Cara Kerja dan Cara Mengatasi Trojan

Tugas 4 Keamanan Jaringan Komputer

Oleh :

Muhammad Fikri Rabbani

09011181621013

Kelas : SK8P Indralaya

Dosen pengampu : Deris Stiawan, M.T., Ph.D.

Jurusan Sistem Komputer

Fakultas Ilmu Komputer

Universitas Sriwijaya

1. Apa itu Trojan?

Trojan merupakan program dengan tujuan merusak yang biasanya tersamar sebagai software yang resmi. Trojan biasa digunakan untuk mengambil hak akses suatu sistem. Setelah dieksekusi trojan akan dapat merusak sistem tujuan atau membuka keamanan sistem dari dalam agar penyerang dapat dengan mudah mengakses sistem tujuan. Mendorong korban untuk menjalankan program yang mencurigakan akan sulit, sehingga trojan biasanya akan disematkan dalam program yang terlihat seperti program biasa, dengan ini trojan akan kasat mata oleh korban yang awam keamanan komputer. Korban umumnya akan terbujuk untuk menjalankan trojan dengan suatu bentuk *social engineering.* Ketika aktif, trojan akan mendapatkan akses *backdoor* terhadap sistem korban.

2. Document Trojan

Trojan untuk bisa beraksi haruslah dieksekusi terlebih dahulu oleh korban. Korban yang kurang paham akan keamanan komputer akan mudah tertipu dengan sembarangan membuka file tanpa mencurigai fungsi dan tujuan file tersebut. Salah satu cara agar trojan tersebut lebih mudah dipercaya oleh korban adalah dengan menyematkan trojan tersebut dalam file dokumen. File dokumen, umumnya docx, biasanya memiliki program macro. Macro adalah bahasa pemrograman yang di-*embed* dalam aplikasi perangkat lunak (misalnya aplikasi word dan excel). Program macro tersebut akan secara otomatis tereksekusi ketika dokumen word dibuka. Mekanisme seperti ini dapat memudahkan penyebaran trojan. Ini merupakan salah satu alasan kenapa kita seharusnya berhati-hati dalam membuka dokumen asing yang datang dari e-mail.

3. Cara Kerja Document Trojan

Trojan macro dapat mudah menyebar melalui lampiran e-mail, flashdisk, internet dan lain-lain dan biasanya sangat sulit untuk dideteksi. Macro bekerja dengan menanamkan code jahat dalam macro yang di asosiasikan dalam dokumen word, spreadsheet atau file lainnya. Macro ini akan berjalan dan mengeksekusi code jahatnya seketika program tersebut dibuka. Umumnya, macro ditransmisikan melalui e-mail pishing yang terdapat lampiran file. Ketika macro yang terinfeksi berjalan, macro tersebut akan melakukan perusakan sistem dari dalam. Trojan tersebut juga dapat melumpuhkan lapisan keamanan sistem sehingga sistem mudah diretas. Malware macro yang lainnya juga dapat mengakses

akun e-mail dan mengirimkan copynya ke semua kontak korban, yang kemudian akan membuka file tersebut karena mereka pikir datang dari sumber yang dipercaya. Virus macro bekerja tidak bergantung pada sistem operasi, ia dapat menginfeksi sistem operasi apa saja yang memiliki program aplikasi yang sama. Sebagai contoh, windows dan macintosh memiliki perangkat lunak aplikasi word, sehingga virus macro ini dapat menginfeksi kedua sistem operasi ini.

4. Contoh Trojan Macro

Pertama diketahui pada tahun 2014, Hancitor (atau juga dikenal sebagai Chanitor) adalah malware downloader berbasis macro yang tersembunyi dalam dokumen word yang ditransmisikan melalui e-mail pishing. Tujuan utama dari malware ini adalah mengunduh *payload* jahat seperti trojan banking.

Trojan Rovnix menggunakan macro yang ditanam dalam dokumen microsoft word untuk menginfeksi komputer dan mencuri data. Vawtrak adalah trojan yang didistribusikan ke korban dalam dokumen word dan dapat mengambil screenshot, membajak webcam dan melakukan logging keystroke. Rovnix dan Vawtrak biasanya menargetkan organisasi finansial.

Dridex banking Trojan dilaporkan dapat mem-bypass virtual machine. Penyerang tahu bahwa peneliti keamanan akan menggunakan virtual machine untuk menganalisa malware karena melalui lingkungan virtual machine peneliti dapat melihat aktifitas malware tanpa menginfeksi sistem produksi. Salah satu standar yang digunakan pembuat malware adalah memeriksa apakah host yang diserang merupakan virtual machine. Jika memang demikian, malware akan berhenti berjalan dan merubah sikapnya untuk mencegah dianalisa. Ada beberapa cara berbeda malware dapat menentukan jika host merupakan virtual machine, seperti memeriksa apakah driver perangkat atau tool virtual machine tertentu diinstall. Dridex banking trojan secara khusus menggunakan fungsi macro excel untuk mendeteksi jika malware berjalan dalam lingkungan virtual.

5. Mengidentifikasi dan Meghapus malware Trojan

Dokumen yang terinfeksi oleh trojan dapat di transmisikan melalui e-mail. Hati-hatilah dalam membuka file dokumen yang dilampirkan dalam e-mail, walaupun file

tersebut datang dari orang yang terpercaya. Trojan biasanya disematkan dalam dokumen docx microsoft word karena banyaknya pengguna yang menggunakan microsoft word. Banyak nya pengguna microsoft word akan memudah kan penyerang untuk menyebarkan trojan tersebut karena kebanyakan pengguna microsoft tersebut merupakan orang yang kurang paham terhadap keamanan komputer. Untungnya, ketika file malware tersebut dibuka, korban tidak akan langsung terinfeksi. Microsoft word terbaru memiliki fitur keamanan tambahan. Ketika user membuka file dokumen yang berasal dari sumber yang kurang dipercaya atau tidak diketahui, mircosoft word akan membuka file word dalam mode keamanan. Dalam mode keamanan user dapat melihat isi file dokumen, tetapi user tidak dapat meng-edit file tersebut. File tersebut akan nampak seperti file dokumen biasa tanpa ada hal yang mencurigakan, akan tetapi bukan text dari file dokumen itu sendiri yang harus kita curigai. File word tersebut bisa jadi memiliki program macro, program macro ini yang diblokir oleh word ketika dalam mode keamanan. Dengan sendirinya microsoft word hanya memberikan peringatan. Microsoft word tidak dapat menghapus program macro jahat, walaupun program tersebut tidak memiliki malware microsoft word juga akan mengunci dokumen word asing ketika dibuka, ini artinya kita tidak dapat mengetahui pasti apakah dokumen tersebut malware atau bukan. Untuk mendeteksi word yang dicurigai sebagai trojan dibutuhkan program anti virus. Anti virus dapat mendeteksi sebagaian besar program macro, tetapi tentu saja tidak seratus persen ampuh, karena macro sulit dideteksi. Untuk menjaga keamanan sistem, kembali ke kesadaran pengguna masing-masing, untuk tidak membuka sembarangan dokumen yang datang dari e-mail maupun media lainnya. User juga dapat memverifikasi terlebih dahulu dokumen yang dikirimkan oleh rekan agar mengetahui apakah dokumen yang dikirimkan benar-benar dari mereka.