Paghahanda para sa at pagtugon sa mga denial-of-service na pag-atake

Unang nailathala: Setyembre 2011
Huling na-update: Marso 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

Panimula

Ang publikasyong ito ay binuo ng Australian Signals Directorate (ASD) sa pakikipagtulungan sa New Zealand's National Cyber Security Center (NCSC-NZ), Akamai Technologies Ltd at Cloudflare Pty Ltd, bilang tugon sa tumaas na denial-of-service (DoS) na pag-atake sa ating rehiyon. Nag-aalok ito ng patnubay sa mga organisasyon para sa pinakamahuhusay na pagsagawa ng pagpapagaan o mitigasyon batay sa kontemporaryong tradecraft threat, upang makapaghanda at tumugon sa mga pag-atake ng DoS.

Inirerekomenda naming basahin ang payong ito kasabay ng *mga Internet of Things device* ng ASD at *I-secure ang iyong Wi-Fi at router* na mga publikasyon. Ang mga publikasyong ito ay tumutulong sa mga indibidwal na maiwasan ang hindi sinasadyang pag-ambag sa mga pag-atake ng DoS na maaaring makaapekto sa iba.

Ang mga pag-atake ng DoS ay mga cyberattack na idinisenyo upang guluhin o sirain ang mga online na serbisyo tulad ng mga website, email at mga serbisyo ng Domain Name System (DNS), upang tanggihan ang access sa mga lehitimong user. Ito ay karaniwang nakakamit sa pamamagitan ng pagdagsa ng mga datos, mga koneksyon o mga kahilingan sa isang online service upang mapuno ang serbisyo at masira ang paggana (functionality) nito.

Ang mga pag-atake ng DoS ay karaniwang nangangailangan ng malaking dagsa ng traffic sa network upang maging matagumpay. Ang mga ito ay nagiging mas karaniwan dahil sa pagtaas ng bilang ng mga madaling makompromiso na Internet of Things (IoT) device. Dahil madalas na inuuna ng mga manufacturer ng IoT ang user experience kaysa sa cybersecurity, ang mga vulnerable na device ay maaaring magsama ng mga regular na gamit sa bahay na kumokonekta sa internet gaya ng mga smart TV, kettle, vacuum cleaner, at security system. Ang mga device na ito ay kadalasang maaaring malayuang makompromiso ng mga malicious actor upang lumikha ng isang 'botnet' ng mga device kung saan bubuo ng trapiko sa network na ito, na maaaring magresulta sa mga sambahayan at organisasyon na hindi sinasadyang mag-ambag sa imprastraktura na magbibigay-daan sa mga pag-atake ng DoS.

Ipinapahiwatig ng kamakailang aktibidad na kapag nakompromiso na ng mga malicious actor ang malaking bilang ng mga IoT device, maaari nilang arkilahin o ibenta ang imprastraktura na ito sa mga cybercriminal at hacktivist, na higit na interesadong magsagawa ng mga pag-atake ng DoS laban sa mga target na kanilang pinili. Sa karamihan ng mga kaso, ang mga pag-atake ng DoS ay ginagawa upang magsanhi ng pagkawala ng pagiging produktibo at ng pananalapi ng isang organisasyon, o upang makuha ang atensyon ng publiko para sa isang ipinaglalabang dahilan. Ang isang halimbawa ng ganitong aktibidad ay inilalarawan sa advisory ng ASD na *People's Republic of China-linked na mga actor ay nagkompromiso sa mga router at IoT device para sa mga pagpapatakbo ng botnet*.

Habang patuloy na nagdi-digitise ang ating ekonomiya at lumalaki ang bilang ng mga IoT device na hindi gaanong secured na konektado sa internet, malamang na patuloy na tataas ang mga pag-atake ng DoS.

