BAB III

TINDAK PIDANA *CRACKING* MENGGUNAKAN *BOTNET* TERHADAP SISTEM KOMPUTER

A. Modus Operandi Tindak Pidana *Cracking* Menggunakan *Botnet* Terhadap Sistem Komputer

Pada perkembangannya internet ternyata membawa sisi negatif, dengan membuka peluang munculnya tindakan-tindakan anti sosial yang selama ini dianggap tidak mungkin terjadi atau tidak pernah terpikirkan akan terjadi. Sebuah teori menyatakan *crime is product of society its self* yang secara sederhana dapat diartikan bahwa masyarakat itu sendirilah yang menghasilkan kejahatan. Kejahatan yang lahir sebagai dampak negatif dari perkembangan aplikasi internet ini sering disebut *cyber crime*. Berdasarkan pengertian tersebut, tampak bahwa *cyber crime* mencakup semua jenis kejahatan beserta modus operandinya yang dilakukan sebagai dampak negatif apikasi internet. Definisi di atas tidak menyebutkan secara spesifik dari karakteristik *cyber crime*. Definisi ini mencakup segala kejahatan yang dalam modus operandinya menggunakan fasilitas internet[58].

Kejahatan dunia maya sudah pasti membutuhkan kemampuan *crytanalysis* (*cryptanalysis* atau analisis sandi ini adalah ilmu untuk mendapatkan

[58] Abdul Wahid dan Mohammad Labib, *Op.Cit*, Hal. 39-40

plaintext pesan tanpa harus mengetahui kunci secara wajar. Pemecahan sandi rahasia yang berhasil akan menghasilkan *plaintext* atau kunci. Analisis sandi juga dapat menemukan kelemahan dalam *kriptosistem* yang pada akhirya dapat menemukan kunci atau *plaintext*. Kehilangan kata kunci melalui peralatan *noncryptanalitic* disebut *compromise*[59]) yang relatif sulit karena untuk menembus keamanan komputer-komputer dan aplikasi-aplikasi di dalam dunia maya, seorang penyerang pasti menemukan kode-kode hasil enkripsi yang harus dipecahkan untuk dapat melanjutkan aksinya. Apalagi saat ini teknik-teknik enkripsi yang digunakan oleh penyedia layanan pada jaringan komunikasi elektronik sebagian besar hampir tidak mungkin untuk dipecahkan. Salah satu versi membagi kejahatan dunia maya menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan. Versi yang lain membagi tipe-tipe kejahatan dunia maya menjadi tujuh, yaitu[60]:

1. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer. Penggunaan waktu operasi komputer lain banyak digunakan untuk mengirimkan *spam e-mail* agar tidak terlacak. Saat ini terdapat sekitar 3 sampai 4 juta *bot* yang aktif di Internet. *Botnet* telah menjadi pasukan penggerak di balik organisasi kejahatan *online* karena mereka memiliki risiko yang rendah dengan potensi keuntungan yang tinggi;

[59] http://www.total.or.id/info.php?kk=Cryptanalysis, 12, Mei, 08.58 WIB

[60] Philip Renata dalam Suplemen BisTek Warta Ekonomi No. 24 edisi Juli 2000, hal.52

2. *Hacking* (istilah sebenarnya *cracking*), yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal. Menurut sebuah penelitian di Inggris, *cracker* biasanya melakukan serangan ke sistem komputer rumahan sebanyak 50 kali per malam. Serangan tersebut dapat berupa pembajakan sistem komputer seutuhnya atau hanya menjadikan komputer korban menjadi PC zombie. Selama satu bulan penelitian, salah satu PC rumahan dibiarkan terkoneksi terus dengan internet. Ternyata para *cracker* berupaya memperoleh data di dalam PC dengan menggunakan virus dan *malware* untuk menjumput informasi penting pemiliknya;
3. *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain. Salah satu kasus terbaru dengan *Trojan* terjadi pada pengguna *Voice over Internet Protoco*l (*VoIP*) *Skype*. Trojan tersebut menyebar melalui *software* komunikasi *VoIP Skype* dan berupaya mencuri *password* aplikasi tersebut. Trojan mengirim sebuah pesan melalui *tool Skype Chat* dan meminta penerimanya untuk menjemput *file sp.exe*. Virus di dalam *file* tersebut akan menyebar jika program dijalankan dan akan men-*download* kode pemrograman *Skype*, menggandakan diri, dan mengambil alih *password*. Situs *web* yang diserang oleh *trojan* ini telah ditutup untuk menghindari kerugian lebih lanjut. *Skype* adalah sebuah program

komunikasi dengan teknologi P2P (*peer to peer*). Program ini merupakan program bebas (dapat diunduh gratis) dan dibuat dengan tujuan penyediaan sarana komunikasi suara (*voice*) berkualitas tinggi yang murah berbasiskan internet untuk semua orang di berbagai belahan dunia. Pengguna *Skype* dapat berbicara dengan pengguna *Skype* lainnya dengan gratis, menghubungi telepon tradisional dengan biaya (*skypeout*), menerima panggilan dari telepon tradisional (*SkypeIn*), dan menerima pesan suara. Teknologi *skype* ditemukan oleh wirausahawan Niklas Zennström dan Janus Friis, orang yang sama yang menemukan *Kazaa* dan *Joost* (P2P untuk televisi). *Skype* lalu berkompetisi dengan protokol terbuka VoIP yang sudah ada seperti SIP, IAX, dan H.323. Grup *Skype* yang dibentuk pada bulan September 2003 lalu dibeli oleh perusahaan lelang internet raksasa di Amerika *e-Bay* pada bulan September 2005 dan bermarkas di Luxembourg, Jerman dengan kantor-kantor di London, Inggris, Praha, Rusia dan San Jose, California, A.S.[61];

4. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu dapat berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu. Ilustrasi salah satu contoh tindakan kejahatan dunia maya oleh seorang penyusup (*intruder*) melalui komputernya untuk mencuri data

[61] http://id.wikipedia.org/wiki/skype , 2, Juni, 2010, 21.29 WIB

yang sedang dipertukarkan antara dua komputer lain dengan cara memperlambat respon server;

5. *Data Diddling*, yaitu suatu perbuatan yang mengubah data *valid* atau sah dengan cara tidak sah, mengubah *input* data atau *output* data. Perbuatan penyusup yang memasuki ruang komunikasi antara para pengguna yang sah dapat berlanjut kepada *data didling*;
6. *To frustate data communication* atau penyia-nyiaan data computer;
7. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HaKI (Hak Kekayaan Intelektual). Salah satu jenis kejahatan lain pada dunia maya yang termasuk baru tetapi telah cukup banyak merugikan konsumen internet adalah *phishing*. *Phishing* adalah suatu tindak kejahatan yang menggunakan cara sosial. Pelakunya mencoba untuk mendapatkan informasi sensitif seperti *password* dan informasi detil kartu kredit dengan cara yang curang seperti dengan menyamar menjadi seseorang atau perusahaan pada suatu jaringan komunikasi elektronik, baik melalui surat elektronik, pesan instan, dengan membuat *website* yang seakan-akan dari perusahaan dagang elektronik yang menawarkan berbagai barang, ataupun sejenisnya. *Phishing* sebelumnya telah banyak dilakukan melalui telepon.

