Bersiapsiaga untuk dan bertindak balas kepada serangan penafian-perkhidmatan

Pertama kali diterbitkan pada: September 2011
Kali terakhir dikemaskini pada: 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

Pengenalan

Penerbitan ini telah dimajukan oleh Direktorat Semboyan Australia (Australian Signals Directorate) (ASD) dengan usahasama Pusat Keselamatan Siber Kebangsaan New Zealand (New Zealand's National Cyber Security Centre) (NCSC-NZ), Akamai Technologies Ltd dan Cloudflare Pty Ltd, sebagai respons kepada trend yang semakin meningkat dalam serangan penafian-perkhidmatan (denial-of-service) (DoS) di dalam rantau kami. Ia menawarkan panduan kepada organisasi mengenai amalan terbaik dalam pemitigasian berdasarkan teknik-teknik pengintipan (tradecraft) ancaman kontemporari, untuk bersiapsiaga dan bertindak balas kepada serangan DoS.

Kami menyarankan agar nasihat ini dibaca sejajar dengan siri penerbitan *Internet of Things devices* dan *Secure your Wi-Fi and router* ASD. Hasil penerbitan ini membantu individu untuk mengelakkan diri daripada menyumbang secara tidak sengaja kepada serangan DoS yang berupaya berimpak ke atas pihak lain.

Serangan DoS ialah serangan siber yang direkacipta untuk mengganggu-gugat atau menghakis perkhidmatan dalam talian seperti laman web, e-mel dan perkhidmatan Sistem Nama Domain (Domain Name System) (DNS), untuk menafikan akses kepada para pengguna yang sah. Hal ini lazimnya dicapai dengan membanjiri sebuah perkhidmatan dalam talian dengan data, hubungan atau permintaan yang akan menenggelami perkhidmatan tersebut dan menghakis kefungsiannya.

Serangan DoS lazimnya memerlukan sejumlah besar trafik jaringan untuk memastikan ia berjaya. Ia semakin menjadi biasa, sebahagiannya disebabkan peningkatan dalam jumlah alat peranti Internet of Things (IoT) yang mudah dikompromi. Oleh kerana pembuat IoT sering mementingkan pengalaman pengguna lebih daripada keselamatan siber, alat peranti yang terdedah boleh meliputi barangan perkakas rumah yang dihubungkan kepada internet seperti TV pintar, cerek, pembersih hampagas dan sistem-sistem keselamatan. Alat-alat peranti ini sering boleh dikompromi dari jarak jauh oleh pelaku berniat jahat untuk mewujudkan sebuah 'botnet' bagi alat peranti untuk menjanakan trafik jaringan ini, yang berupaya mengakibatkan isi rumah dan organisasi-organisasi menyumbang secara tidak sengaja kepada infrastruktur yang membenarkan serangan DoS untuk berlaku.

Aktiviti kebelakangan ini menunjukkan bahawa apabila pelaku berniat jahat sudah mengkompromikan sejumlah besar alat peranti IoT, mereka mungkin akan menyewa atau menjualkan infrastruktur ini kepada penjenayah siber atau aktivis penggodam, yang semakin tertarik untuk melakukan serangan DoS ke atas sasaran-sasaran pilihan mereka. Dalam sebahagian besar kes, serangan DoS dilakukan untuk menyebabkan kerugian kewangan dan produktiviti terhadap sesebuah organisasi, atau untuk meraih perhatian ramai kepada kempen mereka. Satu contoh aktiviti ini dibutirkan dalam nasihat *People's Republic of China-linked actors compromise routers and IoT devices for botnet operations* ASD.

Dengan semakin berkembangnya pendigitasian ekonomi kami selain peningkatan dalam jumlah bilangan alat peranti IoT yang terhubung kepada internet dengan lindungan keselamatan yang lemah, serangan DoS berkemungkinan besar atau terus meningkat.

Untuk mengganggu-gugat atau menghakis perkhidmatan dalam talian sesebuah organisasi, pelaku berniat jahat menggunakan beberapa pendekatan, termasuk:

- mengarahkan sejumlah besar trafik jaringan yang tidak dikehendaki kepada perkhidmatan dalam talian dalam satu usaha untuk menghabiskan semua bandwith jaringan yang ada.
- mengarahkan trafik jaringan tersusun kepada perkhidmatan dalam talian dalam satu usaha untuk menghabiskan sumber-sumber pemerosesan komputer mereka.
- menggunakan komputer, alat peranti IoT atau alat peranti yang terhubung kepada internet secara berganda untuk mengarahkan trafik jaringan kepada perkhidmatan dalam talian daripada pelbagai arah dan atas skala yang jauh lebih besar, satu jenis serangan DoS yang biasanya dirujuk sebagai serangan Dos (DDos) yang diedar.
- merampas pendaftaran domain atau server DNS sesebuah organisasi dalam satu usaha untuk mengalihkan pengguna sah daripada perkhidmatan dalam talian sesebuah organisasi.

Para organisasi tidak boleh mengelakkan diri mereka daripada menjadi sasaran serangan DoS, tetapi terdapat beberapa langkah yang boleh dilaksanakan oleh organisasi-organisasi ini untuk bersiapsiaga dan berpotensi untuk mengurangkan impaknya. Bersiapsiaga untuk serangan DoS sebelum ia terjadi ialah strategi terbaik, kerana tanpa persiapan, ianya akan menjadi sukar dan kurang berkesan untuk berespons semasa serangan DoS sedang berlaku.

Walaupun organisasi secara utamanya berfokus ke arah melindungi mereka daripada serangan DoS, mereka juga sepatutnya mengambil langkah untuk menghalang perkhidmatan dalam talian dan alat peranti terhubung kepada internet mereka daripada disalahguna oleh pelaku berniat jahat untuk menyasarkan pihak lain.

Bersiapsiaga untuk serangan DoS

Dalam konteks jumlah bilangan serangan DoS yang semakin meningkat di seluruh rantau kami, sebelum sebarang langkah bersiapsiaga untuk serangan DoS dilaksanakan, organisasi anda sepatutnya menilai terlebih dahulu keperluan bisnesnya untuk menentukan jika setiap perkhidmatan dalam talian anda perlu kekal beroperasi semasa serangan DoS, atau jika gangguan perkhidmatan sementara boleh diterima.

Jika organisasi anda mahu meningkatkan keupayaannya untuk menahan serangan DoS, anda sepatutnya melaksanakan langkah-langkah berikut secara pro-aktif, di mana ia berpatutan dan praktikal, sebelum terjadinya serangan DoS.

- Jika organisasi anda sedang menggunakan sebuah jaringan penyampaian konten (content delivery network) (CDN), anda sepatutnya melaksanakan langkah-langkah tambahan berikut, di mana ia berpatutan dan praktikal.
  - Pertimbangkan penggunaan sebuah CDN yang meliputi kefungsian untuk melindungi server web asal (origin web server) anda daripada pelbagai serangan aplikasi dan lapisan jaringan – sesetengah CDN mungkin mengandungi ciri-ciri ini sebagai sebahagian daripada sesebuah aplikasi penghadang api (firewall) web pada pinggirannya.
  - Elakkan pendedahan yang tidak perlu kepada pihak umum mengenai alamat Protokol Internet (Internet Protocol) (IP) server web asal anda, dan pastikan bahawa sebarang pendedahan umum adalah dilindungi daripada serangan DoS.
  - Elakkan penggunaan sebuah alamat IP untuk server web asal anda yang boleh dijangka oleh pelaku berniat jahat, misalnya, sebuah alamat IP dalam subnet jaringan sama bagi alamat-alamat IP yang didedahkan kepada pihak umum bagi perkhidmatan dalam talian anda.
  - Gunakan kawalan akses jaringan (misalnya penghadang api (firewall)) untuk memastikan hanya CDN dan jaringan pengurusan yang diberikuasa oleh organisasi anda boleh mengakses server web asal anda.
  - Pertimbangkan penggunaan keterhubungan jaringan berdaya tahan yang pelbagai, yang mungkin meliputi keterhubungan jaringan peribadi, antara server web asal anda dan penyedia CDN anda, jika anda memerlukan tahap perlindungan yang lebih tinggi bagi server web asal anda.

  - Konfigurkan CDN, server web asal dan header HTTP klien untuk mengoptimumkan jumlah caching yang dilakukan.
  - Pertimbangkan pembahagian server web asal supaya permintaan daripada alamat-alamat IP berisiko rendah akan ditangani secara berasingan daripada alamat-alamat IP berisiko tinggi, jika anda memerlukan tahap ketersediaan yang lebih tinggi.
- Tentukan kefungisan dan kualiti perkhidmatan apa yang boleh diterima bagi pengguna sah bagi perkhidmatan dalam talian anda, bagaimana untuk mengekalkan kefungisan tersebut, dan kefungsian apa yang tidak diperlukan sewaktu berlakunya serangan DoS.
- Perolehi dan gunakan perkhidmatan pemitigasian serangan DoS berdasarkan-awan.
- Pertimbangkan pengurangan permukaan serangan organisasi anda dengan:
  - Menyumberluarkan perkhidmatan dalam talian asasi (misalnya DSN) kepada penyedia perkhidmatan yang boleh diyakini yang boleh menahan serangan DoS.
  - Membahagikan perkhidmatan dalam talian kritikal (misalnya e-mel) daripada perkhidmatan dalam talian lain yang lebih berkemungkinan untuk dijadikan sasaran (misalnya laman web)
  - Memastikan bahawa perkhidmatan pemitigasian serangan DoS hanya membenarkan trafik jaringan yang berkaitan dengan port(-port) jaringan perkhidmatan dalam talian tersebut.
- Bincangkan butir-butir strategi penghalangan dan pemitigasian serangan DoS penyedia perkhidmatan anda dengan mereka, khususnya:
  - Keupayaan yang terbukti untuk menahan serangan DoS dari seluruh dunia
  - Sejarah yang didemonstrasikan dalam menangani serangan DoS mahupun ujian serangan DoS komprehensif yang diluluskan.
  - Keupayaan untuk memitigasikan sebahagian besar jenis-jenis serangan DoS secara automatik tanpa penglibatan manusia, misalnya analisis manual trafik jaringan.
  - Mengorak langkah untuk mengenakan harga ke atas perkhidmatan mereka, misalnya sama ada kos tersebut diletakkan pada kadar tetap atau adakah ia akan berubah berpandukan jumlah trafik jaringan dan sumber pemerosesan komputer yang digunakan, dan sama ada anda boleh menetapkan had bil yang dikenakan.
  - had hadangan untuk menyampaikan notifikasi kepada anda atau menutup perkhidmatan dalam talian mereka semasa serangan DoS berlaku
  - tindakan yang diluluskan terlebih dahulu yang boleh dilaksanakan semasa serangan DoS
  - Aturan halangan serangan DoS dengan penyedia huluan.
- Melaksanakan langkah-langkah untuk mengesan serangan DoS, misalnya pemantauan masa nyata dan amaran kebersediaan sistem, trafik jaringan, sumber-sumber pemerosesan komputer, dan kos-kos berkaitan.
- Menyediakan sebuah versi statik laman web anda yang memerlukan pemerosesan dan bandwith minimum untuk memudahkan kelangsungan perkhidmatan semasa serangan DoS berlaku.
- Memperolehi dan menggunakan perkhidmatan dalam talian yang berdaya tahan tinggi dengan bandwith luas, sumber-sumber pemerosesan komputer yang mencukupi, lokasi penghosan yang tersebar secara geografi dan pemadaman trafik berdasarkan-awan untuk membuangkan trafik jaringan yang tidak diingini – ini lazimnya termasuk menggunakan sebuah CDN yang boleh dipercayai untuk melakukan cache kontent laman web statik dan melindungi server web asal anda daripada trafik jaringan yang tidak diingini.
- Lindungi nama-nama domain organisasi anda dengan menggunakan penguncian pendaftar, mengesahkan butir-butir kontak pendaftaran domain dan butir-butir lain yang betul, dan mematuhi panduan tambahan yang digariskan dalam penerbitan *Domain Name System security for domain owners* ASD.
- Memastikan pengemaskinian butir-butir kontak anda kepada penyedia perkhidmatan anda dan berkongsi butir-butir kontak organisasi anda dengan mereka, dengan memastikan semua kontak senantiasa bersiap sedia berdasarkan keperluan organisasi anda, contohnya, 24 jam sehari, 7 hari seminggu.

- Sediakan butir-butir kontak out-of-band organisasi anda bagi sebuah saluran komunikasi yang boleh dipercayai kepada penyedia perkhidmatan anda, untuk apabila saluran komunikasi biasa mengalami kegagalan.
- Membangunkan, melaksanakan dan mengekalkan sebuah pelan respons insiden keselamatan siber, yang meliputi pelbagai jenis serangan DoS terhadap setiap satu daripada perkhidmatan dalam talian anda yang perlu menahan serangan DoS, dan melatihkan pelan tersebut sekurang-kurangnya setiap tahun.
- Aplikasi arkitek untuk melindungi kefungisan yang lazim disalahguna yang menghabiskan sumber-sumber pemerosesan komputer dengan lebih tinggi atau yang mengenakan kos-kos kewangan tambahan (misalnya menghantar pesanan SMS).
  - Perlindungan termasuk pengehadan kadar dan menentusahkan bahawa permintaan sebenarnya datang daripada seorang manusia.
  - Melakukan ujian serangan DoS termasuk menyasarkan aliran logik yang tidak sah dalam kefungsian aplikasi.
  - Laksanakan ujian bebanan meluas untuk mengenal pasti dan memulihkan vektor-vektor DoS.

Berespons kepada serangan DoS

Jika organisasi anda tidak bersiapsiaga untuk serangan DoS, anda boleh cuba untuk melaksanakan beberapa daripada langkah-langkah di atas semasa berlakunya serangan DoS, namun ia mungkin kurang berkesan dan akan mengambil masa untuk dilaksanakan, yang akan mengurangkan keupayaan organisasi anda untuk bertindak.

Organisasi anda patut melaksanakan langkah-langkah berikut sewaktu berlakunya serangan DoS, di mana ia berpatutan dan praktikal.

- Gerakkan pelan respons insiden keselamatan siber anda.
- Tanya penyedia perkhidmatan anda jika mereka boleh melaksanakan tindakan responsif dengan segera – jika anda tidak pernah membincangkan keupayaan mereka untuk berespons, anda mungkin akan mendapati bahawa mereka tidak berupaya atau tidak bersedia untuk berespons, atau mengenakan fi tambahan.
- Nyahupayakan kefungsian yang tidak penting atau buangkan konten tidak penting daripada perkhidmatan dalam talian anda yang menjadikan serangan DoS semasa efektif, contohnya, aturgerakkan satu versi laman web anda tanpa kefungsian carian, konten dinamik atau fail-fail besar.
- Kekal berkomunikasi dengan pelanggan anda dan penyedia perkhidmatan anda, termasuk penyedia perkhidmatan pemitigasian serangan DoS anda, dan teruskan pemantauan ketersediaan perkhidmatan dalam talian anda.
- Pertimbangkan penukaran alamat IP server web asal anda jika ia sedang disasarkan secara langsung, dan elakkan pendedahan umum alamat IP baharu itu tanpa menetapkan perlindungan terhadapnya terlebih dahulu.
- Laporkan serangan DoS tersebut kepada pihak-pihak berkaitan, termasuk ASD dan NCSC-NZ sebagai mana disyorkan dalam seksyen ‘Contact Details’ dalam penerbitan ini.

Elakkan daripada menyumbang kepada serangan DoS

Organisasi anda patut melaksanakan langkah-langkah berikut bagi mengelakkan daripada menyumbang secara tidak sengaja kepada serangan DoS yang mungkin akan mengimpakkan pihak lain.

