Internet Worms

Jim Geovedi
jim@corebsd.or.id

Abstrak

Internet worms, program-program komputer yang mampu menyebar dan menggandakan-diri secara otomatis dan berpotensi untuk menyebar dengan sangat cepat di Internet. Worms pertama kali muncul diakhir tahun 1980an, dan terus meningkat dan menginfeksi banyak sistim target secara dramatis.

Terdapat dua hal yang harus dipahami ketika hendak membangun perlindungan jaringan terhadap bahaya Worms: seberapa cepat sebuah worm dapat menyebar dan seberapa jauh worm tersebut dapat menjadi sebuah ancaman yang menakutkan di Internet. Untuk memahami dua hal tersebut, perlu pengetahuan mengenai worms itu sendiri dan strategi yang digunakan untuk mendeteksi keberadaan worms dalam suatu jaringan. Pengetahuan-pengetahuan tersebut akan menuntun kita agar dapat mencari solusi yang paling tepat untuk menanggulangi ancaman Internet worms.

1 Pendahuluan

Internet worms aktif yang menyebar melalui jaringan dengan mencari, menyerang, dan meninfeksi target, telah menjadi isu serius semenjak dikenalnya Internet worm generasi awal Morris [03], dan dalam waktu relatif singkat, dunia Internet mengalami ketakukan akan acaman sebuah worm generasi moderen yang dikenal sebagai worm Code Red.

Dua jenis worms yang disebutkan diatas adalah worms yang menginfeksi sebagian besar mesin-mesin yang menggunakan Windows OS. Pada perkembangan terakhir, worms juga menjadikan mesin-mesin yang menggunakan Linux OS sebagai target. Tercatat pada bulan Mei 1998, dunia Internet dikejutkan dengan munculnya ADMw0rm-v1 yang memanfaatkan kelemahan aplikasi bind. Pada tahun berikutnya, pada bulan September 1999, muncul generasi baru Linux worm yang dikenal sebagai Millennium Worm. Memang acaman yang terjadi akibat Linux worm tidak sebanding dengan ancaman yang dirasakan pada mesin-mesin Windows OS, sampai pada akhirnya muncul secara berturut-turut Ramen Worm dan pengembangannya Lion Worm pada bulan Januari sampai bulan Maret tahun 2001 yang memanfaatkan kelemahan-kelemahan aplikasi yang umum digunakan pada mesin Linux seperti wu-ftpd, rpc.statd, bind, LPRng, mountd dan qpopper.

Di tahun 2001, seorang peneliti di U.C. Berkeley Nicholas C Weaver melakukan analisis terhadap teknik penyebaran Internet Worms yang disebutnya sebagai "Warhol Worm" yang dapat menyebarluas di Internet dan menginfeksi semua mesin-mesin yang vulnerable dalam waktu kurang dari 15 menit [03].

Waktu itu, saya meyakini bahwa ada variant lain dari strategi penyebaran "Warhol Worm" yang mungkin saja digunakan pada worm modern, dan dapat menyebabkan semua mesin-mesin yang vulnerable terinfeksi oleh worm tersebut. Waktu yang digunakan oleh "Warhol Worm" untuk menyebarkan diri terdengar seperti sebuah hiperbola, namun hal tersebut adalah nyata. Terbukti setelah kasus Code Red worm beroperasi melakukan probing alamat-alamat secara acak di Internet, Code Red II (versi lanjutan dan pengembangan dari versi pertama) melakukan metode probing lebih baik dengan melakukan scanning pada local subnet terlebih dahulu sebelum menghabiskan banyak bandwidth untuk melakukan probing ke seluruh bagian dari Internet secara acak.

Dalam kurun waktu yang relatif singkat, sekelompok peneliti yang tergabung dalam kelompok Crimelabs yang dimotori oleh Joze Nazario, melakukan prediksi tentang bagaimana sebuah Internet Worm diwaktu yang akan datang. Dalam tulisannya, "The Future of Internet Worms" [01] yang dipresentasikan pada acara BlackHat Briefing 2001, secara teori dijelaskan komponen-komponen (bagian [?]) yang membentuk sebuah worm.

Terdapat target eksploitasi (bagian [?]) yang sangat baik bagi Internet Worms: Microsoft IIS, Microsoft Exchange, bermacam-macam program P2P (peer-to-peer), dan program messenger. Eksploit yang baru-baru ini ditemukan berhubungan dengan aplikasi-aplikasi tersebut memungkinkan bangkitnya worm yang ganas. Walaupun sebuah eksploit dapat saja membuat sebuah worm menjadi efektif, worms yang memiliki kemampuan mengeksploitasi banyak services dan vulnerability holes akan lebih cepat menyebar dan menimbulkan lebih banyak korban.

Internet Worms modern memiliki kemampuan (bagian [?]) scanning target yang sangat baik, dan juga dilengkapi dengan kemampuan melindungi diri dari proses pembersihan yang dilakukan oleh Antivirus, serta memiliki kemampuan mengeksploitasi attacks baru setelah worm tersebut dirilis ke Internet.

Beruntung, seiring dengan tingkat ancaman yang semakin tinggi, para pakar Internet berupaya dan bekerjasama menanggulagi masalah ini dan menyediakan beberapa solusi yang dapat digunakan sebagai langkah perlindungan dan pembersihan dari worm. Kerjasama antar banyak pihak seperti koordinasi antar ISP (Internet Services Provider) dan CERT (Computer Emergency Response Team) sangat banyak membantu dalam memecahkan masalah ini dan mengurangi tingkat ancaman Internet Worm. Perlindungan yang dapat dilakukan untuk melindungi sistim komputer dan jaringan dari ancaman Internet Worm dijelaskan pada bagian [?].

2 Teori Pembentukan Sebuah Worm

Joze Nazario pada tulisannya, "The Future of Internet Worms" [01], membahas komponen-komponen pembentuk sebuah worm secara teoritis. Sangat penting untuk diingat bahwa istilah 'worm' adalah bentuk mudah penjabaran istilah 'autonomous intrusion agent' dimana worm adalah program komputer yang mampu menyebar dan menggandakan-diri secara otomatis dan berpotensi untuk menyebar dengan sangat cepat di Internet. Dengan sudut pandang teoritis, kita dapat memilah-milah bagian dari sebuah worm dan membaginya menjadi beberapa kategori komponen [01].

Pada core system worm jenis apapun terdapat enam komponen pembentuk. Sebuah worm dapat mempunyai salah satu atau semua dari komponen-komponen tersebut, namun yang sering digunakan adalah kombinasinya. Sejak awal tahun 2001, kebanyakan worm bersifat monolitik, yang berarti setiap salinan dari worm adalah identik dengan worm pembentuknya [01].

Komponen-komponen tersebut adalah:

- kemampuan melakukan pengintaian
- kemampuan melakukan attack secara spesifik
- sebuah command interface
- kemampuan berkomunikasi
- kecerdasan, dan
- kemampuan attack yang tidak digunakan

Berdasarkan beberapa komponen tersebut, strategi deteksi dan preventif dapat dikembangkan lebih teliti ketika sebuah worm atau struktur sistim worm tersebut cacat pada komponen-komponen tersebut.

Definisi dari komponen-komponen pembentuk sebuah worm dijelaskan pada sub-bagian berikut ini.

2.1 Pengintaian

Mekanisme pengintaian atau pengumpulan informasi yang dilakukan oleh worm dilakukan untuk mendapatkan informasi tentang sistim-sistim komputer dan jaringan terdekat, mengidentifikasi, dan menjadikannya sebagai target.

Dengan mengindentifikasi karakteristik sebuah sistim secara lebih spesifik, atau lebih tepat pada informasi vulnerability-nya, worm dapat menentukan targetnya. Hal yang serupa umumnya dilakukan oleh seorang penyusup yang melakukan attack secara manual. Namun yang membedakan adalah worms dapat melakukan aksinya secara otomatis ketika menemukan target.

2.2 Kemampuan Melakukan Attack Secara Spesifik

Sebuah worm dapat melakukan attack secara spesifik didahului oleh proses pengintaian atau tidak, dengan

tujuan mendapatkan akses masuk dan menguasai sistim yang menjadi target. Proses mendapatkan akses masuk biasanya melibatkan penggunaan remote eksploit memanfaatkan kelemahan sistim target seperti buffer overflows, error pada CGI-BIN, format string bugs, atau sejenisnya. Sedangkan untuk proses mendapatkan akses penuh untuk menguasai sistim, jika tidak mendapatkan akses penuh pada saat melakukan attack pertama (untuk mendapatkan akses masuk), akan melibatkan penggunaan injeksi Trojan Horse atau metode lain yang sejenis seperti eksploitasi sistim dari localhost.

Worms yang memiliki kemampuan attack pada banyak tipe sistim, biasanya berukuran besar, dan tentu saja hal ini sangat tidak efektif dan efisien dalam melangsungkan proses attack. Mensiasati hal itu, dan menjaga agar ukuran worm tetap mungil, worm dapat saja menggunakan teknik mail message, mengirim notifikasi kepada pembuat worm atau siapapun yang menjalankan attack menggunakan worm untuk pertama kali, yang mengabarkan bahwa sistim X telah dikuasai dan menyerahkan wewenang sepenuhnya untuk melakukan proses eksekusi secara manual. Metode lain yang dapat digunakan sebagai alternatif adalah dengan melakukan file transfer, yaitu dengan mendownload sub-program yang dapat dieksekusi untuk target yang spesifik.

2.3 Command Interface

Sebuah sistim yang terdiri dari banyak titik hanya dapat berguna jika dikontrol oleh sesuatu yang sama. Dapat berupa mekanisme kontrol interaktif, ketika seorang penguna mampu mengarahkan titik-titik tersebut, aau melalui kanal komunikasi yang meneruskan kontrol pada setiap titik dibawahnya.

Jaringan worms adalah anak sebuah sistim jaringan dalam sebuah lingkaran Distributed Denial of Service (DDoS). Biasanya pada titik-titik tersebut terdapat dua tipe command interface, satu adalah tipe interaktif, dimana ketika sebuah remote control shell didapatkan, dan yang lainnya adalah otomatis, dimana titik tersebut dikontrol oleh beberapa master.

Secara tradisional, penyusup telah menempatkan beberapa bentuk backdoor kedalam sistim. Bentuknya beragam, seperti pada sistim UNIX, backdoor tersebut dapat dikonfigurasikan untuk menerima sebuah password yang dapat memberikan akses penuh secara administratif (root access), atau pada sistim dekstop seperti Windows PC atau Macintosh, program backdoor dapat berupa Trojan Horse yang mendengarkan network socket untuk menerima perintah.

2.4 Kemampuan Berkomunikasi

Karena yang menjadi target berada pada titik lain dalam sebuah jaringan, worms harus memiliki kemampuan berkomunikasi seperti: mengirim request, melakukan network scanning, melakukan attack, atau kegiatan berkomunikasi menggunakan media jaringan lainnya.

Kanal komunikasi yang digunakan biasanya tersembunyi atau dienkrip. Metode ini umum digunakan oleh cracker yang melakukan attack secara manual. Mekanisme transport pun beragam, seperti paket-paket ICMP atau covert channel.

2.5 Kecerdasan

Internet worms modern mampu mencatat korban dan lokasi yang telah dilalui. Hal ini biasanya menggabungkan beberapa komponen pembentuk seperti command interface, dan kemampuan berkomunikasi.

Sebagai contoh, banyak worms berbasis Windows OS menggunakan IRC sebagai media notifikasi atau mekanisme intelejensi. Ketika mereka berhasil menginfeksi sebuah sistim, mereka akan melakukan sebuah koneksi ke IRC server yang telah ditentukan, dan masuk kedalam sebuah channel IRC yang rahasia, memberitahukan lokasi dan password yang dapat digunakan sebagai akses masuk.

2.6 Kemampuan Attack yang Tidak Digunakan

Komponen ini adalah salah satu dari komponen yang sulit diimplementasikan. Secara garis besar, worm dilengkapi oleh sejumlah kemampuan melakukan attack secara komplit untuk banyak tipikal sistim target. Hal tersebut akan semakin memperbesar konstanta sistim yang menjadi target. Karena kemampuan attack yang tidak digunakan tersebut, ukuran dari worm akan menjadi lebih besar, dan

cenderung memperlambat proses penyebaran, namun disisi lain, worm yang memiliki komponen ini sangat berbahaya sekali karena memilik kriteria target yang lebih banyak dari worm yang biasanya.

3 Target Potensial

Telah disinggung dibagian [?], terdapat target eksploitasi yang sangat baik bagi Internet Worms: Microsoft IIS, Microsoft Exchange, bermacam-macam program P2P (peer-to-peer), dan program messenger. Eksploit yang baru-baru ini ditemukan berhubungan dengan aplikasi-aplikasi tersebut memungkinkan bangkitnya worm yang ganas. Walaupun sebuah eksploit dapat saja membuat sebuah worm menjadi efektif, worms yang memiliki kemampuan mengeksploitasi banyak services dan vulnerability holes akan lebih cepat menyebar dan menimbulkan lebih banyak korban.

Sepertinya Microsoft IIS telah menjadi target favorit Internet worms, bahkan setelah Code Red I dan II. IIS yang terinstal secara default pada OS Windows 2000 server dan telihat menyediakan target yang sangat homogen. Akan semakin besar kemungkinan menjadi target worms ketika lalai melakukan update.

Nilai Microsoft Exchange umumnya lebih rendah jika dibandingkan dengan IIS sebagai target worms attacks, namun akan menjadi sangat tinggi nilainya terutama pada worm tipe multimode, yang memiliki kemampuan target lebih banyak. Worm dapat menyebar dengan cepat melalui e-mail, dan karena protokol yang digunakan e-mail sudah termasuk dalam kategori "firewal friendly", perlindungan firewall tidak dapat dijadikan pegangan untuk melindungi sistim dan jaringan dari worm.

Aplikasi-aplikasi messenger seperti Yahoo! Messenger, MSN Messenger, dan, AOL IM serta program sharing file peer-to-peer seperti Kazaa, dan Bittorent juga dapat menjadi target dari Internet worms. Walaupun pada umumnya aplikasi-aplikasi tersebut digunakan pada sistim yang tidak terlalu memiliki kualitas koneksi Internet yang bagus, aplikasi-aplikasi tersebut dapat menjadi pemicu ancaman pada jaringan setingkat diatasnya, yaitu level ISP.

Penempatan aplikasi-aplikasi tersebut sebagai target Internet worm menjadi tidak relevan ketika proses update yang umumnya sering terjadi pada proses pengembangan aplikasi tersebut, sehingga untuk menggunakan fasilitas yang ditawarkan oleh aplikasi tersebut seseorang harus mendownload versi yang terbaru, dan hal ini tentunya akan mempersulit gerak penyebaran Internet worms.

4 Kemampuan Worms Dalam Melakukan Attack

Pada bagian [?] telah disinggung kemampuan yang dimilik worm secara teoritis, namun pada bagian ini dibahas mengenai kemampuan worm secara lebih spesifik dalam melakukan Attack pada sistim target.

4.1 Scanning

Secara tradisional, worm melakukan scanning secara acak pada IP Address yang dibuat menggunakan random IP Address generator, dikenal sebagai hitlist scanning. Proses pertama yang dilakukan adalah melakukan pemeriksaan terhadap status sistim target. Jika target ditemukan sedang dalam kondisi menyala, proses selanjutnya adalah mendeteksi services yang tersedia pada remote.

Worm modern tidak lagi melakukan random scanning. Metode yang digunakan lebih efektif dan efisien. Metode yang umum digunakan adalah Local Subnet Scanning. Worm akan melakukan scanning pada sistim "tetangga" yang berada pada subnet yang sama.

Selain local subnet scanning, worm modern dapat menggunakan metode scanning permutasi, berdasarkan perubahan urutan angka. Dalam sebuah proses scan permutasi, semua worms saling berbagi sebuah pseudo random permutation pada alokasi IP address. Setiap mesin-mesin yang terinfeksi selama fase hitlist atau local subnet scanning akan melakukan scanning pada titik mereka dalam permutasi yang sudah ditentukan untuk mencari mesin-mesin yang vulnerable. Ketika semua mesin yang vulnerable terinfeksi, sebuah start point baru dan memulai lagi proses scanning permutasi pada titik tersebut.

Metode scanning permutasi adalah yang paling efektif untuk digunakan namun juga menjadi ancaman yang sangat besar bagi Internet.

4.2 Multimode dan Dual Mode

Indikasi perbedaan antara worm jenis multimode dan dual mode adalah proses scanning yang dilakukan. Worm jenis multimode akan secara otomatis melakukan scanning pada banyak vulnerabilty holes secara sekaligus pada setiap titik target, sementara worm jenis dual mode akan menyelesaikan proses scanning sebuah vulnerability hole pada sejumlah target dan akan mengulanginya lagi pada vulnerability hole kedua.

4.3 Stealth Defense

Worms biasanya dilengkapi oleh kemampuan menyembunyikan dan melindungi diri dari antivirus yang umum. Hal ini menyebabkan worm akan terus bercokol meskipun pemeriksaan antivirus pada sistim menyatakan bahwa mesin tersebut telah benar-benar bersih, atau jika antivirus menemukan sebuah worm, antivirus maupun sistim yang menjadi korban tidak mampu membersihkan worm tersebut.

Worm yang telah berhasil menginfeksi file-file penting yang dibutuhkan oleh sistim untuk berjalan, menyebabkan proses removal worm akan menjadi sangat sulit.

4.4 Self Update

Walaupun keberadaannya sendiri masih diragukan, namun saya meyakini bahwa Internet Worm jenis ini telah ada. Worm ini dilengkapi dengan kemampuan mengupdate eksploit yang dibawanya untuk melakukan penyerangan, sehingga dapat ditebak, worm jenis ini sulit sekali dibasmi karena selalu memperbaharui database eksploit yang digunakan untuk membobol sistim target dengan eksploit pada vulnerability yang baru. Tentu saja, worm ini membutuhkan kemampuan untuk berkomunikasi dengan worm master dan mendownload informasi vulnerabilty terbaru.

4.5 Perlindungan Terhadap Worms

Perlindungan paling efektif adalah: keamanan berdasarkan desain, wajar (dalam konteks mudah dipantau) dan mengklasifikasikan target (sebagai contoh implementasi DMZ pada jaringan).

Walaupun attack buffer overflow bukanlah hal baru, namun ada banyak sekali network services yang masih dibuat dengan code yang tidak "safe". Audit pada source code menjadi salah satu metode antisipasi yang memungkinkan proses perlindungan jaringan terhadap Internet worms dapat berlangsung. Jika menggunakan produk yang tidak menyertakan source code, keteraturan dalam melakukan update adalah sebuah catatan tersendiri yang harus diperhatikan dengan seksama.

Firewall menyediakan kontrol akses yang sangat baik, mampu memisahkan source dan destination address dengan baik, serta melakukan NAT (Network Address Translation). Namun, Firewall bukanlah peralatan yang tepat untuk digunakan dalam melindungi tipikal intrusion seperti Worms attacks, terlebih jika worm dilengkapi dengan kemampuan-kemampuan taktis sehingga mampu membobol pertahanan sebuah Firewall.

Untuk itu, perlu dilakukan pengabungan antara Firewall dengan komponen lain seperti IDS (Intrusion Detection System), baik NIDS (Network Intrusion Detection System) maupun HIDS (Host-based Intrusion Detection System) dapat dipergunakan untuk mendeteksi adanya worm attack.

5 Kesimpulan

Tulisan ini menyediakan kerangka kerja dalam mengevaluasi Internet worms dan menganalisisnya kedalam konteks yang lebih spesifik. Sehingga dapat menjadi panduan bagi siapa saja yang hendak merencanakan atau memberikan perlindungan pada jaringan terhadap worms attack.

Analisis terhadap kemampuan attack Internet Worms yang lebih spesifik memberikan kenyataan bahwa penanggunalangan ancaman worms tersebut tidak dapat dilakukan oleh satu pihak saja. Penanggulangan membutuhkan kerjasama banyak pihak yang terkait untuk membatasi ruang gerak penyebaran worms.

Pencegahan adalah obat terbaik. Sehubungan dengan hal tersebut, maka langkah preventif yang harus diambil adalah terus menjaga sistim dan

jaringan untuk selalu update. Pengintegrasian sistim deteksi akan dapat membantu banyak mengingat kontrol akses yang dilakukan Firewall tidak dapat membendung attack yang dilakukan oleh worms.

Daftar Pustaka

[01] J. Nazario, *The Future of Internet Worms*, (2001).

[02] M. Visions, *Recent Internet Worms*, (2001).

[03] N. Weaver, *Potential Strategies for High Speed Active Worms: A Worst Case Analysis*, (2002).

[04] M. Zalewski, *I Don't Think I Really Love You, Or Writing Internet Worms for Fun and Profit*, (2001).