Tindak pidana *cracking* menggunakan *botnet* merupakan gabungan dari:

1. Membuat virus,

2. Melakukan serangan DoS (*Deniel of Service*) ke sebuah web,
3. *The Trojan Horse,*
4. Berbagai teknik yang digabungkan sehingga dapat menciptakan suatu zombie (*botnet*) misal teknik XSS (*Cross site scripting*).

Virus komputer merupakan program komputer yang dapat menggandakan atau menyalin dirinya sendiri dan menyebar dengan cara menyisipkan salinan dirinya ke dalam program atau dokumen lain. Virus komputer dapat dianalogikan dengan virus biologis yang menyebar dengan cara menyisipkan dirinya sendiri ke sel makhluk hidup. Virus komputer dapat merusak (misalnya dengan merusak data pada dokumen), membuat pengguna komputer merasa terganggu, maupun tidak menimbulkan efek sama sekali[62].

Virus komputer umumnya dapat merusak perangkat lunak komputer dan tidak dapat secara langsung merusak perangkat keras komputer dengan cara memuat program yang memaksa *over process* ke perangkat tertentu misalnya VGA (*Video Graphics Adapter)*, Memory bahkan Procesor terutama pada sistem operasi , seperti sistem operasi berbasis Windows (Windows 95, Windows 98/98SE, Windows NT, Windows NT Server, Windows 2000, Windows 2000 Server, Windows 2003, Windows 2003 Server, Windows XP Home Edition, Windows XP Professional, Windows XP Service Pack 1, Windows XP Service Pack 2, Windows Vista Service Pack 1) bahkan GNU/Linux. Efek negatif virus komputer terutama adalah memperbanyak dirinya sendiri, yang membuat

[62] http://id.wikipedia.org/wiki/virus_komputer, 12, Mei, 2010, 10.07 WIB

sumber daya pada komputer (seperti *CPU Real Time*, penggunaan memori) menjadi berkurang secara signifikan. Hampir 95% Virus adalah virus komputer berbasis sistem operasi Windows. Sisanya, 2% menyerang Linux/GNU dengan versi *kernel* dibawah 1.4 (dan Unix, sebagai source dari Linux, tentunya), 1% menyerang Mac terutama Mac OS 9, Mac OS X (Tiger, Leopard). 2% lagi menyerang sistim operasi lain seperti FreeBSD, OS/2 IBM, dan *Sun Operating System*. Virus yang ganas akan merusak *hardware* dan sejenisnya[63].

Virus komputer sendiri adalah sebuah istilah umum untuk menggambarkan segala jenis serangan terhadap komputer. Namun, bila dikategorikan dari cara kerjanya, virus komputer dapat dikelompokkan ke dalam kategori sebagai berikut[64]:

1. *Worm*, menduplikatkan dirinya sendiri pada *harddisk*. Ini membuat sumber daya komputer (*Harddisk*) menjadi penuh akan *worm* itu.
2. Trojan, mengambil data pada komputer yang telah terinfeksi dan mengirimkannya pada pembuat *trojan* itu sendiri.
3. Cracking, merupakan serangan langsung dari *cracker* terhadap komputer pengguna yang mengakses halaman internet tertentu, dengan atau tanpa program bantuan yang telah disisipkan di komputer pengguna.
4. *Backdoor*, hampir sama dengan *trojan*. Namun, *Backdoor* bisanya menyerupai *file* yang baik-baik saja. Misalnya *game*.
5. *Spyware*, virus yang memantau komputer yang terinfeksi.

[63] Loc.Cit.
[64] Loc.Cit.

6. *Rogue* dan *Ransomware*, merupakan program yang meniru program antivirus dan menampilkan aktivitas layaknya antivirus normal, dan memberikan peringatan-peringatan palsu tentang adanya virus. Tujuannya adalah agar pengguna membeli dan mengaktivasi program antivirus palsu itu dan mendatangkan uang bagi pembuat virus *rogue* tersebut.
7. *Rootkit*, Virus yang bekerja menyerupai kerja sistem komputer yang biasa saja.
8. *Polymorphic Virus*, virus yang gemar beubah-ubah agar tidak dapat terdeteksi.
9. Virus Telepon Seluler, merupakan virus yang khusus berjalan di telepon seluler, dan dapat menimbulkan berbagai macam efek, mulai dari merusak telepon seluler, mencuri data-data di dalam telepon seluler, sampai membuat panggilan-panggilan diam-diam dan menghabiskan pulsa pengguna telepon seluler.

Pada tipe koneksi jaringan biasa, *user* (pengguna) mengirimkan sebuah pesan untuk menanyakan otentikasi *user* yang bersangkutan ke server. Kemudian *server* merespon permintaan *user* tersebut dengan memberikan jawaban persetujuan otentikasi ke *user* tersebut. *User* tersebut mendapatkan ijin otentikasi selanjutnya dapat masuk kedalam sistem. Pada serangan DoS, *user* akan mengirimkan beberapa permintaan otentikasi ke *server*, dengan memenuhi *bandwidth server*. (*Bandwidth*/Lebar pita bahasa Inggris: *bandwidth* dalam

