TUGAS

KEAMANAN JARINGAN KOMPUTER

Kasus Serangan DDoS Ke Jaringan Server Spamhaus Pada Tahun 2013

Nama : Ega Aldo Firmansyah

NIM : 09011281419057

FAKULTAS ILMU KOMPUTER

JURUSAN SISTEM KOMPUTER

UNIVERSITAS SRIWIJAYA

Kasus Serangan DDoS Ke Jaringan Server Spamhaus Pada Tahun 2013

Seorang pria berkebangsaan Belanda ditangkap di Spanyol karena dicurigai sebagai pelaku serangan dunia maya terbesar dalam sejarah internet yang dioperasikan dari "bunker" dekat Barcelona dari dalam mobil van yang dilengkapi dengan scanner hi-tech.

Sven Olaf Kamphuis yang berusia 35 tahun, ditangkap pada Kamis di Granollers, sebuah kota 22 km sebelah utara dari ibukota Catalan atas dugaan perannya dalam hacking Spamhaus kelompok anti-spam Eropa.

Tersangka berkeliling Spanyol dalam sebuah van oranye yang merupakan "kantor berjalanan yang dilengkapi dengan berbagai antena untuk memindai frekuensi," sebagaimana pernyataan yang dikeluarkan oleh kementerian dalam negeri Spanyol.

Pihak berwenang Spanyol pertama kali diberitahu di bulan Maret bahwa sejumlah besar serangan cyber mempengaruhi layanan internet di AS, Inggris dan Belanda sedang diluncurkan dari Spanyol.

Polisi Spanyol melacak tersangka sebuah properti di Granollers. Tersangka mengatakan kepada polisi bahwa ia adalah seorang diplomat yang mewakili "Kementerian Telekomunikasi dan Luar Negeri Republik Cyberbunker" dan telah menggambarkan dirinya sebagai "pejuang kebebasan berinternet ".

Sebuah serangan cyber berjenis distributed denial of service (DDoS) terhadap perusahaan keamanan jaringan Spamhaus memiliki dampak yang sangat besar. Akibat serangan tersebut, dikabarkan kecepatan internet dunia, terutama di benua Eropa, terus melambat. Tidak itu saja, serangan ini diduga dapat membuat dampak yang lebih buruk dari sekadar melambatnya kecepatan internet.

Menurut beberapa ahli keamanan komputer, melihat skala serangan yang semakin kuat, para pengguna bisa saja tidak dapat mengakses layanan dasar internet, seperti e-mail dan layanan perbankan online.

Sebenarnya, seberapa besarkah skala serangan cyber ini? Menurut Matthew Price, Chief Executive of CloudFlare, serangan DDos ini dapat dikatakan sebagai yang terbesar dalam sejarah. Sekadar catatan, CloudFlare merupakan perusahaan yang ditunjuk oleh Spamhaus untuk melindungi perusahaan tersebut dari serangan DDos ini.

"Serangan ini mirip dengan bom nuklir. Serangan ini mudah untuk menghasilkan kerusakan yang begitu besar," kata Price, seperti dikutip dari NY Times, Kamis (28/3/2013).

Serangan DDoS ini juga mampu mencapai nilai yang luar biasa besar, yaitu 300 miliar bit per detik. Dikatakan, serangan ini berpuluh kali lipat dibandingkan serangan DDos pada umumnya.

Serangan ini diduga dimulai saat Spamhaus menambahkan sebuah perusahaan asal Belanda, Cyberbunker, ke daftar hitam (blacklist) miliknya. Spamhaus merupakan perusahaan pembuat daftar hitam yang digunakan oleh penyedia layanan internet sebagai acuan pemblokiran situs-situs web berbahaya.

Distributed Denial of Service (DDoS) atau dalam Bahasa Indonesia diterjemahkan sebagai Penolakan Layanan secara Terdistribusi adalah salah satu jenis serangan Denial of Service yang menggunakan banyak host penyerang (baik itu menggunakan komputer yang didedikasikan untuk

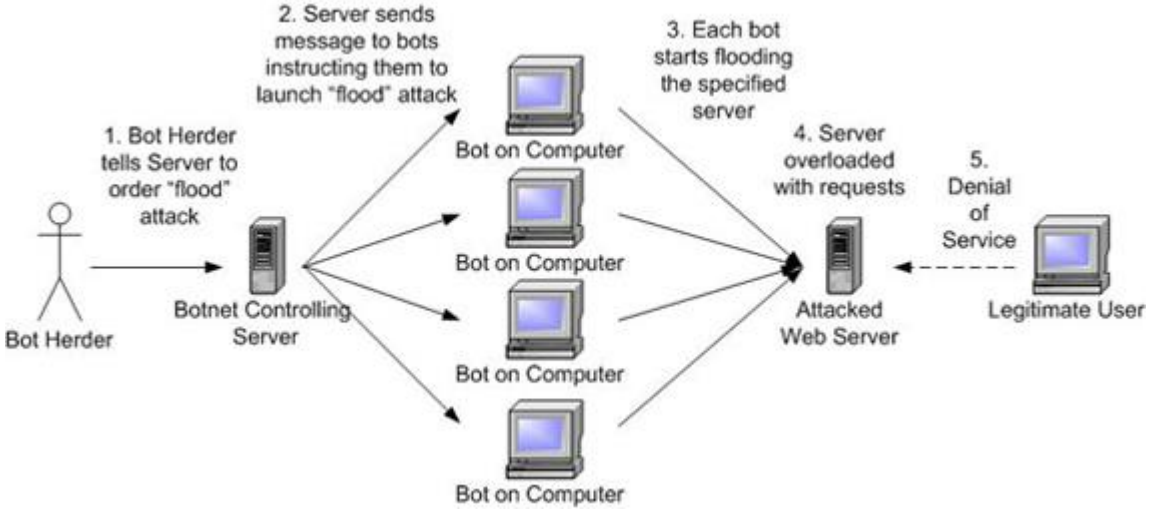
melakukan penyerangan atau komputer yang "dipaksa" menjadi zombie) untuk menyerang satu buah host target dalam sebuah jaringan.

Serangan Denial of Service klasik bersifat "satu lawan satu", sehingga dibutuhkan sebuah host yang kuat (baik itu dari kekuatan pemrosesan atau sistem operasinya) demi membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan. Serangan DDoS ini menggunakan teknik yang lebih canggih dibandingkan dengan serangan Denial of Service yang klasik, yakni dengan meningkatkan serangan beberapa kali dengan menggunakan beberapa buah komputer sekaligus, sehingga dapat mengakibatkan server atau keseluruhan segmen jaringan dapat menjadi "tidak berguna sama sekali" bagi klien.

Serangan DDoS pertama kali muncul pada tahun 1999, tiga tahun setelah serangan Denial of Service yang klasik muncul, dengan menggunakan serangan SYN Flooding, yang mengakibatkan beberapa server web di Internet mengalami "downtime". Pada awal Februari 2000, sebuah serangan yang besar dilakukan sehingga beberapa situs web terkenal seperti Amazon, CNN, eBay, dan Yahoo! mengalami "downtime" selama beberapa jam. Serangan yang lebih baru lagi pernah dilancarkan pada bulan Oktober 2002 ketika 9 dari 13 root DNS Server diserang dengan menggunakan DDoS yang sangat besar yang disebut dengan "Ping Flood". Pada puncak serangan, beberapa server tersebut pada tiap detiknya mendapatkan lebih dari 150.000 request paket Internet Control Message Protocol (ICMP). Untungnya, karena serangan hanya dilakukan selama setengah jam saja, lalu lintas Internet pun tidak terlalu terpengaruh dengan serangan tersebut (setidaknya tidak semuanya mengalami kerusakan).

SKEMA PERETASAN

Tidak seperti akibatnya yang menjadi suatu kerumitan yang sangat tinggi (bagi para administrator jaringan dan server yang melakukan perbaikan server akibat dari serangan), teori dan praktik untuk melakukan serangan DDoS justru sederhana, yakni sebagai berikut:



Dapat dilakukan dengan menjalankan tool (biasanya berupa program (perangkat lunak) kecil) yang secara otomatis akan memindai jaringan untuk menemukan host-host yang rentan (vulnerable) yang terkoneksi ke Internet. Setelah host yang rentan ditemukan, tool tersebut dapat menginstalasikan salah satu jenis dari Trojan Horse yang disebut sebagai DDoS Trojan, yang akan mengakibatkan host tersebut menjadi zombie yang dapat dikontrol secara jarak jauh (bahasa Inggris: remote) oleh sebuah komputer master yang digunakan oleh si penyerang asli untuk melancarkan

serangan. Beberapa tool (software} yang digunakan untuk melakukan serangan serperti ini adalah TFN, TFN2K, Trinoo, dan Stacheldraht, yang dapat diunduh secara bebas di Internet.

Ketika si penyerang merasa telah mendapatkan jumlah host yang cukup (sebagai zombie) untuk melakukan penyerangan, penyerang akan menggunakan komputer master untuk memberikan sinyal penyerangan terhadap jaringan target atau host target. Serangan ini umumnya dilakukan dengan menggunakan beberapa bentuk SYN Flood atau skema serangan DoS yang sederhana, tapi karena dilakukan oleh banyak host zombie, maka jumlah lalu lintas jaringan yang diciptakan oleh mereka adalah sangat besar, sehingga "memakan habis" semua sumber daya Transmission Control Protocol yang terdapat di dalam komputer atau jaringan target dan dapat mengakibatkan host atau jaringan tersebut mengalami "downtime".

Hampir semua platform komputer dapat dibajak sebagai sebuah zombie untuk melakukan serangan seperti ini. Sistem-sistem populer, semacam Solaris, Linux, Microsoft Windows dan beberapa varian UNIX dapat menjadi zombie, jika memang sistem tersebut atau aplikasi yang berjalan di atasnya memiliki kelemahan yang dieksploitasi oleh penyerang.

DAMPAK YANG DITIMBULKAN

Akibat serangan tersebut, dikabarkan kecepatan internet dunia, terutama di benua Eropa, terus melambat.Tidak itu saja, serangan ini diduga dapat membuat dampak yang lebih buruk dari sekadar melambatnya kecepatan internet.

Menurut beberapa ahli keamanan komputer, melihat skala serangan yang semakin kuat, para pengguna bisa saja tidak dapat mengakses layanan dasar internet, seperti e-mail dan layanan perbankan online.

Sumber :

http://www.telegraph.co.uk/technology/internet-security/10025858/Dutchman-planned-biggest-ever-cyber-attack-from-bunker-near-Barcelona.html

http://tekno.kompas.com/read/2013/03/28/11571269/Pakar.Ini.Serangan.Cyber.Terbesar.Sepanjang.Sejarah