Upang guluhin o sirain ang mga online na serbisyo ng isang organisasyon, gumagamit ang mga malicious actor ng ilang paraan, kabilang ang:

- pagdidirekta ng malaking dami ng di-ginustong network traffic sa mga online na serbisyo sa pagtatangkang ubusin ang lahat ng magagamit na bandwidth ng network
- pagdidirekta ng iniangkop na network traffic sa mga online na serbisyo sa pagtatangkang ubusin ang kanilang mga computer processing resource
- gumagamit ng maraming mga computer, IoT device o iba pang device na nakakonekta sa internet upang idirekta ang network traffic sa mga online na serbisyo mula sa maraming direksyon at sa mas malaking sukat (larger scale), isang karaniwang uri ng pag-atake ng DoS na tinutukoy bilang distributed DoS (DDoS) attack
- pag-hijack sa pagpaparehistro ng domain o mga DNS server ng organisasyon sa pagtatangkang i-redirect ang mga lehitimong user palayo sa mga online na serbisyo ng organisasyon.

Hindi maiiwasan ng mga organisasyon na maging target ng mga pag-atake ng DoS, ngunit may ilang mga hakbang na maaaring ipatupad ng mga organisasyon upang paghandaan at potensyal na mabawasan ang epekto nito. Ang paghahanda para sa mga pag-atake ng DoS bago mangyari ang mga ito ay ang pinakamahusay na diskarte, dahil kung walang paghahanda, mahirap at hindi gaanong epektibo ang pagtugon sa pag-atake ng DoS.

Bagama't pangunahing nakatuon ang mga organisasyon sa pagprotekta sa kanilang sarili mula sa mga pag-atake ng DoS, dapat din silang gumawa ng mga hakbang upang maiwasang maabuso, ang kanilang mga online na serbisyo at mga device na nakakonekta sa internet, ng mga malicious actor upang mag-target ng iba.

Paghahanda para sa mga pag-atake ng DoS

Sa konteksto ng dumaraming pag-atake ng DoS sa ating rehiyon, bago magpatupad ng anumang mga hakbang upang maghanda para sa mga pag-atake ng DoS, dapat munang tasahin ng iyong organisasyon ang mga kinakailangan sa negosyo nito upang matukoy kung ang bawat isa sa iyong mga online na serbisyo ay dapat manatiling gumagana sa panahon ng mga pag-atake ng DoS, o kung katanggap-tanggap ang mga pansamantalang pagkaantala sa serbisyo.

Kung gusto ng iyong organisasyon na mapalakas ang kakayahan nitong makayanan ang mga pag-atake ng DoS, dapat mong aktibong ipatupad ang mga sumusunod na hakbang, kung naaangkop at praktikal, bago mangyari ang mga pag-atake ng DoS.

- Kung gumagamit ang iyong organisasyon ng content delivery network (CDN), dapat mong ipatupad ang mga sumusunod na karagdagang hakbang, kung saan naaangkop at praktikal.
  - Isaalang-alang ang paggamit ng CDN na may kasamang functionality upang protektahan ang iyong pinagmulang web server mula sa iba't ibang mga pag-atake ng application at network layer – maaaring isama ng ilang CDN ang mga feature na ito bilang bahagi ng isang web application firewall.
  - Iwasan ang hindi kinakailangang pampublikong pagsisiwalat (disclosure) ng Internet Protocol (IP) address ng iyong pinagmulang web server, at tiyaking protektado ang anumang mga pagkalantad ng publiko (public exposure) mula sa mga pag-atake ng DoS.
  - Iwasang gumamit ng IP address para sa iyong origin web server na maaaring hulaan ng mga malicious actor, halimbawa, ang IP address sa parehong subnet ng network ng mga IP address na isiniwalat sa publiko ng iyong mga online na serbisyo.
  - Gumamit ng mga kontrol sa pag-access sa network (tulad ng firewall) upang matiyak na tanging ang CDN at ang mga awtorisadong network ng pamamahala ng iyong organisasyon ang makaka-access sa iyong origin web server.

