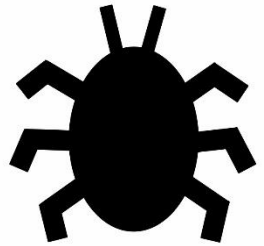
Digital Channel, Digital Services and Security Issues

*Materi ini dipresentasikan oleh **Dr. Budi Sulistyo, S.T, M.T, CISA** di event*
***Sharing Vision CIO Meeting in Digital Channel & Services: Security Update**,*
8 September 2016 di Sari Pan Pacific Hotel, Jakarta

-www.sharingvision.com-



2015

431 juta varian malware baru ditemukan
Total 13,783 varian mobile malware di android
3.3 juta aplikasi dideteksi sebagai malware

2015

Fiat Chrysler menarik 1.4 juta mobil setelah ditemukan proof of concept mobil dapat **dikendalikan** secara **remote** oleh pihak **illegal**.

2015

Targetted attack paling banyak menyerang sektor kesehatan (120 kejadian).
78 juta data pasien terekspos awal 2015.
33% *data breach* mengekspos informasi finansial.

Sumber: Symantec 2016

1. ORGANIZED CRIME

Serangan oleh individu atau satu kelompok(1)

Anatomi serangan pada EDC/ ATM

Apply for some jobs in dept store

Membawa tools, misalnya skimmer

Mencuri informasi dalam kartu dengan menggesekkan kartu ke skimmer

Mencuri uang

Mengundurkan diri setelah beraksi

Sebelum 2004.

Seluruh rangkaian langkah-langkah dalam serangan dilakukan oleh satu orang atau satu kelompok.

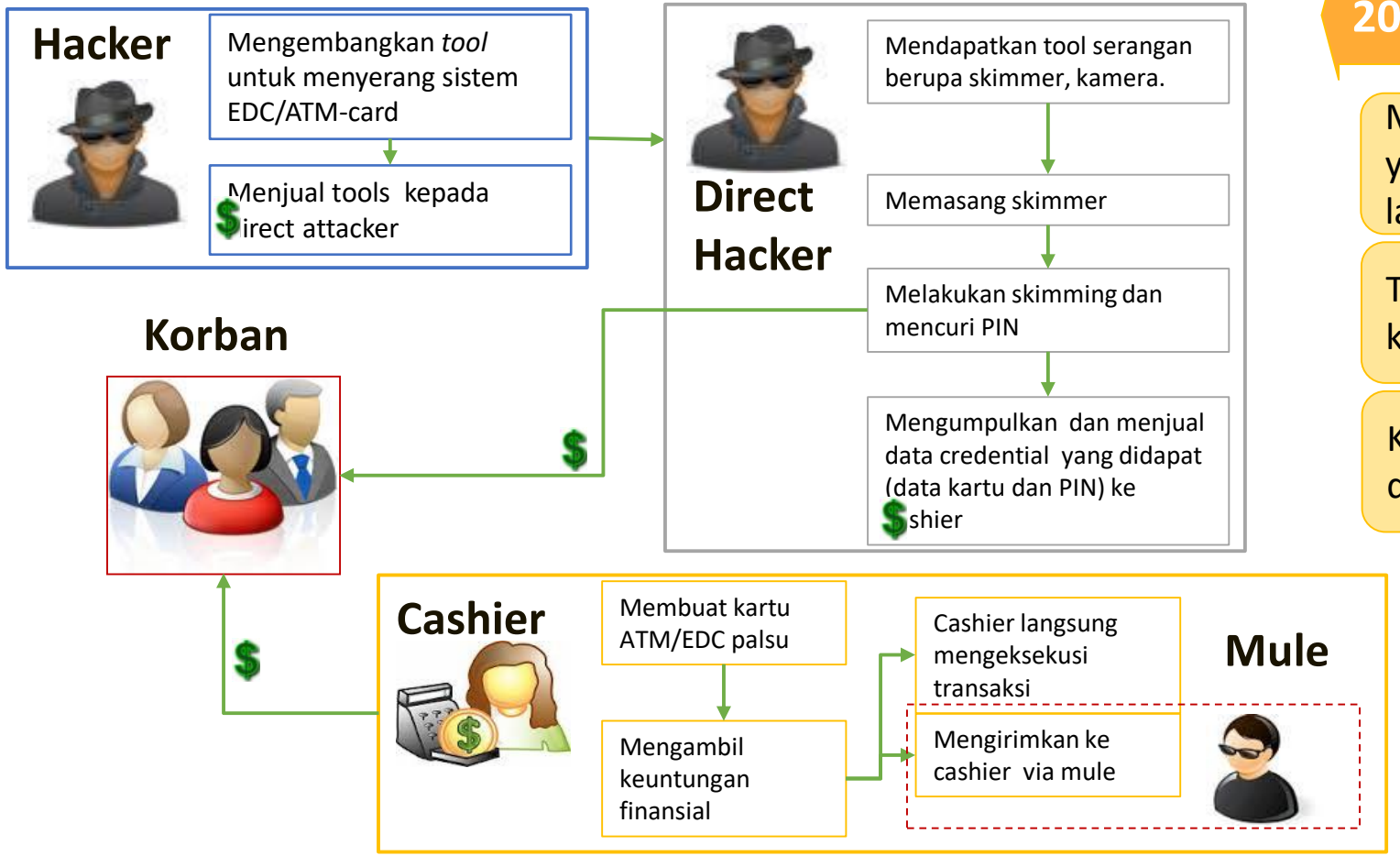
Orang/kelompok tersebut harus menguasai semua teknik serangan yang dibutuhkan.

Sangat sedikit terjadi transaksi jual beli dalam kelompok tersebut.

Sumber: Ross Anderson, *The Economics of Online Crime* dan sumber lain

Serangan oleh individu atau satu kelompok(2)

