Malware dan Cybercrime Ecosystem
Kamis, 22 Desember 2016 | 19:11:41 WIB |

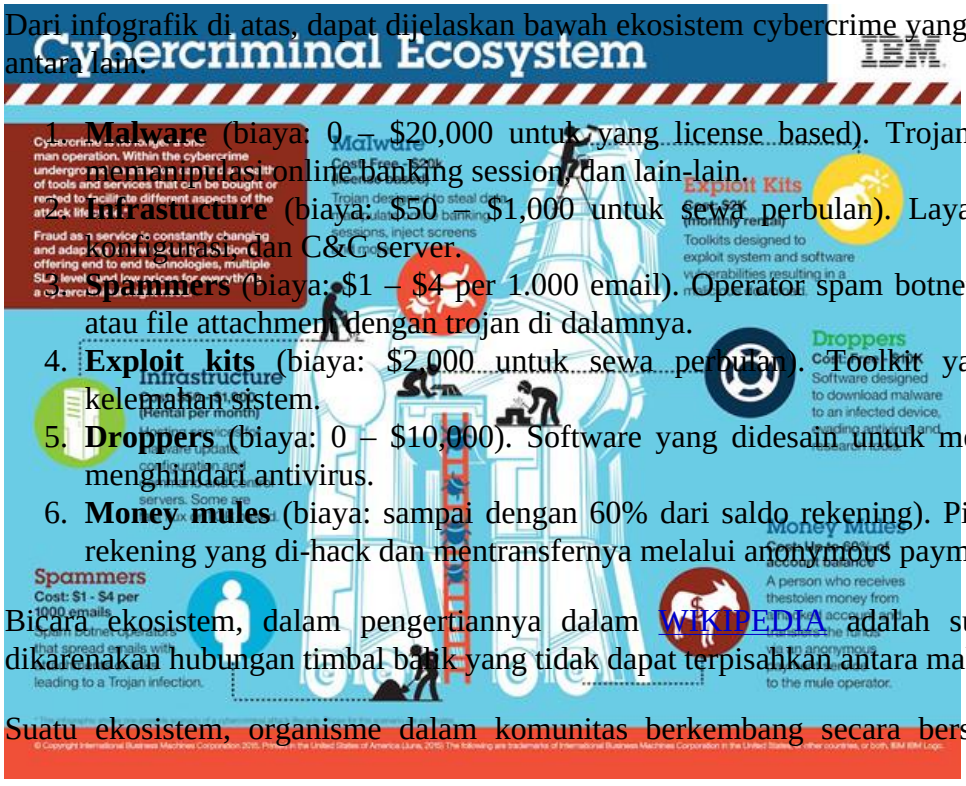
Masih seputar cybercrime, beberapa tulisan yang ada dalam website ini, salah satunya membahas tentang Black Market Underground (baca : The Cybercrime Black Market : UNCOVERED). Dalam tulisan ini dijelaskan bagaimana cara kerja pelaku kejahatan memanfaatkan internet untuk mengambil keuntungan dalam menjalankan bisnisnya. Salah satu teknik yang digunakan pelaku kejahatan ini adalah *Destructive Devices*. Pelaku kejahatan menciptakan virus yang bertujuan untuk mencuri data-data target yang kemudian akan diperjual belikan kepada pihak-pihak yang berkepentingan atas data-data tersebut.

Jenis virus yang digunakan beraneka ragam, salah satunya malware (baca : Virus Malware). Malware berasal dari kata malicious dan software adalah perangkat lunak yang di ciptakan untuk atau merusak sistem komputer atau jaringan komputer tanpa izin dari pemilik.

Pengertian Malware sangat luas dan yang akan dibahas pada tulisan ini adalah jenis malware yang berada di website dan ekosistem kejahatan komputer. Penyebab utama malware di website disebabkan karena komputer yang digunakan untuk melakukan koneksi FTP atau cPanel terkena virus. Sehingga script malware tersebut menginjeksi beberapa file website Anda, ketika google melakukan scaning atau crawling ke website anda maka google akan menemukan script malware tersebut dan memberikan notifikasi malware yang bekerja sama dengan browser ketika ada pengunjung yang mengunjungi website tersebut.

Didalam penjelasan “Ecosystem of a major cybercrime organization”, program-program malware dijual bebas dan dapat didownload secara gratis. Akibatnya, banyak perusahaan-perusahaan yang merugi akibat banyaknya data yang dicuri ataupun hilang oleh para pelaku kejahatan komputer yang disebabkan “program jahat” ini.

Sebagaimana yang dipublikasikan oleh IBM, dalam laporannya mengatakan bahwa masing-masing tindakan dalam kejahatan komputer tidak dilakukan oleh satu orang tapi dilakukan secara bersama-sama dan lebih terorganisir, baik dalam pembuatan maupun dalam penyerangannya. Untuk lebih jelasnya, berikut infografik tersebut :



Dari infografik di atas, dapat dijelaskan bawah ekosistem cybercrime yang terbentuk melibatkan berbagai pihak, antara lain:

1. **Malware** (biaya: 0 – $20,000 untuk yang license based). Trojan yang didesain untuk mencuri data, memanuptasi online banking session, dan lain-lain.
2. **Infrastucture** (biaya: $50 – $1,000 untuk sewa perbulan). Layanan hosting untuk update malware, konfigurasi dan C&C server.
3. **Spammers** (biaya: $1 – $4 per 1.000 email). Operator spam botnet yang mengirimkan email berisi link atau file attachment dengan trojan di dalamnya.
4. **Exploit kits** (biaya: $2.000 untuk sewa perbulan). Toolkit yang didesain untuk mengeksploitasi kelemahan sistem.
5. **Droppers** (biaya: 0 – $10,000). Software yang didesain untuk men-download malware ke device dan menghindari antivirus.
6. **Money mules** (biaya: sampai dengan 60% dari saldo rekening). Pihak yang menerima dana curian dari rekening yang di-hack dan mentransfernya melalui anonymous payment service ke operator dana curian.

Bicara ekosistem, dalam pengertiannya dalam WIKIPEDIA adalah suatu sistem ekologi yang terbentuk dikarenakan hubungan timbal balik yang tidak dapat terpisahkan antara makhluk hidup dengan lingkungannya.

Suatu ekosistem, organisme dalam komunitas berkembang secara bersama-sama dengan lingkungan fisik.

Organisme tersebut akan beradaptasi dengan lingkungan fisik dan sebaliknya organisme juga dapat memengaruhi lingkungan fisik yang digunakan untuk keperluan hidup

Dalam cybercrime, entitas dari kejahatan ini berawal dari pembuat program yang bisa disebut sebagai produsen, sampai kepada penjualan ke pihak-pihak yang membutuhkan jasanya. Cara kerjanyapun beragam, dari mulai melakukan phising, spoofing, scanner, sineffer, hingga Destructive device dimana proses pembuatan virus ada didalam bagian ini, proses inilah yang menjadi satu kesatuan dalam rantai kejahatan komputer. Efek yang ditimbulkan dari permasalahan ini, sebagaimana data yang pernah di keluarkan oleh Symantec (baca : Cybercrime and the Underground Market) serangan web diseluruh dunia mencapai 4.500 setiap harinya. Breach Level Index juga mengeluarkan data yang sungguh mengkhawatirkan bagi pelaku usaha di dunia, bahwa 1,023,108,267 data-data perusahaan berhasil dicuri atapun hilang.

Pertumbuhan ekosistem malware sudah cukup mengkhawatirkan. Para pelaku kejahatan komputer ini telah memahami bagaimana cara menyerang yang efektif dalam mencapai tujuannya. Beberapa anti virus yang beredar di pasaran, dibuat “tidak berdaya” oleh serangan malware ini.

Atas fenomena ini, maka dibuatlah Project MALICIA oleh IMDEA Software Institute yang bertujuan untuk mempelajari peranan dari malware di cybercrime dan tingginya kasus black market atau underground economy yang terkait dengan malware dan serangan terhadap komputer yang tersambung ke Internet.

Sebagai langkah pertama, MALICIA bekerjasama dengan peneliti dari University of California, Berkeley dan the International Computer Science Institute untuk menyelidiki distribusi malware dalam bentuk jasa pay-per-install (PPI).

Dari beberapa hal yang penulis sampaikan dalam tulisannya kali ini, dapat di buat suatu kesimpulan diantaranya :

1. Masih banyak yang harus dipelajari tentang ekosistem malware dan cybercrime. Kemajuan teknik encryption membuat celah malware dalam menyusup sulit dideteksi oleh beberapa anti virus yang sudah beredar di pasaran.
2. Kejahatan malware sudah semakin terorganisir dalam menentukan target kejahatannya.
3. Penggunaan anti virus yang selalu ter-update, senantiasa diperlukan bagi pengembang aplikasi untuk meminimalkan resiko kehilangan data.

Sumber :

- Cybercrime Ecosystem: Everything Is for Sale by Etay Maor
- The cybercrime ecosystem, resources,motivations and methods
- Understanding the Role of Malware in Cybercrime
- Ecosystem of a major cybercrime organization
