PERTEMUAN 4
VIRUSES AND OTHER WILD LIFE

A. TUJUAN PEMBELAJARAN

Pada pertemuan ini akan dijelaskan mengenai virus dan ancaman lainnya. Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Mendefinisikan pengertian virus
2. Mengklasifikasi metode penyebaran virus
3. Mengidentifikasi jenis ancaman virus

B. URAIAN MATERI

1. Mendefinisikan Pengertian Virus

Menurut definisi, virus komputer adalah program yang menggandakan diri. Umumnya, virus juga akan memiliki beberapa fungsi tidak menyenangkan lainnya, tetapi replikasi diri dan penyebaran yang cepat adalah ciri khas virus. Virus adalah "program kecil yang mereplikasi dan bersembunyi di dalam program lain, biasanya tanpa sepengetahuan Anda" (Symantec, 2003). Seringkali virus berkembang dengan sendirinya dan dapat menjadi masalah bagi jaringan yang terinfeksi. Virus yang menyebar dengan cepat dapat mengurangi fungsionalitas dan daya tanggap sebuah jaringan. Hanya dengan melebihi beban lalu lintas yang dirancang untuk dibawa oleh jaringan, maka jaringan tersebut dapat dibuat tidak berfungsi untuk sementara. Penyebutan pertama virus komputer adalah dalam fiksi ilmiah pada awal tahun 1970-an, dengan *The Scarred Man* karya Gregory Benford pada 1970, dan *When Harlie Was One* karya David Gerrold pada tahun 1972. Keduanya juga bercerita menyebutkan program yang bertindak untuk melawan virus, jadi ini adalah penyebutan pertama perangkat lunak anti-virus juga. Penelitian akademis nyata paling awal tentang virus dilakukan oleh Fred Cohen pada tahun 1983, dengan nama "virus" yang diciptakan oleh Len Adleman.

Virus merupakan malware yang ketika dijalankan, mencoba menggandakan dirinya menjadi kode lain yang dapat dijalankan. Bila berhasil dijalankan, kode yang terinfeksi ketika dijalankan dapat menginfeksi kode baru secara bergantian. Replikasi diri ini menjadi kode yang dapat dijalankan yang

ada adalah kunci yang menentukan karakteristik sebuah virus. Ketika dihadapkan pada lebih dari satu virus untuk dideskripsikan, masalah yang agak konyol muncul. Tidak ada kesepakatan tentang bentuk jamak dari "virus." Dua pesaing utama adalah "virus" dan "virii"; bentuk terakhir ini sering digunakan oleh penulis virus itu sendiri, tetapi jarang terlihat ini digunakan dalam komunitas keamanan, yang lebih menyukai "virus". Secara sederhana, virus dapat menyebar dalam satu komputer, atau dapat berpindah dari satu komputer ke komputer lain menggunakan media yang dibawa oleh manusia, seperti floppy disk, CD-ROM, DVD-ROM, atau USB flash drive. Dengan kata lain, virus tidak menyebar melalui jaringan komputer, jaringan adalah domain worm sebagai gantinya. Namun, label "virus" telah diterapkan pada perangkat lunak perusak yang secara sederhana dianggap sebagai worm, dan istilah tersebut telah diklasifikasikan dalam penggunaan umum untuk merujuk pada segala jenis perangkat lunak perusak yang menggandakan diri. Virus dapat diklasifikasi dalam berbagai tahap menggandakan diri. Kuman adalah bentuk asli virus, sebelum replikasi apa pun. Virus yang gagal mereplikasi disebut dimaksudkan. Hal ini dapat terjadi karena bug pada sebuah virus, atau menghadapi versi sistem operasi yang tidak terduga. Virus dapat tidak aktif, jika ada tetapi belum menginfeksi apapun misalnya, virus Windows dapat berada di server file berbasis Unix namun tidak berpengaruh, akan tetapi dapat diekspor ke mesin Windows.

