**KEAMANAN JARINGAN KOMPUTER**



**RENDIKA ADHA TANJUNG**

**(09011181419008)**

**FAKULTAS ILMU KOMPUTER**

**JURUSAN SISTEM KOMPUTER**

**UNIVERSITAS SRIWIJAYA**

**KASUS HACKING INTERNASIONAL**



Sumber : <http://www.bankingtech.com/2015/02/banks-warned-to-brace-for-the-coming-storm-as-carbanak->malware-steals-1-billion/

Berbagai macam kejahatan cyber dilakukan para ahli IT yag tidak bertanggung jawab untuk keuntungannya sendiri, seperti yang telah saya dapat contoh kasus hacking, sebagai berikut. Perusahaan keamanan internet, Kaspersky Lab, mengungkap bahwa Carbanak merupakan dalang di balik perampokan cyber sebesar US$1 miliar dari sejumlah akun di seluruh dunia. Setidaknya ada ratusan akun bank dari 30 negara yang berhasil dibobolnya.

Menurut salah satu perusahaan antivirus Kaspersky Lab dalam keterangannya, Selasa, 17 Februari 2015, ada tiga skenario kenapa Carbanak mampu mencuri uang bank di seluruh dunia yaitu dapat kita lihat pada skema dan scenario yang telah saya buat dibawah.

1. **SKEMA / SKENARIO HACKING**

Pertama tama, ketika tiba saatnya untuk menarik uang tunai hasil tindak kejahatan mereka, penjahat menggunakan online banking atau sistem e-payment internasional untuk mengirim uang dari rekening bank ke rekening mereka sendiri. Uang yang dicuri dan mereka simpan ke bank-bank yang berlokasi di negara Tiongkok atau Amerika. Tetapi, para ahli mengungkapkan ada kemungkinan bank-bank di negara lain juga digunakan sebagai bank receiver.

Kedua, dalam kasus lain penjahat cyber menembus tepat ke jantung sistem akuntansi, menggembungkan saldo rekening sebelum mengantongi dana tambahan melalui transaksi penipuan. Contohnya, jika ada akun yang memiliki uang sebesar US$1.000, para penjahat ini mengubah nilainya menjadi US$10.000 yang kemudian ia kirim US$9.000 untuk mereka sendiri. Pemegang rekening tidak menduga ada masalah karena jumlahnya masih tidak berubah, yakni US$1.000.

Ketiga, para penjahat dunia maya ini menguasai ATM bank dan memerintahkan mereka untuk mengeluarkan uang tunai pada waktu yang telah ditentukan. Ketika pembayaran jatuh tempo, salah satu anak buah geng kriminal ini menunggu di samping mesin untuk mengumpulkan pembayaran 'sukarela' tersebut.

Sergey Golovanov, Principal Security Researcher di Kaspersky Lab Global Research and Analysis Team mengatakan perampokan bank di dunia maya ini sangat mengejutkan karena tidak ada bedanya perangkat lunak yang digunakan pejahat dengan bank.

"Para penjahat bahkan tidak perlu meretas layanan bank, setelah mereka masuk ke jaringan, mereka belajar bagaimana menyembunyikan rencana jahat di balik tindakan yang sah. Hal tersebut adalah perampokan cyber yang sangat licin dan profesional," kata dia.

Vendor keamanan asal Rusia ini mendesak organisasi keuangan untuk waspada dan hati-hati untuk merespons kejahatan dunia siber. Bila saat memindai menemukan jaringan akan kehadiran Carbanak, maka laporkan kepada penegak hukum.

Selain itu juga, Kaspersky Lab memberikan informasi lebih lanjut atas modus kejahatan yang dilakukan oleh Carbanak dengan mengunggah blog yang tersedia di laman Securelist.com.

**2. FLOW DIAGRAM**