Anatomi serangan pada EDC/ ATM

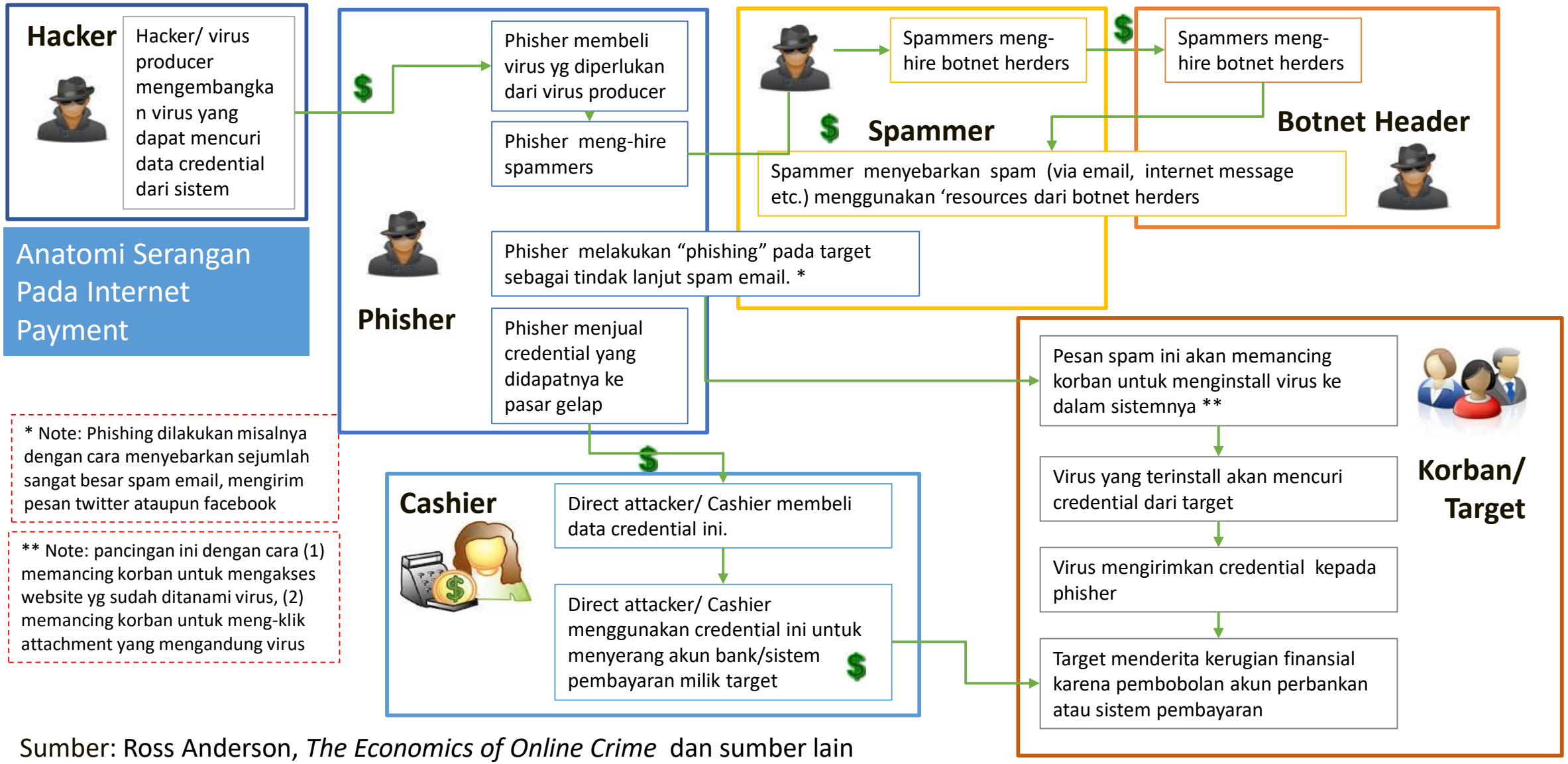


2004 - sekarang

- Melibatkan kelompok-kelompok yang terpisah yang masing-masing hanya melakukan sebagian langkah serangan saja.
- Terdapat spesialisasi keahlian untuk tiap-tiap kelompok.
- Kerjasama antar kelompok yang berbeda dilakukan dengan transaksi bisnis (pasar gelap).

Sumber: Ross Anderson, *The Economics of Online Crime* dan sumber lain

Tren anatomi: serangan terorganisasi



Sumber: Ross Anderson, *The Economics of Online Crime* dan sumber lain

Karakteristik serangan lebih “silent”

Pencurian data Akun dalam jumlah besar

Relasi antar akun di social media	Data pribadi dari social media

Analisis Data

Melakukan Berbagai kemungkinan fraud

Data dan hasil analisis dapat diperjualbelikan

PlayStation™

77 juta akun pengguna playstation jaringan Sony telah dicuri. Hacker mencuri **data pribadi** termasuk **informasi mengenai kartu kredit dan debit**.

- name
- address
- e-mail address
- birth date
- gender
- phone number
- login name
- hashed password

Sampai sekarang pihak sony tidak tahu data yang dicuri digunakan untuk apa.

Sumber: www.csmonitor.com/B

2. TEKNIK SERANGAN BEREVOLUSI SEMAKIN CEPAT

Mengapa berevolusi dengan cepat?

1.

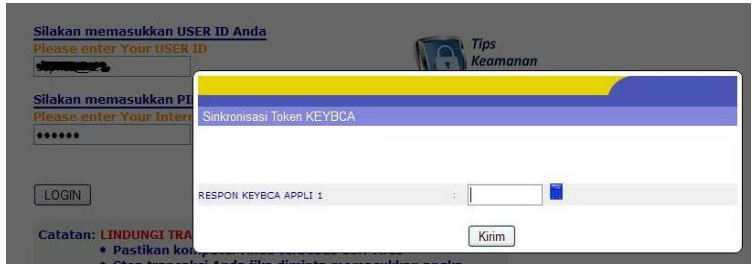
2. Adanya spesialisasi dalam organized crime

3. Keterlibatan lembaga negara ataupun militer untuk menciptakan tool dengan kualifikasi *military-grade*

Contoh evolusi serangan internet banking

Serangan ‘Sinkronisasi’ token terhadap internet banking

Sinkronisasi token



- PC yang diinfeksi virus memunculkan perintah kepada nasabah untuk melakukan konfirmasi kode token ibanking
- Pop up window tidak dapat dihapus, memaksa nasabah mengetikkan kode di token ibanking
- Kode token yang diinput nasabah digunakan oleh criminal untuk melakukan transaksi ilegal.
- Kasus yang telah terjadi membobol saldo nasabah Rp 13 juta.

Transaksi normal dan terjadi MITM

"Saya memiliki rekaman video dan fotonya. *Lagian* untuk apa saya berbohong, uang saya hilang sampai sekarang tak jelas pertanggungjawabannya," ungkap Firdaus.

Sebelumnya, dalam konferensi pers, Sabtu (8/8/2015) di Bengkulu, salah satu nasabah bernama Firdaus mengatakan, peristiwa tersebut terjadi pada tanggal 15 Juni 2015. Saat itu, ia melakukan transaksi melalui *mobile banking* senilai Rp 8.465.000. Setelah transaksi berhasil, ia kemudian melakukan pengecekan saldo, dan terkejut mengetahui saldonya banyak berkurang, lebih dari nilai transfernya saat itu.

"Setelah melakukan pengecekan, ternyata uang saya terpotong Rp 49.157.889 yang ditransfer ke BTN cabang Nusa Dua, Bali, atas nama Risto Matillah, yang merupakan warga negara Finlandia," kata Firdaus.

http://regional.kompas.com/read/2015/08/10/19230711/Uang.Nasabah.Hilang.Bank.Mandiri.Salahkan.Virus.Komputer

Serangan berlanjut dengan metode yang lebih *tersembunyi*

http://inet.detik.com/read/2015/09/21/092054/3023993/323/mengkaji-ulang-satpam-internet-banking

Contoh serangan internet banking

Mengambil alih kredensial pengguna internet banking

Senin 18 Jan 2016, 08:31 WIB

Polda Metro Tangkap Komplotan Pembobol Internet Banking, Kuras Dana Rp 245 Juta

Mei Amelia R - detikNews

26 SHARES | 26 | 0 | 14

Senin 18 Jan 2016, 08:42 WIB

Pembobol Modus Internet Banking Beli Data Nasabah dari Seseorang Rp 15 Juta

Mei Amelia R - detikNews

0 SHARED | 15 komentar

Pelaku mendatangi service center operator HP dengan membawa fotokopi KTP korban & surat kuasa palsu dari korban. Pelaku mengganti SIM card nomor korban dengan alasan kartu hilang.

Pelaku menghubungi call center bank mengaku sebagai pemilik untuk melakukan reset password.

SIM Card baru, digunakan untuk me-reset password internet banking dan mendapatkan OTP.