Virus komputer mirip dengan virus biologis; keduanya dirancang untuk mereplikasi dan menyebar. Metode paling umum untuk menyebarkan virus adalah menggunakan akun email korban untuk menyebarkan virus ke semua orang di buku alamat mereka. Beberapa virus sebenarnya tidak membahayakan sistem itu sendiri, tetapi semuanya menyebabkan perlambatan jaringan karena lalu lintas jaringan yang padat yang disebabkan oleh replikasi virus. Metode lainnya yaitu dengan memindai komputer untuk koneksi ke sebuah jaringan, lalu menyalin dirinya sendiri ke komputer lain di jaringan yang sama. Ini adalah cara yang paling efisien bagi virus untuk menyebar. Namun, metode ini membutuhkan lebih banyak keterampilan pemrograman daripada metode lainnya. Virus juga dapat berada di media portabel seperti perangkat USB, CD, atau DVD. Kemungkinan juga untuk menutupi virus dengan file yang benar dan sah; dalam hal ini disebut Trojan Horse. Terkadang sebuah situs web terinfeksi virus, dan ketika seseorang mengunjungi situs web tersebut, komputer orang tersebut menjadi terinfeksi. Virus komputer memiliki tiga bagian, yaitu:

a. Mekanisme infeksi, bagaimana virus menyebar, dengan memodifikasi kode lain agar berisi salinan virus (yang mungkin telah diubah). Cara tepat virus penyebaran disebut sebagai infection vector. sebuah virus yang menginfeksi dengan berbagai cara disebut multipartite.
b. Trigger, cara memutuskan apakah akan mengirimkan muatan atau tidak.
c. Payload, apa yang dilakukan virus selain menyebar. Muatan mungkin melibatkan kerusakan, baik disengaja atau tidak disengaja. Kerusakan yang tidak disengaja dapat disebabkan oleh bug pada virus, menghadapi jenis sistem yang tidak dikenal, atau mungkin beberapa infeksi virus yang tidak terduga.

2. Mengklasifikasi Metode Penyebaran Virus

Virus dapat diklasifikasikan berdasarkan metode penyebarannya atau aktivitasnya pada suatu komputer, sebagai berikut:

a. Makro

Virus makro menginfeksi makro di dokumen kantor. Banyak produk perkantoran, termasuk Microsoft Office, memungkinkan pengguna untuk menulis program mini yang disebut makro. Makro ini juga dapat ditulis sebagai virus. Virus makro ditulis ke dalam makro di beberapa aplikasi bisnis. Misalnya, Microsoft Office memungkinkan pengguna menulis makro untuk mengotomatiskan beberapa tugas. Microsoft Outlook dirancang agar programmer dapat menulis skrip menggunakan subset dari bahasa pemrograman Visual Basic, yang disebut Visual Basic for Applications (VBA). Faktanya, bahasa skrip ini dibangun di semua produk Microsoft Office. Pemrogram juga dapat menggunakan bahasa VBScript yang terkait erat. Kedua bahasa tersebut cukup mudah dipelajari. Jika skrip seperti itu dilampirkan ke email dan penerima menggunakan Outlook, maka skrip tersebut dapat dijalankan. Eksekusi itu dapat melakukan banyak hal.

b. Multi-partit

Virus ini menyerang komputer dengan berbagai cara, misalnya, menginfeksi sektor boot hard disk dan satu atau beberapa file.

c. Penghuni memori

Virus yang menetap di memori menginstal dirinya sendiri dan kemudian tetap berada di RAM sejak komputer di-boot hingga dimatikan.

d. Lapis baja

Virus lapis baja menggunakan teknik yang membuatnya sulit untuk dianalisis. Kebingungan kode adalah salah satu metode tersebut. Kode tersebut ditulis sedemikian rupa sehingga jika virus dibongkar, kode tersebut tidak akan mudah diikuti. Kode terkompresi adalah metode lain untuk melindungi virus.

e. Sparse Infector

Virus Sparse Infector (infector jarang) mencoba mengelak dari deteksi dengan melakukan aktivitas berbahaya hanya secara sporadis. Dengan virus infektor jarang, pengguna akan melihat gejala untuk waktu yang singkat, kemudian tidak ada gejala untuk sementara waktu. Dalam beberapa kasus, infektor jarang menargetkan program tertentu tetapi virus hanya dijalankan setiap 10 atau 20 kali program target dijalankan. Atau infektor jarang mungkin mengalami ledakan aktivitas dan kemudian tertidur selama jangka waktu tertentu. Ada beberapa variasi pada tema, tetapi prinsip dasarnya sama: mengurangi frekuensi serangan dan dengan demikian mengurangi kemungkinan deteksi.

f. Polymorphic

Virus Polymorphic (polimorfik) secara harfiah mengubah bentuknya dari waktu ke waktu untuk menghindari deteksi oleh perangkat lunak antivirus.

g. Metamorphic

Virus Metamorphic (metamorf) adalah kasus khusus dari virus polimorfik yang menulis ulang dirinya sendiri secara berkala. Virus semacam itu sangat jarang.

h. Sektor boot

Seperti namanya, virus jenis ini menginfeksi sektor boot dari drive. Virus semacam itu mungkin sulit ditemukan oleh perangkat lunak antivirus karena sebagian besar perangkat lunak antivirus berjalan di dalam sistem operasi, bukan di sektor boot.

