionality.
  - Mekim ol bikpela load testing long luksave na stretim ol DoS vector.

Wei bilong kam bek taim yu kisim DoS attack

Sapos organisation bilong yu em no redim em yet long ol DoS attack, yu ken traim long bihainim ol dispela samting ol toktok long em antap taim DoS attack kamap, tasol sampela taim dispela em bai no inap long helpim yu and bai yu nidim taim long mekim, na dispela em ken daunim strong bilong organisation long sanap.

Organisation bilong yu mas bihainim ol dispela samting taim DoS attack kamap, sapos ol inap long mekim.

- Bihainim cybersecurity incident response plan bilong organisation bilong yu.
- Askim ol service provider bilong yu sapos ol inap mekim ol responsive actions hariap tasol – sapos yu no toktok wantaim ol bipo long strong bilong ol mekim dispela samting, yu ken painim olsem ol bai no inap long helpim yu, o bai askim yu long baim ol additional fee.
- Stopim ol non-vital functionality o rausim ol non-vital content long ol online service we em ken givim strong ol wanem DoS attack em kamap, kain olsem, putim website em nogat search functionality, ol dynamic content o ol bikpela file.
- Lukautim communication wantaim ol customer na ol service provider bilong yu, em tu wantaim DoS attack mitigation service provider bilong yu, na go het long sekim availability bilong ol online service bilong yu.
- Tingting long senisim IP address bilong origin web server bilong yu sapos ol birua wok long traim bagarapim, na noken mekim bikpela toksave long niupela IP address bilong yu sapos yu no sanapim ol banis long lukautim.
- Toksave long ol DoS attack long ol organisation em ken helpim yu, kain olsem ASD na NCSC-NZ aninit long ol 'Contact details' section long dispela pablikesin.

Traim long noken helpim ol DoS attack

Organisation bilong yu mas bihainim ol dispela samting long helpim ol luksave na noken helpim ol DoS attack we em ken bringim bagarap long ol arapela manmeri.

- Traim long noken soim ol service, IoT device na ol arapela device em save connect go long internet em yu no nidim, em nogat strongpela banis o em ol no lukautim gut.

- Strongim gut, lukautim na sekim ol service, IoT device na ol arapela device em save connect go long internet em ol ken painim long internet.
  - Sampela moa guidance, o helpim, bilong ol liklik business em stap long ol dispela pablikesin bilong ASD *Internet of Things devices* na *Secure your Wi-Fi and router*.

Sapos organisation bilong yu gat ol online service, yu mas mekim ol dispela samting.

- Mekim olsem bikpela samting ol review bilong ol protocol em ol makim insait long dispela advice *UDP-Based Amplification Attacks* bilong United States' Cybersecurity and Infrastructure Agency (CISA).
- Sekim na luksave long ol niupela amplification vector taim ol tokaut long ol na strongim ol online service bilong yu long ol dispela birua.
- Strongim ol inbound na outbound network access controls long larim ol authorised online service na organisation tasol long kalap go insait.
- Pasim anonymous public access long ol online service em ken bringim bikpela moa birua sapos yu no nidim.
- Tingting long putim wanpela rate-limiting mechanism long daunim hevi em ken kamap taim yu painim birua, sapos yu no inap long pasim o putim ol access control long stopim birua.

Sampela moa infomesin

Information security manual bilong ASD em wanpela cybersecurity framework em ken helpim ol organisation long banisim na strongim ol system na data bilong ol long ol cyberthreat o birua. Ol advice stap insait long *Strategies to mitigate cybersecurity incidents*, na tu long Essential Eight, em wok gut tru wantaim dispela framework.

New Zealand Information Security Manual em manual bilong New Zealand Government long information assurance na information systems security. Dispela em olsem manual bilong ol practitioner, o manmeri save wokim dispela wok, em ol kamapim long helpim ol agency information security executive wantaim ol vendor, contractor na consultant husait save givim service long ol dispela agency.

Sampela moa infomesin long ol kainkain DoS attack em stap long ol dispela pablikesin bilong CISA *DDoS Quick Guide* na *Understanding and Responding to Distributed Denial-Of-Service Attacks*.

Contact details (Rot bilong painim o toktok wantaim mipela)

Long Australia, sapos yu gat ol askim long dispela guidance o toksave *rait go long ASD* o ringim 1300 CYBER1 (1300 292 371).

Long New Zealand, sapos yu laik ripotim ol cybersecurity incident o birua, salim email long incidents@ncsc.govt.nz o go long webpage Report an incident bilong NCSC-NZ.

Disclaimer

Ol samting stap insait long dispela guide o toksave em karamapim ol bikpela tingting na yu mas noken kisim olsem legal advice o yusim long helpim yu long olgeta kain hevi. Sapos yu nidim helpim long ol bikpela samting, toktok wantaim wanpela independent professional o save manmeri long dispela samting na bai ol i ken helpim yu.

Commonwealth em bai no nap luksave o helpim yu taim ol samting bruk o yu lusim moni sapos yu bihainim ol infomesin stap long dispela guide o toksave.

Copyright

Wei bilong yusim Coat of Arms

Wei bilong yusim dispela Coat of Arms em stap long website bilong Department of the Prime Minister and Cabinet Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Sapos yu laik painim sampela moa infomesin, o yu laik ripotim cyber security birua o taim samting olsem kamap, toksave long mipela:

cyber.gov.au | 1300 CYBER1 (1300 292 371)
Dispela namba bai yu ken yusim insait long Australia tasol.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre