Internet Worms

Jim Geovedi, Bayu Krisna
jim@corebsd.or.id, krisna@corebsd.or.id

Anda tentu masih ingat iklan di media televisi beberapa tahun silam, “Anak anda cacingan?”. Berhubungan dengan cacing, tulisan ini membahas cacing yang berbeda bentuk. Cacing-cacing di Internet (Worms) adalah autonomous intrusion agents yang mampu melakukan penggandaan-diri dan menyebar dengan memanfaatkan kelemahan-kelemahan sekuriti (security flaws) pada services yang umum digunakan. Worm bukanlah sebuah fenomena baru, ditemukan pertama kali penyebarannya pada tahun 1988. Worms telah menjadi sebuah ancaman yang mematikan di Internet, walaupun sebagian besar kasus yang terjadi secara spesifik adalah pada sistim berbasis Windows. Beberapa jenis worms terbaru memanfaatkan electronic mail (e-mail) sebagai medium penyebarannya.

1 Metode Aktivasi dan Mekanisme Penyebaran

Perbedaan mendasar antara worm dan virus terletak pada bagaimana mereka membutuhkan intervensi user untuk melakukan penggandaan-diri dan menyebar menginfeksi sistim komputer. Virus lebih lambat dalam melakukan penyebaran jika dibandingkan dengan worm. Namun virus mempunyai kemampuan lebih untuk menghindari deteksi program-program anti-virus yang berusaha mengidentifikasi dan mengontrol penyebaran virus pada sistim komputer. Namun pada praktek penyebarannya sebuah virus dapat menjadi sebuah worm.

Untuk memudahkan pembahasan, kita membatasi terminologi antara worm dan virus dengan mempertimbangkan metode aktivasi yang dilakukan oleh sebuah worm -- proses yang dilakukan sebuah worm untuk mengeksekusi pada sebuah sistim komputer -- dan mekanisme penyebaran -- proses yang memungkinkan sebuah worm berkelana dari satu host ke host yang lain.

1.1 Metode Aktivasi

Pengertian bagaimana worm dapat aktif pada sebuah host berhubungan erat dengan kemampuan worm untuk menyebarkan diri, sejumlah worms dapat diatur untuk aktif secara langsung (activated nearly immediately), sementara yang lain dapat menunggu beberapa hari, minggu atau bahkan bulan untuk dapat teraktivasi dan kemudian menyebarkan-dirinya.

Aktivasi dengan intervensi user. Merupakan proses aktivasi paling lambat karena membutuhkan intervensi user untuk mengeksekusi worm tersebut, baik disadari

maupun tidak oleh user tersebut. Namun karena sosialisasi yang gencar dilakukan mengenai bahaya worm dan virus, user dapat lebih cermat dengan tidak mengeksekusi program asing atau membuka attachment e-mail dari orang yang tidak dikenalnya, hal ini tentu akan memperlambat proses aktivasi worm. Tetapi pembuat worm tidak putus asa dengan kondisi tersebut sehingga mereka melakukan teknik social engineering seperti yang dilakukan oleh virus Melissa yang seolah-olah mengirimkan informasi penting dari orang yang telah dikenal oleh korban atau pesan-pesan personal lainnya yang dikirimkan oleh virus ILOVEYOU. Walaupun Melissa adalah sebuah virus macro pada program Microsoft Word namun dengan intervensi user maka penyebaran Melissa di Internet sempat menjadi ancaman yang paling menakutkan.

Aktivasi terjadwal. Metode aktivasi worm yang lebih cepat adalah dengan menggunakan proses terjadwal pada sistim (scheduled system proces). Ada banyak program yang berjalan pada lingkungan desktop maupun server untuk melakukan proses sesuai dengan jadwal yang diberikan. Metode ini tetap membutuhkan intervesi manusia namun kali ini intervensi attacker yang dibutuhkan. Sebagai contoh, program auto-update dari sistim yang melakukan proses updating ke server vendor. Dengan melakukan update ke remote host sebagai master, seorang attacker yang cerdik dapat memanfaatkan proses tersebut untuk menyebarkan worm dengan terlebih dahulu menguasai remote host atau gateway pada network maupun di Internet dan mengganti atau menginfeksi file yang dibutuhkan pada proses update dengan kode program worm.

Aktivasi mandiri. Metode aktivasi mandiri adalah metode tercepat worm dalam menggandakandiri, menyebar, dan menginfeksi host korban. Metode ini paling populer digunakan oleh para penulis worm. Umumnya worm yang menggunakan metode ini memanfaatkan kelemahan-kelemahan sekuriti (security flaws) pada service yang umum digunakan. Sebagai contoh, worm CodeRed yang mengeksploitasi webserver IIS. Worm akan menyertakan dirinya pada service daemon yang sudah dikuasainya atau mengeksekusi perintah-perintah lain dengan privilege yang sama dengan yang digunakan oleh daemon tersebut. Proses eksekusi tersebut akan berlangsung ketika worm menemukan vulnerable service dan melakukan eksploitasi terhadap service tersebut.

1.2 Mekanisme Penyebaran

Worm menginfeksi host korban dan memasukkan kode program -- sebagai bagian dari program worm -- ke dalamnya. Kode program tersebut dapat berupa machine code, atau routine untuk menjalankan program lain yang sudah ada pada host korban. Dalam proses penyebarannya, worm harus mencari korban baru dan menginfeksi korban dengan salinan dirinya. Proses pendistribusian tersebut dapat berlangsung sebagai proses distribusi satuan (dari satu host ke host yang lain) atau sebagai proses distribusi masal (dari satu host ke banyak host). Proses distribusi masal dipertimbangkan sebagai metode penyebaran tercepat dengan asumsi batasan yang digunakan adalah satuan waktu.

Terdapat beberapa mekanisme penyebaran yang digunakan worm untuk menemukan calon korban yaitu dengan melakukan scanning, mencari korban berdasarkan target list yang sudah dipersiapkan terlebih dahulu oleh penulis worm atau berdasarkan list yang ditemukan pada sistim korban maupun di metaserver, serta melakukan monitoring secara pasif.

Scanning. Metode scanning melibatkan proses probing terhadap sejumlah alamat di Internet dan kemudian mengidentifikasi host yang vulnerable. Dua format sederhana dari metode scanning adalah sequential (mencoba mengidentifikasi sebuah blok alamat dari awal sampai akhir) dan random (secara acak).

Penyebaran worm dengan metode scanning baik sequential maupun random, secara komparatif dapat dikatakan lambat, namun jika dikombinasikan dengan aktivasi secara otomatis, worm dapat menyebar lebih cepat lagi. Worm yang menggunakan metode scanning biasanya mengeksploitasi security holes yang sudah teridentifikasi sebelumnya sehingga secara relatif hanya akan menginfeksi sejumlah host saja.

Metode scanning lainnya yang dinilai cukup efektif adalah dengan menggunakan bandwidth-limited routine (seperti yang digunakan oleh CodeRed, yaitu dengan membatasi target dengan latensi koneksi dari sistim yang sudah terinfeksi dengan calon korban yang baru), mendefinisikan target yang hanya terdapat pada local address (seperti dalam sebuah LAN maupun WAN), dan permutasi pada proses pencarian.

Scanning yang dilakukan worm tidaklah spesifik terhadap aplikasi sehingga attacker dapat menambahkan sebuah exploit baru pada sebuah worm yang sudah dikenal. Sebagai contoh, worm Slapper mendapatkan muatan exploit baru dan menjadikannya sebuah worm baru yaitu Scalper.

Secara umum, kecepatan scanning yang dilakukan adalah terbatas pada kombinasi faktor seperti; jumlah mesin-mesin yang vulnerable, desain dari scanner, dan kemampuan network monitoring system yang mampu mengidentifikasikan keberadaan worm dengan meningkatnya trafik yang cukup signifikan.

Target Lists. Sebuah worm dapat memiliki target list yang sudah ditentukan sebelumnya oleh penulis worm tersebut. Dengan target list yang sudah ditentukan terlebih dahulu membuat sebuah worm lebih cepat dalam menyebar, namun tentu saja penyebaran tersebut akan sangat terbatas karena target berdasarkan sejumlah alamat di Internet yang sudah ditentukan.

Selain itu, worm dapat menemukan list yang dibutuhkan pada host korban yang sudah dikuasainya, list ini umumnya digunakan oleh worm yang metode penyebarannya berdasarkan topologi network. Informasi yang didapat contohnya adalah IP address sistim tersebut dan worm mengembangkannya menjadi sebuah subnet pada LAN atau WAN.

Target list juga dapat diperoleh pada metaserver (server yang memberikan informasi sejumlah server yang memiliki service yang sama). Sebagai contoh, metaserver Gamespy memiliki daftar server yang menyediakan service game online. Sebuah worm yang memanfaatkan metaserver akan melakukan query terlebih dahulu untuk mengetahui keberadaan target yang baru. Metode ini juga dapat mempercepat proses penyebaran sebuah worm yang menyerang webserver, worm dapat menggunakan Google atau mesin pencari lainnya sebagai metaserver untuk menemukan target.

Monitoring secara Pasif. Worm pasif tidak mencari korbannya, namun worm tersebut akan menunggu calon korban potensial dan kemudian menginfeksinya. Walaupun metode ini lebih lambat namun worm pasif tidak menghasilkan anomalous traffic patterns sehingga keberadaan mereka akan sulit diketahui. Sebagai contoh, "anti-worm" CRClean tidak membutuhkan aktivasi user, worm ini menunggu serangan worm CodeRed dan turunannya, kemudian melakukan respon dengan melakukan counter-attack. Jika proses counter-attack berhasil, CRClean akan menghapus CodeRed dan menginfeksi korban dengan menginstal dirinya pada mesin. Sehingga CRClean dapat menyebar tanpa melakukan proses scanning.

2 Motivasi dan Muatan

2.1 Motivasi Serangan

Walaupun sangat penting untuk mengetahui teknologi yang digunakan oleh Internet worms, namun untuk dapat memahami ancaman yang berasal dari sebuah worm secara alam perlu dipahami motivasi dari intruders (seperti penulis worm), serta jika memungkinkan dapat mengidentifikasi siapa sebenarnya intruder tersebut.

Ada banyak motivasi yang menyebabkan sebuah worm dibuat namun berikut ini adalah motivasi umum yang mendasari serangan worm.

Pride and Power. Intruder (juga pembuat worm) termotivasi untuk mendapatkan kekuasaan dan show-off pengetahuan mereka dengan merusak host orang lain. Intruders ini umumnya tidak terorganisir dengan baik dan menemukan targetnya secara random. Jika mereka menemukan sebuah sistim yang lemah dan vulnerable terhadap sebuah attack maka mereka akan melangsungkan attack pada sistim tersebut.

Keuntungan Komersial. Berkaitan dengan perkembangan dunia ekonomi yang semakin hari semakin bergantung pada kinerja komputer untuk menjalankan operasional bisnis sehari-hari, serangan elektronik yang ditujukan ke sebuah domain dapat secara serius menganggu transaksi yang sedang berlangsung. Sebuah serangan worm dapat dilakukan untuk mendapatkan profit dengan melakukan manipulasi finansial atau membatasi ruang-gerak kompetitor.

Pemerasan. Karena sebuah worm dapat dibuat untuk melangsungkan serangan DOS (Denial of Service) tanpa henti, pemerasan terhadap sebuah perusahaan dapat dilakukan dan serangan baru dapat dihentikan jika terjadi transaksi pembayaran sesuai yang diinginkan oleh attacker. Motivasi ini lebih terorganisi secara individual maupun kelompok.

Protes. Seseorang yang memiliki pengetahuan yang cukup untuk menulis sebuah worm dapat melangsungkan serangan jika ia merasa dirugikan oleh suatu pihak tertentuk. Ia melakukan protes terselubung dengan menyebarkan worm di Internet. Protes tersebut juga dapat berdampak negatif pada institusi yang menjadi target, seperti SCO dan Microsoft yang baru-baru ini mendapatkan serangan DOS yang ditujukan kepadanya. Protes politik juga dapat menjadi muatan dari serangan worm. Sebagai contoh, worm Yaha Mail dibuat sebagai tool dari protes politik yang diklaim sebagai pro India dan melakukan serangan DOS pada websites milik pemerintah Pakistan.

Terorisme. Secara obyektif, worm dapat dimanfaatkan oleh kelompok teroris. Oleh karena ada banyak sistim komputer yang terhubungkan ke Internet berlokasi di negara-negara maju, maka sebuah serangan worm dapat ditujukan sebagai bentuk terorisme. Attacker dapat menyertakan muatan teror Al-Qaeda atau kelompok-kelompok anti-globalisasi lainnya untuk menyerang.

2.2 Muatan (Payload)

Berkaitan dengan motivasi penyebaran, muatan yang ada pada sebuah worm dapat beragam. Berikut ini adalah muatan yang sering ditemukan pada worm.

Tanpa muatan atau non-fungsional. Sebuah worm yang memiliki bug pada kode program yang berhubungan metode penyebaran biasanya gagal untuk menyebar, namun worm yang memiliki bug pada muatannya tetap dapat menyebar dan menimbulkan efek serius seperti peningkatan network traffic atau secara aktif melakukan identifikasi host yang vulnerable.

Backdoor. Worm CodeRed II membuat sebuah backdoor pada host korban yang memungkinkan semua orang dapat mengeksekusi program pada korban dari sebuah browser. Hal tersebut juga memicu peningkatan serangan worm anti-CodeRed yang berusaha mengeksploitasi backdoor tersebut.

Remote DOS. Muatan umum dari worm adalah kemampuan untuk melakukan serangan DoS (Denial of Service). Worm tersebut memiliki tool yang dapat melakukan serangan terhadap sebuah target yang sudah ditentukan atau tergantung pada komando seseorang yang membuatnya mampu melakukan serangan DDoS (Distributed Denial of Service).

Melakukan update. Sejumlah worm terdahulu seperti W32/Sonic memiliki muatan untuk melakukan update. W32/Sonice melakukan proses query terhadap sejumlah

website untuk mendapatkan kode program yang baru bagi dirinya. Kemampuan ini dapat digunakan oleh DDoS tool untuk melakukan update pada program-program yang menjadi zombie. Jika kontrol untuk melakukan update masih terus berlangsung maka sebuah modul eksploit dapat disertakan sehingga menjadikan worm tersebut mampu menyebar lebih cepat dan mendapatkan korban lebih banyak lagi.

Spionase dan Pengumpulan Data. Worm dapat dilakukan sebagai alat untuk melakukan spionasi dan pengumpulan data dengan mencari keyword tertentu seperti nomor kartu kredit atau informasi penting lainnya pada dokumen-dokumen yang tersimpan pada host yang sudah menjadi korban.

Pengerusakan Data. Ada banyak virus dan worm yang melakukan pengerusakan data seperti Chernobyl dan Klez, yang memiliki perintah-perintah penghapusan data. Karena worm dapat menyebar dengan cepat, mereka dapat mulai menghapus atau memanipulasi data dari awal proses infeksi.

Pengerusakan Hardware. Walaupun sebagian besar BIOS memiliki kemampuan untuk mencegah proses reflashing, beberapa worm memiliki routine yang mampu melakukan pengerusakan terhadap BIOS jenis tertentu.

Coercion. Dengan muatan yang coercive, sebuah worm tidak menimbukan kerusakan kecuali jika worm tersebut diganggu. Seperti worm yang memberikan pilihan pada user: mengijinkan worm tersebut tinggal pada sistim dan tidak melakukan pengerusakan, atau menghapus worm tersebut namun menimbulkan efek yang buruk dengan kerusakan pada sistim.

3 Mendeteksi Internet Worms

Sebuah firewall telah dikembangkan sebagai alat untuk mendeteksi anomali traffic yang berasal dari Internet dan menghasilkan logfile yang memberikan peringatan bahwa worm menyerang dengan sebuah port tertentu sebagai target. Firewall dapat melakukan blocking akses sampai administrator melakukan analisis dan recovery jika diperlukan.

Masalah yang umum ditemukan dalam melakukan respon otomatis secara akurat adalah mendeteksi dan menganalisa sebuah worm yang sedang beroperasi dan menginfeksi ke sebuah network. Bagian ini mendiskusikan strategi-strategi yang telah eksis maupun baru dalam mendeteksi keberadaan sebuah worm.

Detektor dapat berupa sebuah komputer atau device lain yang berdiri sendiri, terletak pada DMZ (De-Militarized Zone), atau pada sebuah backbone, yang memiliki kemampuan mendeteksi secara lokal atau terpusat. Apapun detektor yang digunakan haruslah sensitif dalam skala network yang besar untuk mengurangi false positives dan false negatives. Detektor dapat dikatakan berhasil jika mampu mendeteksi kejadian anomali dari beberapa tipe worm, kejadian anomali tersebut dapat diketahui

dari pola trafik yang dihasilkan sebagai konsekuensi dari teknik penyebaran worm tersebut.

3.1 Deteksi pada Host

Host detection. Program peer-to-peer maupun protokol Windows sharing dapat digunakan sebagai medium penyebaran worm, akibatnya mekanisme query worm sama seperti yang dihasilkan oleh program peer-to-peer 'biasa'. Hal tersebut menyebabkan proses deteksi pada network-level akan mengalami kesulitan kecuali implementasi IDS dilakukan untuk mengenali pola-pola tersebut. Dalam implementasinya, IDS akan menganalisa pola-pola tertentu pada trafik berdasarkan signature database yang dimilikinya.

Anti-virus Behavior Blocking. Behavior blocking adalah teknik yang digunakan anti-virus dalam menghentikan program-program jahat dalam melakukan aksinya. Walaupun dinilai sebagai upaya yang berhasil, teknik ini tidak diberdayakan secara luas karena faktor usability dan false positives.

Wormholes dan Honeyfarms. Sebuah honeypot adalah sebuah host yang ditujukan untuk dikuasai oleh intruder dalam upaya mendeteksi dan menganalisa perilaku intruder. Honeypot yang didistribusikan pada sebuah network (honeynet) dapat membentuk detektor yang akurat kecuali faktor harga (terutama hardware dan admistration costs) menjadi faktor penghalang diimplementasikannya honeynet.

Sebagai contoh implementasi honeypot yang 'hemat' adalah dengan membuat sebuah honeypot system pada network yang terpisah dari workstations atau server dan melakukan traffic redirection pada port-port tertentu, yang diduga sebagai trafik yang digunakan oleh worm untuk menyebar, ke honeypot tersebut. Sebuah honeypot dapat menggunakan teknologi 'virtual machine' untuk membuat image dari banyak sistim yang vulnerable.

3.2 Deteksi pada Network

Deteksi pada LAN atau WAN. Sebuah mesin yang terinfeksi oleh worm akan menghasilkan trafik scanning yang dapat dideteksi. Proses deteksi dapat dilakukan pada gateway atau IDS yang diletakkan diantara gateway dan LAN atau WAN.

Deteksi pada level ISP atau Backbone. Telah diketahui bahwa untuk menyebarkan dirinya sebuah umumnya worm melakukan proses scanning terlebih dahulu untuk menemukan target yang baru. Meningkatnya network traffic ISP atau backbone secara dramatis dapat mengindikasikan bahwa worm telah menyerang network tersebut.

4 Respon dan Recovery

4.1 Respon

Malware seperti worm dan virus dapat menyebar lebih cepat dari pada kemampuan manusia untuk menganalisa dan meresponinya. Sebuah strategi pertahanan yang baik menghadapi worm haruslah dapat dilakukan secara otomatis. Sebuah respon otomatis dapat memperlambat dan membatasi ruang-gerak worm.

Respon otomatis yang diberikan biasanya berupa blocking terhadap aktifitas worm. Kelemahan respon otomatis yang umum adalah terjadinya respon terhadap false positive dan false negative. False positive adalah situasi dimana respon diberikan namun tidak terjadi indikasi adanya worm, sementara false negative adalah situasi dimana worm benar-benar menyerang namun respon tidak diberikan.

Keputusan untuk menanggapi keberadaan worm pada network haruslah bijak. Berarti dalam pengambilan sebuah keputusan tersebut haruslah berdasarkan analisa teknis yang melibatkan banyak aspek seperti statistik, usage policy, maupun security advisory.

Host Response. Sebuah proses respon pada sistim komputer akan melibatkan personal firewall yang mampu membaca alerts yang dihasilkan oleh host-based IDS. Pada level ini, respon yang diberikan dapat menjadi lebih efektif dalam membendung aktifitas worm.

Network Response. Respon pada level ini haruslah memungkinkan untuk mengkombinasikan teknik blocking ketika mendapat alert dan mampu memilah kelas dari trafik yang diduga sebagai worm yang sedang menyebar. Network-based IDS seperti snort dan prelude dapat digunakan untuk mengidentifikasi keberadaan worm dengan menganalisa network traffic secara pasif.

ISP Response. Walaupun tingkat kesulitan dalam melakukan respon otomatis pada level ini cukup tinggi, namun proteksi dengan skala sistim yang lebih besar dapat menjadi pertimbangan. Implementasi respon otomatis pada level ISP haruslah terlebih dahulu teruji dengan baik karena terjadinya false positive dan false negative dapat dengan mudah terjadi.

4.2 Recovery

Proses recovery dipertimbangkan sebagai salah satu upaya untuk memperlambat penyebaran worm. Dengan memulihkan kondisi sistim yang terinfeksi setidaknya akan mengurangi sebuah penyebaran baru dari worm. Beberapa metode berikut adalah upaya dalam melakukan recovery terhadap serangan worm.

Anti-worms. Walaupun bersifat ilegal dan kurang praktis, sebuah anti-worm atau worm 'putih' dapat menutupi security holes dan membatasi ruang-gerak worm jenis lain. Terlihat sangat atraktif namun beberapa batasan signifikan membuatnya bersifat tidak praktis, selain itu faktor hukum membuat anti-worm tidak dibenarkan secara hukum. Batasan yang signifikan dari anti-worm adalah keterbatasannya untuk memperbaiki kerusakan yang ditimbulkan oleh satu jenis worm saja.

Sekurang-kurangnya terdapat 3 (tiga) jenis anti-worm yang pernah ada di Internet: Cheese worm, yang menyebar dengan menggunakan backdoor yang dibuat oleh 1ion worm, Code Green, yang memanfaatkan hole yang dibuat oleh CodeRed II, dan CRClean yang memberikan respon terhadap serangan CodeRed II.

Distribution patch dan update. Metode recovery dengan mendistribusikan patch update untuk program-program yang vulnerable pada sebuah sistim komputer dinilai sebagai metode yang efektif. Proses distribusi dapat dilakukan oleh vendor software maupun adminstrator yang menangani sejumlah besar host pada LAN atau WAN.

Salah atu kekurangan metode ini adalah ketika intruder dapat menggunakan worm untuk menguasai sejumlah besar host dan melakukan DOS ke host lain yang akan melakukan respon terhadap serangan worm tersebut. Target dari DOS biasanya adalah vendor dari program-program yang vulnerable dan dimanfaatkan oleh worm.