Klasifikasi berdasarkan Target

Salah satu cara untuk mengklasifikasikan virus adalah berdasarkan apa yang mereka coba infeksi. Bagian ini membahas tiga: Boot-sector infectors, File infectors, dan Macro viruses.

a. Boot-Sector Infectors

Meskipun detail pastinya berbeda-beda, urutan boot dasar pada kebanyakan mesin melalui langkah-langkah ini:

1) Hidupkan.
2) Instruksi berbasis ROM dijalankan, melakukan swa-uji, deteksi perangkat, dan inisialisasi. Perangkat booting diidentifikasi, dan blok boot dibaca darinya; biasanya blok boot terdiri dari blok awal pada perangkat. Setelah blok boot dibaca, kontrol ditransfer ke kode yang dimuat. Langkah ini disebut sebagai boot utama.
3) Kode yang dimuat selama langkah boot utama memuat program yang lebih besar dan lebih canggih yang memahami struktur sistem file perangkat booting, dan mentransfer kontrol ke dalamnya. Ini adalah boot kedua.
4) Kode boot sekunder memuat dan menjalankan kernel sistem operasi.

b. File infectors

Sistem operasi memiliki gagasan tentang file yang dapat dieksekusi. Dalam Lebih luas arti yang, file yang dapat dieksekusi juga dapat menyertakan file yang dapat dijalankan oleh baris perintah "shell" pengguna. File infector adalah virus yang menginfeksi file yang operasi dianggap dapat dijalankan oleh sistem atau shell; ini dapat mencakup file batch dan skrip shell, tetapi file biner yang dapat dieksekusi adalah target yang paling umum.

c. Macro viruses

Bukti konsep virus makro diterbitkan pada tahun 1989, sebagai tanggapan terhadap rumor keberadaan mereka. Virus makro tidak mencapai arus utama sampai tahun 1995, ketika konsep sebuah virus didistribusikan, menargetkan dokumen Microsoft Word di berbagai platform. Sistem operasi memiliki gagasan tentang file yang dapat dieksekusi. Dalam Lebih luas arti yang, file yang dapat dieksekusi juga dapat menyertakan file yang dapat dijalankan oleh baris perintah "shell" pengguna. File infector adalah virus yang menginfeksi file yang operasi dianggap dapat dijalankan oleh sistem atau shell; ini dapat

mencakup file batch dan skrip shell, tetapi file biner yang dapat dieksekusi adalah target yang paling umum.

3. Mengidentifikasi Jenis Ancaman Virus

Sebagian besar ancaman pada keamanan komputer dapat dikategorikan sebagai salah satu dari enam kelas besar sebuah serangan, yaitu sebagai berikut:

a. Malware

Malware adalah istilah umum untuk perangkat lunak yang memiliki tujuan jahat. Kategori serangan yang paling umum terjadi pada suatu sistem yaitu; virus, worm, adware, trojan horse dan spyware. Virus dan trojan horse adalah yang paling sering ditemui dalam kasus serangan pada sistem keamanan komputer. Setiap jenis serangan memiliki banyak variasi berbeda. Pada titik ini seharusnya sudah jelas bahwa mengamankan sistem Anda sangatlah penting. Pada titik ini seharusnya sudah jelas bahwa sangat penting dalam mengamankan suatu sistem yang kita miliki. Ada tiga karateristik umum yang tekait dengan jenis malware ini, yaitu:

b. Malware yang menggandakan diri secara aktif berupaya untuk menyebar dengan membuat salinan baru, atau instance, dari dirinya sendiri. Malware juga dapat disebarkan secara pasif, misalnya oleh pengguna yang menyalinnya secara tidak sengaja, tetapi ini bukan replikasi diri.
c. Pertumbuhan populasi malware menggambarkan perubahan keseluruhan dalam jumlah kasus malware karena replikasi diri. Malware yang tidak mereplikasi dirinya sendiri akan selalu memiliki pertumbuhan populasi nol, tetapi malware dengan pertumbuhan populasi nol dapat mereplikasi dirinya sendiri.
d. Malware parasit membutuhkan beberapa kode untuk mengeksekusi suatu sistem. "Dapat dijalankan" dalam konteks ini harus dianggap sangat luas untuk menyertakan apa pun yang dapat dieksekusi, seperti kode blokir boot pada disk, kode biner dalam aplikasi, dan kode yang diinterpretasikan. Ini juga mencakup kode sumber, seperti bahasa skrip aplikasi, dan kode yang mungkin memerlukan kompilasi sebelum dieksekusi.