  - Isaalang-alang ang paggamit ng resilient diverse network connectivity na maaaring kabilang ang pribadong network connectivity, sa pagitan ng iyong origin web server at ng iyong CDN provider, kung kailangan mo ng mas mataas na antas ng proteksyon para sa iyong origin web server.
  - I-configure ang CDN, origin na web server, at mga header ng HTTP ng kliyente para ma-optimise ang dami ng ginawang caching.
  - Isaalang-alang ang paghati sa mga origin web server upang ang mga kahilingan mula sa mga lower risk IP address ay hiwalay na pinangangasiwaan sa mga kahilingan mula sa mga higher risk IP address, kung kailangan mo ng mas mataas na antas ng paggamit (availability).
- Tukuyin kung anong functionality at kalidad ng serbisyo ang katanggap-tanggap para sa mga lehitimong user ng iyong mga online na serbisyo, kung paano panatilihin ang functionality na iyon, at anong functionality ang hindi kinakailangan kung may pag-atake ng DoS.
- Kumuha at gumamit ng cloud-based na DoS attack mitigation service.
- Pag-isipang bawasan ang attack surface ng iyong organisasyon sa pamamagitan ng:
  - outsourcing ng mga pangunahing serbisyo sa online (tulad ng DNS) sa mga mapagkakatiwalaang service provider na nakakayanan ang mga pag-atake ng DoS
  - paghahati ng mga kritikal na serbisyo sa online (tulad ng email) mula sa iba pang mga online na serbisyo na mas malamang na ma-target (tulad ng mga website)
  - pagtiyak na pinahihintulutan lamang ng serbisyo ng mitigasyon sa pag-atake ng DoS (DoS attack mitigation service) ang network traffic na nauugnay sa (mga) port ng network ng serbisyong online.
- Talakayin sa iyong mga service provider ang mga detalye ng kanilang mga diskarte sa pag-iwas at mitigasyon sa pag-atake ng DoS, partikular ang kanilang:
  - napatunayang kakayahan na makayanan ang mga pag-atake ng DoS mula sa buong mundo
  - nagpakita ng kasaysayan ng paghawak sa parehong mga pag-atake ng DoS at komprehensibong awtorisadong pag-test sa pag-atake ng DoS
  - kakayahang awtomatikong mabawasan ang karamihan sa mga uri ng pag-atake ng DoS nang walang pakikilahok ng tao, tulad ng manual analysis ng network traffic
  - paraan sa pagpepresyo ng kanilang mga serbisyo, tulad halimbawa kung ang gastos ay pirmihan o nag-iiba ito batay sa dami ng network traffic at mga mapagkukunan (resources) sa pagpoproseso ng computer na ginamit, at kung maaari kang magtakda ng
  - mga limitasyon sa singilin (billing limit thresholds) para sa pag-abiso sa iyo o pag-off ng kanilang mga online na serbisyo kung may pag-atake ng DoS
  - mga paunang inaprubahang aksyon na maaaring isagawa sa panahon ng mga pag-atake ng DoS
  - mga kaayusan sa pag-iwas sa pag-atake ng DoS sa mga upstream provider.
- Magpatupad ng mga hakbang upang makita ang mga pag-atake ng DoS, tulad ng real-time na pagsubaybay at pag-alerto sa availability ng system, network traffic, mga mapagkukunan sa pagpoproseso ng computer, at mga nauugnay na gastos.
- Maghanda ng static na bersyon ng iyong website na nangangailangan ng kaunting pagproseso at bandwidth upang mapadali ang pagpapatuloy ng serbisyo sa panahon ng mga pag-atake ng DoS.
- Kumuha at gumamit ng mga highly resilient na online service na may malaking bandwidth, sapat na mga mapagkukunan sa pagpoproseso ng computer, mga geographically dispersed hosting location at cloud-based na pag-scrub ng traffic upang itapon ang hindi kanais-nais na network traffic – karaniwang kasama dito ang paggamit ng isang matitiwalaang CDN upang i-cache ang static na nilalaman ng website at protektahan ang iyong origin web server mula sa di-ginustong network traffic.
- Protektahan ang mga domain name ng iyong organisasyon sa pamamagitan ng paggamit ng registrar locking, na nagkukumpirma na ang mga detalye ng contact sa pagpaparehistro ng domain at iba pang mga detalye ay tama, at pagsunod sa karagdagang gabay na nakabalangkas sa *seguridad ng Domain Name System para sa mga may-ari ng domain* ng ASD.
- Panatilihing up-to-date ang mga contact detail para sa iyong mga service provider at ibahagi sa kanila ang mga contact detail ng iyong organisasyon, na tinitiyak na available ang lahat ng mga contact batay sa mga kahingian ng iyong organisasyon, halimbawa, 24 na oras sa isang araw, 7 araw sa isang linggo.

