2016 IIA INDONESIA NATIONAL CONFERENCE 6-8 SEPTEMBER

Technology Trend

A Closer Look at Cyber Security

Gildas Deograt Lumy, CISA, CISSP
Senior Information Security Consultant
XecureIT

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

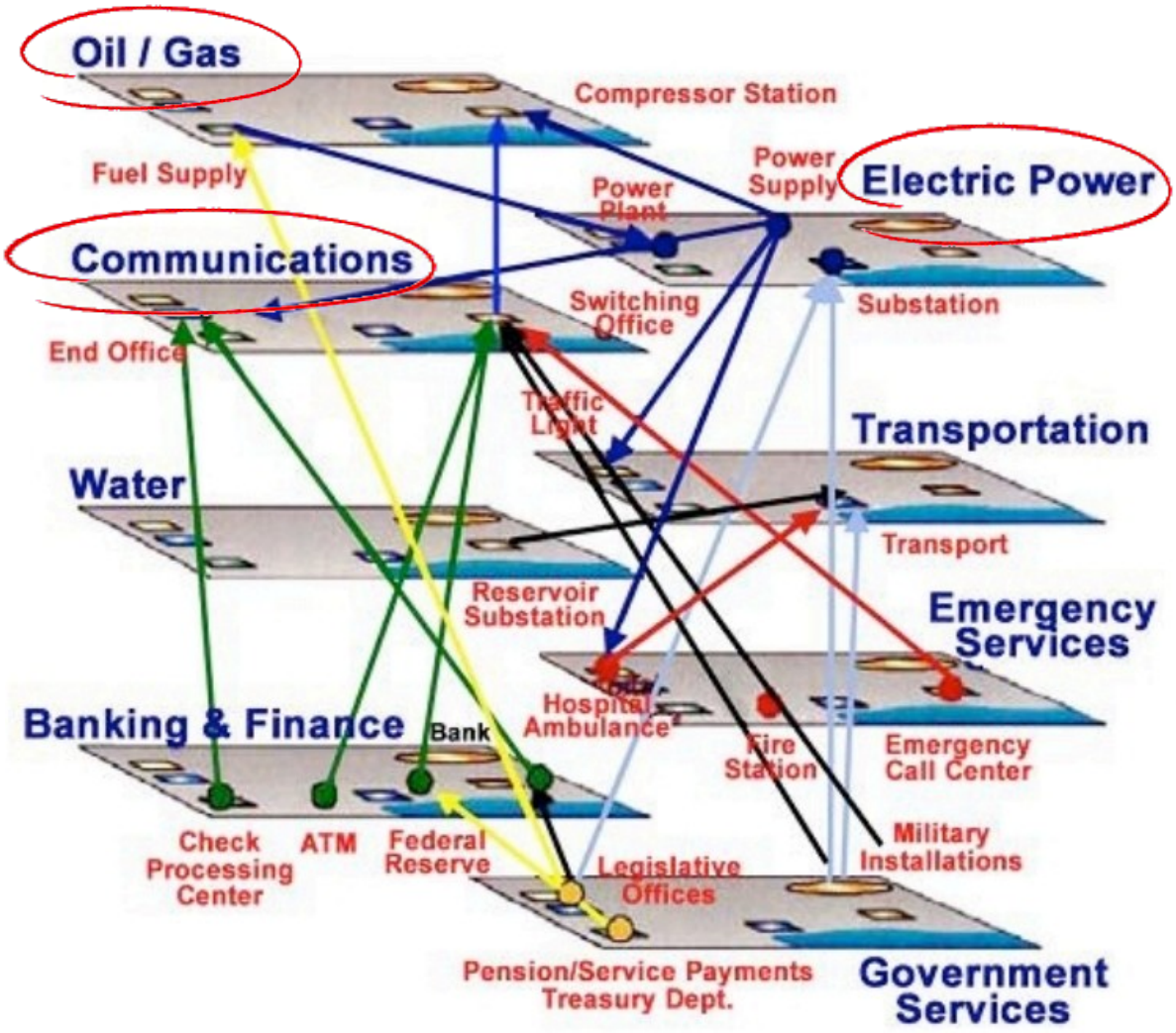
- Senior Information Security Consultant, XecureIT, since 2007
- Cyber Defense Expert, Ministry of Defense, since 2013
- Deputy Director Coordination and Mitigation Group, National Desk for Cyberspace, Coordinating Political, Legal, and Security Affairs Minister, since 2014
- President of Cyber Security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

