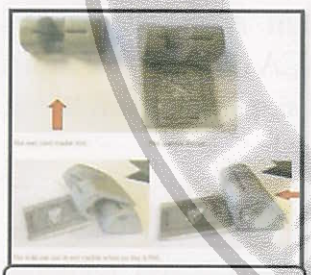
JS-16 - 004

Penanggulangan Kejahatan Cyber melalui Modus Card Skimming

Oleh : KBP HILMAN, SIk., S.H., M.H.

"Maraknya kejahatan *cyber* melalui modus *card skimming* membuat panik para nasabah bank serta menimbulkan kerugian sampai milyaran rupiah. Polri sebenarnya sudah berhasil mengungkap serta menangkap para pelaku kejahatan tersebut, baik warga negara Indonesia maupun warga negara asing (kelompok Malaysia, Kanada dan Bulgaria), namun pelaksanaan pengungkapan kasus tersebut dinilai lamban oleh para stakeholder, terutama masyarakat".



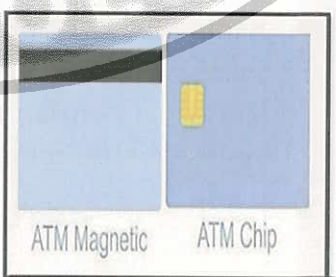
ALAT & BENTUK SKIMMER CARD

PEMASANGAN SKIMMER CARD & KEYPAD PEREKAM PIN

ALAT PEMBUAT KARTU PALSU BERDASARKAN DATA SKIMMER

SALAH SATU TEMPAT PEMASANGAN KAMERA PELAKU

TEMPAT2 PEMASANGAN SKIMMER & KAMERA



ATM TEKNOLOGI PITA MAGNETIC & ATM TEKNOLOGI CHIP

Salah satu gangguan terhadap keamanan dalam negeri adalah adanya perkembangan kejahatan *cyber* (*cyber crime*), seperti pencurian data nasabah bank melalui *card skimming* di ATM-ATM. *Skimming* adalah tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada *strip* magnetik kartu kredit atau debit secara ilegal. *Skimming* adalah salah satu jenis penipuan yang masuk ke dalam metode *phishing*.

Kasus pencurian data nasabah melalui *card skimming* di ATM-ATM meningkat pada tahun 2014. Ratusan nasabah bank, terutama bank BCA dan bank Mandiri, kehilangan uang yang tersimpan dalam rekeningnya. Berikut ini penjelasan Otoritas Jasa Keuangan (OJK)[1] berdasarkan kronologis resmi PT. Bank BCA, Tbk (BBCA) dan PT. Bank Mandiri, Tbk (BMRI) :

a. Ada 1.124 kartu debit Bank Mandiri dan Bank BCA yang ditransaksikan pada 9-10 Mei 2014. Lalu ada transaksi di Kanada, Malaysia, Perancis dan Srilanka. Sebanyak 600 kartu kredit di antaranya digunakan untuk 1.857 transaksi yang secara sistem sudah di-*approve* dengan nilai Rp 3,9 miliar serta 99 di antaranya ditransaksikan di ATM dan sisanya di EDC (*Electronic Data Capture*).
b. Diduga kuat adanya *skimming* kartu di enam ATM. Jumlahnya mencapai 80 ribu kartu. Tindak lanjut Bank BCA dan Bank Mandiri sangat cepat melakukan upaya profiling transaksi, pemblokiran kartu, penggantian kartu dan penggantian dana nasabah.
c. Ada juga transfer rekening nasabah yang tidak sesuai saldo pada April 2014. Transfer rekening nasabah yang tidak mengurangi saldonya. Total transaksi cukup besar 22.961 transaksi dari 2.560 rekening sekitar Rp 7,7 miliar.
d. Bank BCA dan Bank Mandiri sudah melakukan upaya, yakni *follback* dengan tujuan agar transfer dengan kartu ATM ke bank lain dapat berjalan normal. Selain itu, menonaktifkan dan menutup akses rekening, mengganti uang nasabah melalui pendebetan rekening.

1 Lucky Fathul Hadibrata, Deputi Komisioner Manajemen Strategis I OJK (16/5/2014).

e. OJK sudah menyampaikan kepada Bank BCA dan Bank Mandiri untuk melakukan profilling pemblokiran kartu, penggantian kartu, penggantian uang nasabah secara cepat supaya jangan sampai merugikan nasabah itu sendiri.