teknologi komunikasi adalah perbedaan antara frekuensi terendah dan frekuensi tertinggi dalam rentang tertentu. Sebagai contoh, *line* telepon memiliki *bandwidth* 3000Hz *(Hertz)*, yang merupakan rentang antara frekuensi tertinggi (3300Hz) dan frekuensi terendah (300Hz) yang dapat dilewati oleh *line* telepon ini, adalah luas atau lebar cakupan frekuensi yang digunakan oleh sinyal dalam medium transmisi. Dalam kerangka ini, *bandwidth* dapat diartikan sebagai perbedaan antara komponen sinyal frekuensi tinggi dan sinyal frekuensi rendah. Frekuensi sinyal diukur dalam satuan Hertz. sinyal suara tipikal mempunyai *bandwidth* sekitar 3 kHz, analog TV *broadcast* (TV) mempunyai *bandwidth* sekitar 6 MHz. *Bandwidth* diartikan juga sebagai takaran jarak frekuensi atau sebuah takaran lalu lintas data yang masuk dan yang keluar. Dalam dunia *hosting*, kita di berikan jatah *bandwidth* setiap bulan tergantung seberapa dalam kita menghabiskan dana. Habisnya *Bandwidth* ditentukan seberapa banyak kita meng-*upload* atau men-*download*. Semakin banyak anda melakukan aktivitas *upload*, ditambah semakin banyaknya pengunjung yang mengakses, maka semakin berkurang jatah *Bandwidth* yang diberikan, seperti www.namasitus.com diberi jatah *bandwidth* sebesar 1,5 Giga dalam sebulan. Dan sudah sejak bulan Desember rasanya jatah *bandwidth* yang diberikan kurang. Pada bulan Desember, jatah *bandwidth* habis sehari sebelum tahun baru. Dan berturut-turut bulan Januari, Februari, Maret dan April habis dalam 3 minggu. Otomatis, dalam seminggu terakhir *didats.net* tidak bisa diakses)[65]. Semua permintaan yang dilakukan oleh user memiliki alamat pengembalian yang salah, sehingga server tidak dapat

[65] http://id.wikipedia.org/wiki/bandwidth, 3, Juni, 17.23 WIB

menemukan *user* yang bersangkutan ketika ingin mencoba mengirimkan persetujuan otentikasi yang diminta oleh *user* tersebut. *Server* akan menunggu, kadang-kadang lebih dari beberapa menit, sebelum menutup koneksi atas *user* tersebut. Ketika koneksi tersebut ditutup, penyerang akan mengirimkan permintaan baru kepada *server*, dan proses otentikasi akan dimulai lagi dari awal. Begitu seterusnya sehingga mengikat layanan yang diberikan *server* untuk jangka waktu tidak terbatas. Jika hal tersebut terjadi maka user lain yang ingin mengakses sesumber (*resouces*) didalam jaringan tersebut tidak dapat melakukan koneksi karena *server* tersebut disibukkan oleh permintaan otentikasi *user* yang melakukan serangan DoS tadi. Jenis-jenis serangan yang termasuk kategori DoS:

1. *Teardrop*
2. *IP Spoofing*
3. *LAND Attack*
4. *Ping of Death*

Teardrop adalah salah satu tipe serangan *Denial of Service* (DoS). *Teardrop* adalah sebuah serangan yang memanfaatkan kelemahan yang ditemukan pada *internet protocol* dalam pengiriman paket. Ketika sebuah paket diproses, dalam penerapannya biasanya dilakukan pengecekan apakah paket yang diberikan terlalu panjang atau tidak tapi tidak melakukan pengecekan apakah paket tersebut terlalu pendek dan dibatasi. Tumpukan menerima *fragmen*/penggalan pertama paket yang dikirimkan dan mengalokasikan *memory*

untuk *fragmen* tersebut. *Offset* paket berikutnya diletakkan pada akhir dari area *memory* seperti akhir *pointer*. Tumpukan menyangka datagram berikutnya mulai pada *offset* dan menghitung akhir dari *pointer* untuk menunjukkan akhir dari paket baru yang dikirim, ini berarti ukuran paket pertama ditambah ukuran paket kedua dikurangi IP *header* kedua yang terbuang. Jumlah dari memori yang dibutuhkan sama dengan akhir *offset*. Tetapi *offset*-nya di-*spoof* pada paket kedua dan ditempatkan kedalam area memori pertama. Tumpukan mencoba untuk menyusun kembali untuk membetulkan susunannya, tetapi jika paket kedua lumayan pendek, maka *pointer*nya akan berubah tempatnya. *Pointer offset* akan tetap menuju pada akhir dari paket pertama tetapi akhir *pointer* kemudian menuju kedalam area memori, bukan pada akhir dari paket pertama. Hasil perhitungan memori yang diperlukan sama dengan (=) *end-offset* adalah negatif/minus. Pada langkah selanjutnya adalah mengalokasikan memori untuk paket baru, prosedur pengalokasian memori dapat gagal karena diberikan angka negatif sebagai sebuah *argument*. Kesalahan dalam pengalokasian memori dapat menyebabkan *host crash/ system crash* (penumpukan sistem). Serangan *teardrop* mengirimkan satu atau lebih paket UDP (UDP singkatan dari *User Datagram Protocol*, adalah salah satu protokol lapisan transpor TCP/IP yang mendukung komunikasi yang tidak andal (*unreliable*), tanpa koneksi (*connectionless*) antara *host-host* dalam jaringan yang menggunakan TCP/IP. Protokol ini didefinisikan dalam RFC 768)[66]. Paket UDP ini telah dipecah ke

[66] http://id.wikipedia.org/wiki/UDP, 3 Juni, 17.25 WIB

sebuah *host*, dan dengan ukuran *fragmen* yang benar dan *fragmen offset* yang salah, pengalokasian memori pada *host* tujuan menjadi gagal.

IP Spoofing adalah suatu trik *cracking* yang dilakukan pada suatu *server* dengan tujuan untuk mengecoh komputer target agar mengira sedang menerima data bukan dari komputer yang mengirim data tersebut, melainkan komputer target mengira menerima data dari komputer lain yang memiliki IP *Address* yang berbeda dari komputer sebenarnya yang telah mengirim data. Suatu contoh dari IP *Spoofing* adalah sebagai berikut, misalkan :

1. IP Address komputer sumber yang mengirim data adalah 203.45.98.1
2. IP Address komputer yang akan dijadikan target adalah 202.14.12.1
3. IP Address sistem yang digunakan untuk mengirimkan data adalah 173.23.45.89

Secara normal komputer target akan mengidentifikasi IP *Address* dari komputer yang mengirimkan data adalah 203.45.98.1, namun dalam trik IP *Spoofing* komputer target akan mengira bahwa data yang dikirim adalah dari komputer dengan IP *Address* 173.23.45.89. IP *Spoofing* adalah suatu teknik yang sulit untuk dilakukan karena pada kenyataannya saat melakukan teknik ini penyerang (*cracker*) tidak mendapatkan pesan atau *feedback* dari proses yang telah dilakukan apakah berhasil atau gagal. Hal ini biasa disebut dengan *blind attack*, dimana *cracker* akan selalu berasumsi bahwa serangan yang dilakukannya sudah berjalan dengan benar. Permasalahan utama dari teknik ini adalah walaupun komputer sumber berhasil mengirim data dengan IP *Address*

komputer sumber yang telah disamarkan, dan komputer yang menjadi target telah mempercayai bahwa data telah dikirm oleh komputer dengan IP *Address* yang dipalsukan, kemudian komputer target akan membalas melalui IP *Address* yang dipalsukan, bukan IP *Address* komputer sumber. IP *Spoofing* dilakukan dengan menggunakan konsep *three-way* handshake agar terjadi koneksi TCP/IP. *Transmission Control Protocol* (TCP) adalah suatu protokol yang berada di lapisan transpor (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (*connection-oriented*) dan dapat diandalkan (*reliable*). TCP dispesifikasikan dalam RFC 793. Proses pembuatan koneksi TCP disebut juga dengan *Three-way Handshake*. Tujuan metode ini adalah agar dapat melakukan sinkronisasi terhadap nomor urut dan nomor *acknowledgement* yang dikirimkan oleh kedua pihak dan saling bertukar ukuran TCP Window[67]. Secara normal three-way handshake yang terjadi adalah:

1. Komputer sumber mengirim paket SYN ke komputer target
2. Komputer target mengirim kembali paket SYN/ACK ke komputer sumber. ACK (singkatan dari bahasa Inggris: *acknowledgment*) dalam teknologi informasi adalah sebuah transmisi yang dikirimkan oleh pihak station penerima dalam jaringan kepada pihak pengirim bahwa data yang dikirimkan telah diterima dengan sempurna tanpa ada kesalahan. Jika station penerima menemukan bahwa transmisi data mengalami keterlambatan atau tidak sampai ke tujuan, maka station penerima akan mengirimkan sinyal NAK (*Negative Acknowledgment*)

[67] http://id.wikipedia.org/wiki/tcp, 3 Juni, 17.28 WIB

yang menandakan bahwa data yang dikirimkan oleh pengirim tidak sampai dan memintanya untuk mengirim kembali data yang sama[68].

3. Komputer sumber akan mengakui paket SYN dari komputer target dengan mengirim balasan berupa paket SYN ke komputer target.

Adapun yang terjadi dalam IP *Spoofing* adalah :

1. Komputer sumber mengirim paket SYN ke komputer target tapi dengan menggunakan IP *Address* yang telah dipalsukan.
2. Komputer target akan mengirim paket SYN/ACK kepada komputer dengan IP *Address* yang palsu tersebut. Dalam hal ini tidak ada cara bagi komputer sumber untuk menentukan kapan dan apakah komputer target benar-benar membalas dengan mengirimkan paket SYN/ACK ke IP *Address* yang telah dipalsukan tersebut. Hal ini merupakan bagian yang tidak diketahui oleh komputer sumber (*blind part*) dan komputer sumber hanya dapat berasumsi bahwa komputer target telah mengirim paket SYN/ACK ke IP *Address* yang telah dipalsukan tersebut.
3. Kemudian setelah beberapa waktu komputer sumber harus mengirimkan paket SYN ke komputer target untuk mengakui bahwa komputer dengan IP *Address* yang palsu telah menerima paket SYN/ACK. Koneksi TCP/IP hanya akan terjadi jika dan hanya jika ketiga langkah di atas terjadi.

[68] http://id.wikipedia.org/wiki/acknowledgment, 3 Juni, 17.26 WIB

LAND Attack atau biasa juga disebut *LAND DoS Attack* bekerja dengan cara mengirimkan paket SYN dengan IP *Address* yang telah dipalsukan yang biasa digunakan pada *handshake* antara *client* dan *host* dari suatu *host* ke semua *port* yang sedang terbuka dan mendengarkan. *port* adalah mekanisme yang mengizinkan sebuah komputer untuk mendukung beberapa sesi koneksi dengan komputer lainnya dan program di dalam jaringan. *Port* dapat mengidentifikasikan aplikasi dan layanan yang menggunakan koneksi di dalam jaringan TCP/IP. Sehingga, *port* juga mengidentifikasikan sebuah proses tertentu di mana sebuah server dapat memberikan sebuah layanan kepada klien atau bagaimana sebuah klien dapat mengakses sebuah layanan yang ada dalam *server*.

Port dapat dikenali dengan angka 16-bit (dua byte) yang disebut dengan *Port Number* dan diklasifikasikan dengan jenis *protokol transport* apa yang digunakan, ke dalam *Port* TCP dan *Port* UDP. Karena memiliki angka 16-bit, maka total maksimum jumlah *port* untuk setiap *protokol transport* yang digunakan adalah 65536 buah[69]. Jika paket diatur untuk memiliki IP *Address* sumber (*source*) dan tujuan (*destination*) yang sama, maka pada saat paket ini dikirim ke sebuah mesin (melalui IP Spoofing) akan dapat membohongi atau mengecoh mesin tersebut agar mengira bahwa mesin itu sendiri yang telah mengirim paket tersebut, dimana hal ini dapat mengakibatkan mesin *crash* (tergantung dari sistem operasi yang terdapat pada mesin tersebut). Jenis

[69] http://id.wikipedia.org/wiki/*acknowledgment*, 3 Juni, 17.26 WIB

serangan ini dapat mempengaruhi mesin dengan sistem operasi Windows 95/NT, berbagai jenis dari UNIX, termasuk juga SunOS, beberapa versi BSD UNIX, serta Macintosh. Serangan ini juga dapat mempengaruhi beberapa Cisco router, dan peralatan cetak yang berbasiskan TCP/IP (TCP/IP-*based printing devices*). *LAND Attack* dapat mempengaruhi berbagai sistem operasi dalam berbagai cara. Sebagai contoh, serangan jenis ini dapat menyebabkan mesin dengan sistem operasi Windows NT 4.0 (dengan *Service Pack 3* dan seluruh aplikasinya) menjadi lambat kira-kira dalam waktu 6 detik, setelah itu akan kembali normal tanpa ada efek lainnya. Serangan ini jika terjadi pada mesin dengan sistem operasi Windows 95 dapat menyebabkan baik itu *crash* maupun *lock-up*, sehingga mesin-mesin tersebut perlu di boot ulang. Sementara sebagian besar mesin dengan sistem operasi UNIX yang mendapat serangan ini akan *crash* atau *hang* dan user tidak dapat melakukan akes ke servis-servis yang terdapat pada mesin tersebut.