CONTACT

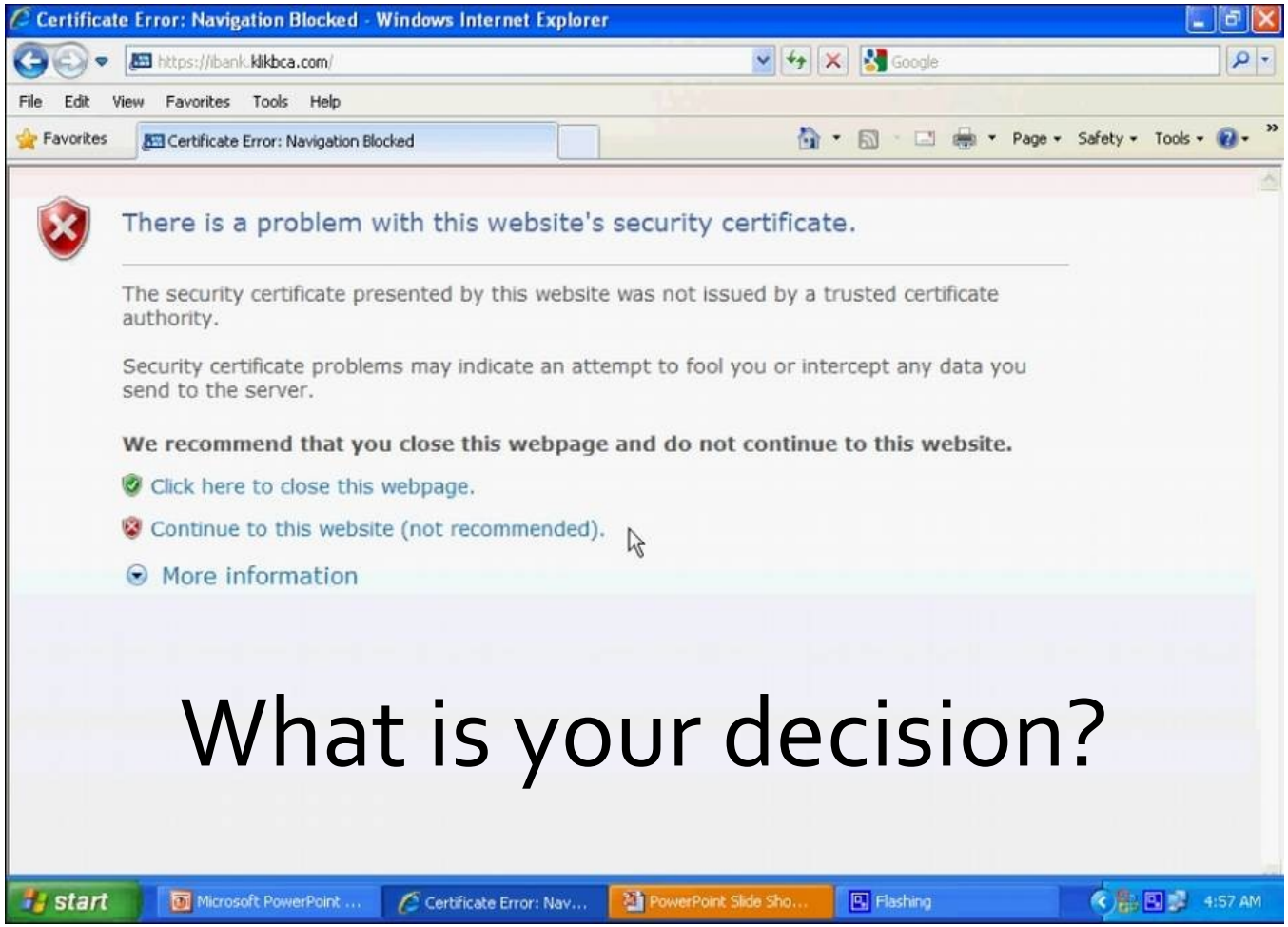
gildas.deograt@xecureit.id Signal/Telegram +62 813 1773 7474 www.linkedin.com/in/gildasdeograt

R U Sure U R Secure?

Critical Infrastructure Interdependency



Security Warning...



What is your decision?

Zero Day Vulnerability:
We are the sitting ducks


BBC | BBC iD | Menu | Search

NEWS | Sections

Microsoft fixes '19-year-old' bug with emergency patch

By Dave Lee
Technology reporter, BBC News

12 November 2014 | Technology


ZDNet | MENU | AS

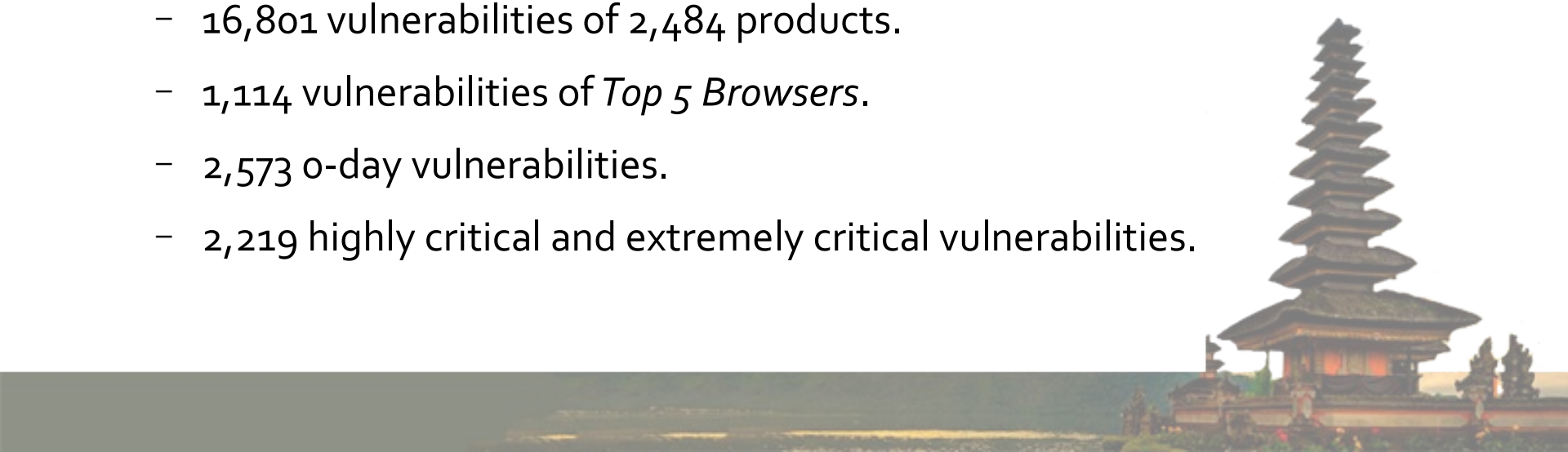
Apple zero-day vulnerability fully compromises your devices

The severe and previously unknown flaw circumvents Apple's stringent security features to compromise devices.