Andi Hamzah dalam bukunya *Aspek-aspek Pidana di Bidang Komputer* (1989) mengartikan *Cyber crime* sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Forester dan **Morrison** mendefinisikan kejahatan komputer sebagai aksi kriminal dimana komputer digunakan sebagai senjata utama. **Tavani** (2000) memberikan definisi *cyber crime* yang lebih menarik, yaitu tindakan kriminal yang hanya bisa dilakukan dengan menggunakan teknologi *cyber* dan terjadi di dunia *cyber* (dunia maya).

Pada dasarnya, *Cyber crime* meliputi tindak pidana yang berkenaan dengan sistem informasi, baik sistem informasi itu sendiri juga sistem komunikasi yang merupakan sarana untuk penyampaian/ pertukaran informasi kepada pihak lainnya.

Ada banyak jenis *Cyber crime* yang terjadi di dunia global dan beberapa di antaranya telah sering terjadi di Indonesia:

a. **Illegal content.**
Illegal content adalah tindakan memasukkan data atau informasi ke dalam internet yang dianggap tidak benar, tidak etis dan melanggar hukum atau mengganggu ketertiban umum. Salah satu contoh kasus *illegal content* yang sering ditemui adalah dalam bidang pornografi (*cyberporn*). *Cyberporn* itu sendiri merupakan kegiatan yang dilakukan dengan membuat, memasang, mendistribusikan dan menyebarkan material yang berbau pornografi, cabul dan mengekspos hal-hal yang tidak pantas.

b. **Carding (credit card fraud).**
Merupakan tindakan mencuri nomor *credit card* orang lain untuk digunakan dalam transaksi perdagangan di Internet. *Carding* merupakan bagian dari *cyber fraud*, sejenis manipulasi informasi

keuangan dengan tujuan untuk mengeruk keuntungan sebesar-besarnya.

Ada beberapa cara yang digunakan hacker dalam mencuri kartu kredit, antara lain:

1) **Paket *Sniffer***

Sniffing adalah tindakan untuk mendapatkan data dengan memasukkan program paket *sniffer* untuk mendapatkan *account name* dan *password* yang bisa digunakan. Menurut *The Computer Emergency Response Team Coordination Center* (CERT CC), Paket *sniffing* adalah salah satu insiden yang paling banyak terjadi. Pada umumnya yang diincar adalah *website* yang tidak dilengkapi *security encryption* atau situs yang tidak memiliki keamanan yang bagus.

2) **Membuat program *spyware, trojan, worm dan sebagainya.***

Spyware, trojan, worm dan sebagainya digunakan sebagai *keylogger* (*keyboard logger*, program mencatat aktivitas *keyboard*) dan program ini disebar lewat *e-mail spamming* dengan meletakkan *file*-nya di *attachment* atau fasilitas *chatting* lainnya, atau situs-situs tertentu dengan *icon* atau iming-iming yang menarik *netter* untuk men-*download* dan membuka *file* tersebut. Program ini akan mencatat semua aktivitas komputer target ke dalam sebuah *file*, dan akan mengirimnya ke *email cracker* (Pelaku).

3) **Membuat situs *phissing***

Phising digunakan untuk memancing pengguna internet mengunjungi sebuah situs tertentu. Dalam hal pencurian *account credit card*, pelaku membuat situs dengan nama yang hampir sama dengan situs aslinya. Contohnya, situs klik bca www.klikbca.com, dibuat dengan nama yang mirip yaitu www.clickbca.com atau www.kikbca.com. Hal ini memungkinkan untuk mengambil keuntungan dari kemungkinan salah ketik yang dilakukan oleh *netter*.

4) **Membobol situs *e-commerce***

Cara ini agak sulit dan perlu pakar *cracker* atau *cracker* yang sudah pengalaman untuk melakukannya. Pada umumnya mereka memakai metode *injection* (memasukan *script* yang dapat dijalankan oleh situs/server) bagi situs yang memiliki *firewall*.

5) Card Skimming

Card skimming adalah tindakan pencurian informasi kartu kredit atau debit dengan cara menyalin informasi yang terdapat pada strip magnetik kartu kredit atau debit secara ilegal. *Skimming* adalah salah satu jenis penipuan *phishing*. Pelaku bisa mendapatkan data nomor kartu kredit atau debit korban menggunakan metode sederhana seperti halnya fotokopi atau metode yang lebih canggih seperti menggunakan perangkat elektronik kecil (*skimmer*) untuk menggesek kartu lalu menyimpan ratusan nomor kartu kredit korban.

c. Hacking dan Cracking.

Ada kesalahan pada pola pikir masyarakat pada umumnya mengenai perbedaan kata *hacker* dan *cracker*. *Hacker* adalah orang yang memiliki keinginan yang kuat untuk mengetahui atau mempelajari suatu sistem komputer secara detail dan bagaimana cara meningkatkan kapabilitasnya.

Hacker biasanya melakukan tindakannya dengan dasar yang positif yaitu mengetahui kelemahan sistem untuk mempermudah perbaikan yang akan dilakukan pada sistem tersebut.

Sedangkan *cracker* adalah orang yang menyusup masuk ke dalam sistem orang lain dengan tujuan untuk memenuhi kepentingan pribadi maupun golongan dengan dalih ekonomi dan lainnya atau sebatas kesenangan pribadi. Aktivitas *cracking* di internet memiliki lingkup yang sangat luas, mulai dari pembajakan *account* milik orang lain, pembajakan situs *web*, penyebaran virus, hingga pelumpuhan target sasaran yang sering disebut *Denial of Services* (DoS). DoS merupakan upaya untuk membuat target mengalami *crash* atau *hang* sehingga tidak dapat memberikan layanan.

d. Gambling.

Gambling atau judi biasanya dilakukan di dunia nyata dengan uang dan pemain (pejudi) yang *real*. Namun seiring dengan berkembangnya teknologi internet, banyak perjudian yang dilakukan secara *online*. Perjudian di dunia maya sulit dijerat sebagai pelanggaran hukum apabila hanya memakai hukum nasional suatu negara layaknya di dunia nyata.

Hal ini disebabkan tidak jelasnya tempat kejadian perkara karena para pelaku dengan mudah dapat memindahkan tempat permainan judi mereka dengan sarana komputer dan internet.

e. Cyber Terrorism.

Suatu tindakan *cyber crime* akan tergolong *cyber terorism* jika tindakan tersebut mengancam pemerintah atau warganegara, termasuk *cracking* ke situs pemerintah atau militer. Biasanya pula, *political hacker* atau aktivis politik melakukan perusakan terhadap ratusan situs *web* untuk mengkampanyekan diri dan program-program mereka atau bahkan menempelkan informasi-informasi yang salah atau dianggap salah untuk mendiskreditkan lawan politik mereka.

f. Pencurian Dokumen

Modus dari kejahatan tersebut adalah mencuri data atau data *theft*, yaitu kegiatan memperoleh data komputer secara tidak sah, baik digunakan sendiri ataupun untuk diberikan kepada orang lain. *Indentity Theft* merupakan salah satu jenis kejahatan ini yang sering diikuti dengan kejahatan penipuan. Kejahatan ini juga sering diikuti dengan kejahatan data *leakage*. Perbuatan melakukan pencurian data sampai saat ini tidak ada diatur secara khusus.

g. **Kejahatan yang berhubungan dengan nama *domain*.**

Istilah yang sering digunakan adalah *cyber squatting*, yaitu mendaftar, menjual atau menggunakan nama domain dengan maksud mengambil keuntungan dari merek dagang atau nama orang lain. Umumnya mengacu pada praktek membeli nama domain yang menggunakan nama-nama bisnis yang sudah ada atau nama orang orang terkenal dengan maksud untuk menjual nama untuk keuntungan bagi bisnis mereka.

Penanggulangan kejahatan *cyber* seperti *card skimming* sudah berhasil dilakukan penyidik Polri, di antaranya dengan berhasil ditangkapnya para pelaku kejahatan tersebut, baik warga negara Indonesia maupun warga negara asing. Keberhasilan terbaru adalah ditangkapnya 6 (enam) pelaku pembobolan ATM dengan metode *card skimming* di Salatiga bulan April 2015 kemarin.

