

Tren Serangan Siber Nasional 2016 Dan Prediksi 2017



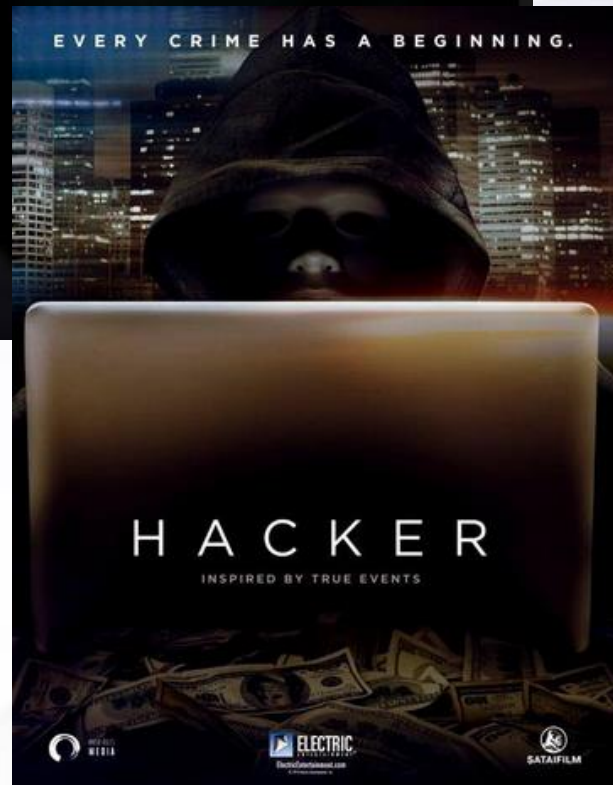
Iwan Sumantri

Ketua NCSD (National Cyber Security Defence)

Wakil Ketua IDSIRTII - Kemenkominfo

Jakarta, 4 Maret 2017

Anda terinspirasi dengan Film ini?



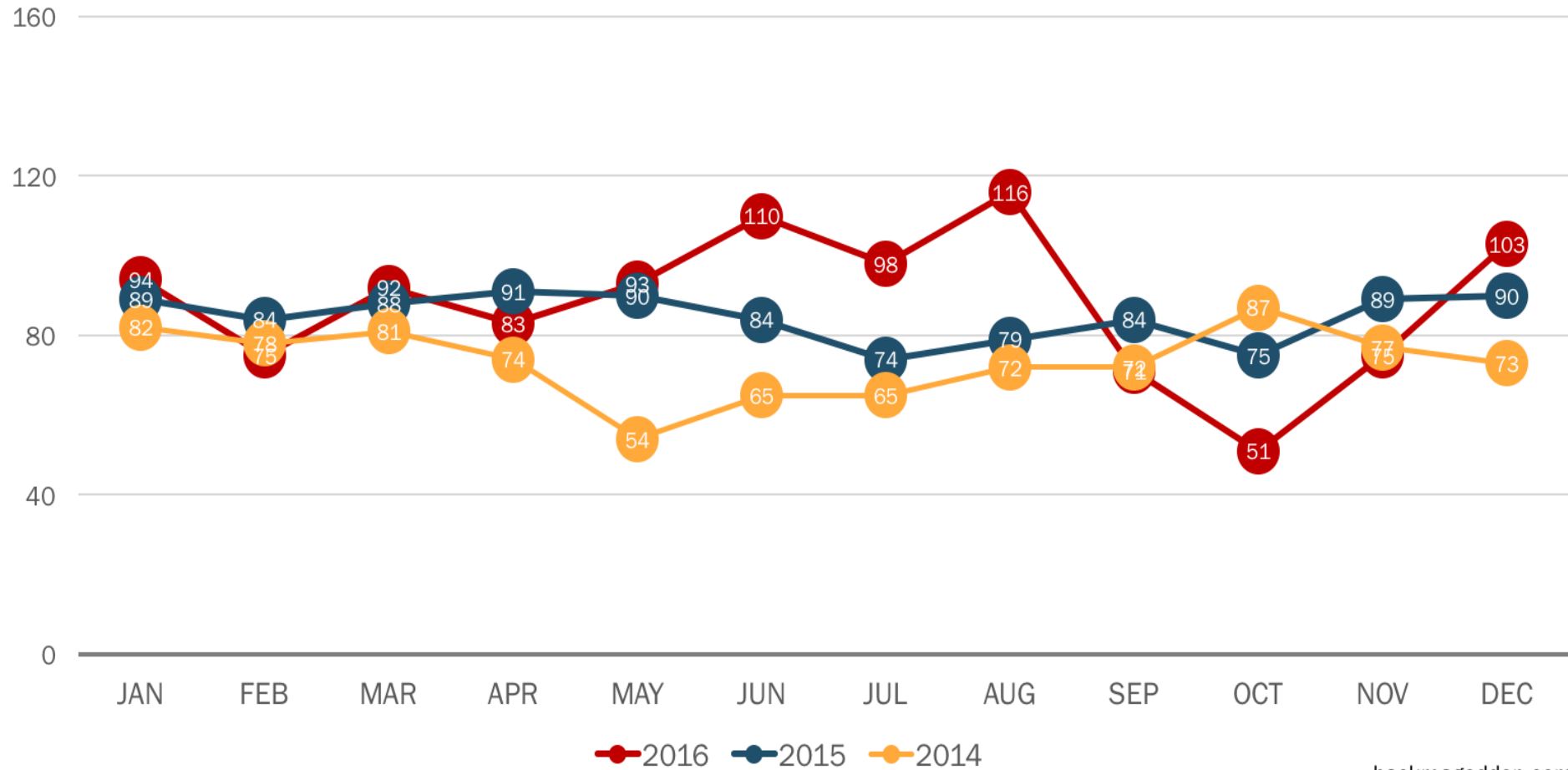
The image features two identical green tanks, possibly T-72s, positioned diagonally on a grey grid background. The tanks are rendered in a semi-transparent green color. Behind the tanks, there are large, white, 3D-style binary digits (0s and 1s) that appear to be floating or projected. A dark grey horizontal band is superimposed over the center of the image, containing the title text in white.

Serangan Siber - Cyber ATTACK

“to take over the resources”

Tren Global : Serangan Siber

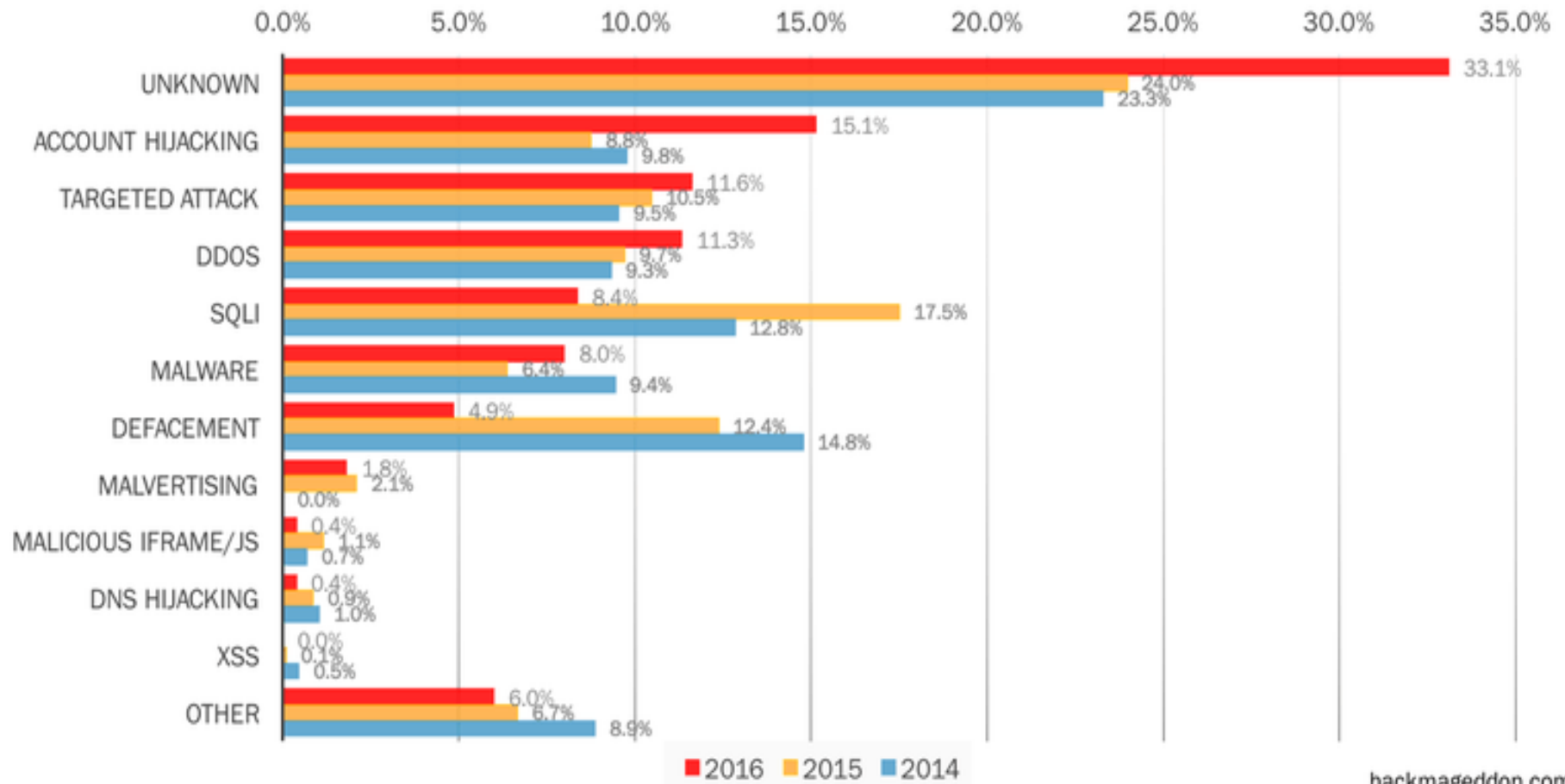
Monthly Attacks (2016 vs 2015 vs 2014)



hackmageddon.com

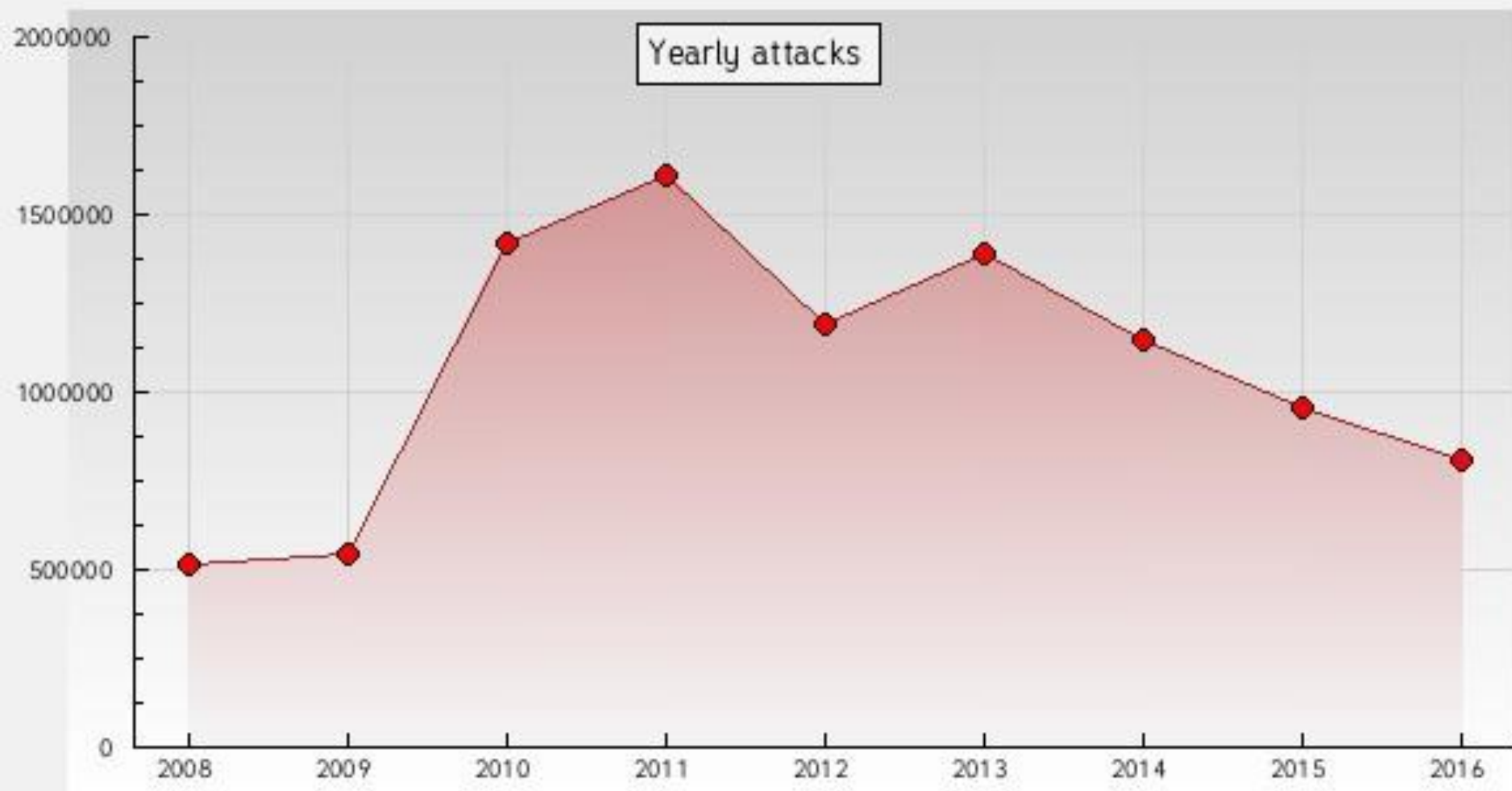
Tren Global : Teknik Serangan

Top 10 Attack Techniques
2016 vs 2015 vs 2014



hackmageddon.com

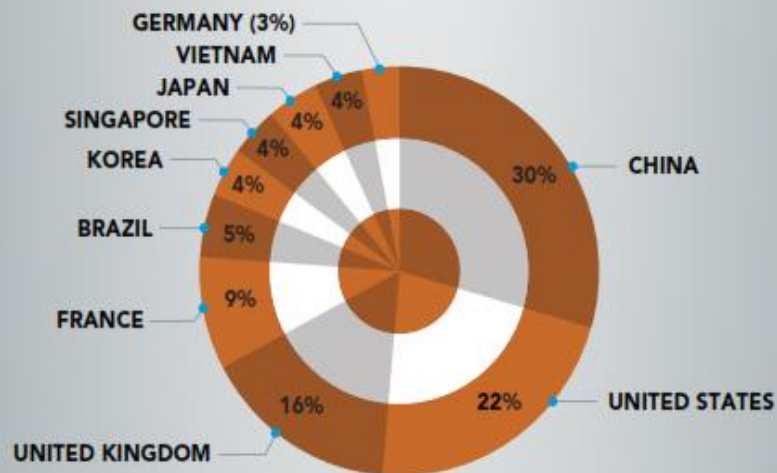
Tren Global : Insiden website



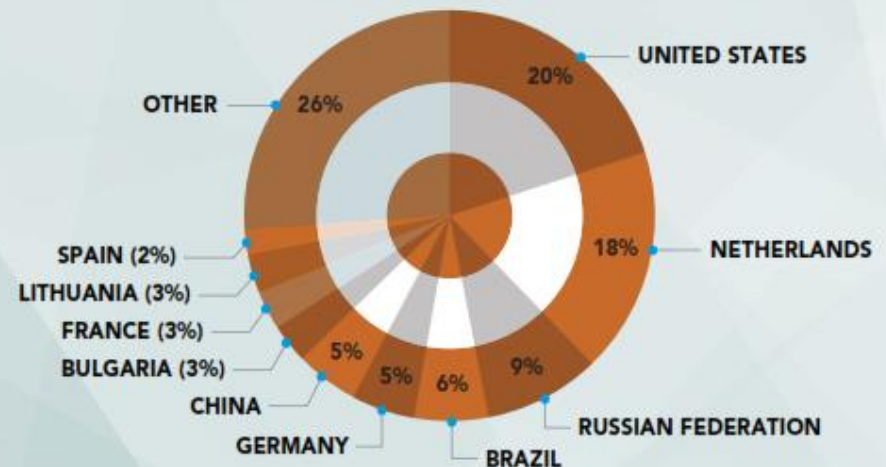
Security Attack Traffic

Top Originating Countries 2016

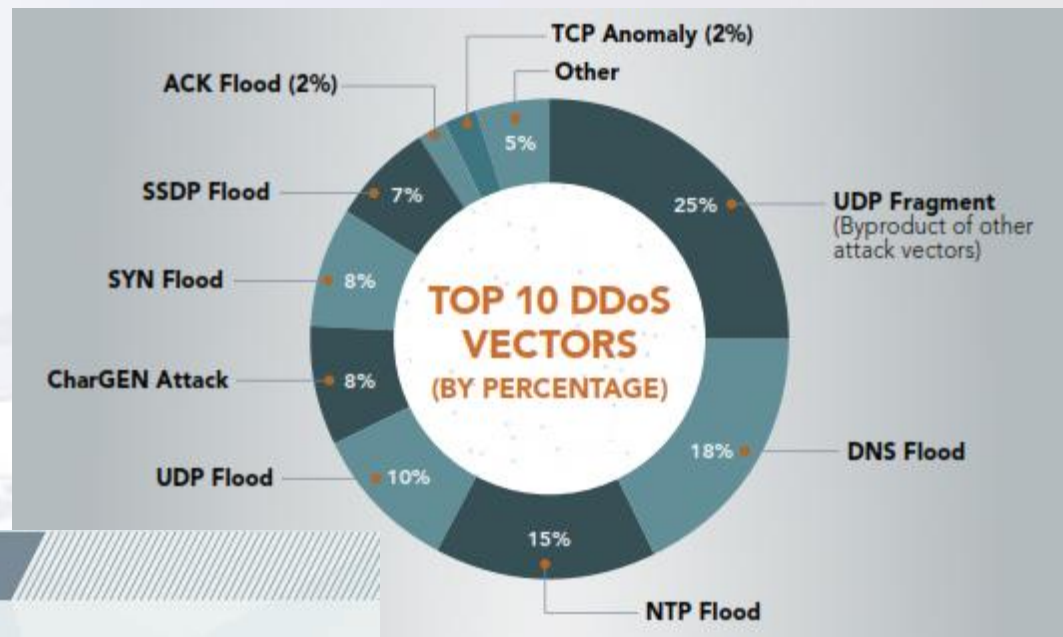
TOP SOURCE COUNTRIES FOR DDoS ATTACKS



TOP SOURCE COUNTRIES FOR WEB APPLICATION ATTACKS

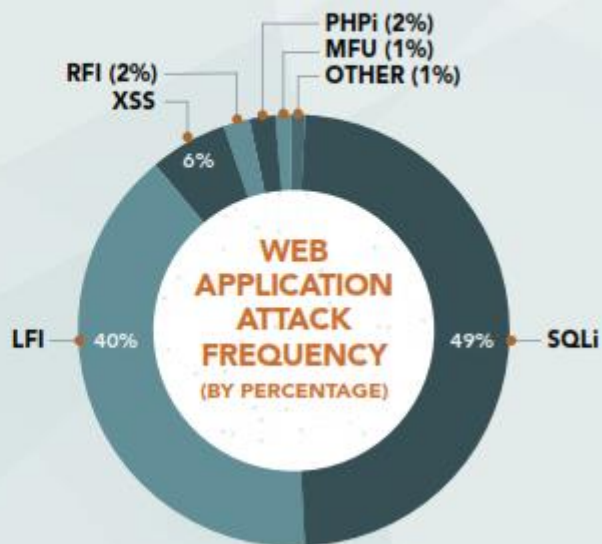


DDoS AND WEB APPLICATION ATTACKS



WEB APP ATTACK TRENDS

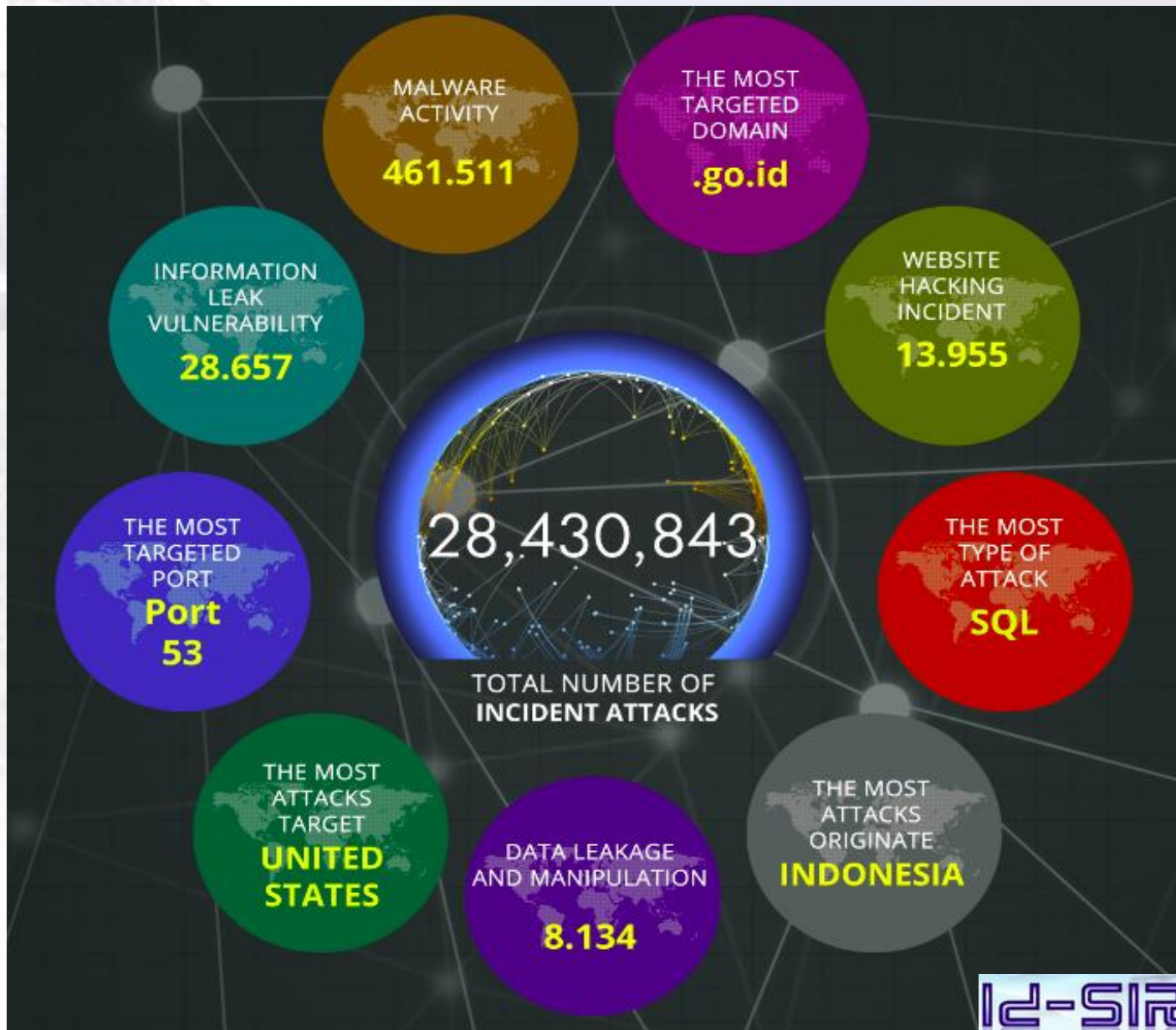
HTTP vs. HTTPS



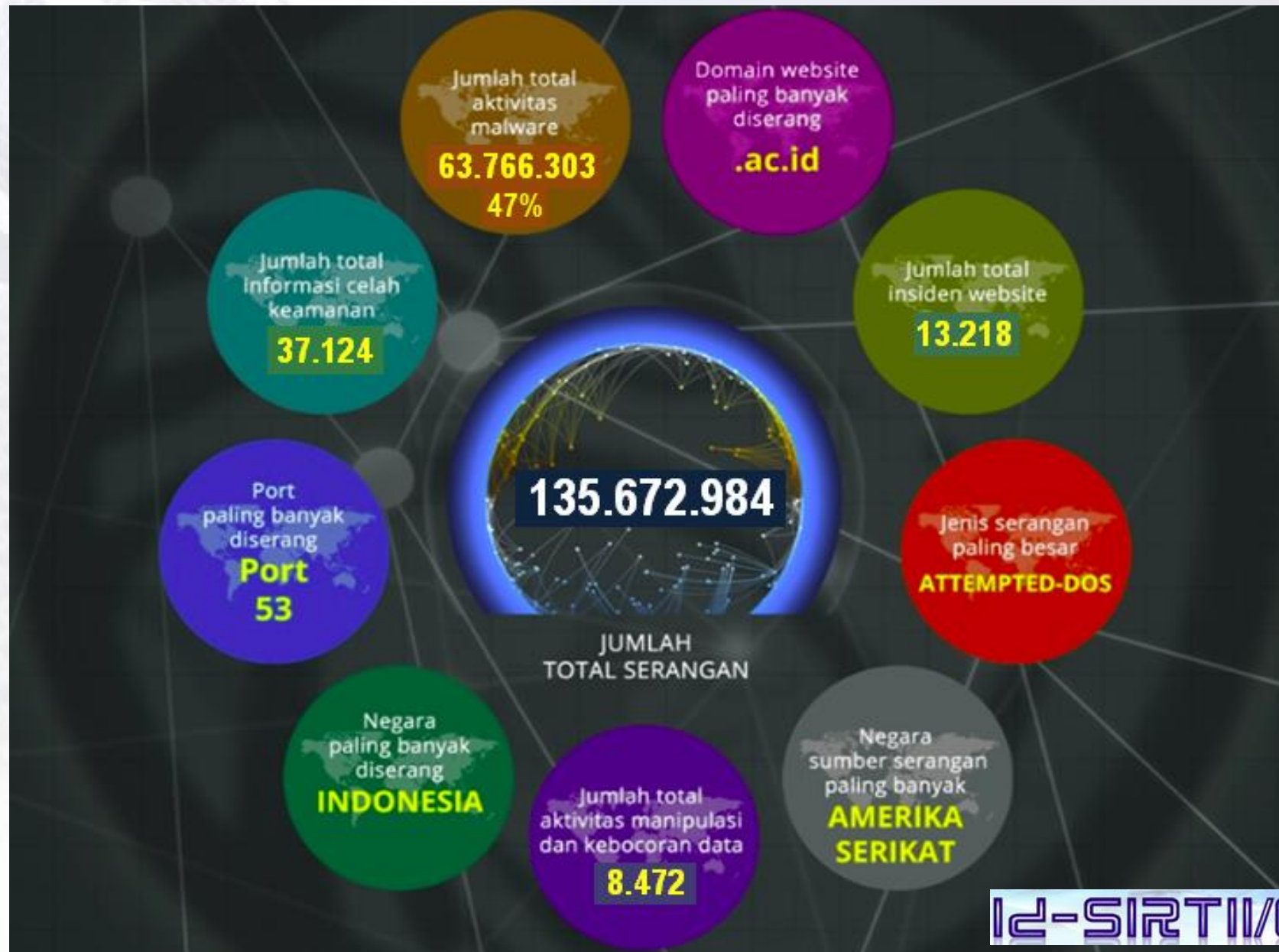
Tren Serangan Siber Nasional Tahun 2015 - 2016



Security Attack Traffic 2015 (Indonesia)

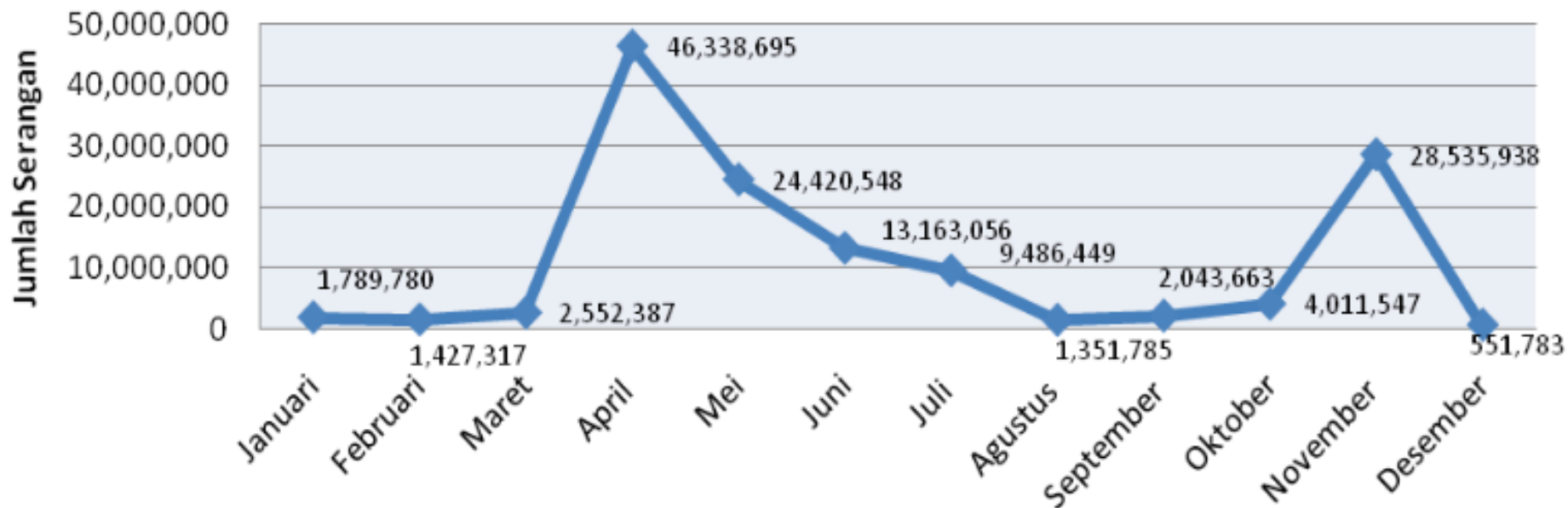


Security Attack Traffic 2016 (Indonesia)

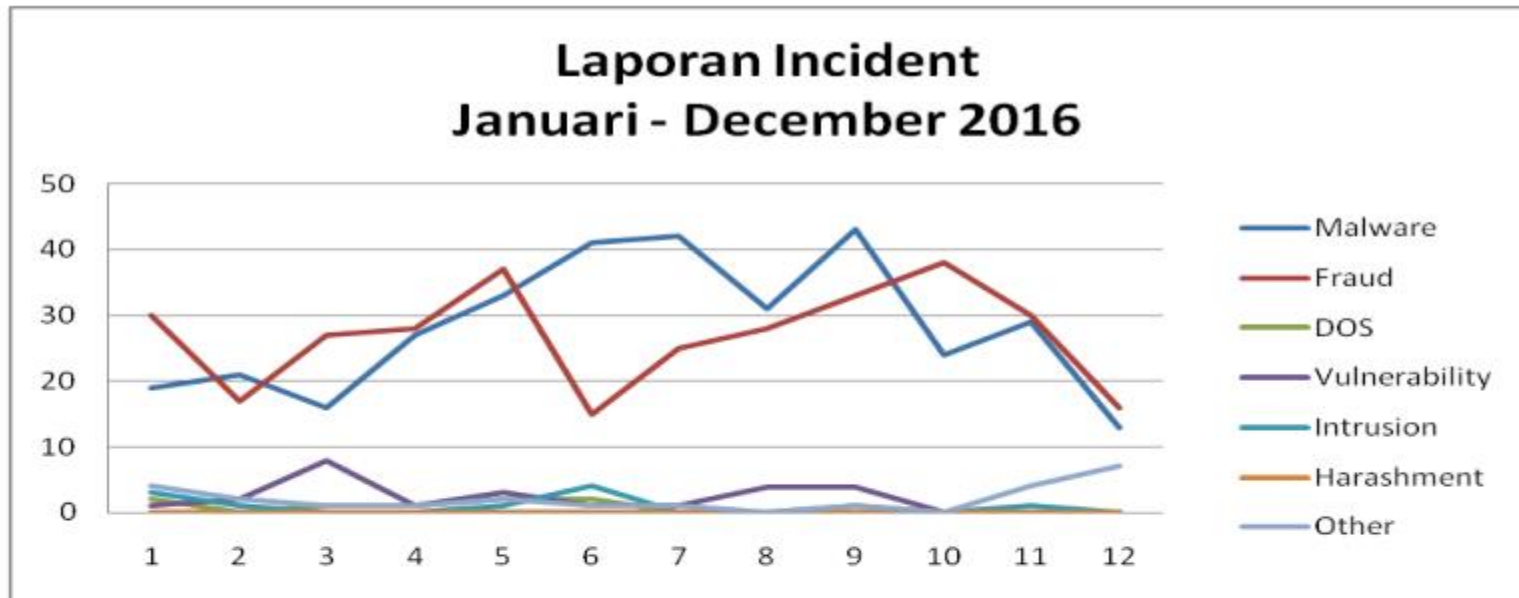


Security Attack Traffic 2016 (Indonesia)

Grafik Serangan 2016



Security Attack Traffic 2016 (Indonesia)



Malware

47%

Fraud

44%

Vulnerability

4%

Intrusion




















1%

Malware Infection Index Asia Pacific 2016

Once Microsoft identifies new malware threats, malicious strains are investigated to understand their risks, origins and engineering, and how widespread their impact is. Here's a snapshot of the threat landscape in the region.

Top markets in Asia Pacific under malware threats:

Ranked by number of malware detections
based on counts of machines

1	Pakistan	
2	Indonesia	
3	Bangladesh	
4	Nepal	
5	Vietnam	
6	Philippines	
7	Cambodia	
8	India	
9	Sri Lanka	
10	Thailand	
11	Malaysia	
12	Singapore	
13	Taiwan	
14	China	
15	Hong Kong	
16	Australia	
16	Korea	
18	New Zealand	
19	Japan	

“

It takes an average
of 200 days for
organizations to find
out they have been
victims of cyber
attacks. ”

Keshav Dhakad
Regional Director,
IP & Digital Crimes Unit,
Microsoft Asia

Most
affected

Least
affected



Top 3 Encountered Malware

Gamarue
Skeeyah
Peals

Major Cyber Attacks



Malware

• Short for malicious software like Gamarue, Skeeyah and Peals, designed to cause damage to a single computer, server, or computer network, whether it's virus or spyware.



DDoS (Distributed Denial of Service)

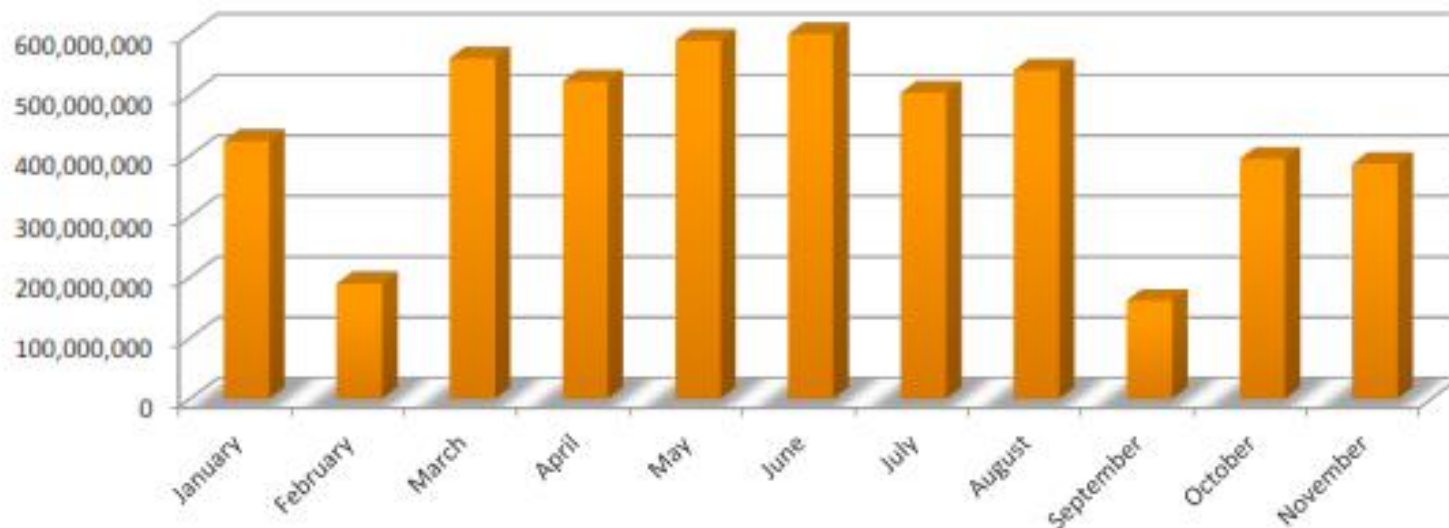
• An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.



Identity Theft

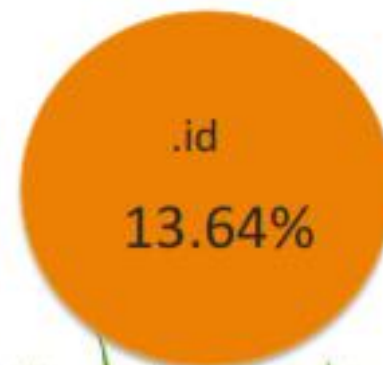
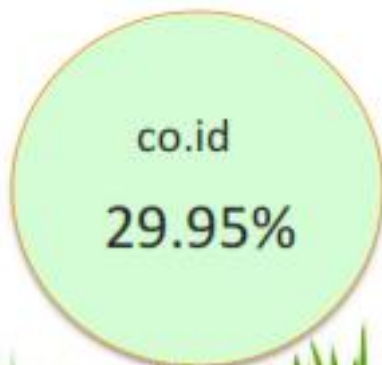
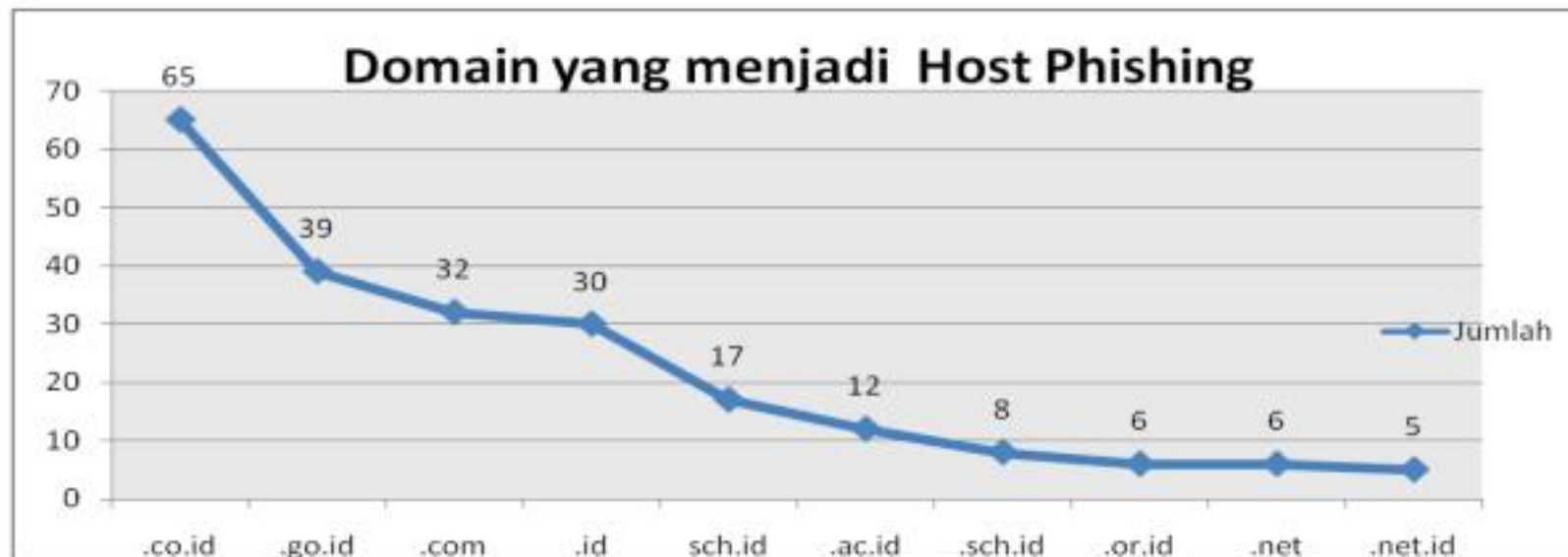
• A crime in which an imposter obtains key pieces of personal information in order to impersonate someone else and gain access to sensitive data online.

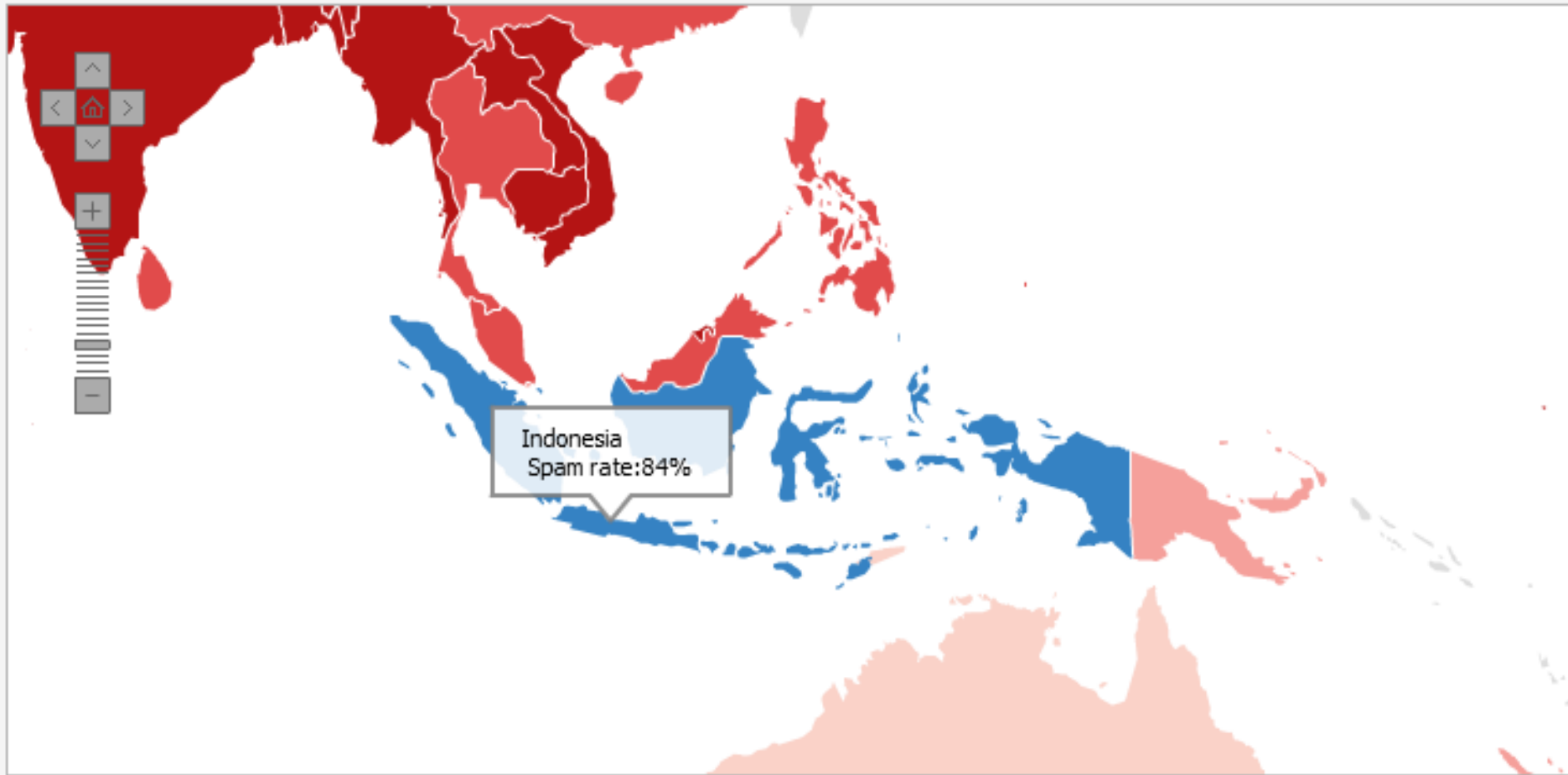
Pemantauan Malware



Jumlah indikasi akses serangan malware dari host Indonesia tahun 2016 lebih dari 5 Milyar !

Pemantauan Insiden





Security Attack Traffic 2015, 2016 & Prediksi 2017



2015

2016

THE MOST
TARGETED
PORT
Port 53

MALWARE
ACTIVITY

461.511

Jumlah total
aktivitas
malware

63.766.303

THE MOST
TYPE OF
ATTACK
SQL

Jenis serangan
paling besar
ATTEMPTED-DOS

THE MOST
ATTACKS
ORIGINATE
INDONESIA

Prediksi 2017 : Meningkat

- Serangan Malware yang lebih beragam, dengan banyaknya implementasi IoT (Internet of Things), sehingga memunculkan beberapa isyu serangan baru dalam bentuk : Botnet of Things (BoT), Ransomware of Things, dan Mobile malware
- Serangan DDoS
- Service yang paling dominan mendapat serangan masih ditempati Port 53.
- Dan Serangan paling dominan adalah DoS dan Web Injection (A1-Owasp)
- Dan Serangan terbesar berasal dari Indonesia dengan target Indonesia.

INSIDEN

WEBSITE

JANUARI-DESEMBER 2015

Total jumlah aktivitas serangan defacement terhadap website dengan cara melakukan perubahan tampilan atau merusak keseluruhan konten website oleh penyerang (*attacker*).

13.955

serangan

.name	13.955
.asia	13.955
.biz	13.955
.co	13.955
.org	13.955
.net	13.955
.com	13.955
.web.id	13.955
.my.id	13.955

.go.id

4.599

serangan

Domain website yang paling banyak diserang.

ID-SIRTII/CC

Insiden Website 2015, 2016 & Prediksi 2017

WEBSITE
HACKING
INCIDENT

13.955

2015

Jumlah total
insiden website

13.218

2016

THE MOST
TARGETED
DOMAIN

.go.id

Domain website
paling banyak
diserang

.ac.id

THE MOST
TARGETED
DOMAIN

.go.id

2017

Prediksi 2017 : Menurun

- Perubahan orientasi serangan.
- Meningkatnya security awareness.
- Serangan ditujukan ke domain **.go.id**
- Jenis vulnerability yang masih dominan Web Injection & Local File Inclusion.
- Ransomweb akan memakan korban lebih banyak lagi terhadap website2 Indonesia dengan tujuan mendapat imbalan atas jasa recovery data.



.id	10
.sch.id	2756
.ac.id	5533
.co.id	3718
.net.id	151
.or.id	1407
.biz.id	11
.desa.id	0
.go.id	5770
.mil.id	77
.my.id	42
.web.id	1388
Others	5758

Web Vulnerability, Aktivitas Manipulasi dan Kebocoran Data 2015, 2016 & Prediksi 2017



2015



2016



Prediksi 2017 : Menurun

- Meningkatnya security awareness.

Buzzer “Hacker” Medsos

- Isyu Pilkada, SARA dan ketidak puasan masyarakat terhadap Kebijakan Pemerintah.
- Cyber Army Medsos (Buzzer, situs berita hoax, kampanye hitam, dll).
- “Cukup dengan perintah Ping & Traceroute sudah bisa memonitor penyerang situs KPU”



**I HACKED
127.0.0.1**

Hack The Vote:

Hacker Bayaran Pilkada & Pilpres

- Skill lebih baik dari Hacker “Buzzer” medsos.
- Target memenangkan Pilkada dan Pilpres dengan melakukan hacktivism pada situs KPU dan situs lawan Politik.
- Meretas akun2 email, dan medsos lawan politik.
- Melakukan Stalking (penyadapan) dan Recon lawan politiknya.
- Melakukan serangan DDoS pada infrastruktur KPU, situs Pemerintah dan situs lawan Politik.
- Membongkar dokumen atau rahasia lawan Politik.

Internet of malicious Things

- Perkembangan teknologi menyebabkan semua perangkat elektronik dapat dihubungkan ke internet yang lebih dikenal dengan Internet of Things (IoT).
- IoT dapat digunakan sebagai perangkat untuk melakukan serangan dan juga menjadi target.
- IoT dapat digunakan sebagai media penyebaran malware.
- Serangan DDoS, cracking password, meretas sistem/aplikasi, backdoor, ransomware dan APTs dapat dilakukan dengan IoT.

Hack IoT

- Banyaknya perangkat yang terhubung ke internet atau yang menggunakan IP Address (CCTV, smart home/building/City, selular, LTR SDR, Drone, Red Furry dan perangkat lainnya yang terkoneksi ke Internet atau memiliki IP Address dan kurangnya pemahaman keamanan, menyebabkan perangkat dapat digunakan atau diambil alih oleh pihak lain.



Internet Fraud dan Carding (Siber Maling)

- Mendapatkan info CC dari Warnet atau Medsos, atau Komunitas dan mencoba Transaksi di Online Shopping.
- Memanfaatkan kelemahan pada Online Shopping dan situs2 transaksi elektronik dan menjual jasanya ke pihak lain.



Internet Fraud dan Carding (Siber Maling)

APA ITU "SIM SWAP" ?

SIM swap adalah pengambilalihan kartu SIM ponsel untuk mengakses akun perbankan seseorang



Berbekal informasi perbankan calon korban, pelaku mendatangi operator seluler dengan identitas palsu. Dengan mengaku nomornya rusak atau hilang mereka meminta penggantian kartu SIM.



Setelah melakukan verifikasi, operator seluler akan menerbitkan kartu SIM pengganti dan menonaktifkan kartu SIM yang masih berada di tangan pemilik yang sah.



Pelaku melakukan transaksi finansial, melalui ponsel, lalu bank penerbit akan mengirim OTP ke nomor SIM baru dan pelaku bebas mengurus rekening korban



TIPS AGAR TIDAK MENJADI KORBAN SIM SWAP



Jika SIM ponsel Anda mendadak tidak aktif laporkan secepatnya ke operator seluler Anda



Jika menerima sms atau email yang meminta Anda untuk mengklik tautan ke situs yang tidak jelas jangan mengklik tautan tersebut



Jika Anda menggunakan layanan internet banking pastikan situs tersebut adalah benar milik bank dan bukan situs phishing



Jaga rahasia perbankan Anda (password internet banking, m-banking, PIN ATM, PIN telepon)



Jangan menjawab telepon/sms tidak dikenal yang menanyakan nomor kartu kredit, nomor rekening bank atau nomor ponsel bank Anda



Jangan memublikasikan nomor ponsel atau email yang digunakan untuk transaksi perbankan di media sosial



Aktifkan fitur layanan SMS dan email alert (peringatan email) untuk menerima notifikasi transaksi finansial atau perubahan pada rekening Anda

Internet Fraud dan Carding (Siber Maling)

Jual Akun Gojek Dan e-commerce



Yok Siap Dibeli .

- Amazon US Card Visa/Masterdcard : 25K/5Akun + Method
- Amazon US Card Amex/Discover : 50K/5Akun + Method
- Lazada ID : 20K/Akun
- Zalora ID : 30K/Akun

I-Rules :

- *Beli – Bisa Make
- *Barang yang udh dibeli egk bisa dikembalikan / dibarter.
- *Setelah akun diterima selanjutnya bukan urusan saya .
- *Tidak ada komplain untuk akun yang saya jual .
- *Komplain dan Refund hanya untuk akun yang tidak bisa login

Rekber / Pulber Aris Suhana / Nabil .

Fee buyer

Internet Fraud dan Carding (Siber Maling)

Jual Voucher
Hotel
Diskon 50%



The screenshot shows a Facebook post by Farhan Budiman dated 28 April. The post text is "Open hotel seindonesia 😊 diskon 50% no cancel no refund no apa lah itu sistem bayar-bookingin Or Rekber Biar Ngga ruwet , hahaha". The post has 1 like and 1 comment. The comment by Arinal Haqqo asks "COD gimana??". Farhan Budiman replies "4 Balasan". Another comment by Fista Frestanikova Islami asks "Cod hotel..?". The bottom part of the screenshot shows a post by Fista Frestanikova Islami dated 8 Juli pukul 23:27, which says "#WTB arep tumbas.. Cari hp hasil card udah di tangan Utamakan s7 edge n xiaomi mi5".

Farhan Budiman
28 April

Open hotel seindonesia 😊 diskon 50%
no cancel no refund no apa lah itu
sistem bayar-bookingin Or Rekber Biar Ngga ruwet , hahaha

Suka Komentari

1

Arinal Haqqo COD gimana??
Suka · Balas · 28 April pukul 21:44
↳ **Farhan Budiman** membalas · 4 Balasan

Fista Frestanikova Islami Cod hotel..?
Suka · Balas · 8 Juli pukul 23:54

Tulis komentar...

Fista Frestanikova Islami
8 Juli pukul 23:27

#WTB arep tumbas..
Cari hp hasil card udah di tangan
Utamakan s7 edge n xiaomi mi5

Suka Komentari

Internet Fraud dan Carding (Siber Maling)

Jual tiket Pesawat diskon 50%



David Hughes

29 Juli pukul 14:27

Open Maskapai :

- Garuda
- Lion
- Air Asia

Open Hotel :

- Seluruh Indonesia

RATE : 50%

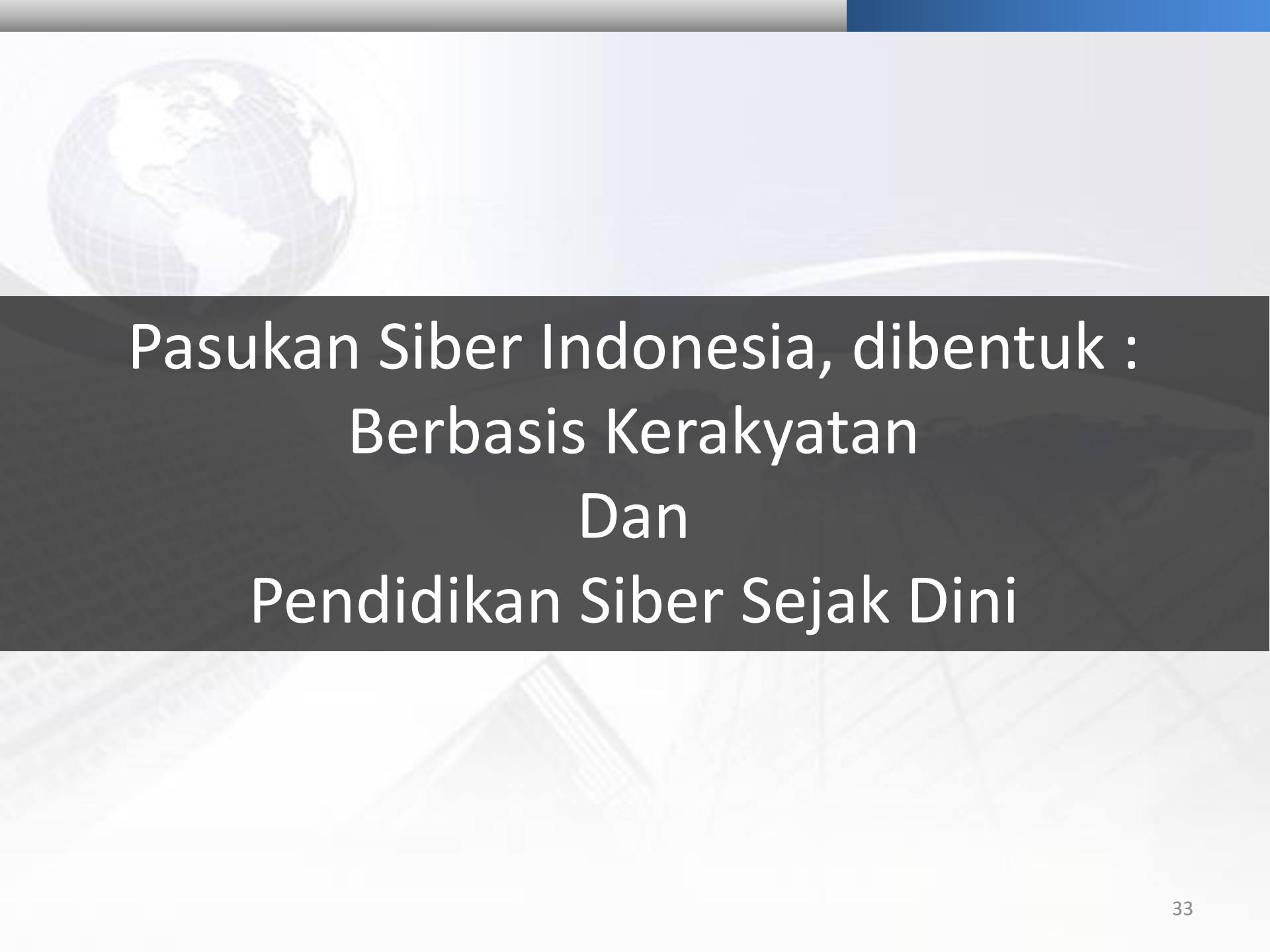
REKBER : NABIL / ARIS

👍 Suka

💬 Komentari

Internet Fraud dan Carding (Siber Maling)





Pasukan Siber Indonesia, dibentuk : Berbasis Kerakyatan Dan Pendidikan Siber Sejak Dini

US Cyber Army



China Cyber Army



North Korea Cyber Army

Indonesian Cyber Army



Hatur Nuhun

Iwan Sumantri

0817427366

iwan@idsirtii.or.id ;

iwan@hotmail.com;

iwansumantri@gmail.com