By Charlie Osborne for Zero Day | March 24, 2016 -- 08:35 GMT (16:35 GMT+08:00) | Topic: Security

Zero Day Vulnerability: We are the sitting ducks

- In enterprise system, a *critical* security patch is installed in more than one week.
  - The majority of enterprises can "finished" the installation in 6 months.
- Exploit development requires <1 hour using patch reverse engineering technique.
- Security Vulnerability Statistics in 2015:
  - 16,801 vulnerabilities of 2,484 products.
  - 1,114 vulnerabilities of *Top 5 Browsers*.
  - 2,573 0-day vulnerabilities.
  - 2,219 highly critical and extremely critical vulnerabilities.



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

Share

Secret backdoors found in firewall, VPN gear from Barracuda Networks

The undocumented accounts may have been around for a decade.

by **Dan Goodin** - Jan 24, 2013 4:08 pm UTC

IDENTITY NETWORKING 69

A variety of firewall, VPN, and spam filtering gear sold by Barracuda Networks contains undocumented backdoor accounts that allow people to remotely log in and access sensitive information, researchers with an Austrian security firm have warned.

The SSH, or secure shell, backdoor is hardcoded into "multiple Barracuda Networks products" and can be used to gain shell access to vulnerable appliances, according to an advisory published Thursday by SEC Consult Vulnerability Lab.

HP Confirms Backdoor In StoreOnce Backup Product Line

By Ryan Naraine on June 26, 2013

Tweet Saranikan 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.

tories: Forums Subscribe Jobs

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

Telecommunication Services

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

iidnight on
29 October, during

UK telco TalkTalk hacked, 4m customers affected

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.

Telecommunication Services

- The priority of information security aspect: Availability.
- SIM Swop attack has been known since 2007.
- GSM (voice and SMS interception is cheap and easy.
- Fake BTS attack is "common"

Ransomware

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 |

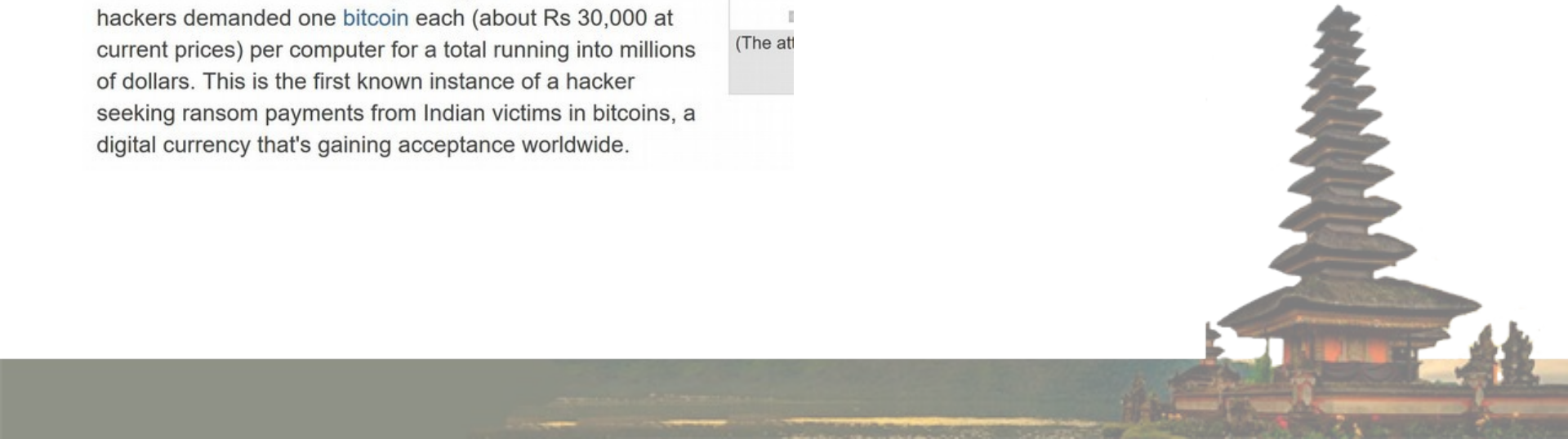
MUMBAI: Hackers seized control of computers at three banks and a pharmaceutical company about a week ago, then demanded a ransom in bitcoins for the decryption keys to unfreeze them.

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.

(The att

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).



Distributed Denial of Service (DDoS)

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, Citig
durir

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.

Malware Hijacks SmartCard and PIN

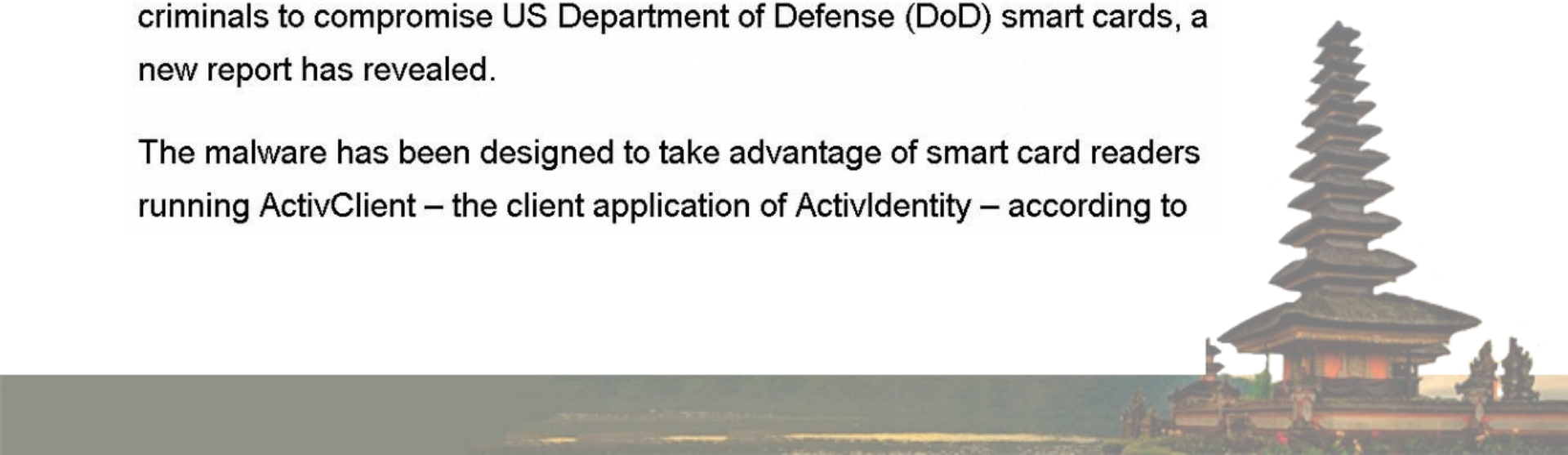
Chinese 'attack US DoD smart cards' with Sykipot malware

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



Internet Banking vs Mobile Banking

Client:
Browser

Front End Servers:
Web Server

Internet Banking

Back End Servers

Client:
Mobile Banking
Application

Front End Servers:
Web Service

Mobile Banking

Internet Banking vs Mobile Banking

The Sydney Morning Herald
Digital Life

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

March 10, 2016

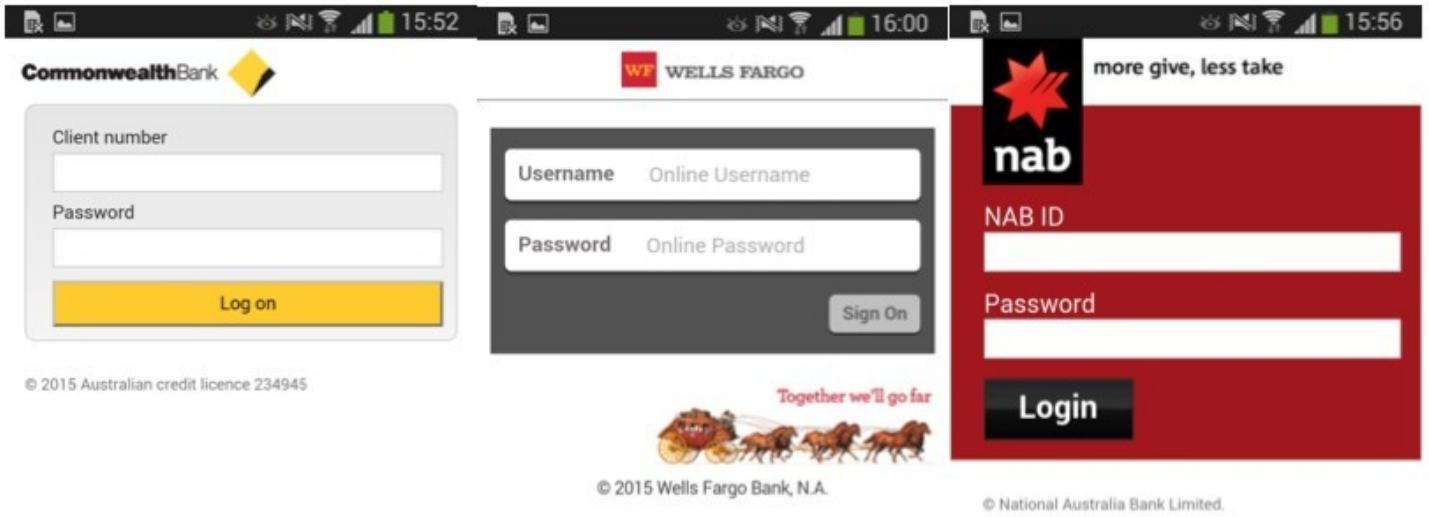
Millions of customers of Australia's largest banks are the target of a sophisticated Android attack which steals banking details and thwarts two-factor authentication security.

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.

Internet Banking vs Mobile Banking

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



Internet Banking vs Mobile Banking

PCWorld
Work. Life. Productivity.