5 Kesimpulan

Sebagai autonomous intrusion agents, Internet worms merupakan ancaman bagi network dalam skala kecil maupun besar. Setelah diketahui bagaimana metode umum penyebaran, mekanisme, motivasi dibuatnya sebuah worm, dan deteksi keberadaan worm pada sebuah host maupun network, maka perlu penanganan secara serius dalam menanggulagi wabah Internet worms. Bagaimana mengantisipasi serangan worm saat ini maupun dimasa mendatang yang lebih beragam menjadi sebuah pekerjaan rumah baru yang tidak mudah. Perlu kerjasama berbagai pihak terkait seperti penyelenggara jasa layanan akses Internet agar tidak terjadi dampak yang lebih buruk.

6 Referensi

1. Vern Paxson, Stuart Staniford, and Nicholas Weaver, How to Own the Internet in Your Spare Time, Proceedings of the 11th USENIX Security Symposium (Security '02), 2002.
2. David Moore, Colleen Shannon, Geoffrey Voelker and Stefan Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code, Proceedings of the 2003 IEEE Infocom Conference, San Francisco, CA, April 2003.
3. Jose Nazario, The Future of Internet Worms, Blackhat Briefings, July 2001.

4. CERT, CERT Advisory CA-2000-04 Love Letter Worm, http://www.cert.org/advisories/CA-2000-04.html.
5. Arno Wagner, Thomas Dübendorfer, Bernhard Plattner, Roman Hiestand, Experiences with Worm Propagation Simulations, ACM Workshop on Rapid Malcode (WORM) 2003, November 2003.
6. Nicholas C Weaver, Warhol Worms: The Potential for Very Fast Internet Plagues, http://www.cs.berkeley.edu/ ~ nweaver/warhol.html.
7. Eugene H. Spafford, The Internet Worm Program: An Analysis, ACM SIGCOMM Computer Communication Review, 19(1):17--59, January 1989.
8. Paul Boutin, The Fix Is In – Programmers can stop Internet worms. Will they?, http://slate.msn.com/id/2081943/.
9. Symantec, Security Response, http://securityresponse.symantec.com/.
10. Networm.org, The Worm Information Center, http://www.networm.org/.

7 Tambahan

7.1 W32.Netsky.U

W32.Netsky merupakan sebuah worm yang mengandakan dirinya melalui e-mail yang dikirimkan secara masal. Memiliki banyak varian, sampai tulisan ini dibuat varian terbaru worm W32.Netsky adalah W32.Netsky.U@mm (juga dikenal sebagai W32/Netsky.u@MM, W32/Netsky-U, WORM_NETSKY.U, Win32.Netsky.U). Menginfeksi sistim operasi Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, dan Windows XP.

Muatan worm W32.Netsky.U adalah melakukan DoS ke sejumlah website pada tanggal 14 April 2004 sampai 23 April 2004, selain itu worm ini akan mengirimkan banyak email ke alamat yang diperoleh pada file yang terdapat pada host korban. W32.Netsky juga menginstal sebuah backdoor yang memungkinkan seseorang dapat login ke dalam sistim tanpa melewati proses otentifikasi yang semestinya.

Setelah berhasil mengeksploitasi host korban, W32.Netsky.U akan menyalinkan diri sebagai `%Windir%\SymAV.exe` (`%Windir%` merupakan variable dimana lokasi instalasi default Windows berada). Selanjutnya worm tersebut akan melakukan serangkaian perintah seperti membuat mutex, membuat sebuah file MIME-encoded, dan menambahkan sebuah entry pada registry Windows.

Worm W32.Netsky.U menginstal sebuah backdoor yang mendengarkan port TCP 6789 yang memungkinkan oranglain untuk mengirimkan executable file dan kemudian secara otomatis mengeksekusinya.