Ping of Death adalah salah satu bentuk serangan *ping attack*. Pada internet, bentuk serangan ini adalah bentuk serangan DoS (*denial of service attack*) yang disebabkan oleh penyerang yang dengan sengaja mengirimkan sebuah paket IP yang ukurannya lebih besar dari yang diijinkan oleh protokol IP yaitu 65.536 byte. Salah satu fitur dari TCP/IP adalah *fragmentation*, yang mengijinkan sebuah paket IP tunggal dipecah ke dalam bagian yang lebih kecil. Pada tahun 1996, para penyerang mulai mengambil keuntungan dari fitur ini, yaitu saat mereka menemukan bahwa sebuah paket yang dipecah menjadi bagian-bagian kecil dapat ditambah menjadi lebih besar dari yang diijinkan yaitu

65.536 *byte*. Banyak sistem operasi tidak tahu apa yang harus dilakukan ketika menerima paket dengan ukuran yang berlebihan tersebut, sehingga akhirnya sistem operasi tersebut berhenti bekerja, *crashed*, atau *rebooted*.

Serangan ping of death sangat tidak menyenangkan karena tanda-tanda atau identitas penyerang saat mengirim paket dengan ukuran yang berlebihan dapat dengan mudah disamarkan, dan karena para penyerang tidak perlu mengetahui apapun tentang mesin yang akan mereka serang kecuali IP Addressnya. Pada akhir tahun 1997, *vendor-vendor* sistem operasi telah membuat sejumlah *patch* yang memungkinkan untuk menghindari serangan ini. Beberapa *Web site* melakukan blok terhadap pesan ping ICMP pada firewall. *Firewall* atau tembok-api adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah tembok-api diterapkan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya yang mereka miliki untuk mencegah berbagai variasi berikutnya dari serangan jenis ini[70]. Ping of death juga dikenal sebagai Long ICMP. Variasi dari serangan ini termasuk jolt, sPING, ICMP bug, dan IceNewk.

Di internet banyak sekali *tools* yang dapat digunakan untuk menyerang sebuah sistem jaringan dengan menggunakan metode DoS. *Tool* tersebut adalah *attacker*. Berikut adalah penjelasan singkat tentang *attacker* dan proses kerja *tool* ini.

[70] http://id.wikipedia.org/wiki/firewall, 3 Juni, 17.29 WIB

Pada level aplikasi dimana software ini mengirmkan packet pada alamat yang telah dituju. *Software* ini membutuhkan pengetahuan mengenai IP *address* yang akan diserang dan harus terlebih dahulu mencari *port-port* yang terbuka dari Komputer tempat IP *address* yang akan diserang tersebut. *Software* ini terdiri dari 3 jenis serangan yang dapat dipilih yaitu :

1. *Syn attack*;
2. *Echo spoof*;
3. *UDP Flooding*.

Ketiga jenis serangan ini adalah termasuk jenis serangan DOS *attack* atau disebut *Denial of Service Attack* dimana serangan yang dilakukan akan menyebabkan terganggunya atau terhentinya kerja sistem yang diserang.

Syn attack adalah serangan yang menggunakan *Synhcronazation flood attack* pada pertukaran data yang menggunakan three way handshake. Pada saat penyerang mengirimkan paket pada komputer yang diserang dengan menggunakan alamat internet palsu (*spoofing*) maka komputer yang menerima akan mengirim kembali pada pada komputer penyerang dan menunggu balasan selama kurang lebih 20 detik. Pada saat bersamaan penyerang akan mengirim paket lagi sebanyakbanyaknya sehingga komputer korban akan terjadi antrian dan akhirnya *hang*.

Echo spoof merupakan serangan pada *port t* (*Echo Service*) dimana penyerang akan mengirim paket pada port 7 pada komputer korban menggunakan IP lokal palsu (*local host address*). *Echo Service* akan

memberikan respon pada alamat tersebut (pada dirinya sendiri) dan akan terjadi *loop* yang tidak terbatas. Ini akan menyebabkan sistem terganggu.

UDP flooding merupakan pengiriman data pada *port* UDP dengan menggunakan Alamat palsu. Hampir sama dengan *Syn flood attacks*. Serangan menggunakan *attacker* dapat dicegah melalui beberapa cara yaitu dengan menggunakan :

1. *Firewall* dan melakukan konfigurasi yang optimal
2. Memperbesar *Half Open* antrian pada suatu koneksi
3. Membatasi *Half Open Connection* pada satu alamat sehingga tidak dapat terlalu banyak mengirim paket.
4. Mengurangi waktu antrian suatu paket sehingga apabila terlalu lama merespon akan dihilangkan
5. Menggunakan IDS (*Intrusion Detection System*)

Trojan horse atau Kuda Troya atau yang lebih dikenal sebagai *Trojan* dalam keamanan komputer merujuk kepada sebuah bentuk perangkat lunak yang mencurigakan (*malicious software*/*malware*) yang dapat merusak sebuah sistem atau jaringan. Tujuan dari *Trojan* adalah memperoleh informasi dari target (password, kebiasaan *user* yang tercatat dalam *system log*, data, dan lain-lain), dan mengendalikan target (memperoleh hak akses pada target)[71].

Trojan berbeda dengan jenis perangkat lunak mencurigakan lainnya seperti virus komputer atau *worm* karena dua hal berikut[72]:

[71] http://id.wikipedia.org/wiki/trojan, 12, Mei, 2010, 10.09 WIB
[72] Loc.Cit.

1. *Trojan* bersifat *stealth* (siluman dan tidak terlihat) dalam operasinya dan seringkali berbentuk seolah-olah program tersebut merupakan program baik-baik, sementara virus komputer atau *worm* bertindak lebih agresif dengan merusak sistem atau membuat sistem menjadi *crash* (bertabrakan).
2. Trojan tidak mereplikasi dirinya sendiri, sementara virus komputer dan *worm* melakukannya.
3. Pada umumnya *Trojan* tidak berbahaya selama pengguna tidak terhubung pada internet atau jaringan. Karena *Trojan* dikendalikan dari komputer lain (komputer *attacker*).

Penggunaan istilah *Trojan* atau *Trojan horse* dimaksudkan untuk menyusupkan kode-kode mencurigakan dan merusak di dalam sebuah program baik-baik dan berguna; seperti halnya dalam Perang Troya, para prajurit Sparta bersembunyi di dalam Kuda Troya yang ditujukan sebagai pengabdian kepada *Poseidon*. Kuda Troya tersebut menurut para petinggi Troya dianggap tidak berbahaya, dan diizinkan masuk ke dalam benteng Troya yang tidak dapat ditembus oleh para prajurit Yunani selama kurang lebih 10 tahun perang Troya bergejolak. Kebanyakan *Trojan* saat ini berupa sebuah berkas yang dapat dieksekusi (*.EXE atau *.COM dalam sistem operasi Windows dan DOS atau program dengan nama yang sering dieksekusi dalam sistem operasi UNIX, seperti *ls*, *cat*, dan lain-lain) yang dimasukkan ke dalam sistem yang ditembus oleh seorang *cracker* untuk mencuri data yang penting bagi pengguna

(*password*, data kartu kredit, dan lain-lain). *Trojan* juga dapat menginfeksi sistem ketika pengguna mengunduh aplikasi (seringnya berupa game komputer) dari sumber yang tidak dapat dipercayai dalam jaringan Internet. Aplikasi-aplikasi tersebut dapat memiliki kode *Trojan* yang diintegrasikan di dalam dirinya dan mengizinkan seorang *cracker* untuk dapat mengacak-acak sistem yang bersangkutan[73].