Home / Security

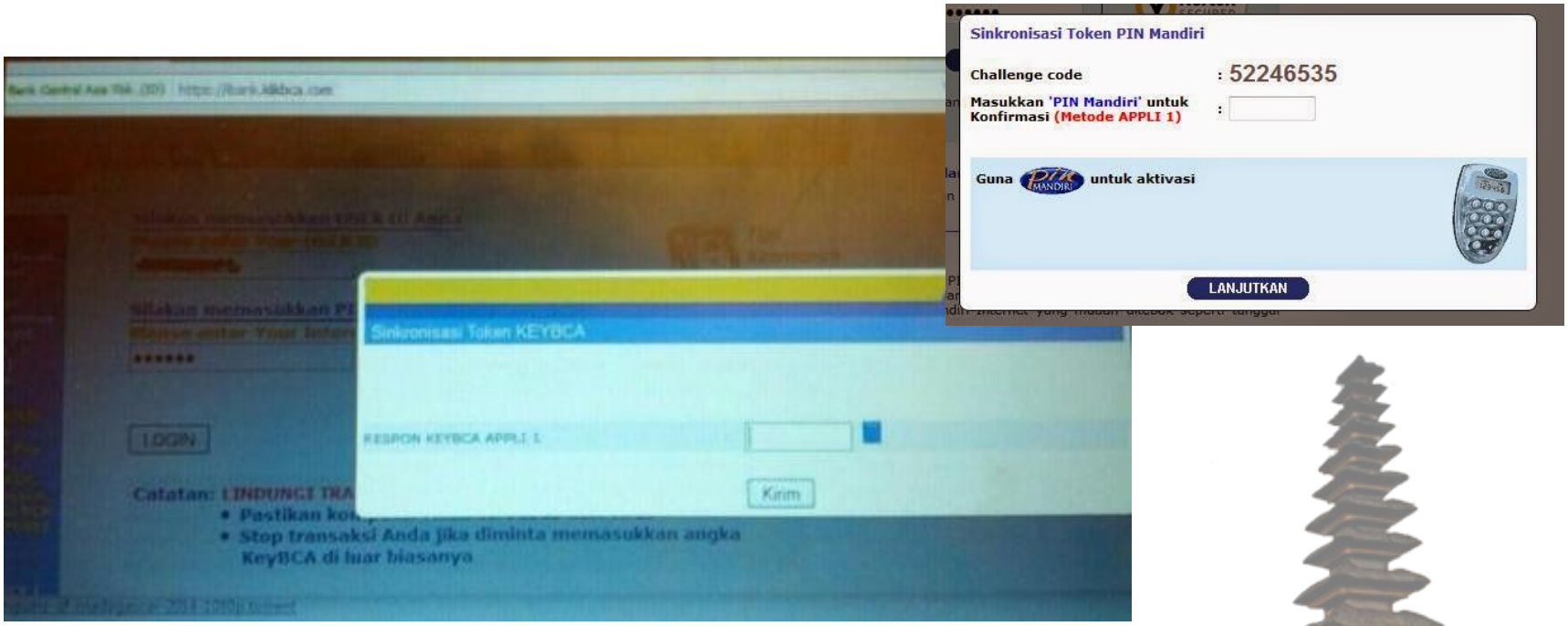
Tricky new malware replaces your entire browser with a dangerous Chrome lookalike

This malicious browser looks and acts just like Chrome--except for all the pop-up ads, system file hijacking, and activity monitoring.

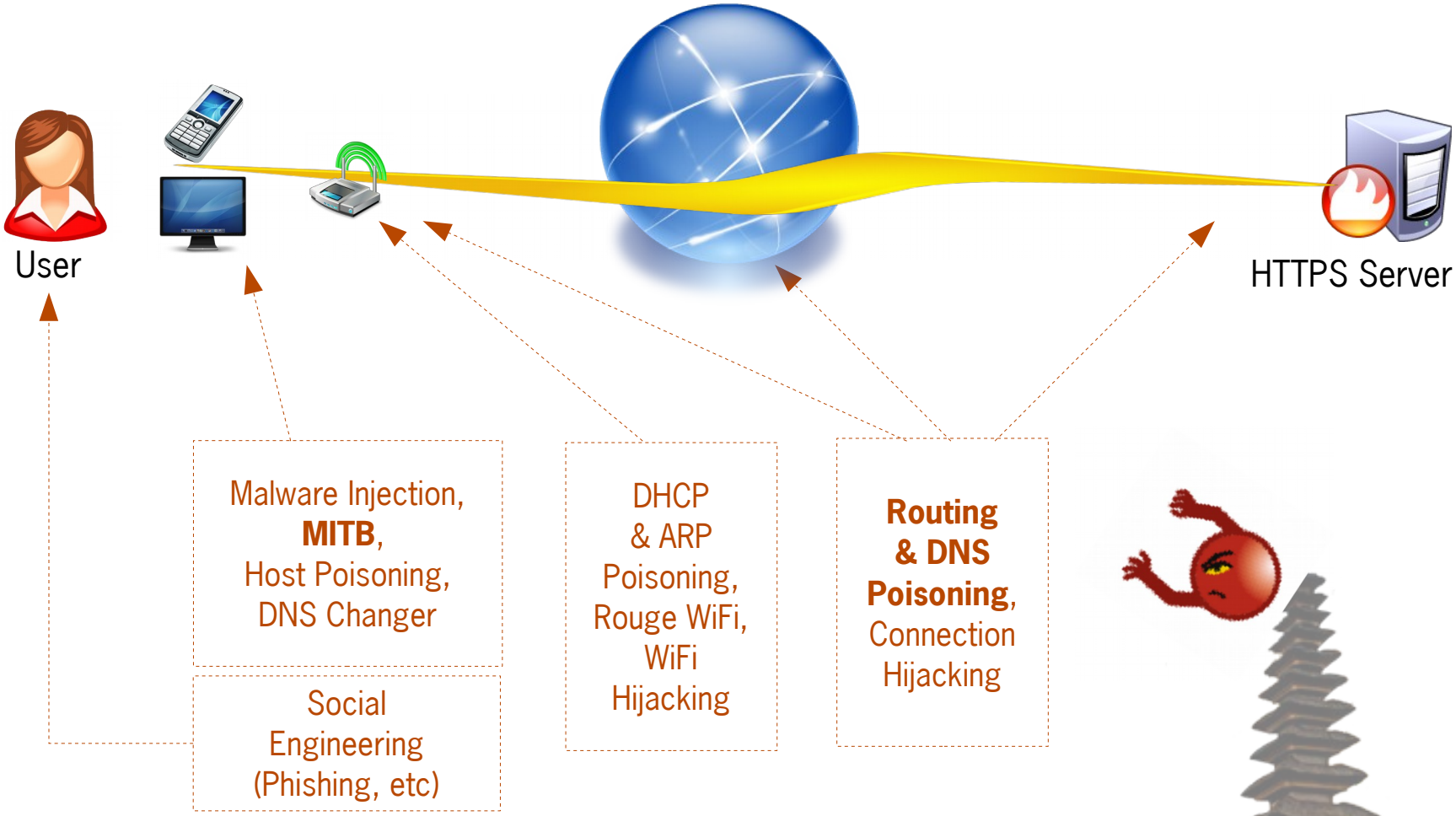
- Malware in The Browser
- Malware as a Browser

“Token Synchronization”

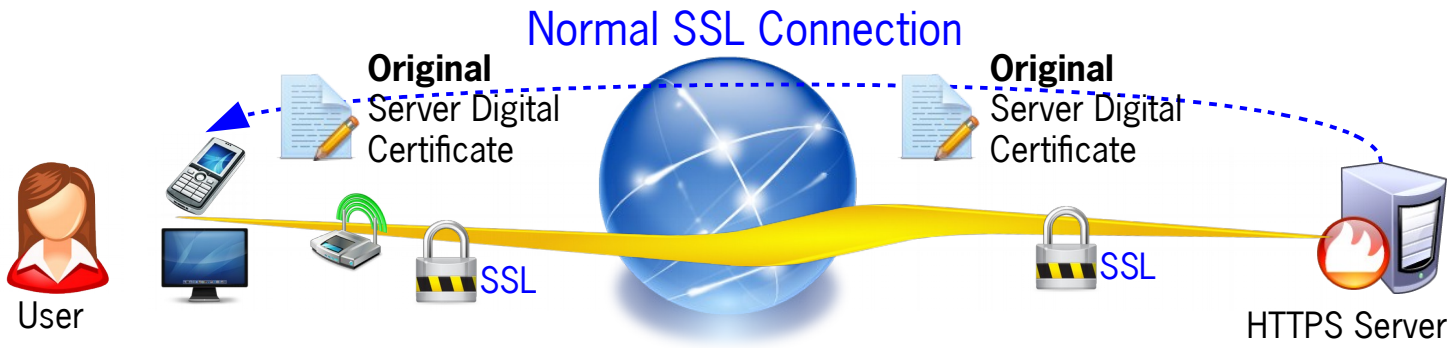
- “Token Synchronization” cases http://tinyurl.com/guown7h

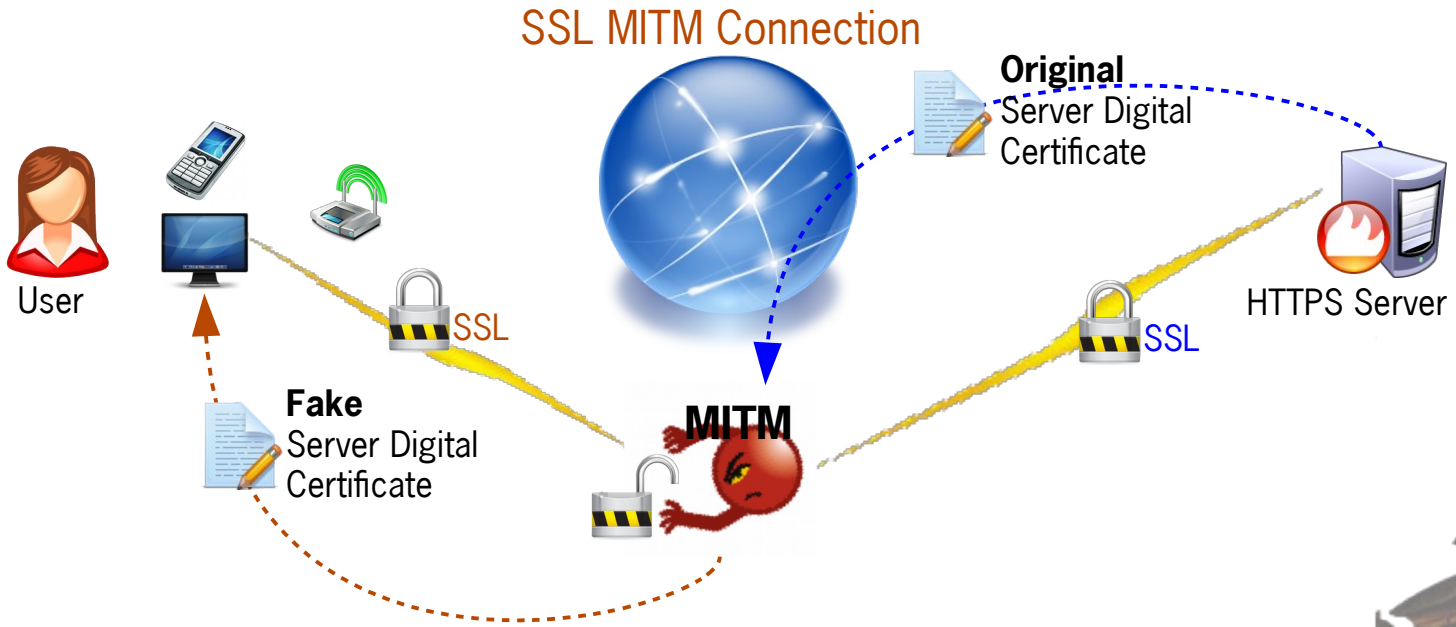


“Token Synchronization”
SSL Man in The Middle (MiTM) Attack

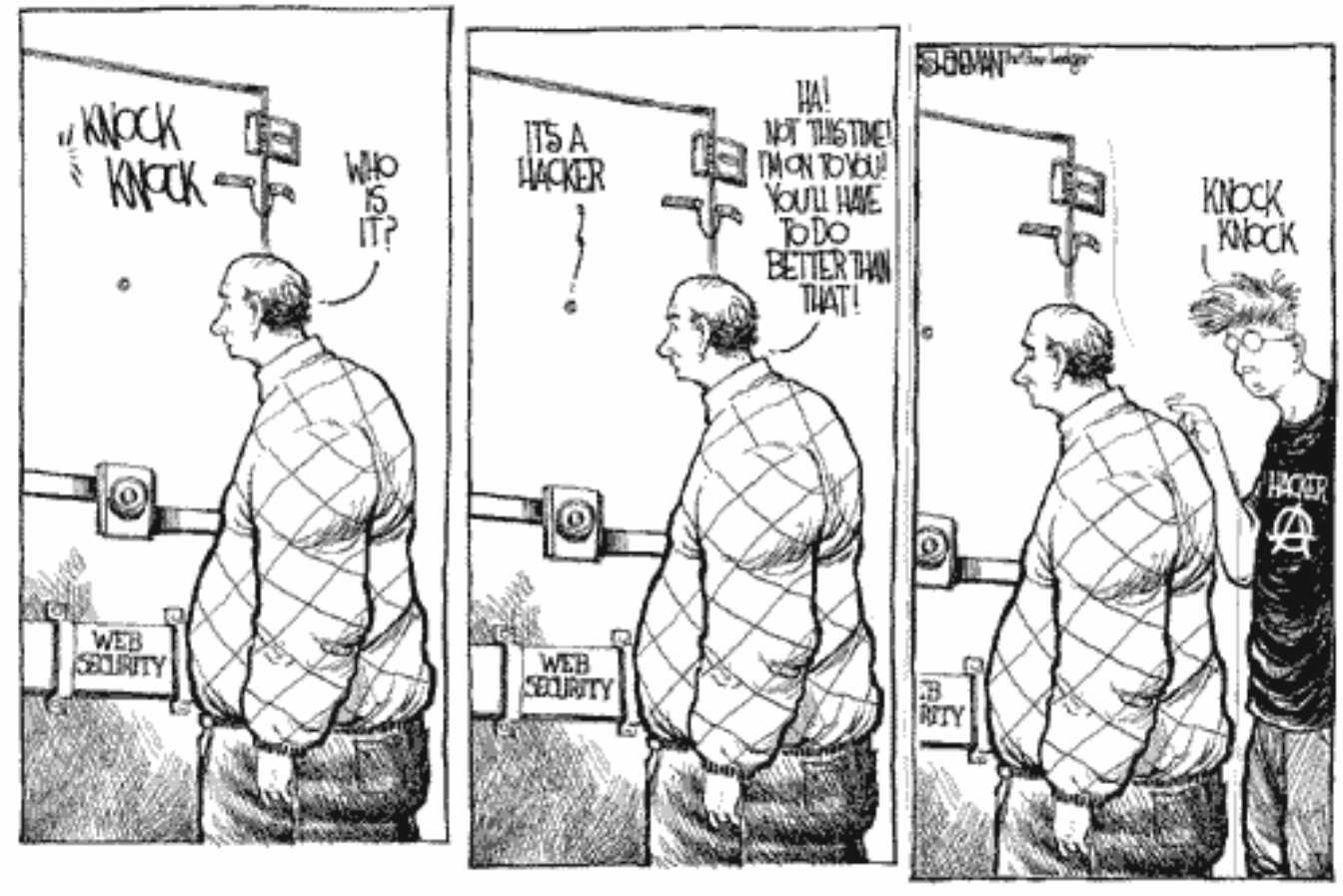


“Token Synchronization”
SSL Man in The Middle (MiTM) Attack





Hacker's Inside ;)



Hacker's Mindset ;)

IT Auditor vs Hacker

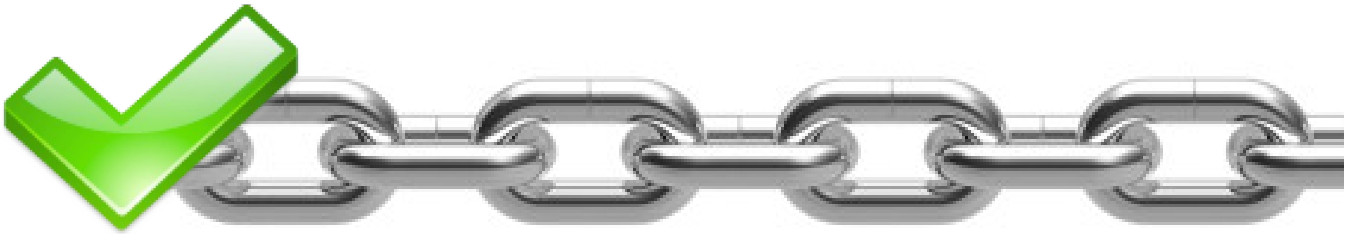
	IT Auditor	Hacker
Objective	Securing target	Securing / compromising target
Purpose	How to find the root cause and improve the process . **++**	**Good**: How to improve the human life through technology. **++** **Bad**: How to steal or damage others through technology.
Mindset	Inside the box. How to check (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) **++**

Challenges

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 !"