Keberhasilan-keberhasilan pengungkapan kasus *cyber* tersebut membuat Polri dianugerahi penghargaan *Law Enforcement Award* dari Visa Internasional pada acara *Asia Pacific Visa Security Summit* 2015 yang diselenggarakan di Sydney, Australia pada 19-21 Mei 2015.

Modus Card Skimming

Berkaitan dengan penanggulangan kejahatan *card skimming*, setelah Polri melakukan penyelidikan, maka terdapat beberapa modus dalam kejahatan *card skimming* tersebut, yaitu modus pertama, pelaku mencuri data digital kartu ATM nasabah dengan *skimmer* yang terpasang di mesin ATM. Kemudian untuk mencuri nomor PIN nasabah, pelaku menggunakan bantuan kamera pengintai yang terpasang di dalam ruang ATM atau dengan mengintip langsung ketika nasabah mengetik nomor PIN. Pelaku kemudian menyalin data ke kartu palsu dan selanjutnya menguras tabungan nasabah.


Gambar ATM Skimmer yang dipasangkan ke mulut ATM

Gambar 1
Contoh ATM Skimmer

Gambar 2
Contoh Alat Pembuatan Kartu ATM Palsu

Modus kedua, pelaku memasang suatu alat di dalam mesin ATM untuk menjepit kartu ketika nasabah memasukkan kartu. Pelaku juga memasang stiker palsu di *body* mesin. Di stiker tertulis nomor *hotline* palsu yang dapat dihubungi jika mengalami gangguan.

Setelah kartu tertahan di dalam mesin, korban kemudian menghubungi nomor *hotline* tersebut dan diterima oleh petugas bank gadungan. Petugas gadungan tersebut pura-pura meminta identitas nasabah, seperti nama, alamat, tanggal lahir dan nomor PIN. Setelah korban pergi, pelaku kemudian mendatangi mesin ATM dan mengambil kartu korban lalu menguras tabungan.

Modus ketiga, hampir sama dengan modus kedua. Namun pada modus ketiga, pelaku tidak menggunakan stiker, tetapi pelaku sendiri yang menghampiri korban dan menyarankan kepada korban untuk menghubungi *call center*. Tapi ketika dihubungi yang menerima operator gadungan.

Modus keempat, sama dengan modus ketiga, pelaku mencuri data digital kartu ATM beserta nomor PIN lalu menjualnya kepada pelaku lain seharga Rp 1 juta per data.

Penanggulangan Kejahatan *Card Skimming*

Menyikapi maraknya kejahatan *card skimming* yang dapat mengganggu kondusivitas Kamdagri tersebut, maka Polri melakukan berbagai langkah penanggulangannya, seperti berikut ini:

a. Sosialisasi dan pelatihan internal, melalui :
   1) Mengadakan sosialisasi dan pelatihan internal mengenai Peraturan Perundang-Undangan serta Ketentuan, yaitu UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, penerapan pasal dalam KUHP serta Keputusan Kapolri Nomor : Kep/54/X/2002 tanggal 17 Oktober 2002 tentang Penyelidikan dan Penyidikan Tindak Pidana Khusus guna menambah pengetahuan (*knowledge*) dan pemahaman penyidik sehingga bisa mengimplementasikannya di lapangan dalam pelaksanaan tugas penanggulangan kejahatan *card skimming*.

2) Melakukan peningkatan kompetensi penyidik dengan menyelenggarakan pelatihan mengenai komunikasi dan penggunaan *hardware* serta *software* guna meningkatkan keterampilan (*skill*) penyidik dalam penanggulangan kejahatan *card skimming*.
3) Meningkatkan pengetahuan (*knowledge*) penyidik Polri melalui sosialisasi internal dan pelatihan secara rutin mengenai teknologi, baik untuk kejahatan *cyber* secara umum maupun kejahatan transaksi perbankan melalui elektronik (ATM, EDC, Internet Banking) dengan mengundang ahli atau pakar di bidangnya.
4) Secara konsisten menerapkan *reward and punishment* di internal Polri guna meningkatkan motivasi penyidik dalam penanggulangan kejahatan *card skimming*.

b. Penjajakan dan pembuatan MoU dengan BI dan OJK, melalui:
1) Mengundang BI dan OJK guna duduk bersama membahas rancangan MoU sebagai pedoman mekanisme penanggulangan kejahatan *cyber* di bidang perbankan khususnya *card skimming*.
2) Melakukan kerjasama secara formal dengan BI dan OJK melalui penandatanganan MoU tentang penanggulangan kejahatan *cyber* di bidang perbankan.
3) Meningkatkan komunikasi, koordinasi dan kolaborasi antara Polri dengan pihak perbankan, BI dan OJK dalam penanggulangan kejahatan *cyber* dengan berpedoman kepada MoU yang telah dibuat.
4) Mewajibkan penyidik untuk membuat laporan pelaksanaan komunikasi, koordinasi dan kolaborasi dengan perbankan, BI dan OJK dalam penanggulangan kejahatan *cyber* seperti *card skimming* sehingga memudahkan pimpinan dalam melakukan analisa dan evaluasi.
5) Melaksanakan sosialisasi baik internal maupun eksternal secara terpadu mengenai MoU Polri dengan BI dan OJK guna penanggulangan kejahatan *cyber*, termasuk *card skimming*.
6) Bersama BI dan OJK secara rutin mengadakan seminar, *workshop* tentang cara-cara pengamanan transaksi perbankan melalui elektronik (ATM, EDC, Internet Banking).

c. Melakukan revisi sistem dan metode penanggulangan kejahatan *cyber*, termasuk *card skimming*, melalui :
   1) Meninjau kembali dan melakukan revisi atas sistem dan metode penanganan kejahatan *cyber*, termasuk *card skimming*.
   2) Memberikan arahan agar revisi sistem dan metode disesuaikan dengan perkembangan teknologi sebagai tempat dimulainya kejahatan *cyber*, seperti *card skimming*.

d. Meningkatkan sarana dan prasarana, melalui :
   1) Melakukan penambahan secara bertahap sarana dan prasarana baik *hardware* maupun *software* baik di *Cyber crime investigation centre* (CCIC) Bareskrim Polri serta Ditreskrimsus Polda-polda yang menunjang penanggulangan kejahatan *cyber* seperti *card skimming*.
   2) Secara rutin mengarahkan personil agar selalu dilakukan *upgrade* terhadap *hardware* maupun *update* terhadap *software* sesuai dengan perkembangan teknologi terkini.
   3) Meningkatkan aspek pemeliharaan dan perawatan terhadap sarana dan prasarana baik melalui pelatihan personil maupun bekerjasama dengan vendor-vendor jasa IT sehingga sarana dan prasarana selalu siap didayagunakan mendukung penanggulangan kejahatan *cyber* seperti *card skimming*.

e. Meningkatkan kerjasama penanggulangan *card skimming*, melalui :
   1) Memberdayakan instansi yang tergabung dalam Indonesia *Security Incident Response Team on Internet Infrastructure* (ID-SIRTII) sehingga turut mengawasi transaksi perbankan via elektronik (ATM, EDC, Internet Banking). Selama ini ID-SIRTII hanya melaksanakan pemantauan tentang IT *security* (keamanan sistem informasi), melakukan pemantauan dini, pendeteksian dini, peringatan dini terhadap ancaman terhadap jaringan telekomunikasi dari dalam maupun luar negeri khususnya dalam tindakan pengamanan pemanfaatan jaringan, membuat / menjalankan / mengembangkan dan *database log file* serta statistik keamanan Internet di Indonesia.
   2) Meningkatkan kerjasama dengan pihak perbankan berdasarkan MoU yang telah dibuat antara Polri dengan BI dan OJK sehingga

bisa memangkas birokrasi dalam permintaan informasi atau data terkait dengan kejahatan *cyber* seperti *card skimming*.

Selain itu, Polri dapat membentuk Satuan Tugas Khusus sebagai *back up* Satuan Kewilayahan dalam penanggulangan kejahatan *cyber*, khususnya *card skimming*. Terakhir, Polri dapat mengusulkan kepada BI dan OJK agar perbankan melakukan perubahan kartu ATM dan *credit card* dari yang memakai teknologi pita *magnetic* menjadi teknologi *chip* sebagai langkah antisipasi dan pengamanan transaksi perbankan via elektronik.

Dengan adanya pelaksanaan implementasi strategi tersebut maka diharapkan Polri dapat optimal dalam penanggulangan kejahatan *card skimming*.*


PERGURUAN TINGGI
ILMU KEPOLISIAN