Pada tanggal 14 April 2004 sampai 23 April 2004, worm akan melakukan serangan DoS ke sejumlah website seperti: www.cracks.am, www.emule.de, www.kazaa.com, www.freemule.net, dan www.keygen.us.

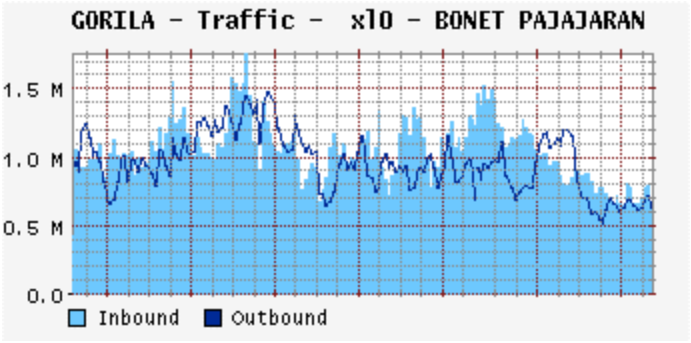
Untuk menyebarkan dirinya, worm W32.Netsky.U akan melakukan pencarian sejumlah file seperti file yang berekstensi .asp, .cgi, .html, .php, dan lain-lain guna mendapatkan daftar alamat e-mail yang nantikan akan dikirimi salinan worm tersebut. Dengan ukuran attachment sebesar 18,432 bytes dan target yang banyak, network yang terkena worm ini dapat dipastikan akan mengalami gangguan dengan terjadinya lonjakan trafik pada transmisi e-mail.

Informasi detail mengenai W32.Netsky.U serta bagaimana cara mengatasinya dapat dilihat pada website Symantec, http://www.symantec.com/avcenter/venc/data/w32.netsky.u@mm.html.

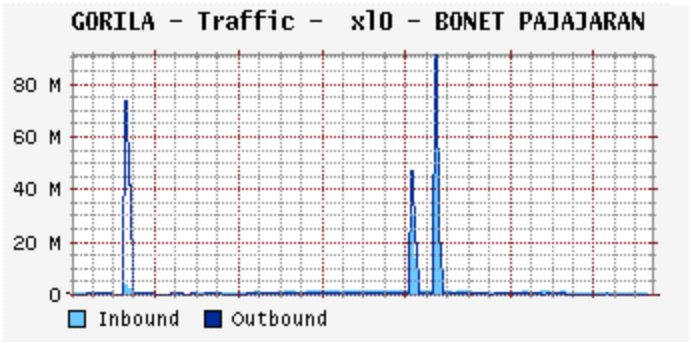
7.2 Lonjakan Network Traffic

Selama bulan Februari sampai Maret 2004, network PT. BoNET Utama (salah satu subnet ISP IndoNET yang berlokasi di Bogor), telah terjadi serangkaian gangguan pada network akibat penyebaran worm yang menginfeksi sejumlah besar klien dial-up dan wireless.

Umumnya, POP (Point of Presence) Bonet Pajajaran setiap harinya mendistribusikan traffik dengan rata-rata 750 kbps.



Ketika worm sedang aktif untuk melakukan scanning atau mengirimkan e-mail secara masal, terjadi lonjakan network traffic yang cukup drastis mencapai 90 Mbps.



8 Kredit

Michael S. Sunggiardi dan Team BoNET, Judith MS.

Hengky Anwar, Stephen Chen, Syam A. Yanuar, Y. Fery Wibowo, Chiank, Dominick Dreiser, Reza Muhammad, Randi Malikul Mulki, Arif Wicaksono, Indra Kusuma, D. Wangsa Sunarya.

CoreBSD Digital Research Group adalah sekelompok anak muda yang tertarik pada bidang computer security dan sistim operasi komputer *BSD. Kelompok yang tidak pernah mendeklarasikan secara resmi kapan berdirinya, berkumpul pada sebuah ruang chat #corebsd di IRC server Efnet. Informasi lengkap mengenai kelompok CoreBSD dapat dilihat pada website http://corebsd.or.id/.