Redefine Cyber Security Architecture: Comprehensive and Consistent

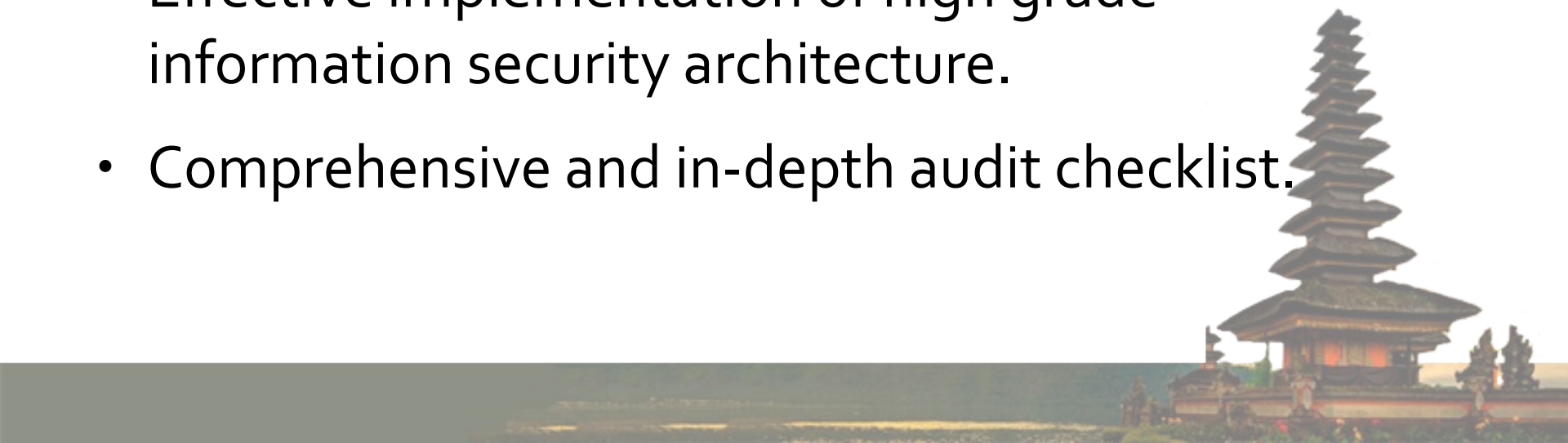


Redefine Cyber Security Architecture: Integrated Information Security

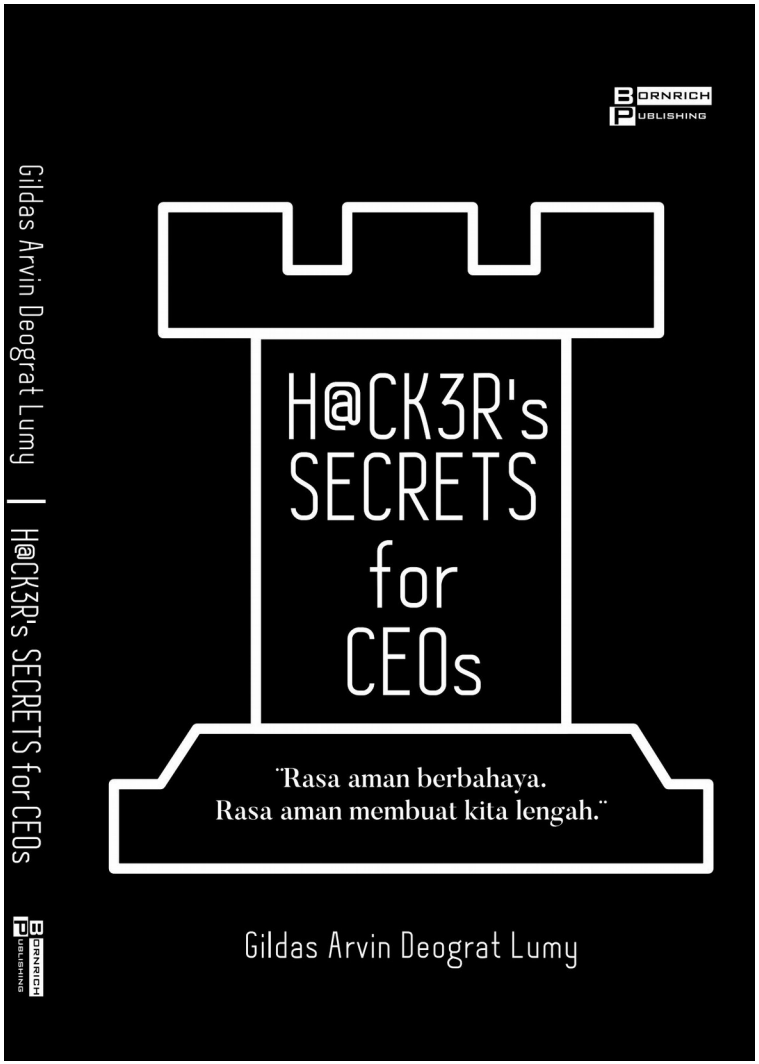
SAKTTI is a high grade information security architecture to effectively implement integrated information security concept.

Cyber Security Auditor's Focuses

- Appropriate **business** risk management.
  - Ensure the compliance with law and regulation.
  - Understand the security priority (integrity / confidentiality / availability) of your business context related with industry, customers, and "partners" (may across industry).
  - In general, IT team doesn't know the business ;)
- Effective implementation of high grade information security architecture.
- Comprehensive and in-depth audit checklist.



My New Book ...



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