- Ibigay ang out-of-band na mga contact detail ng iyong organisasyon para sa isang mapagkakatiwalaang channel ng komunikasyon sa iyong mga service provider, kapag nabigo ang mga normal na channel ng komunikasyon.
- Bumuo, magpatupad at magpanatili ng plano sa pagtugon sa insidente ng cyber security, na sumasaklaw sa iba't ibang uri ng pag-atake ng DoS laban sa bawat isa sa iyong mga online na serbisyo na kinakailangan upang makayanan ang mga pag-atake ng DoS, at gamitin ang plano nang hindi bababa sa taun-taon.
- Mga architect application upang protektahan ang mga karaniwang inaabusong functionality na kumukonsumo ng mas mataas na mapagkukunan sa pagpoproseso ng computer o na nagkakaroon ng karagdagang mga gastos sa pananalapi (tulad ng pagpapadala ng mga SMS message).
  - Kasama sa mga proteksyon ang paglilimita sa rate at pag-verify na ang mga kahilingan ay mula sa isang tao.
  - Magsagawa ng pag-test sa pag-atake ng DoS kasama ang pag-target sa mga improper logic flow sa application functionality.
  - Magsagawa ng mas malawak na pag-test sa load upang matukoy at ma-remediate ang mga vector ng DoS.

Pagtugon sa mga pag-atake ng DoS

Kung hindi naghanda ang iyong organisasyon para sa mga pag-atake ng DoS, maaari mong subukang ipatupad ang ilan sa mga hakbang sa itaas sa panahon ng mga pag-atake ng DoS, kahit na maaaring hindi gaanong epektibo ang mga ito at matagal bago maipatupad, na binabawasan ang kakayahan ng iyong organisasyon na tumugon.

Dapat ipatupad ng iyong organisasyon ang mga sumusunod na hakbang sa panahon ng pag-atake ng DoS, kung saan naaangkop at praktikal.

- Isagawa ang iyong plano sa pagtugon sa insidente ng cyber security.
- Tanungin ang iyong mga service provider kung nagagawa nilang agad na magpatupad ng mga tumutugong aksyon – kung hindi mo pa napag-usapan dati ang kanilang kakayahang tumugon, maaari mong matuklasan na hindi nila magawa o ayaw tumugon, o maningil ng mga karagdagang bayarin.
- I-disable ang non-vital functionality o alisin ang non-vital content mula sa iyong mga online na serbisyo na ginagawang epektibo ang kasalukuyang pag-atake ng DoS, halimbawa, mag-deploy ng bersyon ng iyong website nang walang search functionality, dynamic na content o malalaking file.
- Panatilihin ang komunikasyon sa iyong mga customer at sa iyong mga service provider, kabilang ang iyong DoS attack mitigation service provider, at ipagpatuloy ang pagsubaybay sa availability ng iyong mga online na serbisyo.
- Pag-isipang baguhin ang IP address ng iyong origin web server kung ito ay direktang tina-target, at iwasan ang pampublikong pagsisiwalat ng bagong IP address nang walang mga proteksyon umiiral.
- Iulat ang pag-atake ng DoS sa mga nauugnay na partido, kabilang ang ASD at NCSC-NZ ayon sa seksyong ‘Mga contact detail’ ng publikasyong ito.

Pag-iwas sa pag-ambag sa mga pag-atake ng DoS

Dapat ipatupad ng iyong organisasyon ang mga sumusunod na hakbang upang maiwasan ang hindi sinasadyang pag-ambag sa mga pag-atake ng DoS na maaaring makaapekto sa iba.

- Iwasang ilantad sa internet ang mga serbisyo, IoT device at iba pang device na nakakonekta sa internet na hindi kailangan, hindi secure na na-configure o hindi sapat na namentena.

- Ligtas na i-configure, imentena at subaybayan ang mga serbisyo, IoT device at iba pang device na nakakonekta sa internet na naka-expose sa internet.
  - Ang karagdagang gabay para sa maliliit na negosyo ay available sa *mga Internet of Things device* at *I-secure ang iyong Wi-Fi at router* na mga lathalain.

Kung nagpapatakbo ang iyong organisasyon ng mga online na serbisyo, dapat mong ipatupad ang mga sumusunod na karagdagang hakbang.

- Unahin ang pagsusuri sa mga protocol na nakabalangkas sa payo ng United States' Cyber security and Infrastructure Security Agency (CISA) *UDP-Based Amplification Attacks*.
- Subaybayan ang mga bagong amplification vector kapag natukoy ang mga ito at na-secure ang iyong mga online na serbisyo laban sa kanila.
- I-configure ang parehong mga inbound at outbound network access control para limitahan ang access sa mga awtorisadong online na serbisyo at organisasyon.
- I-block ang anonymous na pampublikong pag-access para sa amplification-prone na online na mga serbisyo kung hindi kinakailangan.
- Isaalang-alang ang pagpapatupad ng mekanismong naglilimita sa rate upang mabawasan ang mga kahihinatnang pang-aabuso, kung ang pagharang o paglalapat ng mga kontrol sa pag-access ay hindi posible o naaangkop.

Karagdagang impormasyon

Ang *Manwal sa seguridad ng impormasyon* ng ASD ay isang cyber security framework na maaaring ilapat ng mga organisasyon upang protektahan ang kanilang mga system at datos laban sa mga cyberthreat. Ang payo sa *Mga diskarte upang mabawasan ang mga insidente ng cyber security*, kasama ang Essential Eight (Mahalagang Walo), ay umaakma sa framework na ito.

Ang *New Zealand Information Security Manual (Manwal para sa Seguridad ng Impormasyon ng New Zealand)* ay ang manwal ng Pamahalaan ng New Zealand sa pagtiyak ng impormasyon at seguridad ng mga sistema ng impormasyon. Ito ay isang practitioner's manual na idinisenyo upang matugunan ang mga pangangailangan ng mga agency information security executive pati na rin ang mga vendor, contractor at consultant na nagbibigay ng mga serbisyo sa mga ahensya.

Higit pang impormasyon sa iba't ibang uri ng pag-atake ng DoS ay makukuhae sa *DDoS Quick Guide* at *Understanding and Responding to Distributed Denial-Of-Service Attacks* na mga publikasyon ng CISA.

Mga detalye ng contact

Sa Australya, kung mayroon kang anumang mga tanong tungkol sa gabay na ito *sumulat sa ASD* o tumawag sa 1300 CYBER1 (1300 292 371).

Sa New Zealand, upang mag-ulat ng insidente ng cyber security sa email insidents@ncsc.govt.nz o bisitahin ang webpage na Report an incident ng NCSC-NZ.

Pagtatatwa

Ang materyal sa gabay na ito ay may pangkalahatang katangian at hindi dapat ituring bilang legal na payo o pagsalalayan para sa tulong sa anumang partikular na sitwasyon o emerhensya. Sa anumang mahalagang bagay, dapat kang humingi ng naaangkop na independiyenteng propesyonal na payo hinggil sa iyong sariling mga kalagayan.

Ang Commonwealth ay hindi tumatanggap ng responsibilidad o pananagutan para sa anumang pinsala, pagkalugi o gastos na natamo bilang resulta ng pagsalalay sa impormasyong nakapaloob sa gabay na ito.

Copyright

Paggamit ng Coat of Arms

Ang mga tuntunin kung saan maaaring gamitin ang Coat of Arms ay nakadetalye sa website ng Departamento ng Punong Ministro at Gabinete Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Para sa higit pang impormasyon, o para mag-ulat ng insidente sa cyber security, makipag-ugnayan sa amin:

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

Ang numerong ito ay magagamit lamang sa loob ng Australia.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre