



Ryan Hanif

Analisis Serangan DDos: Studi Kasus Syn (2016)

Distributed Denial of Service (DDoS) adalah upaya untuk membuat sumber daya online (seperti website atau layanan) tidak tersedia bagi pengguna yang sah dengan cara membanjirinya dengan lalu lintas internet dari berbagai sumber.




Latar Belakang



Dyn, sebuah perusahaan infrastruktur internet terkemuka yang berbasis di Amerika Serikat. Pada saat itu, Dyn adalah salah satu penyedia layanan Managed DNS terbesar di dunia. 21 Oktober 2016, sebuah hari yang akan diingat sebagai salah satu gangguan internet terparah. Infrastruktur Internet.

Dyn menyediakan layanan DNS untuk banyak perusahaan besar. DNS berfungsi sebagai "buku telepon" internet yang vital, menerjemahkan nama domain yang mudah diingat (misal: www.netflix.com) menjadi alamat IP numerik (8.8.4.4) yang digunakan mesin untuk berkomunikasi. Tanpa DNS yang berfungsi, internet modern tidak dapat digunakan.



Skala Dampak: Efek Domino di seluruh Dunia



Serangan terhadap satu perusahaan, Dyn, menciptakan efek domino yang melumpuhkan akses ke situs-situs dan layanan paling populer di dunia, terutama bagi pengguna di Amerika Utara dan Eropa.

Media Sosial

Twitter , Reddit

Streaming & Hiburan

Netflix, Spotify, SoundCloud

Berita

CNN, The Gurdian, The New York Times



Kronologi Serangan Kompleks

Gelombang 1 (07:00 EDT)

- Serangan awal menargetkan pusat data Dyn di Pantai Timur AS.
- Tim teknisi Dyn berhasil mengidentifikasi dan memitigasi serangan dalam waktu sekitar dua jam. Situasi tampak terkendali.

Gelombang 2 (12:00 EDT)

- Penyerang meluncurkan serangan kedua dengan skala yang jauh lebih besar dan distribusi geografis yang lebih luas, menargetkan pusat data Dyn di seluruh dunia.
- (9((Gelombang ini menyebabkan dampak yang paling parah dan meluas.

Gelombang 3 (Sore hari)

- Sebuah gelombang serangan terakhir dilancarkan saat tim Dyn masih berjuang untuk memulihkan layanan sepenuhnya.
- Durasi Total: Gangguan signifikan berlangsung selama lebih dari 10 jam.

Teknik Serangan (1): “Tentara Zombie”

Botnet Mirai

Sumber kekuatan:

Serangan ini dilancarkan oleh Botnet Mirai, sebuah jaringan perangkat "zombie"

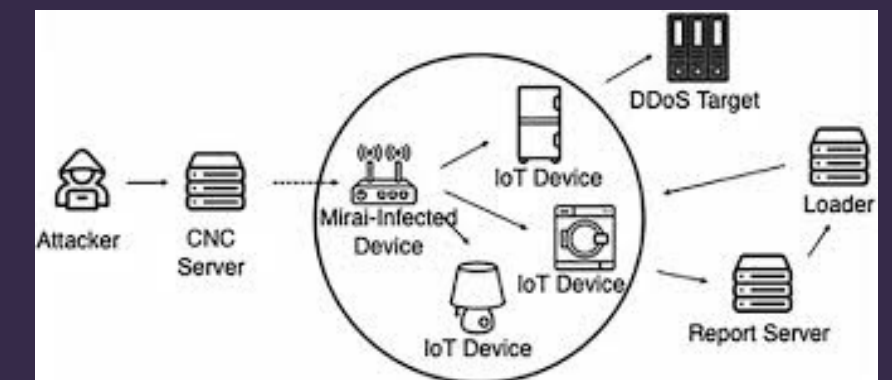
Apa itu “Mirai”?:

Sebuah malware canggih yang secara otomatis memindai internet untuk mencari perangkat Internet of Things (IoT) yang rentan. Target utamanya adalah: Kamera CCTV dan IP Camera Router rumahan dan SOHO (Small Office/Home Office) Perekam video digital (DVR)

Metode Infeksi:

Mirai mengeksploitasi kelemahan paling dasar: perangkat-perangkat ini sering kali masih menggunakan kombinasi nama pengguna dan kata sandi bawaan pabrik (seperti admin/admin atau user/password)

Setelah terinfeksi, puluhan ribu perangkat ini membentuk "pasukan" yang dapat dikendalikan dari jarak jauh untuk menyerang target secara bersamaan





Teknik Serangan (2): Banjir DNS Query

Layer 7

Jenis serangan:

Volumetric Attack yang sangat canggih pada Layer 7 (Application Layer). Ini berbeda dari serangan jaringan (Layer 3/4) yang lebih sederhana

Mekanisme serangan:

Botnet Mirai tidak hanya mengirim data sampah. Sebaliknya, botnet ini membanjiri server Dyn dengan puluhan juta permintaan resolusi DNS (TCP dan UDP DNS query flood) yang dirancang agar terlihat seperti permintaan dari pengguna yang sah

Volume serangan:

Lalu lintas serangan mencapai puncaknya hingga 1.2 Terabit per detik (Tbps). Volume ini belum pernah terjadi sebelumnya dan cukup untuk melumpuhkan bahkan infrastruktur yang paling kuat sekalipun

Hasil:

Server Dyn menjadi terlalu sibuk memproses permintaan palsu sehingga tidak dapat merespons permintaan DNS dari pengguna yang sebenarnya, membuat internet "rusak" bagi banyak orang



Analisis Dampak Teknis

Layanan mati (Downtime):

Ini adalah dampak yang paling jelas. Website dan aplikasi besar menjadi tidak dapat diakses sama sekali atau sangat lambat, menyebabkan frustrasi pengguna secara massal

Kelebihan beban (Overload):

CPU dan memori server DNS Dyn mencapai 100% kapasitas, menyebabkan crash dan kegagalan sistem. Mereka tidak sanggup lagi memproses antrian permintaan yang tak ada habisnya

Saturasi bandwidth:

Serangan ini sepenuhnya menghabiskan kapasitas bandwidth jaringan Dyn. Ini ibarat pipa air yang diisi penuh sehingga tidak ada lagi ruang untuk air bersih mengalir

Peningkatan latensi:

Bahkan ketika layanan mulai pulih, latensi (waktu respons) untuk permintaan DNS meningkat secara drastis, membuat pengalaman internet menjadi sangat lambat



Analisis Dampak bisnis & Kerugian



Kerugian finansial Langsung:

- Perusahaan e-commerce seperti Amazon dan eBay (yang juga terdampak) kehilangan jutaan dolar dalam penjualan yang gagal.
- Situs berbasis iklan kehilangan pendapatan karena iklan tidak dapat ditampilkan kepada pengguna.
- Layanan berlangganan seperti Netflix dan Spotify menghadapi keluhan pelanggan.
- Secara total, kerugian ekonomi kolektif diperkirakan mencapai lebih dari \$100 juta dolar AS untuk satu hari gangguan

Kerusakan Reputasi jangka panjang:

- Kepercayaan publik terhadap keandalan layanan online yang terdampak menurun.
- Serangan ini memaksa perusahaan di seluruh dunia untuk meninjau kembali strategi keamanan dan ketergantungan mereka pada vendor tunggal.
- Bagi Dyn, meskipun mereka adalah korban, insiden ini merusak reputasi mereka sebagai penyedia infrastruktur yang tangguh

Mitigasi & Respon Cepat



Traffic Scrubbing

Ini adalah pertahanan utama. Semua lalu lintas yang masuk ke jaringan Dyn dialihkan ke "pusat pembersihan" (scrubbing centers) global. Di fasilitas ini, algoritma canggih dan analisis real-time memisahkan lalu lintas berbahaya dari botnet dan memblokirnya, sementara lalu lintas yang sah diizinkan untuk diteruskan ke server


BGP Flowspec

Teknik ini digunakan untuk menyebarkan "aturan pemblokiran" secara cepat ke seluruh router di jaringan mereka, secara efektif menghentikan lalu lintas dari alamat IP berbahaya bahkan sebelum mencapai server



Kolaborasi Industri

Dyn secara aktif bekerja sama dengan penyedia infrastruktur internet besar lainnya untuk berbagi informasi ancaman dan mendapatkan bantuan dalam memblokir lalu lintas serangan di tingkat hulu (sebelum mencapai jaringan Dyn)





Pembelajaran & Rekomendasi Strategis



Pembelajaran Utama

- Keamanan IoT adalah Tanggung Jawab Bersama: Perangkat IoT yang tidak aman bukan hanya risiko bagi pemiliknya, tetapi juga bagi seluruh internet.
- Infrastruktur Kritis adalah Target Utama: Penyerang kini menyadari bahwa melumpuhkan satu titik sentral seperti DNS jauh lebih efektif daripada menyerang ribuan target individual.
- Skala Serangan DDoS Terus Meningkat: Serangan berskala Terabit per detik kini menjadi norma baru yang harus diantisipasi

Rekomendasi pencegahan ke Depan

- Untuk Produsen & Pengguna IoT: Produsen harus menerapkan kebijakan "aman sejak awal" (secure-by-design) dan melarang kata sandi default. Pengguna harus dididik untuk selalu mengubah kredensial bawaan.
- Arsitektur Multi-DNS dan Redundansi: Perusahaan tidak boleh bergantung pada satu penyedia DNS. Menggunakan dua atau lebih penyedia DNS secara bersamaan dapat memastikan kelangsungan layanan jika salah satu diserang.
- Mengadopsi Solusi Anti-DDoS Proaktif: Jangan menunggu serangan terjadi. Berlangganan layanan proteksi DDoS yang selalu aktif (always-on) adalah investasi penting untuk bisnis yang bergantung pada ketersediaan online



Referensi

Krebs on Security, "DDoS on Dyn Impacts Twitter, Spotify, Reddit" (2016).

Dyn/Oracle Blog, "Dyn Analysis Summary Of Friday October 21 Attack" (2016).

Laporan Keamanan Tahunan dari Cloudflare, Akamai, dan NETSCOUT.

Artikel investigasi dari Wired, "The Looming Digital Disaster of the IoT" (2016).

