The Cybercrime Black Market : UNCOVERED
Rabu, 21 Desember 2016 | 12:05:31 WIB **| Endang Kurniawan**

Setelah 2 (dua) hari menikmati indahnya lebaran 1436 H di kampung tercinta, penulis ingin berbagi informasi mengenai Black Market dimana salah satu dari sekian banyak kejahatan komputer yang terjadi akibat perkembangan teknologi informasi yang secara *massive* 'menyerang' semua elemen kehidupan.

Di musim lebaran ini, banyak para netizen membeli kebutuhan sebagai persiapan menyambut hari raya iedul fitri, dari mulai mempersiapkan makanan, baju, dan perlengkapan lainnya. Semua berlomba-lomba untuk menyajikan yang terbaik untuk menyambut hari 'kemenangan' bagi umat muslim setelah sebulan lamanya 'berpuasa'.

Bagi netizen yang sibuk, mungkin keterbatasan waktu menjadi alasan untuk mencari kebutuhan yang diperlukan. Dengan perkembangan Teknologi Informasi, semua bisa 'dilakukan' hanya dengan 'satu sentuhan' saja maka permasalahan waktu dapat diselesaikan. Kok Bisa…???

Layanan internet, sudah menjangkau semua kalangan, mau itu professional, praktisi, anak sekolah, sampai pembantu rumah tangga sudah terbiasa dengan layanan ini. Dengan adanya internet, semua kebutuhan yang diperlukan bisa dilayani dengan baik. Mau nyari produk apapun, dari mulai kecantikan, perlengkapan dapur, makanan, perlengkapan sekolah, sampai urusan liburan sudah tersedia. Mau bayar pake kartu kredit, pake debet, bahkan bayar cash setelah barang diterimapun sudah bisa dilakukan.

Atas fenomena ini, banyak para netizen mencari produk-produk yang *up to date* dengan harga murah, karena banyak layanan yang sejenis dengan variasi harga yang 'menggoda' untuk selalu mencari barang bagus dengan harga paling murah. Kondisi ini sering tidak disadari oleh para netizen, karena ketidaktahuan atas layanan yang diberikan untuk memenuhi kebutuhannya tersebut melalui internet.

Tidak sedikit para netizen menjadi 'korban' penipuan dengan modus yang dilakukan oleh pelaku kejatahan di internet ini. Dari mulai barang tidak sesuai dengan pesanan, sampai kehilangan barang yang tidak di kirim setelah uang di transfer ke rekening tertentu sebagai tanda transaksi pembelian di internet.

Kejahatan komputer atau dikenal dengan istilah cybercrime bagi banyak orang mungkin masih terdengar asing bahkan mungkin tidak mengetahui sama sekali. Cybercrime adalah tidak kriminal yang dilakkukan dengan menggunakan teknologi komputer sebagai alat kejahatan utama. Cybercrime merupakan kejahatan yang memanfaatkan perkembangan teknologi informasi didunia maya dengan koneksi internet sebagai alat dalam melakukan kejahatan. (baca : Antara Cybercrime dan Cyber Computer).

Untuk memenuhi permintaan netizen, para produsen ataupun penyedia layanan pembelian online harus bisa berpikir 'keras' untuk mensiasati kebiasaan netizen yang mencari 'barang bagus, dengan harga murah' tersebut. Dengan alasan tersebutlah, banyak para 'pelaku' bisnis online menggunakan cara-cara yang 'illegal' untuk meraih keuntungan tanpa harus bermodal besar.

Cara-cara illegal ini dilakukan produsen untuk memenuhi minat netizen. Merujuk pada literatur yang penulis baca di WIKIPEDIA, "…sektor kegiatan ekonomi yang melibatkan transaksi ekonomi ilegal, khususnya pembelian dan penjualan barang dagangan secara tak sah. Barang-barangnya sendiri bisa ilegal, seperti penjualan senjata atau obat-obatan terlarang; barang dagangan bisa curian; atau barang dagangan barangkali sebaliknya merupakan barang resmi yang dijual secara gelap untuk menghindari pembayaran pajak atau syarat lisensi, seperti rokok atau senjata api tak terdaftar…" disebut sebagai Pasar Gelap atau istilahnya Black Market.

Pasar gelap sangat erat kaitannya dengan penyelundupan. Penyelundupan adalah semua bentuk proses memperoleh barang yang dilarang/dibatasi tersebut menggunakan cara-cara yang melanggar hukum, oleh

karena itu barang-barang yang terdapat di pasar gelap biasanya adalah barang hasil penyelundupan.

Dilihat dari cara "memproduksi" barangnya yang dilakukan dengan cara illegal, maka secara langsung akan mempengaruhi harga produk yang dijualnya akan semakin murah. Hal ini terjadi karena dalam proses pengadaan barang dilakukan dengan cara-cara yang melanggar hukum, "penyelundupan".

Dalam definisi lainnya mengenai Black Market adalah *"…All commerce on which applicable taxes are being evaded. The market includes not only legally-prihibited commerce (for example, drugs, prostitution, and gambling activities that are illegal in some locales), but also trade in legal goods and services because some income is not reported and consequently taxation is evaded…"*

Dari definisi diatas, penulis dapat menyimpulkan bahwa ***"…black market terletak pada transaksi jual beli yang dilakukan secara sembunyi-sembunyi untuk menghindari pajak…".***

Penulis berpikir, bahwa definisi diatas masih bersifat umum untuk melahirkan pemahaman baru dari arti black market tersebut. Karena setiap definisi yang ada bisa bermuatan lokal dan sesuai konteks yang ada. Namun penulis lebih menyoroti pada praktek *penyelundupan* dalam *proses transaksi perniagaan.*

Pelaku 'black market', sering menggunakan cara-cara tertentu dalam melakukan aksinya. Penulis akhirnya mencoba mengeksplorasi arti dari 'black market' tidak dalam wilayah produk yang dapat dikonsumsi oleh netizen. Tapi, masalah pengiriman TKI ke luar negeri. Apakah betul pengiriman manusia besar-besaran sebagai pembantu rumah tangga (PRT) ke luar negeri ini tidak termasuk black market?. Karena penulis meyakini bahwa dalam prosesnya, praktek-praktek penyelundupan dan pemalsuan berkas-berkas dan data-data dalam proses perekrutan sampai penempatan bisa saja terjadi.

Tapi, untuk kesempatan ini penulis tidak membahas mengenai kasus PRT dan sejenisnya, penulis akan membahas black market dalam cybercrime dengan transaksi online yang banyak tindakan illegal dimana didalamnya terdapat kegiatan transaksi jual beli, transaksi penjualan data pelanggan, bahkan pencurian data-data dari para netizen yang melakukan transaksi di black market.

Dari uraian penulis diatas, menarik untuk dijelaskan bagaimana si "aktor" kejahatan ini bekerja, siapa saja yang terlibat, modus yang digunakan, dan bagaimana cara 'menangkal' tindakan kejahatan ini untuk netizen. Berikut ulasan yang penulis berikan dari beberapa sumber yang berhasil penulis rangkum.

CARA KERJA

Dengan memanfaatkan internet, para pelaku kejahatan black market dapat mengambil keuntungan yang besar dalam menjalankan bisnis ini. Dari data pribadi netizen seperti data kartu kredit, data perusahaan, sampai data keluarga atau teman, sampai data di sosial media dapat diketahui oleh pelaku kejahatan cybercrime jenis black market ini. Selain itu juga dapat sebagai informasi untuk melakukan kegiatan pencurian uang/pencucian Uang, tergantung dari permintaan pasar ataupun permintaan dari konsumen pada Black Market tersebut

Para pelaku biasanya melancarkan aksinya dengan menggunakan beberapa teknik, seperti :

1. Phising
Teknik ini menggunakan halaman web palsu untuk "mencuri" data-data netizen yang dibutuhkan oleh si pelaku.

2. Spoofing
Merupakan kegiatan pemalsuan dengan metode seorang hacker atau cyber terrprist memalsukan (to masquerade) identitas seorang user hingga dia berhasil secara illegal logon atau login ke dalam satu jaringan komputer seolah-olah seperti user aslinya

3. Scanner
Merupakan sebuah program dengan metode secara otomatis mendeteksi kelemahan (security weakness) sebuah komputer di jaringan lokal (local host) ataupun jaringan komputer dengan lokasi berjauhan (remote host). Sehingga dengan menggunakan program ini maka hacker yang secara disik berada di suatu tempat bahkan di Negara yang berbeda dapat mudah menemukan kelemahan pada sebuah server tanpa harus meninggalkan ruangannya.

4. Sniffer
Sniffer adalah kata lain dari network analyzer yang berfungsi sebagai alat untuk memonitor jaringan komputer. Alat ini dapat dioperasikan hamper pada seluruh tipe protocol komunikasi data, seperti Ethernet, TCP/IP, IPX, dan lainnya

5. Password Cracker
Sebuah program yang dapat membuka enkripsi sebuah password atau sebaliknya malah dapat mematikan sistem pengamanan password itu sendiri.

6. Destructive Devices
Sekumpulan program-program virus yang dibuat khusus untuk melakukan penghancuran data-data, diantaranya, Trojan Horse, Worms, Email Bombs, Nukes, Malware, dan sebagainya.

Cybercrime black market digunakan untuk melakukan aktivitas ilegal, seperti jual beli malicious code, dan bahkan menyediakan layanan/jasa hacking profesional. Menurut publikasi dari Trend Micro di laman resources.infosecinstitute.com, praktek illegal dalam cybercrime black market adalah mengenai:

1. Layanan/jasa programming dan penjualan software.
2. Layanan/jasa hacking.
3. Penjualan server dedicated dan layanan/jasa hosting anti peluru
4. Layanan/jasa spam & flood, termasuk call & SMS flood.
5. Penjualan download.
6. Layanan/jasa DDoS (Distributed Denial of Service).
7. Penjualan traffic.
8. Layanan/jasa enkripsi file.
9. Penjualan trojan.
10. Layanan/jasa penulisan program exploit dan penjualannya.

Trend Micro mengkonfirmasikan bahwa layanan/jasa programming dan penjualan software adalah yang paling sering dilakukan dalam cybercrime black market. Sementara penjualan alat brute-force, DDoS bot, dan perlengkapan exploit berpotensi meningkat dan menjadi ancaman serius bagi pemerintahan.

PIHAK YANG TERLIBAT

Pertanyaan menarik tentang cybercrime black market ini, kenapa data yang diambil dari para netizen ini tidak digunakan untuk kepentingan sendiri, tetapi malah di tawarkan ke pihak lain (underground market)…? Jika hal ini dilakukan sangatlah beresiko terhadap lalu lintas data yang dimiliki oleh pelaku, karena data yang diambil biasanya masih disekitar satu Negara dimana si pelaku beraksi, jika data ini dijual ke pihak lain melalui media

internet maka rantai kejahatan akan sulit di lacak oleh petugas keamanan dalam memerangi kejatahan cyber ini.

Informasi yang telah didapat oleh pelaku akan diserahkan kepada reseller untuk dijual kepada pihak-pihak yang memerlukan untuk melakukan “kejahatan cyber” dan melakukan kesepakatan. Setelah semua kesepakatan disetujui maka dilakukan transaksi pembayaran. Pembayaran telah diterima oleh reseller maka untuk menutupi jejak transaksinya, reseller akan menugaskan seorang “mules” untuk melakukan “money laundering”.

Secara umum, dalam proses penjualan informasi dalam kejahatan black market dapat dilihat dalam penjelasan dan gambar berikut :

1. Programmer
Mengembangkan exploit dan malware untuk melakukan kejahatan cyber.

2. Distributor
Menukar dan menjual data curian.

3. Technical expert
Bertanggung jawab terhadap infrasturuktur teknologi yang digunakan dalam cybercrime black market, seperti server, enkripsi, database, dan semacamnya.

4. Hacker
Mencari celah keamanan pada sebuah aplikasi, sistem, atau jaringan yang akan dijadikan target.

5. Fraudster
Merancang dan mengaplikasikan skema-skema social engineering, seperti phishing dan spam.

6. Hosted system provider
Sebagai pihak penyedia layanan hosting untuk server dan situs yang punya tujuan ilegal.

7. Cashier
Mengatur rekening keuangan dan menyediakan nama dan akun bagi pelaku kejahatan lain untuk mendapatkan uang.

8. Money mule
Menyelesaikan urusan transfer antar bank. Seorang mules dapat menggunakan perantara seorang pelajar bahkan juga dapat menggunakan visa bekerja ke luar negeri untuk membuka rekening bank.

9. Teller
Mentransfer uang secara ilegal melalui layanan uang digital dalam berbagai macam mata uang asing.

10. Organization leader
Penjahat yang menjadi otak setiap kegiatan ilegal. Posisi inilah yang sering mengatur dan mengendalikan setiap orang yang berada pada posisinya, meski terkadang orang ini tidak memiliki kemampuan di bidang IT, mengandalkan kemampuan pendekatan personal dibandingkan kemampuan teknis. Organization leader membentuk team dan memilih targetnya.

PRODUK YANG DITAWARKAN

1. Credit Card.
2. Physical credit cards
3. Card cloners and fake ATMs

4. Bank accounts
5. Bank transfers and cashing checks
6. Sale of online service accounts
7. Design and publishing of fake online stores
8. Purchase and forwarding of products
9. Rental of botnets for sending spam

    - The Contact
    - Methods of payment

AKIBAT BLACK MARKET

Kerugian akibat black market

Image not readable or empty
../files/kerugian_adanya_black_market.jpg

Efek yang ditimbulkan oleh kejahatan black market sangat merugikan. Infografis cybercrime milik Rasmussen College yang dimuat di laman venturebeat.com, pada tahun 2011 aktivitas cybercrime telah menyebabkan kerugian total sebesar US $388 miliar dolar.

Sedangkan menurut data dari Symantec (2011) yang dimuat di laman resources.infosecinstitute.com, cybercrime telah menyebabkan:

- Serangan web meningkat 36% dengan jumlah total serangan per hari adalah 4.500 serangan.
- 403 juta varian malware telah tercipta di 2011, meningkat 41% dibandingkan tahun 2010.
- 39% serangan malware melalui email menggunakan tautan (link) yang mengarah ke halaman web.
- Celah keamanan pada perangkat mobile terus meningkat dengan temuan sebanyak 315 di 2011.

kerusakan yang diakibatkan Black Market

Image not readable or empty
../files/black-market-infographics_country.jpeg

Banyak perusahaan yang melaporkan kerugiaanya akibat aksi black market ini, dari mulai pencurian data sampai sabotase terhadap sistem dan jaringan komputer. Diperkirakan serangan yang berhasil rata-rata per minggunya adalah 1,8 serangan. Oleh karena aktivitas cybercrime ini, AS mengalami kerugian paling besar yaitu sebesar US $8.9 juta, diikuti oleh Jerman dengan US $5.9 juta, Inggris dengan US $5.2 juta, dan Jepang dengan US $5.1 juta.

Pada tahun 2014, Breach Level Index mengeluarkan laporan mengenai data-data yang berhasil dicuri dari beberapa perusahaan yang kehilangan datanya.

Dari penjelasannya, Breach menemukan lebih ada 1.023.108.267 data yang hilang atau dicuri pada tahun 2014 dimana secara rinci terdapat 2.803.036 record yang hilang atau dicuri tiap harinya, 116.793 tiap jamnya, 1.947 tiap menitnya, dan 32 tiap detiknya. dari total data yang berhasil di curi, hanya 4% yang aman dari pencurian.

Banyak perusahaan yang kehilangan datanya, sektor retail yang paling banyak terjadi kasus pencurian data hingga 55%, disusul sektor keuangan 20%, Technology 9%, Pendidikan 5%, Pemerintahan 5%, Kesehatan 3%, dan lainnya 3%. Disini terlihat jelas bahwa, penggunaan internet dalam melakukan transaksi secara online menjadi target bagi para pelaku kejahatan black market.

Berdasarkan wilayah atau Negara, Amerika Utara menempati posisi pertama dengan 1.164 kasus, Eropa 190 kasus, Asia Pasifik termasuk Indonesia 129 kasus, Afrika 38 kasus, dan yang terakhir Amerika Latin sebanyak 12 kasus.

CARA UNTUK MEMINIMALKAN RESIKO DAN CARA PENGAMANANNYA

Setelah dibahas cara kerja, dan siapa saja tokoh dibalik kejahatan black market ini, maka ada beberapa hal yang perlu diperhatikan dalam meminimalkan resiko agar para netizen terhindar dari ‘korban” kejahatan black market.

1. Gunakan password dengan kombinasi karakter dan symbol, dan jangan gunakan karakter yang pendek atau tanggal lahir ataupun yang berkaitan dengan diri anda sendiri serta ganti password secara berkala.
2. Jangan membuka tautan yang “mencurigakan” atau tidak dikenal. Hati-hati dalam menerima email yang sumbernya “tidak dikenal”.
3. Pastikan bahwa inter koneksi yang digunakan bebas dari virus, spam, dan sejenisnya.
4. Jika melakukan transaksi secara online, perhatikan alamat situs, dan metode pembayarannya sudah dalam kondisi di enkripsi oleh vendor ternama seperti verisign, comodo, Norton, dll, dengan memperhatikan “icon gembok” atau “secure” pada halaman web pembayaran onlinenya.
5. Jika mendapat informasi yang mencurigakan untuk memasukan nomor rekening bank atau pun informasi lainnya mengenai keberadaan rekening, segera menghubungi bank bersangkutan.

Sumber :

- Ablon, L., Libicki, M. C., & Golay, A. A. (2014). Markets for cybercrime tools and stolen data: Hackers’ bazaar | rand (RR-610-JNI).
- Infosec Institute. (2013, January 15). Cybercrime and the underground market – infosec institute.
- Kelly, M. (2012, July 12). Cyber crime black market almost as big as illegal drugs industry now.
- Panda Security - Malware
- Panda Security. (2010). The cyber-crime black market: Uncovered
- Phillip, A., Cowen, D., & Davis, C. (2010). Organized cyber crime. In Hacking exposed computer forensics: Secrets & solutions (2nd ed.)
- Resources Infosec Institute