Beberapa jenis Trojan yang beredar antara lain adalah[74]:

1. Pencuri *password*: Jenis Trojan ini dapat mencari password yang disimpan di dalam sistem operasi (/etc/passwd atau /etc/shadow dalam keluarga sistem operasi UNIX atau berkas *Security Account Manager* (SAM) dalam keluarga sistem operasi Windows NT) dan akan mengirimkannya kepada si penyerang yang asli. Selain itu, jenis *Trojan* ini juga dapat menipu pengguna dengan membuat tampilan seolah-olah dirinya adalah layar login (/sbin/login dalam sistem operasi UNIX atau Winlogon.exe dalam sistem operasi Windows NT) serta menunggu pengguna untuk memasukkan *password*-nya dan mengirimkannya kepada penyerang. Contoh dari jenis ini adalah *Passfilt Trojan* yang bertindak seolah-olah dirinya adalah berkas *Passfilt* yang aslinya digunakan untuk menambah keamanan *password* dalam sistem operasi Windows NT, tapi disalahgunakan menjadi sebuah program pencuri *password*.

[73] Loc.Cit.
[74] *Loc.Cit.*

2. Pencatat penekanan tombol (*keystroke logger*/*keylogger*): Jenis *Trojan* ini akan memantau semua yang diketikkan oleh pengguna dan akan mengirimkannya kepada penyerang. Jenis ini berbeda dengan spyware, meski dua hal tersebut melakukan hal yang serupa (memata-matai pengguna).
3. Tool administrasi jarak jauh (*Remote Administration Tools*/*RAT*): Jenis *Trojan* ini mengizinkan para penyerang untuk mengambil alih kontrol secara penuh terhadap sistem dan melakukan apapun yang mereka mau dari jarak jauh, seperti memformat *harddisk*, mencuri atau menghapus data dan lain-lain. Contoh dari *Trojan* ini adalah *Back Orifice*, *Back Orifice* 2000, dan *SubSeven*.
4. DDoS *Trojan* atau Zombie *Trojan*: Jenis *Trojan* ini digunakan untuk menjadikan sistem yang terinfeksi agar dapat melakukan serangan penolakan layanan secara terdistribusi terhadap *host* target.
5. Ada lagi sebuah jenis *Trojan* yang mengimbuhkan dirinya sendiri ke sebuah program untuk memodifikasi cara kerja program yang diimbuhinya. Jenis *Trojan* ini disebut sebagai Trojan virus.

(*Cross site scripting*) XSS adalah suatu teknik untuk mendapatkan *cookie* seorang *user* tertentu. Dengan menyamarkan diri sebagai *hyperlink* atau menambahkan *script* yang dapat meragukan pengunjung *website*, XSS mencuri banyak data pelanggan, seperti *user name* dan *password*. XSS memiliki ciri khas, yaitu hanya ditemukan pada *website* yang memiliki fitur dinamis, seperti

guestbook, *registrationform*, *searchform*, dan lain-lain. *Cookies* itu sendiri adalah sekumpulan teks yang berisi *user's settings* (misalnya identitas unik *user* yang digunakan untuk otentikasi dan otorisasi), *shooping chart contents*, dan data-data yang digunakan oleh suatu *website*. XSS dapat digunakan untuk mengetahui atau mencuri *cookie* dari pengunjung *website* tersebut dengan cara memasukan *script* <script>alert(document.cookie)</script>[75].

Cross site scripting adalah kelemahan keamanan yang terjadi pada penggunaan teknologi dynamic page. *Cross site scripting* dapat diartikan sebagai kelemahan yang terjadi akibat ketidakmampuan *server* dalam memvalidasi *input* yang diberikan oleh pengguna. Algoritma, yang digunakan untuk pembuatan halaman yang diinginkan, tidak mampu melakukan penyaringan terhadap masukkan tersebut. Hal ini memungkinkan halaman yang dihasilkan menyertakan perintah yang sebenarnya tidak diperbolehkan. *Cross site scripting* merupakan kelemahan yang populer untuk dieksploitasi. Namun sayangnya, banyak penyedia layanan yang tidak mengakui kelemahan tersebut dan melakukan perubahan pada sistem yang mereka gunakan. Sayangnya dengan tindakan ini konsumen atau pengguna menjadi pihak yang dirugikan.

Cross site scripting bekerja seperti penipu yang mampu mengelabui orang yang tidak waspada. Elemen penting dari keberhasilan *cross site scripting* adalah *social engineering* yang baik dari si penipu. *Social engineering* merupakan elemen terpenting yang menentukan keberhasilan penipuan yang

[75] Rachmat Saleh, *HTTP ATTACK*, Andi, Yogyakarta, 2006, hal. 67

akan dilakukan. *Cross site scripting* memampukan seseorang yang tidak bertanggung jawab melakukan penyalahgunaan informasi penting.

Sebelum sampai pada proses penyalahgunaan tersebut, penyerang mengambil langkah-langkah dengan mengikuti pola tertentu. Langkah pertama, penyerang melakukakan pengamatan untuk mencari *web-web* yang memiliki kelemahan *cross site scripting*. Langkah kedua, penyerang mencari tahu apakah *web* tersebut menerbitkan informasi yang dapat digunakan untuk melakukan pencurian infomasi lebih lanjut. Informasi tersebut biasanya berupa *cookie*. Langkah kedua ini tidak selalu dijalankan. Langkah ketiga, penyerang membujuk korban untuk mengikuti sebuah *link* yang mengandung kode, ditujukan untuk mendapatkan informasi yang telah disebutkan sebelumnya. Kemampuan *social engineering* dari penyerang diuji disini. Setelah mendapatkan informasi tersebut, penyerang melakukan langkah terakhir, pencurian maupun pengubahan informasi vital. Berikut merupakan contoh kasus dari *cross site scripting*. Anggap sebuah penyedia layanan *message board*, A, memiliki kelemahan *cross site scripting*. *Web* tersebut juga menghasilkan *cookie*. *Cookie* tersebut bertujuan agar pengguna dapat membuka jendela *browser* baru tanpa memasukkan *user name* dan *password* lagi. B, mencoba untuk mengeksploitasi kelemahan ini, meletakkan sebuah *link* yang mengandung kode yang jahat pada *message board* tersebut. C, seorang pengguna, tertarik pada *link* tersebut menekan *link* tersebut. Tanpa disadari C, *cookie* yang terdapat pada komputernya telah dikirimkan ke komputer B. Kini B dapat mengakses *message board* sebagai C hanya dengan menggantikan *cookie*-nya dengan *cookie* yang ia dapatkan dari C.