Pelaku kemudian dapat mengakses internet banking korban dan melakukan transfer dana ke beberapa rekening bank berbeda

Adapun para pelaku mendapatkan data-data korban dari seseorang yang masih diburu

Otentikasi yang digunakan adalah **sms token (OTP)**

- Indikasi kebocoran data nasabah (nama, nomor HP)?
- SMS token terambil alih karena nomor handphone sudah diambil alih penyerang

Sumber:http://news.detik.com/berita/, januari 2016

Trend anatomi serangan :
More sophisticated (military Grade)

2009-sekarang

Zero day exploits dan attacking tools

Pasar Attacking Tools dan zero days exploit

Government menggunakan sebagian budget untuk membeli Zero-Day Exploits

Nilai pasar zero day exploit dan attacking tools meningkat

Semakin banyak expert yang tertarik masuk pasar ini

Effort dan biaya yang dikerahkan dalam pengembangan meningkat

Expertise meningkat

Teknik **serangan semakin canggih**

Virus dan malware semakin canggih

Semakin banyak muncul military-grade attacking tools

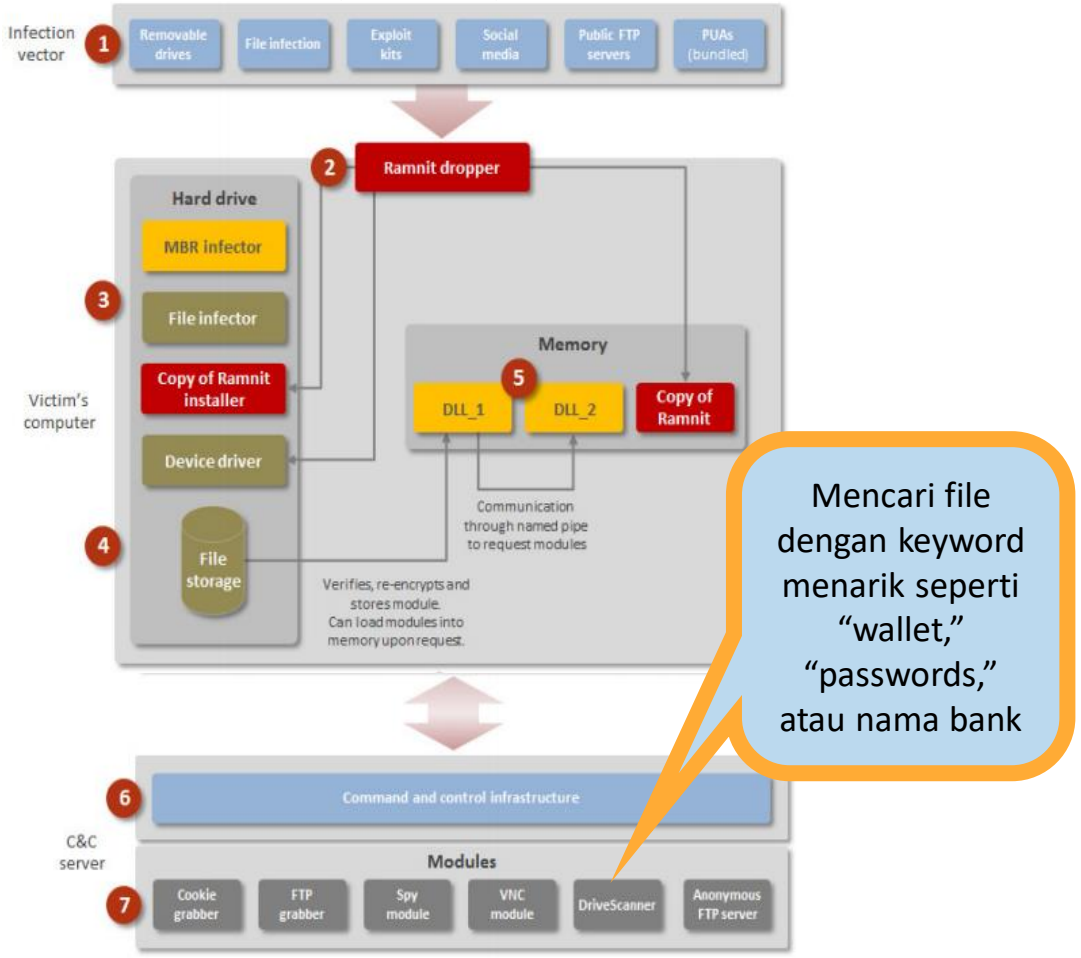
Cybercrime **semakin berbahaya** !!!

Trojan Ramnit diaktifkan kembali untuk menyerang 6 bank besar di UK, setelah di bulan februari 2015 dimatikan servernya oleh National Crime Agency (NCA) UK.

- Ramnit didesain memanipulasi session online banking untuk mencuri kredesnial dan melakukan fraud transfer uang.
- Penyerang juga menyebarkan konfigurasi Trojan yang baru yang dilengkapi web injection malware untuk menyerang pelanggan personal banking.
- Update virus antara lain:
  - Hooker module (Grabber), hook browser, memonitor akses URL, mencuri data secara real time, menampilkan web-injections kepada korban.
- Mitigasi bagi banks dan service provider:
  - menggunakan *adaptive malware detection*
  - melindungi *customer endpoint* dengan *malware intelligence yang memberi gambaran secara* real-time kapabilitas dan teknik fraudster.
- Mitigasi bagi user online banking:
  - Menghapus email asing disebabkan banyak kasus diawali oleh email spam yang dijangkiti malware yang menarik korban untuk membuka sebuah *attachment*.

http://www.computerweekly.com/news/450303199/Ramnit-Trojan-targeting-UK-banks-reactivated

Vektor infeksi, struktur, dan modul malware Ramnit



http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32-ramnit-analysis.pdf

Serangan terhadap smartcard EMV

Transaksi Chip and PIN tanpa PIN

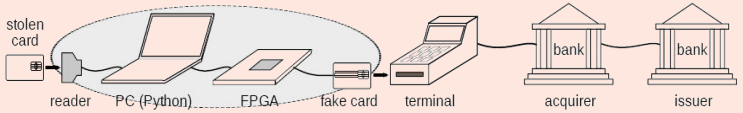
Data bisa dibaca dengan memasukkan konektor ke lubang kecil di bawah EDC. Data ini dapat digunakan untuk membuat kartu magnetic stripe palsu.

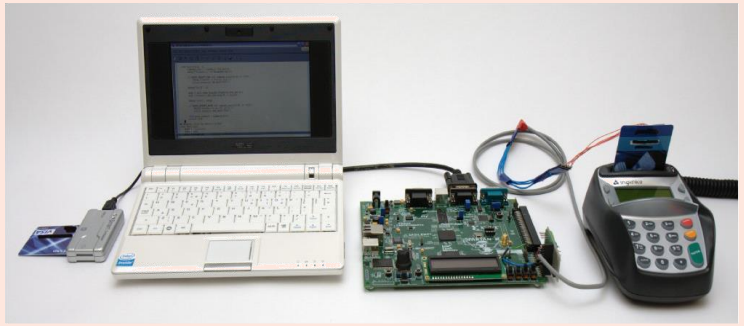
Memasangkan *paper-clips* ke EDC → Merchant dapat mencuri data account dan PIN → Membuat kartu kloning magnetic stripe → Kartu digunakan di lokasi yang masih memperbolehkan magnetic stripe

Sumber: Steven Murdoch and Ross Anderson, Failures of Tamper-Proofing in PIN Entry Devices

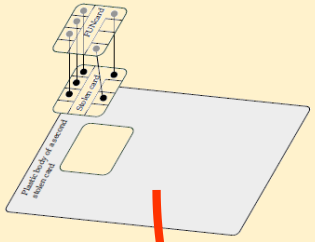
PERBANKAN

Kartu Debit Akan Wajib Gunakan Cip





Sumber: Steven Murdoch and Ross Anderson, Chip and PIN is broken



How a criminal ring defeated the secure chip-and-PIN credit cards

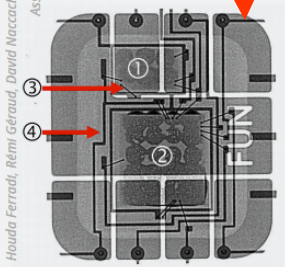
Over $680,000 stolen via a clever man-in-the-middle attack.

MEGAN GEUSS - 10/20/2015, 8:12 PM

Four years ago, about a dozen credit cards equipped with chip-and-PIN technology were stolen in France. In May 2011, a banking group noticed that those stolen cards were being used in Belgium, something that should have been impossible without the card holders inputting their PINs. That's when the police got involved.

The police obtained the international mobile subscriber identity (IMSI) numbers present at the locations where the cards were used and at the times they were used, and then they correlated those IMSI numbers to SIM cards.

Using that information, the police were able to arrest a



Houda Ferradi, Rémi Géraud, David Naccache, and Assia Tria

FUN card X-ray analysis. (1) External memory (AT24C64); (2) Microcontroller (AT90S8515A); (3) Connection wires; (4) Connection grid

Sumber: http://arstechnica.com/tech-policy/2015/10/how-a-criminal-ring-defeated-the-secure-chip-and-pin-credit-cards/

Serangan baru mencuri SSNs, alamat e-mail, dan lainnya dari halaman HTTPS

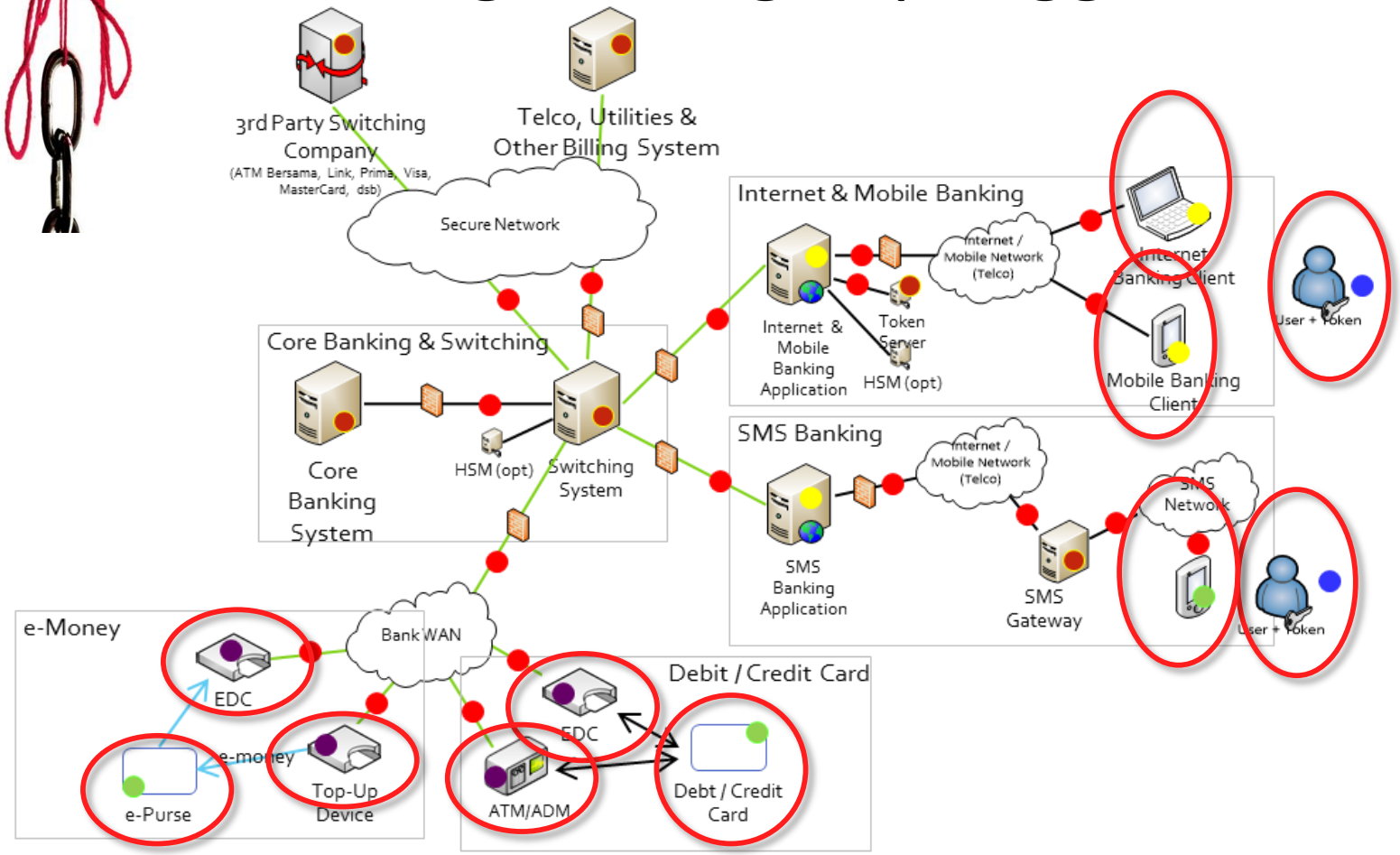
- HTTPs yang selama ini dikenal sebagai skema kriptografi yang melindungi jutaan situs kini **rentan** terhadap serangan baru yang dapat mengekspos alamat email, nomor jaminan sosial, dan data sensitive lain yang telah dienkripsi.
- Serangan **tidak** memerlukan posisi man-in-the-middle .
- **End user** hanya perlu **menemukan file Javascript** berbahaya yang tersembunyi di iklan di web atau host langsung pada halaman web.
- Malicious code kemudian dapat melakukan **query** berbagai halaman yang dilindungi *secure sockets layer* atau *transport layer security protocols* dan mengukur ukuran file yang tepat dari data yang terenkripsi yang mereka kirimkan.
- Teknik HEIST **(HTTP Encrypted Information can be Stolen Through TCP-Windows)** bekerja dengan memanfaatkan jalur tanggapan HTTPs yang dikirimkan keluar *transmission control protocol*, salah satu blok dasar di internet.

Menyerang https tanpa perlu melakukan *man-in-the-middle-attack* !!!

Sumber: http://arstechnica.com/security/2016/08/new-attack-steals-ssns-e-mail-addresses-and-more-from-https-pages/

3. SERANGAN SEMAKIN BANYAK DITUJUKAN KE PENGGUNA DAN DEVICE

Target serangan: pengguna dan device yang berhubungan dengan pengguna



Titik lemah di jaringan/kanal

- Sniffing
- SMS Spoofing
- Man in the middle attack
- DoS
- Session hijacking

Titik lemah di core/server

- Pencurian info dari data log (oleh *insider*)
- Virus
- Malware
- Brute force attack
- Manipulasi web site

Titik lemah di device user (handphone, kartu, laptop/PC)

- Skimming
- Kloning kartu
- Spam
- IP Spoofing
- Penanaman malicious software
- Token attack
- Phising

Titik lemah pada terminal (ATM,EDC)

- Skimming

Titik lemah pada aplikasi

- Spam
- Virus
- Malware

Titik lemah pada user

- Password expose/sharing
- User surveilance

Apa itu Identity theft??

Kebocoran Data Pribadi Gawat

Penulis:

Dibaca **4877** kali

Senin, 18 Februari 2013 | 08:16 AM

Photo: Shutterstock

JAKARTA, KOMPAS.com - Keamanan dat
mudah sekali berpindah tangan, baik sec
tidak sengaja. Kondisi ini mencemaskan
kejadian yang telah merugikan warga. Wa
berhati-hati dengan publikasi data privat,
pemerintah diminta segera menjamin kea
dengan membuat Undang-Undang Privas

Identity theft adalah tercurinya informasi pribadi

- Nama – diri, istri, anak, **nama ibu kandung**
- **Alamat** – Rumah tinggal, kantor
- Email – alamat email, **password**
- **Akun sosial media** – facebook, twitter
- **Foto diri** – via facebook, instagram,
- Kartu identitas – KTP

- Identity fraud adalah penggunaan informasi pribadi tersebut untuk melakukan fraud.
  - Membuka **rekening bank**
  - Mendapatkan **kartu kredit**.
  - Melakukan **pembelian barang** atas nama korban.
  - Mengambil alih akun milik korban
  - Mendapatkan dokumen penting, misal **paspor**, SIM dll.

Serangan terhadap layanan eCommerce

Ini Cerita Korban Pembobolan Akun Lazada

Adi Fida Rahman - detikinet
Minggu, 10/04/2016 17:19 WIB

Foto: Gettylmages

INET HIGHLIGHTS
Hacker Kembar Asal Ponorogo

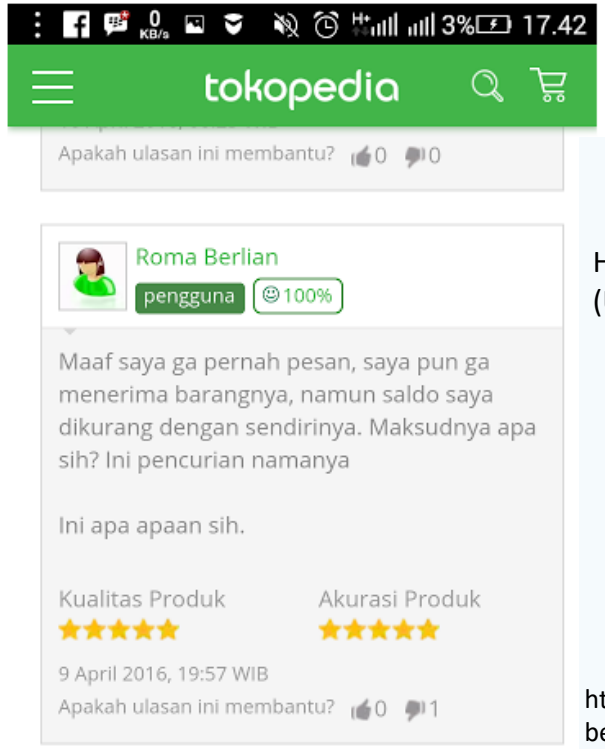
Jakarta - Pembobolan akun Lazada yang dilaporkan salah satu penggunanya, membuka tabir adanya kerentanan keamanan pada e-commerce yang bermarkas di Dubai, Uni Emirat Arab itu.

Sebelumya, Tri Kurniawan Darmoko melaporkan akun Lazadanya dibobol. Dari peristiwa tersebut ternyata banyak korban mengalami hal serupa. Beberapa di antaranya menghubungi redaksi **detikINET** menceritakan kronologis kejadian yang mereka alami.

"Ada 9 transaksi dan bila ditotal mencapai Rp 3.571.400. Akun saya pun diganti emailnya,"

"Istri saya tidak berbelanja padahal. Lucunya sang pemesan bernama Mertina dengan alamat sebuah mal di Bekasi. Istri saya bernama Cicilia,"

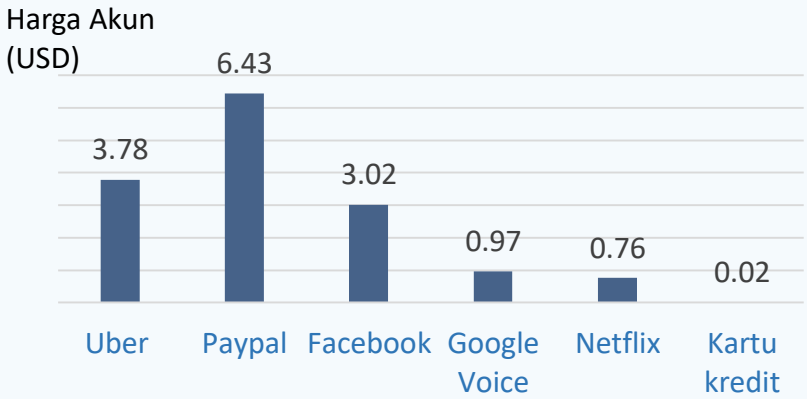
http://inet.detik.com/read/2016/04/10/171959/3184252/323/ini-cerita-korban-pembobolan-akun-lazada



Review pengguna online shop yang merasa akunnya dibajak oleh orang untuk membeli barang menggunakan saldonya.

http://www.cahgalek.com/2016/07/hati-hati-ini-buktinya-banyak-akun-tokopedia-di-bobol.html

Akun eCommerce dijualbelikan.

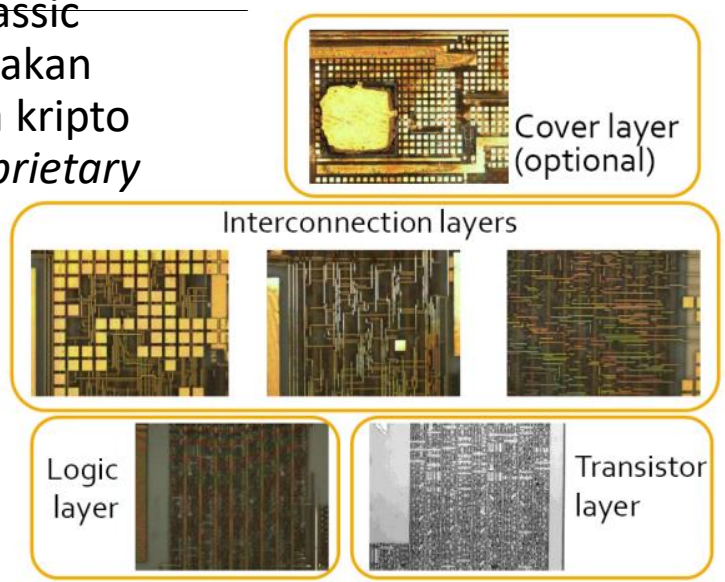


http://palingpopuler.com/software/akun-uber-dan-netflix-lebih-bernilai-dari-data-kartu-kredit/

Serangan terhadap e-banking

Serangan terhadap smartcard Mifare Classic

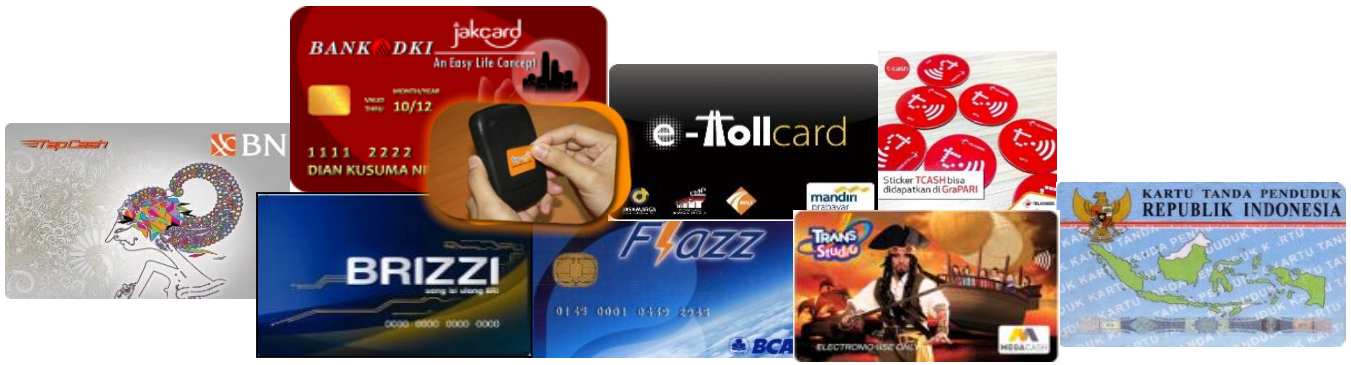
Mifare classic menggunakan algoritma kripto yang *proprietary*

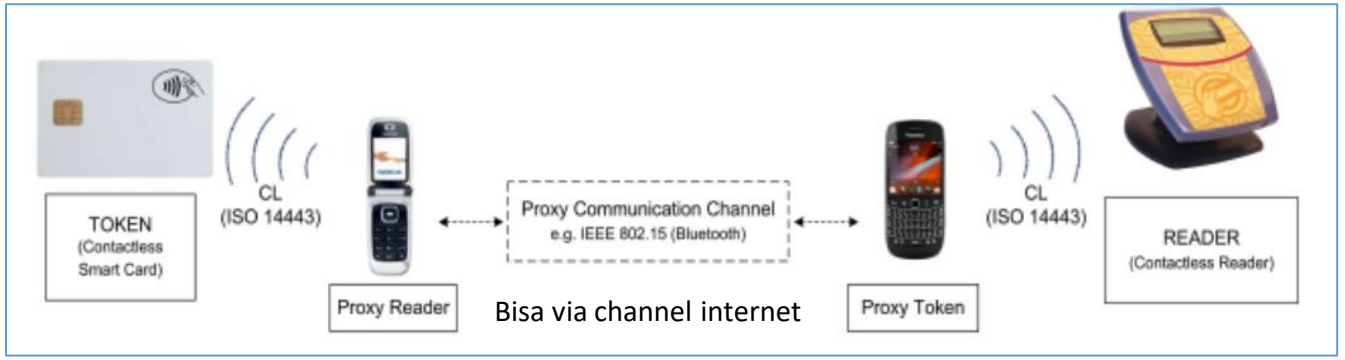


Melakukan reverse engineering terhadap algoritma kripto → Analisis matematis algoritma kripto → Mengembangkan serangan nyata terhadap kartu mifare classic yg beredar

Sumber: Karsten Nohl, Hardware Reverse Engineering

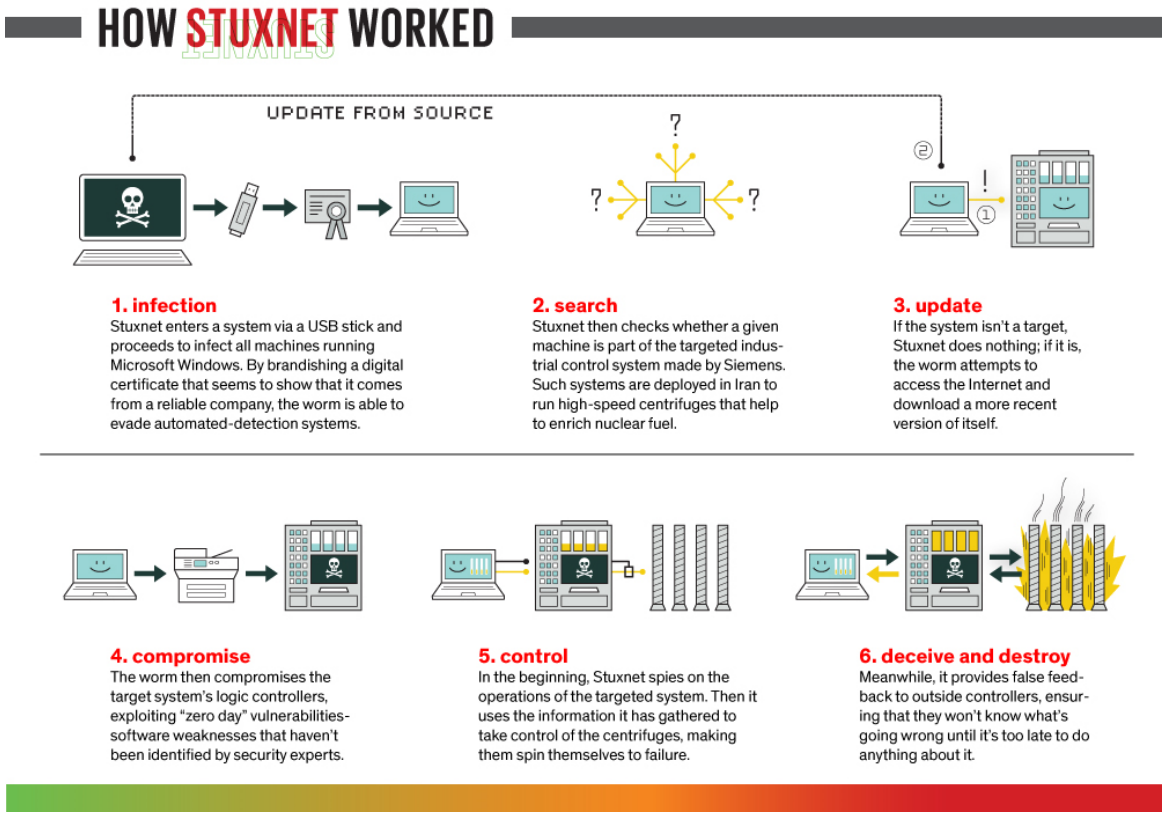
Serangan relay-attack terhadap kartu e-money





Sumber: https://eprint.iacr.org/2011/618.pdf

Device attack



Sumber: The Real Story of Stuxnet, beta.spectrum.ieee.org

Memalsukan *digital certificate* sehingga sulit terdeteksi

Menggunakan 4 jenis *zero day exploit*

Sangat sophisticated

Sangat diduga disponsori oleh suatu negara

Menyerang sistem kendali (SCADA-Siemens) yaitu pengendali dalam sistem pengayaan nuklir.
Tujuan : merusak

Kecil kemungkinan dikembangkan oleh *hacker* biasa
Estimasi: perlu 10 Orang expert dan waktu pengembangan 2-3 tahun

Instalasi trojan ke device

The Only Way You Can Delete This NSA Malware Is to Smash Your Hard Drive to Bits

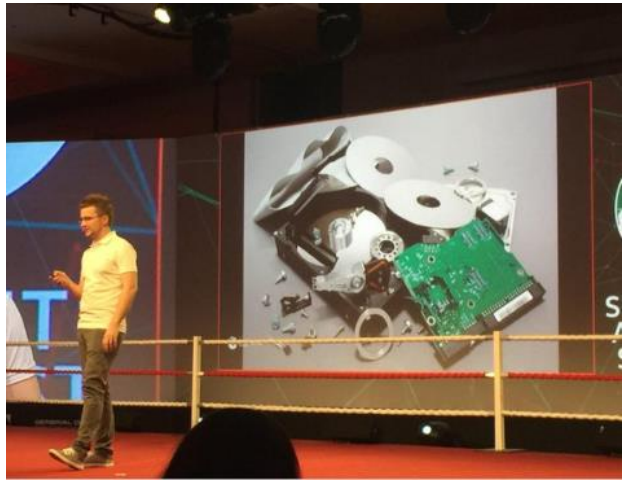
February 16, 2015 // 04:45 PM EST

Russian security company Kaspersky is calling it one of the most sophisticated features it has ever seen in a piece of malware: the ability to infect not just the files stored on a hard drive, but the firmware controlling the hard drive *itself*.

Kaspersky:

- Spy mencatat penemuan baru yaitu teknologi untuk mencari tahu bagaimana meletakkan malicious software didalam kode yang jelas yang dinamakan **firmware,** setiap kali komputer dinyalakan.
- Spies dan ahli sekuriti siber memandang **disk drive firmware** sebagai wilayah yang sangat bernilai di sebuah PC bagi para hacker, karena BIOS code aktif secara otomatis setiap PC dinyalakan.

"The hardware will be able to infect the computer over and over."



Hackers Could Break Into Your Monitor To Spy on You and Manipulate Your Pixels

August 6, 2016 // 11:00 AM EST

We think of our monitors as passive entities. The computer sends them data, and they somehow—magically?—turn it into pixels which make words and pictures.

But what if that wasn't the case? What if hackers could hijack our monitors and turn them against us?

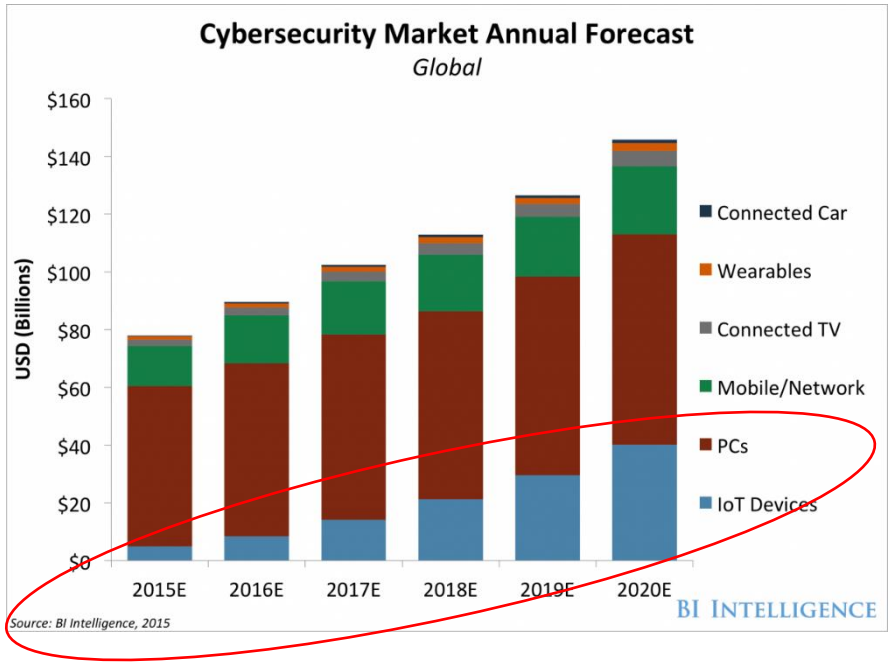
Serangan DDOS memanfaatkan lonjakan jumlah connected device ke internet(IoT)

- 47% berharap jumlah IoT device di jaringan mereka akan naik setidaknya 30% di 2017
- 78% concern terhadap penggunaan IoT devices sebagai senjata dalam melakukan serangan DDoS.

(Arbor Networks, Juni 2016); http://www.computerweekly.com/news/450303211/Less-than-a-third-of-organisations-prepare-for-IoT-security-risks

- Sistem pemanas dan AC sebagai contoh *internet-connected devices* yang dapat digunakan untuk merutekan serangan ke komputer sasaran

(Rob Joyce,US National Security Agency hacking unit); http://www.computerweekly.com/news/4500272024/Address-IoT-security-risks-before-it-is-too-late-urges-reportetwork administrators often overlook, according to MIT Technology Review.

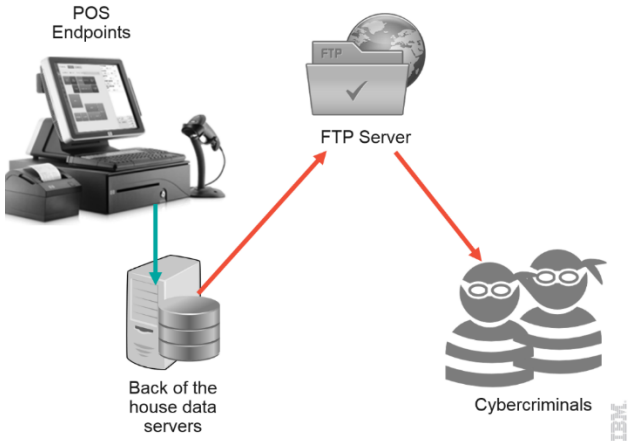


http://www.businessinsider.com/iot-cyber-security-hacking-problems-internet-of-things-2016-3?IR=T&r=US&IR=T

Serangan malware ke terminal POS

2013

Malware terminal POS trennya menyerang **retailer besar,** mensasar kredensial jutaan kartu kredit user



https://securityintelligence.com/the-pos-malware-epidemic-the-most-dangerous-vulnerabilities-and-malware/

2014

Serangan ke rantai hotel besar, perusahaan travel dan transportasi seperti bandara dan jasa parkir terus berlanjut.

Contoh : hotel Trump, hotel Starwood, hotel Hyatt; sejumlah resort dan hotel skala regional

Skenario:

Serangan tidak ditujukan ke sistem front desk reservation payment, melainkan terminal POS di restoran dan gift shop hotel.

Malware diinstal di terminal POS, mencuri:

- ✓ Nama pemegang kartu kredit
- ✓ Nomor kartu
- ✓ Security code
- ✓ Expiration date

2015

Penekanan serangan bergeser ke **retailer lebih kecil**, **POS service provider** dan ***niche payment systems*** (terjadi di US).

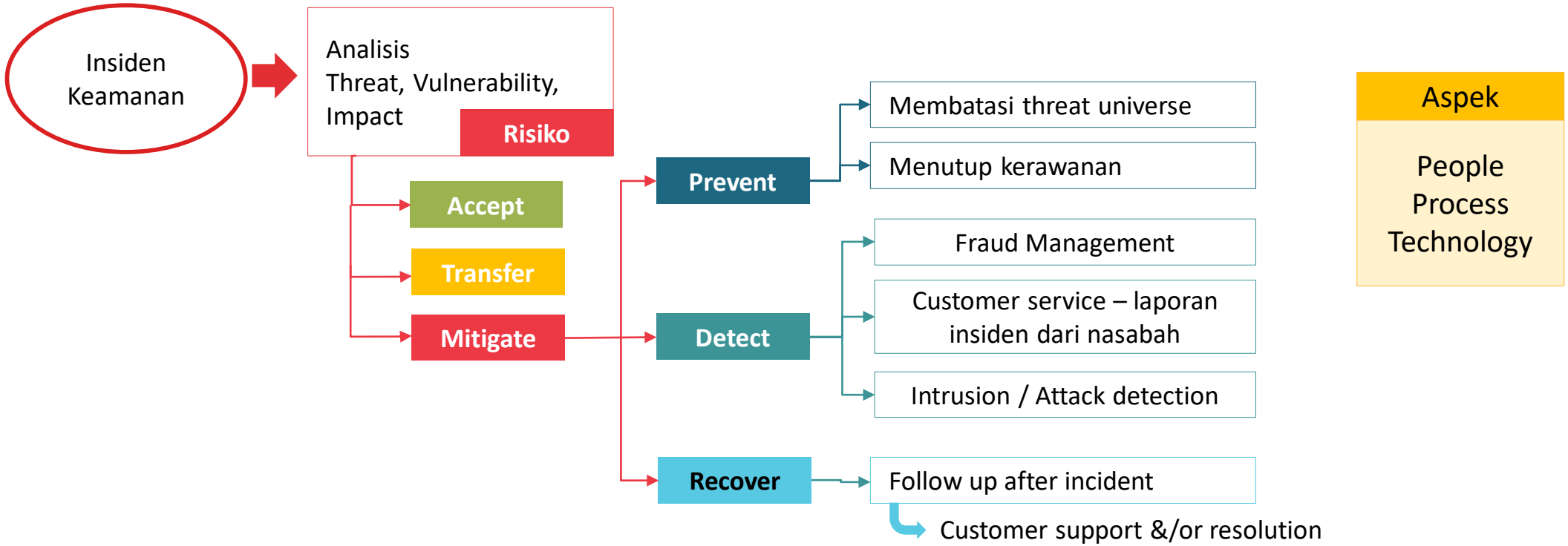
- Target kecil lain adalah kebun binatang dan tempat wisata.
- Dengan menargetkan perusahaan jasa POS yang menyediakan sistem pembayaran *turnkey* ke pebisnis lokal dan restoran, penyerang dapat mencuri data kartu kredit dari ribuan nasabah ritel.

http://www.foerderland.de/fileadmin/pdf/IBM_XForce_Report_2016.pdf

Pengamanan digital services?

Solusi Keamanan

Yang sering dilupakan adalah mengamankan tidak selalu berarti mencegah terjadinya "insiden keamanan"



1. Sistem otentikasi ke depan?
Multifactor authentication

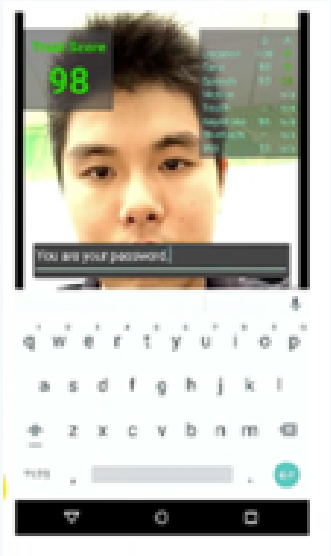
Google password free login

User membuka kunci device atau login ke aplikasi berdasarkan kecocokan nilai **Trust Score**

Trust score menghitung nilai berdasar kombinasi dari berbagai pola user

- Pola mengetik
- Kecepatan mengetik
- Pengenalan suara
- Pengenalan wajah
- Fingerprint
- dll

Penerapan trust scores bervariasi:
Misal untuk games, dibutuhkan low trust score, serta skor lebih tinggi untuk aplikasi yang lebih high-risk seperti aplikasi banking.



You are your password

http://thehackernews.com/2016/05/android-abacus-trust-api.html

Persetujuan login Facebook

Merubah setting security Facebook, memungkinkan user menggunakan otentikasi tambahan saat login yaitu

1. input kode security yang dikirim via mobile phone
2. input kode yang dibangkitkan oleh code generator
3. Input kode yang dibangkitkan oleh third party code generating mobile app (seperti Google Authenticator atau Authy)

Contoh solusi otentikasi internet banking

CVR-Token®
AUTHENTICATION SOLUTION
Powered by SHARING VISION™
www.sharingvision.com

CVR-Token adalah **Soft-Token** pengaman transaksi
Internet Banking yang didesain khusus
untuk melindungi nasabah dari **man-in-the-middle-attack**

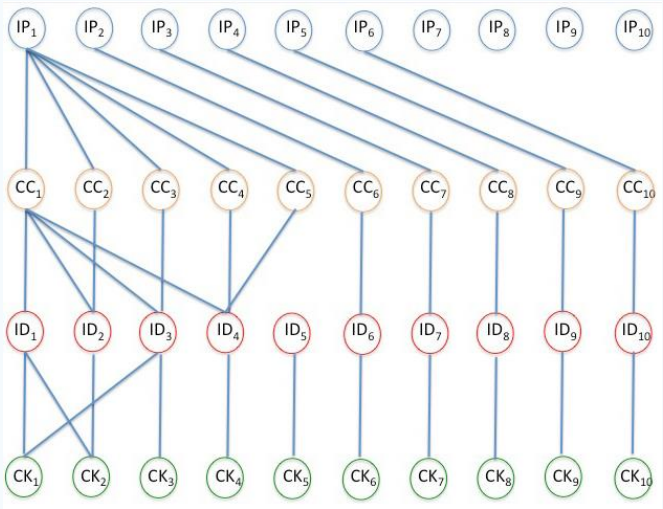
CVR-Token menggunakan mekanisme **challenge-verify-response**
yang secara fundamental memperbaiki
kelemahan token sebelumnya yang hanya menggunakan
mekanisme *challenge* & *response*

2. Fraud analytics masa depan

- **Graph databases:**

Menganalisis pola yang sulit dideteksi jika menggunakan penggambaran tradisional seperti table.

Contoh fraud eCommerce, IP1 melakukan fraud



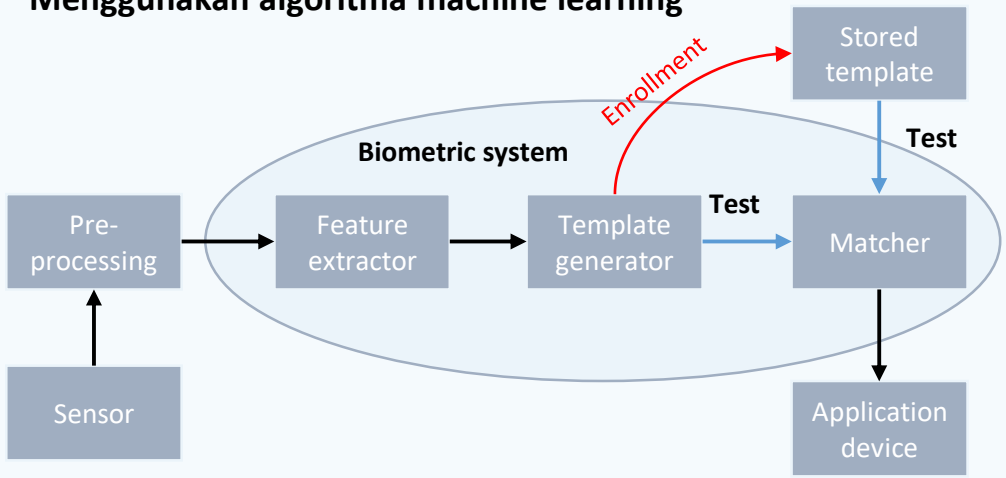
Satu IP melakukan banyak transaksi menggunakan 5 kartu kredit dimana salah satu kartu kredit (CC1) digunakan oleh banyak IS, dimana dua cookies (CK1 dan CK2) masing-masing sharing 2 ID.

http://info.neo4j.com/rs/neotechnology/images/Fraud%20Detection%20Using%20GraphDB%20-%202014.pdf

- **Behaviour analytic**

Behavioral analysis menganalisi perilaku unik user untuk menghasilkan profil perilaku yang normal. Kemudian menandai perilaku yang mencurigakan yang melenceng jauh dari normal sebagai fraud.

Menggunakan algoritma machine learning



http://securedtouch.com/behavioral-analysis-the-future-of-fraud-prevention/

- **Language analytic**

Memfilter email yang mengandung pola naratif terkait symptom sebuah fraud. Misal message yang menyebutkan jumlah uang serta no telp untuk dihubungi.

- **In the moment warning**

Adalah mungkin perusahaan telepon mengumpulkan informasi dari telepon telepon di jaringan mereka kemudian menggunakan voice biometric software untuk mengenali individu serta menangkap pola emosi yang dapat mengindikasi penipuan.

http://www.theatlantic.com/magazine/archive/2016/03/the-future-of-fraud-busting/426867/

3. Kerjasama untuk menghadapi organized crime

Kerjasama antar lembaga pemerintah, pelaku bisnis dan akademisi/peneliti untuk menghadapi *organized crime*.

- Akan sangat sulit bagi perusahaan untuk menghadapi sendiri serangan dilakukan oleh *organized crime.*
- Perlu peran pemerintah: Kominfo, BI, OJK.
  - Melakukan pencegahan dan reaksi terhadap berbagai permasalahan keamanan digital channel.
  - Menjadi fasilitator kerjasama pelaku industri untuk menghadapi permasalahan keamanan.
  - Menjadi mediator permasalahan keamanan antara penyedia layanan dengan pelanggan.
- Perlu kerjasama antara pelaku industri untuk:
  - Menshare informasi mengenai suatu insiden keamanan.
  - Menshare informasi mengenai kerawanan yang telah teridentifikasi.
  - Mencari solusi bersama mitigasi risiko untuk insiden dan kerawanan tersebut.

Merci bien

Arigatoo

Matur Nuwun

Hatur Nuhun

Matur se Kelangkong

Syukron

Kheili Mamnun

Danke

Terima Kasih

GARUDA

the symbol of Indonesia