- Elakkan daripada mendedahkan perkhidmatan, alat peranti IoT dan alat-alat peranti terhubung kepada internet yang lain kepada internet bila ia tidak diperlukan, dikonfigurasi dalam cara yang tidak kukuh atau tidak diselenggarakan dengan secukupnya.
- Konfigurasikan, kekal dan pantaui perkhidmatan, alat peranti IoT dan alat-alat peranti lain yang terhubung kepada internet yang terdedah kepada internet, secara kukuh.
  - Panduan tambahan bagi bisnes kecil-kecilan disediakan dalam penerbitan-penerbitan *Internet of Things devices* and *Secure your Wi-Fi and router* ASD.

Jika organisasi anda menjalankan perkhidmatan dalam talian, anda patut melaksanakan langkah-langkah tambahan berikut.

- Utamakan protokol penilaian kembali dalam nasihat *UDP-Based Amplification Attacks* pihak United States Cyber security and Infrastructure Security Agency (Agensi Keselamatan Infrastruktur dan keselamatan Siber Amerika Syarikat) (CISA).
- Pantaui vektor-vektor amplifikasi baharu bila ia dikenal pasti dan kukuhkan perkhidmatan dalam talian anda untuk menentangnya.
- Konfigurasikan kedua-dua kawalan akses jaringan masuk dan keluar untuk mengehadkan akses kepada perkhidmatan dalam talian dan organisasi yang diberikuasa sahaja.
- Sekatkan akses umum anonim bagi perkhidmatan dalam talian yang sering-diamplifikasi jika ia tidak diperlukan.
- Pertimbangkan pelaksanaan mekanisme pengehadan kadar untuk mengurangkan akibat penyalahgunaan, jika sekatan atau penerapan akses kawalan tidak boleh dilakukan atau tidak sesuai.

Maklumat Lanjut

Information security manual ASD ialah sebuah kerangka kerja keselamatan siber yang boleh diterapkan oleh organisasi-organisasi untuk melindungi sistem-sistem dan data mereka daripada ancaman siber. Nasihat yang terkandung di dalam *Strategies to mitigate cyber security incidents*, beserta Essential Eight, melengkapi kerangka kerja ini.

New Zealand Information Security Manual ialah manual Kerajaan New Zealand bagi jaminan maklumat dan keselamatan sistem-sistem maklumat. Ia merupakan manual pengamal yang direkabentuk untuk memenuhi keperluan para eksekutif keselamatan maklumat agensi selain vendor-vendor, kontraktor-kontraktor dan para perunding yang menyediakan perkhidmatan kepada agensi-agensi.

Maklumat lanjut mengenai pelbagai jenis serangan DoS ada disediakan di dalam penerbitan-penerbitan *DDoS Quick Guide* and *Understanding and Responding to Distributed Denial-Of-Service Attacks* CISA.

Butir-Butir Kontak

Di Australia, jika anda ada sebarang soalan mengenai panduan ini, *sila tulis kepada ASD* atau sila panggil 1300 CYBER1 (1300 292 371).

Di New Zealand, untuk melaporkan sebuah insiden keselamatan siber, sila e-mel incidents@ncsc.govt.nz atau sila layari laman web Report an incident NCSC-NZ.

Penafian

Bahan di dalam panduan ini adalah bersifat umum dan tidak harus dianggap sebagai nasihat perundangan atau digantung sebagai bantuan dalam apa-apa keadaan atau kecemasan tertentu. Dalam sebarang hal mustahak, anda harus mendapatkan nasihat profesional bebas tentang apa yang anda sedang alami sendiri.

Pihak Komanwel tidak menerima tanggungjawab atau tanggungan ke atas sebarang kerosakan, kerugian atau perbelanjaan yang ditanggung akibat daripada pergantungan kepada maklumat yang terkandung dalam panduan ini.

Untuk maklumat lanjut, atau untuk melaporkan sebuah kejadian keselamatan siber, sila hubungi kami:

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

Nombor ini tersedia untuk digunakan di dalam Australia sahaja.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre