Prepara no Responde ba Ataque Nega-Servisu (Denial-of-Service Attacks)

Primeira publika: Setembru 2011
Atualizasaun ikus: Marsu 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

Introdusaun

Publikasaun ida ne'e dezenvolve husi Australian Signals Directorate (ASD) iha kooperasaun ho National Cyber Security Centre (NCSC-NZ) husi Nova Zelândia, Akamai Technologies Ltd no Cloudflare Pty Ltd, hodi resposta ba tendensia aas iha ataque denial-of-service (DoS) iha ami-nia rejiaun laran. Dokumentu ne'e fó orientasaun ba organizasaun sira kona-ba mitigasaun pratika di'ak tebes, bazeia ba estratéjia ameasa modernu, atu prepara no fó resposta ba ataque DoS.

Ami rekomenda atu lee konsellu ida ne'e konjuntu ho ASD *dispozitivu Internet husi Things (IoT)* no *Seguru Ita-nia Wi-Fi no publikasaun router*. Publikasaun sira ne'e ajuda ema sira evita kontribuisaun involuntariamente ba ataque DoS sira ne'ebé bele afeta ema seluk

Ataque DoS (Denial-of-Service) ne'e mak ataque siber ne'ebé planifika atu distrai ka diminui servisu online hanesan website, email no servisu Sistema Naran Domíniu (DNS), atu nega asesu ba uzadór legitimu. Ida ne'e normalmente atinji ho halo inundasaun ba servisu online ho dadus, koneksaun ka pedidu barak tebes atu halo servisu ne'e la di'ak no diminui funsionalidade nia.

Ataque DoS normalemente presija trafiku ho kuantidade boot iha rede atu sai susesu. Sira komún aumenta sai, balun tanba aumentas\ ba númeru dispositivu Internet of Things (IoT) ne'ebé fasil atu kompromete. Tanba fabrikante IoT sira duni fó prioridade ba esperiénsia uzadór duké seguransa siber, dispositivu vulnerável sira bele inklui sasaan uma laran nian ne'ebé konekta ho internét hanesan televizaun intelijente (smart TV), jaleira elétrika, makina aspiradór no sistema seguransa. Dispositivu sira ne'e dalaruma bele kompromete remotamente ho atór malísiozu sira atu kria "botnet" husi dispositivu ida ne'ebé uza atu jera trafiku rede. Kondisaun ida ne'e bele halo uma-kain no organizasaun sira kontribui involuntariamente ba infraestrutura ne'ebé permite ataque DoS akontese.

Atividade dadauk ne'e indika katak bainhira atór malísiozu sira kompromete ona dispositivu IoT barak, sira bele fó aluga ka faan infraestrutura ida ne'e ba siber kriminozu no hacktivistas siber, ne'ebé iha interese boot atu halo ataque DoS kontra alvu ne'ebé sira hili ona. Iha kazu barak, ataque Dos realiza atu kauza produtividade organizasaun no perda finanseiru, ka atu hetan atensaun publiku ba kauza ne'e. Ezemplu ida husi atividade ne'e esplika iha asesoria husi ASD ne'ebé hateten *Atór sira ne'ebé konekta ho República Popular Tionghoa halo ameasa ba router no dispositivu IoT ba halo operasaun botnet*.

Tanba progresy ho digitalizasaun liu tan iha Ita-nia ekonomia no aumenta númeru dispositivu IoT ne'ebé seguransa menus hela no konekta ho internet, ataque DoS bele kontinua aumenta.

Hodi estraga ka hatún servisu online husi organizasaun, atór malisiozu sira uza estratéjia barak, inklui:

- diriji volume boot trafiku rede ne'ebé la presiza ba servisu online ho tenta atu konsume banda rede hotu ne'ebé disponivel.
- diriii trafiku rede ne'ebé ajustadu espesífiku ba servisu online ho tenta atu konsume rekursu prosesamentu komputadór sira-nian.
- uza komputadór barak, dispositivu IoT ka dispositivu seluk ne'ebé konekta ho internet atu diriji trafiku rede ba servisu online husi direksaun barak no iha eskala boot liutan, ne'e mak tipu ataque DoS komún refere nu'udar distribuidu DoS (DDoS) attack.
- Kapta rejistu domíniu organizasaun ka servidór DNS nian no tenta atu rediriji uza-na'in lejítimu sira husi servisu online organizasaun nian.

Organizasaun labele evita sai alvu ho ataque DoS, maibe iha medidas hirak ne'ebé organizasaun sira bele implementa atu prepara no potensialmente redus ataque sira-nia impaktu. Prepara ba ataque DoS molok sira okura ne'e estratejia di'ak tebes, tanba sein preparasaun, ne'e araska duni no ladun efikas atu responde durante ataque DoS.

Maski primariu organizasaun sira foku ba proteje sira-nia aan husi ataque DoS, sira mós tenke foti etapa hirak atu prevene sira-nia servisu online no dispositivu konekta ho internet husi abuzu ho atór malisiozu sira ba alvu sira seluk.

Prepara ba ataque DoS

Iha kontekstu volume ataque DoS mak aumenta iha ami-nia rejiaun, molok implementa kualkér medidas atu prepara ba ataque DoS, Ita-nia organizasaun tenke asesu primeiru ninia rekizitu komersial atu determina karik kada servisu online Ita-nian tenke nafatin operasional durante ataque DoS sira, ka karik interupsaun servisu temporariu aseitavel.

Karik Ita-nia organizasaun hakarak aumenta ninia abilidade kontra ataque DoS sira, Ita tenke proativu implementa medidas tuir mai iha ne'ebé apropriu no prátika, molok ataque DoS akontese.

- Karik Ita-nia organizasaun uza rede distribuisaun konteúdu (CDN), Ita tenek implementa medidas tuir mai iha ne'ebé apropriu no prátika.
  - Konsidera uza CDN ida ne'ebé inklui funsionalidade atu proteje Ita-nia servidór web orijinal husi aplikasaun variedade no ataque xamada rede – CDN balun bele inklui karakterístika sira nu'udar parte husi firewall aplikasaun web iha rede ninin.
  - Evita divulgasaun públiku ne'ebé la presiza kona-ba Protokolu Internet (IP) address husi ita-nia servidór web orijinál, no asegura katak ekspozisaun públiku sira hotu iha proteksaun kontra ataque DoS.
  - Evita uza IP address ba ita-nia servidór web orijinál ne'ebé atór malisiozu bele hetan, por ezemplu, IP address iha subnet rede ida hanesan husi IP address sira ne'ebé revela fó publiku husi Ita-nia servisu online.
  - Uza kontrolu asesu rede (hanesan firewall) atu garante katak CDN deit no Ita-nia rede jestaun autorizadu organizasaun bele asesu Ita-nia servidór web orijen.
  - Konsidera uza konektividade rede diversifikadu reziliente, ne'ebé bele inklui konektividade rede privadu, entre Ita-nia servidór web orijen no Ita-nia fornesedór CDN, karik Ita presija nivel protesaun aas liutan ba Ita-nia servidór web orijen.
  - Konfigura CDN, servidór web orijen no header HTTP sira atu optimiza totál caching mak realiza ona.
  - Konsidera partisiona servidór web orijen sira entaun katak rekere husi IP address ho risku kiik bele jere separadu to'o rekere husi IP address ho risku aas, karik Ita presija disponibilidade nivel aas liu tan.

- Determina funsionalidade no kualidade servisu ida ne'ebé ma aseitavel ba uzadór lejitimu husi Ita-nia servisu online, oinsá mantén funsionalidade no funsionalidade sa'ida mak la presija durante ataque DoS sira.
- Prokura no uza servisu mitigasaun ataque DoS bazeia cloud.
- Konsidera ba redus superfisie ataque iha Ita-nia organizasaun hodi:
  - esternalizadu servisu online fundamentál sira (hanesan DNS) ba fornesedór servisu ne'ebé konfiável no iha kapasidade atu enfrenta ataque DoS.
  - partisiona servisu online kritikál (hanesan email) husi servisu online seluk ne'ebé fasil atu sai alvu (hanesan website),
  - no garante katak servisu mitigasaun ataaki DoS deit permite tráfiku rede ne'ebé konekta ho porta rede husi servisu online relevante.
- Deskute ho Ita-nia fornesedór servisu kona-ba detalle husi sira-nia prevensaun ba ataque DoS sira no estratejia mitigasaun, espesifikamente sira-nia:
  - kapasidade komprovadu atu reziste ataques DoS husi mundu tomak
  - históriku demonstra lidar ataques DoS no teste abranjente ataques DoS autorizadu
  - abilidade atu mitiga automatikamente tipu maioria ataque DoS sein envolvimentu ema, hanesan analize manual husi tráfiku rede.
  - abordajen kona-ba presu servisu sira nian, hanesan karik osan ne'e fixu ka variavel bazeia ba montante tráfiku rede no rekursu prosesamentu komputadór mak uza, no karik Ita bele konfigura limitasaun ba fatura.
  - limite ba notifika Ita ka desliga sira-nia servisu online durante ataque DoS
  - asaun pré-aprovadu ne'ebé Ita bele realiza durante ataque DoS sira
  - aranjamentu prevensaun ataque DoS ho fornesedór upstream.
- Implementa medidas atu detekta ataque DoS sira, hanesan monitoriza tempu real no alerta disponibilidade sistema, tráfegu rede, rekursu prosesamentu komputadór, no kustu asosiadu sira.
- Prepara vesaun estatiku husi Ita-nia website ne'ebé presije prosesamentu minimu no bandwidth atu falisita kontinuidade husi servisu durante ataque DoS.
- Prokura no uza servisu online ho resistente aas, ho bandawidth boot, rekursu prosesamentu komputador adekuadu, lokál hosting ne'ebé geografikamente dispersu, no hamos tráfegu rede ne'ebé la presiza – normalmente inklui uza CDN (Content Delivery Network) ne'ebé konfiável atu cache kontéudu web estátiku no proteje Ita-nia servidor web originál husi tráfegu rede ne'ebé la presija.
- Proteje naran domíniu Ita-nia organizasaun ho uza registrar locking, konfirma katak detalle kontaktu rejistu domíniu no detalle sira seluk ne'e loos oba, no tuir orientasaun adisionál ne'ebé deskreve iha publikasaun husi ASD kona-ba *Seguransa Sistema Naran Domíniu ba nain domíniu sira*.
- Mantén detalle kontaktu ne'ebé atuál ba Ita-nia servisu fornesedór sira no partilla detalle kontaktu husi Ita-nia organizasaun ho sira, hodi garante katak kontaktu sira tomak disponivel tuir rekizitu husi organizasaun, hanesan: oras 24 loron-loron, loron 7 iha semana ida.
- Fornese detalle kontaktu out-of-band husi Ita-nia organizasaun atu uza kanal komunikasaun ne'ebé konfiável ba Ita-nia fornesedór servisu, iha situasaun ne'ebé kanal komunikasaun normal la funsiona.
- Dezenvolve, implementa no mantén planu responde ba insidenti seguransa siber, kobre tipu varia husi ataque DoS sira kontra Ita-nia servisu ida-idak presija ba kontra ataque DoS sira no ezersisiu planu menus liu anualmente.
- Kria aplikasaun atu proteje funsionalidade ne'ebé abuzu komun mak konsume rekursu prosesamentu komputadór boot ka hamosu kustu finanseiru adisionál (hanesan manda mensajen SMS).
  - Protesaun inklui limita taxa no verifika ne'ebé rekere sira husi ema ida.
  - Ezekuta teste ataque DoS inklui foku ba fluxu lójika ne'ebé sala iha funsionalidade aplikasaun.
  - Ezekuta teste karga atu identifika no koriji vetor DoS sira.

Responde ba ataque DoS sira

Karik Ita-nia organizasaun la prepara ba ataque DoS sira, Ita bele tenta ba implementa medidas balun durante ataque DoS sira, maski sira bele sai ladun efika no han tempu atu implementa, redus Ita-nia organizasaun abilidade atu responde.

Ita-nia organizasaun tenke implemente medidas tuir mai durante ataque DoS sira, ne'ebé apropriu no pratikal.

- Implementa Ita-nia planu resposta bainsidenti seguransa siber.
- Husu ba Ita-nia fornesedór servisu sira karik sira bele implementa kedas asaun resposta – karik Ita seidauk diskute antes kona-ba kapasidade sira atu responde, Ita bele hatene katak sira la bele ka lakohi responde, ka husu kustu adisionál.
- Desativa funsionalidade ka kontéudu naun vitál husi Ita-nia servisu online ne'ebé halo ataque DoS atual sai efetivu, por ezemplu: uza versaun web sira sein funsionalidade peskiza, kontéudu dinámiku ka ficheiru boot.
- Mantein komunikasain ho Ita-nia kliente sira no Ita-nia fornesedór servisu sira, inklui Ita-nia fornesedór servisu mitigasaun ataque DoS no kontinua monitoriza disponibilidade husi Ita-nia servisu online.
- Konsidera troka IP address husi Ita-nia servidór web orijen karik ida ne'e sai alvu diretamente, no evita ekspozisaun publiku ba IP address foun sein iha protesaun.
- Relata ataque DoS sira ba parte relevante sira, inklui ASD no NCSC-NZ tuir seksaun 'Detalle Kontaktu sira' husi publikasaun ida ne'e.

Evita halo kontribuisaun ba ataque DoS sira

Ita-nia organizasaun tenke implemente medidas tuir mai atu evita kontribuisaun ba ataque DoS asidentalmente ne'ebé bele impaktu sira seluk

- Evita atu ekspoze servisu sira, dispozitivu IoT no dispositivu seluk ne'ebé konekta ho internét, se la presiza, la konfigura ho seguransa ka la iha manutensaun ne'ebé di'ak.
- Konfigura ho seguru, kontinua halo manutensaun no monitora servisu sira, dispozitivu IoT no dispozitivu seluk ne'ebé konekta ho internét no mak ekspozu ba internét.
  - Orientasaun adisionál ba empressa ki'ik mak disponivel iha publikasaun husi ASD kona-ba *dispozitivu Internet husi Things (IoT)* no *Seguru publikasaun Ita-nia Wi-Fi no ruter*.

Karik ita-nia organizasaun halo operasaun servisu online, Ita tenke implementa medida adisionál sira tuir mai.

- Prioritiza reviza protokolu sira ne'ebé deskreve iha konsellu Ajénsia Seguransa Siber no Infra-Estrutura (CISA) Estadu Unidu *kona-ba Ataque Amplifikasaun bazeia iha UDP*.
- Monitora ba vetor amplifikasaun foun sira bainhira sira identifikadu no halo seguru Ita-nia servisu online kontra sira.
- Konfigura kontrola asesu rede ba diresaun tama no sai (inbound no outbound) hodi limita asesu ba servisu online no organizasaun sira ne'ebé autorizadu deit.
- Blokeia asesu públiku anónimu ba servisu online ne'ebé propensu amplifikasaun, karik la presiza.
- Konsidera ba implementa mekanismu rate-limiting (limita taxa asesu) hodi diminui konsekuénsia abuzu, karik blokadu ka kontrolu asesu la posivél ka la apropriu atu aplika.

Informasaun liutan

Manual Seguransa Informasaun husi ASD mak estrutura seguransa siber ida ne'ebé organizasaun sira bele aplika atu proteje sira-nia sistema no dadus husi ameasa siber. Konsellu iha *Estratejia sira atu mitiga inzidente seguransa siber,* hamutuk ho Essential Eight, kompleta estrutura ida ne'e.

Manual Seguransa Informasaun Nova Zelándia ne'e mak manual husi Governu Nova Zelándia kona-ba asesu informasaun no seguransa sistema informasaun. Ne'e manual ida ba pratikante ne'ebé dezenha hodi atende nesesidade ezekutivu seguransa informasaun iha ajénsia, no mós ba vendór, kontratór no konsultór sira ne'ebé fornese servisu ba ajénsia sira.

Informasaun liutan kona-ba variedade tipu ataque DoS ne'e disponivel iha CISA-nia *Orientasaun Badak DoS* no *Komprensaun no Responde ba publikasaun Distribuisaun Nega Ataque Servisu*.

Detalle Kontaktu sira

In Australia, karik Ita iha kualkér preguntas kona-ba orientasaun ida ne'e *hakerek ba ASD* ka telefonel 1300 CYBER1 (1300 292 371).

Iha Nova Zelándia, atu relata insidente seguransa sibernétika, bele manda email ba incidents@ncsc.govt.nz ka vizita pájina web NCSC-NZ's Report an incident.

Desaprovadór

Materiál iha guia ida ne'e hanesan natureza jeral no la bele konsidera nu'udar sujestaun legal ka depende ba asistênsia iha kondisaun partikulár ka situasaun emerjênsia. Iha kualkér asuntu importante, Ita tenke ba buka sujestaun profisional independente apropriadu mak relasiona ho Ita nia kondisaun rasik.

Commonwealth la aseita responsabilidade ka liabilidade ba kualkér defeitu, lakon ka despeza mak mosu nu'udar rezultadu husi konfiansa ba informasaun mak konteudu iha guia nia laran ida ne'e.

Uza Simbolu Nasional

Termu kona-ba Simbolu ida ne'ebé bele uza, esplika ona ninia detalle iha website Departementu Primeiru Ministru no Gabinete Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

Ba informasaun liutan ka atu relata insidente seguransa sibernétika, kontaktu ami:

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

Númeru ne'e disponivel atu uza deit iha Austrália laran.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre