

Indonesia Latest Trend 2011

Cyber Crime



Id-SIRTII

ICT STATISTICS

- *“Latest Indonesian ICT statistic (compiled)”*

Latest Data

- * Population 242,968,342 (July 2010, est.)
- * More than 178 ISP's, 39 NAP's, 3 IX's
- * Users (mil.): 1 (1999), 45 (2009), 60 (2010)
- * 100.000 subscribers (1999), 7 million (2010)
- * 60 Gbit/s IX traffic, 60 Gbit/s international
- * +3 mil. Comp. (2 mil. notebooks) sales (2010)
- * More than 40 mil. Students connected (2012)
- * 25 million online media regular visitors/day!
- * Facebook 35 mil. #2, Twitter 21% #4 (2011)

Mobile Growth

- Numbers (mil.): 180, 135 unique, 85 GPRS ph.
- Users (mil.): +3 broadband, 12 3G, 45 GPRS
- +2.500.000 Blackberry subscribers (2010)
- 37.000 (Telkomsel), 29.000 (Indosat), 26.000 (XL) BTS GSM/Node B. Serving 99% of 5.748 district (kecamatan). GPRS/EDGE ready
- AXIS, XL, ISAT, TSEL, 3 (GSM/GPRS/3G); ESIA, FLEXI, FREN, SMART (CDMA/EVDO);
- 31.824 villages connected in 2014 (BTIP)

Market Profile

- Price war (promo), low ARPU, VAS
- Computer internet < 5 mil. (US\$500)
- Netbook + cell. data access (US\$300)
- Internet gadget, < 1 mil. (US\$ 100)
- 60 % devices: gadget, netbook, laptops
- 3G access plan (flat), < 100K (US\$ 10)/mo
- Home broadband (flat), < 200K (US\$ 20)/mo
- Always on generation 24/7: news, social net, blogs, micro blog, chat, fun/games

INCREASING RISK

- *“Because of more value in cyberspace”*

Reported Events (1)

- Incident: phishing, identity theft, data stealing & forgery - bot attack, defamation, fraud, industrial espionage, critical information resources hostages, information leakage, insider attack (i.e. virus spread)
- Cases: cyber war, fraud, defamation, hoax, gambling, trafficking, child predator, porn., prostitution, money laundering & terrorism, underground economy - UU ITE 11 / 2008

Reported Events (2)

- Techniques: Malicious code, local virus, common vulnerabilities/zero day - pirateware (counterfeit not updated), phishing, nigerian/love/bride scam (email, SMS), warez activity, local SPAM increase last 2 years, social network/messaging attack, targetted attack, web defacing rally (vandalism)
- Motives: economy, political (ID vs MY), hatred/racism/mass protest, content blocking policy
- CEWAS (sensors): 1,1 million events (possible attack) daily, mostly CN & US IP's

Latest Trend

- Online banking fraud (phishing, MiTM)
- Tax evasion, money laundering, corruption
- Underground economy, transnational crime (organized, cross border, distributed, multi stage, political issues involved, global action)
- Sophistication (individual, skilled, targetted)
- Crimes that not exist yet (not regulated yet), online (cyber), financial (money), integrated (any kind related), more politics

Challenges

- Size of the problems and complexity
- Investigation issues: cross jurisdictions, different search, seizing data and evidence procedures, limited time (investigation, prosecution), human rights and privacy safeguarding (OECD), limited cyber law
- Mutual legal assistance within counterparts
- Ensuring judicial (court) systems compliance
- Rapid exploitation on advanced technology
- Beware of the power of money and politics

Countermeasures

- Multijurisdictional Special Task Force
- Sophistication of skills and capability
- Improved communications and technology
- Intelligence and information sharing
- Multilateral Treaty and Convention
- International collaboration focal point
- Adequate fund and resources support

Strategic Collaboration

- Ratification of UN convention (UNODC)
- Technical assistance by related experts
- Training of criminal justice practitioners
- Information sharing among parties involved
- Periodic organized crimes trends assessment
- Sustainable special witness protection prog.
- Cross border control surveillance and patrol

Government Role

- Manage National Cyber Security framework and standard to assure, evaluate periodically critical information security deployment
- Manage national secure data center and DRC capability, provide secure emergency channel and resources to establish and maintain critical infrastructure for telecommunication and public services during the hard events

Id-SIRTII

- *“Performing CERT/CSIRT/CC daily activities to coordinate national level incident response handling initiatives and to join international collaboration”*

Brief History

- Stakeholders initiatives: police, attorney, ICT society, association (ISP, Internet Café, Credit Card), academia, government (ICT Ministry, Central Bank)
- Steering Committee Board founded in 2006 by Ministry Decree No. 27/2006, Executive board founded in 2007 by Ministry Decree No. 26/2007. New ministerial decree No. 16/2010 (Revised) - as National's CSIRT/CC (single point of contact)
- APCERT General Member (2009)/Full Member (2011), FIRST Full Member (2011)/National CSIRT Forum Member (2009), OIC-CERT Full Member

Mission and Objectives

- Internet traffic monitoring
- Managing log files (law enforcement)
- Conduct security awareness campaign
- Assisting how to managing security
- Providing security training to public
- Conduct R & D, labs & collaboration
- National CSIRT/CC (Coordination Center - single point of contact)

Monitoring Center

- 11 sensors: XL, Indosat, IM2, Telkom, Napinfo, CBN, Biznet, Indonet, Centrin, IIX, 22 more 2011
- Critical infrastructure: Government; Public Services; Defense, Military & Home Land Security; Energy & Natural Resources; Public Transportation; Stock Exchange, Finance, Investment, Bank; Education; Industry & Commerce; Public Health; LEA; Teleco's, Media & Broadcasting; Art, Culture & Tourism; BUMN
- Future deployment (2011) at 8 planned areas of BTIP Local Internet Data Centers & Exchanges

2011, Next Program (1)

- Open public incident report and tracking system
- Direct access to monitoring system for ISP's, NAP's, IX
- Expanding analysis capability, capacity and providing result to the public (security alert, security advisory, early warning, CC – national coordination center, mitigation assistance); Ministerial decree No. 16/2010
- Organizing regular national drill test and cyber attack coordination simulation also joining international drill test event (APCERT) etc.
- Conducting in house monitoring system research and with embedded system for SOHO / low scale orgnz.

2011, Next Program (2)

- Conducting security training center, simulation labs, data mining, malware analysis, digital forensic labs, national honeynet project, secure DNS and anti SPAM project, children protection, OSS repository, local free mail, content delivery
- International project i.e. Tsubame (JPCERT), drill test and research collaboration with vendors
- Participating international events (workshop, research, seminar, exhibitions, convention, etc.)

2011, Next Program (3)

- Road Show Seminar and Workshop to 5 cities
- InfoSec Training for 1.000 + participants
- Public awareness: teacher, student, journalist
- Special Training by request: civil organization, military, LEA, ISPs
- Other Training: Open Source and Security, IT Forensic, Certified EC-Council, CSSIP etc.
- Self training and information security awareness video, poster, leaflet, bulletin

2011, Next Program (4)

- Knowledge repository, social media campaign
- ID-KIDS portal, protect children and online guide
- Collaboration (ICT Watch, AWARI, KKI, etc.)
- Joining international coordination APCERT, FIRST, OICCERT, drill test, staff exchange with MyCERT, workshop/technical colloquium
- Other international forum ITU, APT, APEC etc.
- Expanding National Incident Response Team
- Assisting establishment of other CERT's (sector i.e. banks, Academic CERT, etc.)

2011, Next Program (5)

- Installing More Tsubame Sensors (3 units)
- Conducting Malware Analysis & Data Mining
- Conducting Nation Wide Honey Net Program
- Continue Anti SPAM & DNS Filtering Program
- Enhancing Threat Information Coordination
- Improving Security Technical Training

2011, Next Program (6)

- Revising National InfoSec Policies
- National Internet Child Protection Program
- Developing Digital Forensics Laboratory
- Open Source and Secure Tools Repository
- Secure Content Delivery Network
- Boosting Public Awareness Efforts
- Collaboration with Asian CSIRTs/CERTs

Thank You

- Ravindo Tower 17th Floor
- Kebon Sirih Raya, Kav. 75
- Central Jakarta, 10340
- Ph. +62 21 3192 5551 ; Fax +62 21 3193 5556
- info@idsirtii.or.id ; www.idsirtii.or.id