a. Worm

Worm memiliki beberapa karakteristik yang sama dengan virus. Karakteristik yang paling penting adalah bahwa worm juga dapat menggandakan dirinya sendiri, tetapi replikasi diri worm berbeda dalam dua hal. Pertama, worm berdiri sendiri, dan tidak bergantung pada lainnya seperti kode yang dapat dijalankan. Kedua, worm menyebar dari mesin ke mesin melalui jaringan. Seperti virus, worm pertama bersifat fiksi. Istilah "worm" pertama kali digunakan pada tahun 1975 oleh John Brunner dalam novel fiksi ilmiahnya The Shockwave Rider, Eksperimen dengan worm yang melakukan komputasi terdistribusi adalah dilakukan di Xerox PARC sekitar tahun 1980.

b. Trojan Horse

Dalam komputasi, Trojan horse merupakan program yang bertujuan untuk melakukan beberapa tugas ramah, tetapi diam - diam melakukan beberapa tugas berbahaya tambahan. Contoh klasik adalah program login, pengambilan sandi yang mencetak "nama pengguna" tampak autentik prompt dan "sandi" yang dimana menunggu pengguna mengetik informasi. Ketika ini terjadi, pengambil kata sandi menyembunyikan informasi untuk pembuatnya, lalu mencetak pesan "kata sandi tidak valid" sebelum menjalankan login yang sebenarnya pada program. Pengguna yang tidak curiga mengira mereka melakukan kesalahan pengetikan dan kembali memasukkan informasi, tidak ada yang lebih bijak.

c. Adware

Adware memiliki kemiripan dengan spyware, karena keduanya mengumpulkan informasi tentang pengguna dan kebiasaan mereka. Adware lebih berfokus pada pemasaran, dan dapat memunculkan iklan atau mengarahkan browser web pengguna ke situs web tertentu dengan harapan dapat dijual. Beberapa adware akan mencoba menargetkan iklan agar sesuai dengan konteks apa yang dilakukan pengguna. Misalnya, penelusuran untuk "Calgary" dapat menghasilkan iklan pop-up yang tidak diminta untuk "buku tentang Calgary". Adware juga dapat mengumpulkan dan mengirimkan informasi tentang pengguna yang dapat digunakan untuk tujuan pemasaran. Seperti spyware, adware tidak bertujuan untuk mereplikasi diri sendiri.

d. Spyware

Spyware merupakan perangkat lunak yang mengumpulkan informasi dari komputer dan mengirimkannya ke orang lain. Sebelum kemunculannya dalam beberapa tahun terakhir sebagai ancaman, istilah "spyware" digunakan pada tahun 1995 sebagai bagian dari lelucon, dan dalam postingan Usenet tahun 1994 mencari informasi "spyware". Informasi yang pasti dikumpulkan spyware mungkin berbeda-beda, tetapi dapat mencakup apa saja yang berpotensi bernilai:

1) Nama pengguna dan sandi. Ini mungkin diambil dari file di sistem, atau dengan merekam apa yang diketik pengguna menggunakan *keylogger*. Keylogger berbeda dari Trojan horse karena keylogger secara pasif menangkap penekanan tombol, hanya saja tidak ada penipuan aktif yang terlibat.
2) Alamat email, yang akan memiliki nilai bagi pelaku spam.
3) Rekening bank dan nomor kartu kredit.
4) Kunci lisensi perangkat lunak, untuk memfasilitasi pembajakan perangkat lunak.