Secara singkat cara melakukan *botnet* adalah *file* yang didalamnya berupa *payload* yang dibawa oleh *worm* (virus), saat berhasil melakukan penetrasi ke sistem komputer dengan media penghubung internet dengan beberapa teknik tertentu yang telah dibahas di atas seperti *DoS Attack*, *Trojan Horses* dan *XSS*. *bot* untuk *botnet* biasanya akan langsung mengubah settingan di *registry* agar *file executable botnet* dapat berjalan langsung di masa *start up* komputer, jadi dalam bahasa lain, *botnet* merubah konfigurasi *registry* dan menginfeksi MBR dengan tujuan agar *botnet* dapat aktif saat pertama kali komputer dinyalakan dan sistem operasi diaktifkan. Sebagai media komunikasi antara *bot header* (bot master) dengan *bot* adalah dengan menggunakan *C and C server* atau *command and control server*, jenis *server* yang lazim digunakan adalah *server IRC* karena sangat fleksibel. *Bot header* akan mengintruksikan *playload* yang siap melakukan kendali atas komputer yang terinfeksi.

B. Kasus-Kasus Tindak Pidana *Cracking* Menggunakan *Botnet* Terhadap Sistem Komputer

Roy Suryo, seorang pakar teknologi informasi, dalam penelitiannya yang dikutip oleh Harian Kompas menyatakan[76]:

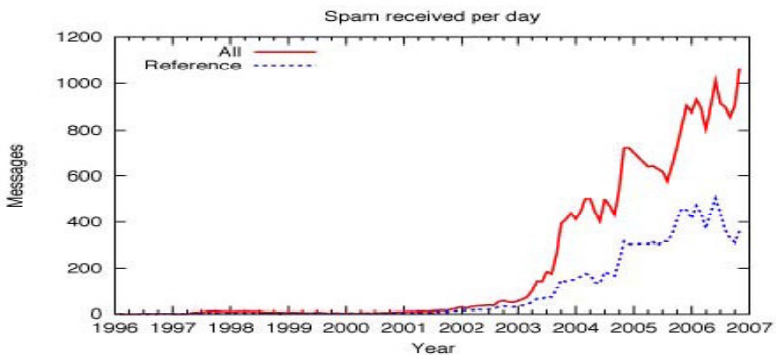
> "Kejahatan *cyber* (*cyber crime*) kini marak di lima kota besar di Indonesia dan dalam taraf yang cukup mengkhawatirkan serta dilakukan oleh para *cracker* yang rata-rata anak muda yang kelihatannya kreatif, tetapi sesungguhnya mereka mencuri nomor kartu kredit melalui internet."

[76] Harian Kompas, 19 November 2001

Serangan infrastruktur adalah serangan yang pada umumnya mempengaruhi komponen penting dari Internet. Serangan tersebut ditakuti karena banyaknya organisasi dan pengguna Internet serta makin tergantungnya mereka pada Internet untuk menjalankan bisnis sehari-hari. Hasil dari serangan infrastruktur antara lain adalah DoS, membahayakan informasi sensitif, penyebaran informasi yang salah, dan pengalihan signifikan sumber daya dari proses lainnya. *Botnet* adalah contoh dari serangan infrastruktur. Istilah *botnet* mengacu pada sekumpulan komputer terinfeksi yang dikendalikan dari jauh oleh sebuah *command control server*. Komputer terinfeksi tersebut menyebarkan *worm* dan *Trojan* melalui sistem jaringan. *Spam* meningkat dengan cepat karena penggunaan *botnet*. *Spam* mengacu pada pesan tidak diinginkan yang berjumlah banyak, yang dikirimkan melalui *e-mail*, pesan instan (*instant messages*), mesin pencari, *blog* dan bahkan telepon bergerak.

Gambar 3.2

Statistik *Spam*[77]



[77] http://spamnation.info/stats/, 31, Mei, 17.18 WIB

Awalnya motivasi utama yang melatarbelakangi *underground research* dan *hacking,* adalah untuk berkomunikasi, berbagi informasi dan pemenuhan rasa penasaran yang tinggi. Akan tetapi, sejalan dengan semakin luasnya partisipasi masyarakat dan bertambahnya jumlah transaksi *e-commerce* dan keuangan *online*, para *cracker* ataupun *attacker* beralih fokus dan berevolusi dari sekadar rasa penasaran belaka menjadi mencari keuntungan finansial. Karena motivasi finansial tersebut, mereka semakin terdorong untuk memperoleh akses terhadap suatu jaringan komputer dan mempergunakan informasi secara ilegal untuk kepentingan mereka.

Scott J. Stein dari Microsoft mengatakan bahwa *botnet* merupakan suatu kejahatan terorganisasi pada suatu *network*, yang setiap tahunnya menciptakan kerugian sebesar ratusan juta dolar Amerika Serikat. *Botnet* merupakan dasar terjadinya jenis kejahatan distribusi *Malware*, penyebaran *Spyware/Adware,* pencurian PII, *piracy* maupun *phising*. Adapun penyidikan atas suatu *botnet* dapat dilakukan dengan cara :

1. Memperoleh *malware* dari mesin-mesin yang terinfeksi;
2. Menganalisis *malware* melalui menemukan IP address/ *domain* dan *password* yang dikirimkan untuk memerintah dan mengontrol dengan *tools* (alat) pembantu *Ethereal, Etherpeek;*
3. Memonitor saluran (*channel*) dan melakukan investigasi atas saluran tersebut seperti menggunakan IRC atau BMAT untuk mengawasi dan menemukan lebih banyak informasi yang berguna;

4. Mempergunakan semua petunjuk-petunjuk antara lain aliran dana *(money* trail), *internet Trail* siapa yang *lookup servers* dan alamat IP, *Ircd Domains*, *DNS servers*, *download points*, *ISPs*, memindahkan informasi terafiliasi dari setiap referensi *adclicks,* mengidentifikasi bot *herder nic* dan mengikuti dengan pencarian sumber publik, mengikuti dengan korban DoS komersial.