Virus dan worm mungkin mengumpulkan informasi serupa, tetapi tidak dianggap sebagai spyware, karena spyware tidak menggandakan dirinya sendiri. Spyware dapat masuk ke sistem dengan berbagai cara, seperti dipaketkan dengan perangkat lunak lain yang diinstal oleh pengguna, atau mengeksploitasi kelemahan teknis di browser web. Metode terakhir menyebabkan spyware dipasang hanya dengan mengunjungi halaman web, dan terkadang disebut drive-by download. Spyware hanyalah perangkat lunak yang secara harfiah memata-matai apa yang Anda lakukan di komputer Anda. Spyware bisa sesederhana cookie, file teks yang dibuat dan disimpan browser di sebuah hard drive yang diunduh oleh situs web yang telah Anda kunjungi ke mesin Anda dan digunakan untuk mengenali Anda saat Anda kembali ke situs tersebut. Namun, file datar itu kemudian dapat dibaca oleh situs web atau situs web lain. Setiap data yang disimpan oleh file tersebut dapat diambil oleh situs web mana pun, sehingga seluruh riwayat penjelajahan Internet pribadi dapat dilacak.

e. Security Breaches

Serangan ini mencakup segala upaya untuk mendapatkan akses tidak sah ke sistem Anda. Serangan ini termasuk dalam meretas kata sandi, meningkatkan hak istimewa, membobol server. Semua hal ini dikaitkan dengan istilah peretasan.

f. Denial of service (DoS)

Serangan Denial of service merupakan salah satu bentuk serangan yang paling umum dan sederhana pada sistem. serangan ini bahkan tidak mencoba untuk mengganggu suatu sistem atau untuk mendapatkan informasi sensitif, serangan ini hanya bertujuan untuk mencegah pengguna yang sah mengakses sistem. Jenis serangan ini cukup mudah dilakukan. Konsep dasar serangannya membutuhkan keterampilan teknis sederhana, mudah dilakukan, tidak memerlukan banyak kecanggihan dari pihak pelakunya, dan dapat memiliki efek yang menghancurkan pada sistem target. Berdasarkan pada fakta bahwa perangkat apa pun memiliki batasan operasional. Misalnya, sebuah truk hanya dapat mengangkut muatan terbatas atau menempuh jarak yang terbatas.

g. Web attacks

Ini adalah serangan yang mencoba untuk menerobos sebuah situs web. Dua dari serangan yang paling umum adalah injeksi SQL dan skrip lintas situs. Setiap bagian dari situs web yang memungkinkan interaksi pengguna juga merupakan titik potensial untuk serangan berbasis web. Injeksi SQL melibatkan memasukkan perintah SQL (Structured Query Language) ke dalam formulir login (kolom teks nama pengguna dan kata sandi) dalam upaya untuk mengelabui server agar menjalankan perintah tersebut. Tujuan paling umum adalah memaksa server untuk memasukkan penyerang, meskipun penyerang tidak memiliki nama pengguna dan kata sandi yang sah.

h. Session hijacking

Serangan ini agak canggih dan bisa dibilang lumayan rumit untuk dilakukan. Karena alasan itu, ini bukanlah bentuk serangan yang umum. Sederhananya, penyerang memantau sesi yang diautentikasi antara mesin klien dan server, dan mengambil alih sesi itu.

i. DNS poisoning

Sebagian besar komunikasi di internet akan melibatkan DNS (Domain Name Service). DNS merupakan apa yang menerjemahkan nama domain menjadi alamat IP yang dipahami oleh sebuah komputer dan router. DNS poisoning menggunakan salah satu dari beberapa teknik untuk berupaya menyusupi server DNS dan mengarahkan pengguna ke situs berbahaya, termasuk situs web phishing, yang seringkali dengan tujuan untuk mencuri informasi pribadi.

C. SOAL LATIHAN/TUGAS

1. Apa kerusakan paling umum yang disebabkan oleh serangan virus?
2. Apa dampak potensial jika sistem terserang sebuah virus?
3. Bagaimana cara yang dapat digunakan untuk melindungi dari serangan virus?
4. Apa yang Anda lakukan pertama kali ketika komputer Anda terserang virus!
5. Berdasarkan informasi yang Anda terima terkait serangan-serangan komputer pada 2 tahun belakangan ini, Jelaskan sifat-sifat peretasan yang dilakukan oleh oknum yang tidak bertanggungjawab tersebut?

D. REFERENSI

Aycock, John. 2006. Computer Viruses and Malware. Springer.

Easttom, Chuck. 2011. Computer Security Fundamentals 2nd edition. Pearson IT Certification.

Easttom, Chuck. 2019. Computer Security Fundamentals 4th edition. Pearson IT Certification.