Kerugian akibat zombie secara keseluruhan belum diketahui. Sejauh ini memang belum ada data yang memperlihatkan kerugian ekonomi yang langsung disebabkan atau dikaitkan dengan aktivitas zombie. Jika ada, umumnya merupakan kejadian yang berdiri sendiri. Tapi, melihat peran zombie sebagai pemicu serangan *DDoS (distributed denial of services)*, *spam* atau *phishing* , bisa dibayangkan berapa potensi kerugian yang mungkin ditimbulkannya. Contoh kasus lumpuhnya situs Yahoo!, Microsoft, Google, AltaVista, Lycos, FedEx, Apple dan Symantec selama beberapa jam. Lumpuhnya situs-situs tersebut disebabkan perusahaan penyedia *hosting*-nya, Akamai, mengalami gangguan pada DNS *server*-nya. Pihak Akamai sendiri mengatakan bahwa gangguan itu disebabkan oleh serangan *spyware botnet* DDoS, yang menyerang *root* DNS *server*-nya[78].

Zombie juga digunakan sebagai sarana kejahatan bermotif ekonomi. Sebagai contoh, serangan botnet DDoS terhadap situs judi *online* Inggris, Blue Square. Ketika itu, pelaku menuntut uang sebesar 40.000 dolar AS. Tentu saja

[78] http://www.indonesiaindonesia.com/f/74127-invasi-zombie-dunia-maya/, 31, Mei, 17.23 WIB

Blue Square menolak, dan akibatnya pun bisa ditebak. Tak lama kemudian, pasukan zombie mulai bergerak membuat ribuan *network protocol request* atau mengeluarkan *request for false pages* yang memaksa *server web* Blue Square menampilkan pesan kesalahan. Situs Blue Square lumpuh dan perusahaan itu pun mengalami kerugian yang tidak sedikit. Yang lebih absurd adalah tren dimana para dukun zombie ini mulai menjual jasanya untuk kepentingan pihak ketiga, dengan menawarkan pasukan zombie bayaran. Kasus paling mutakhir terkait dengan pasukan zombie bayaran ini adalah ketika biro penyelidik federal AS (FBI) menggulung mafia DDoS. Jay Echouafni, CEO perusahaan ritel online Orbit Communication Corp, yang menjual piranti-piranti TV satelit, ditahan dengan dengan tuduhan menggunakan jasa para zombie bayaran untuk melumpuhkan bisnis para pesaingnya. Ia membayar tiga orang dari komunitas *hacker underground* , dimana salah satunya mengendalikan sebuah pasukan terdiri dari 5.000 sampai 10.000 PC zombie siap pakai. Echouafni, seorang warga AS keturunan Maroko membayar ketiga orang itu untuk melumpuhkan tiga situs *e-commerce* pesaingnya, WeaKnees.com, RapidSatellite.com dan Expert Satellite dengan serangan DDoS. Kerugian yang ditimbulkan akibat serangan ini tak kurang dari 2 juta dolar AS. Dalam suatu laporan rutin bertajuk *Internet Security Threat Report* yang dirilis Symantec Maret lalu, terungkap bahwa dalam kurun waktu 2004 terjadi pertumbuhan jumlah komputer yang diidentifikasi telah direkrut ke dalam *botnet* atau menjadi PC zombie. Dalam semester pertama 2004, rata-rata setiap harinya Symantec memantau setidaknya ada sekitar 30.000 komputer yang sudah disusupi *bot*. Tetapi, dalam

kurun waktu Juli sampai Desember 2004, Symantec mencatat penurunan jumlah komputer dalam botnet yang cukup signifikan, dari 30.000 menjadi 5.000 komputer per hari saja. Penurunan cukup signifikan ini terjadi pada bulan Agustus 2004. Perusahaan, yang juga merupakan vendor produk antivirus terkemuka ini menduga, penurunan ini berkaitan erat dengan ketersediaan Windows XP Service Pack 2, yang memang beredar pada masa-masa itu[79].

Berdasarkan aspek demografi penyebarannya, Symantec melaporkan bahwa persentase tertinggi dari keseluruhan jumlah *botnet* atau PC zombie di seluruh dunia terdapat di Inggris, dengan persentase 25,2 persen. Amerika Serikat menduduki posisi kedua dengan 24,6 persen, sementara Cina menempati peringkat ketiga dengan 7,8 persen. Dari pemantauan Symantec, *botnet* yang ada di Inggris cenderung didominasi komputer-komputer yang berlangganan akses *internet broadband* dari ISP-ISP besar. Pertumbuhan pelanggan broadband yang pesat di Inggris kemungkinan salah satu faktor yang menyebabkan tingginya penetrasi *botnet* di negeri itu. Meski terjadi penurunan jumlah PC zombie yang cukup signifikan, bukan berarti ancaman sudah berlalu. Pasalnya, dalam enam bulan terakhir Symantec juga mengamati adanya evolusi dan perkembangan teknologi *bot* yang cukup mengkhawatirkan. Yang mengkhawatirkan, bot-bot yang sudah ada pun mengalami perkembangan jumlah varian yang cukup signifikan. Salah satu *bot* yang populer, *Spybot*, menurut Symantec dalam kurun waktu Juli-Desember 2004 berkembang menjadi lebih dari 4.000 varian *bot* baru[80].

---

[79] *Loc.Cit*
[80] *Loc.Cit*

Di Amerika Serikat, pelaku kejahatan dengan menggunakan *botnet* telah diproses secara hukum karena dianggap telah terbukti melakukan kejahatan. Di antaranya dalam kasus Christopher Maxwell, seorang operator Botrcets berusia 21 tahun asal California. Maxwell dianggap terbukti telah melakukan kejahatan *cracking* dengan cara memasukkan *software* ke dalam ratusan komputer dan merusak kegiatan instalasi militer dan rumah sakit di Amerika Serikat. Untuk itu, Maxwell telah dijatuhi hukuman penjara selama 37 bulan. Kasus yang serupa juga terjadi pada Jeanson James Ancheta, juga pemuda asal California yang berusia 21 tahun. Jeanson menerima hukuman penjara selama 4 tahun 9 bulan atas perbuatannya melakukan *cracking* dengan cara memasukkan *worm* ke dalam jutaan komputer untuk menghasilkan komisi *adware*. Matt Nealy, seorang konsultan *security independen* dari *Miskatonic Research* mengakui bahwa menangkal dan membasmi *botnet* adalah tugas yang sangat berat[81].

[81] http://www.indonesiaindonesia.com/f/74127-invasi-zombie-dunia-maya/, 31, Mei, 17.23 WIB