

VARIOUS WAY OF PROTECTING YOUR CLOUD SERVER PORT

#IDSECCONF2014

@aabdullahfath



Who This Guy!

Abdullah

S1 Informatika

Universitas Brawijaya Malang



PROGRAM TEKNOLOGI INFORMASI DAN ILMU KOMPUTER





MALANG CYBER CREW

Trend Serangan Internet Dunia

Kuartal 2 & 3 Tahun 2013



Country	Q2 '13 % Traffic	Q1 '13 %
1 Indonesia	38%	21%
2 China	33%	34%
3 United States	6.9%	8.3%
4 Taiwan	2.5%	2.5%
5 Turkey	2.4%	4.5%
6 India	2.0%	2.6%
7 Russia	1.7%	2.7%
8 Brazil	1.4%	2.2%
9 Romania	1.0%	2.0%
10 South Korea	0.9%	1.4%
— Other	11%	18%

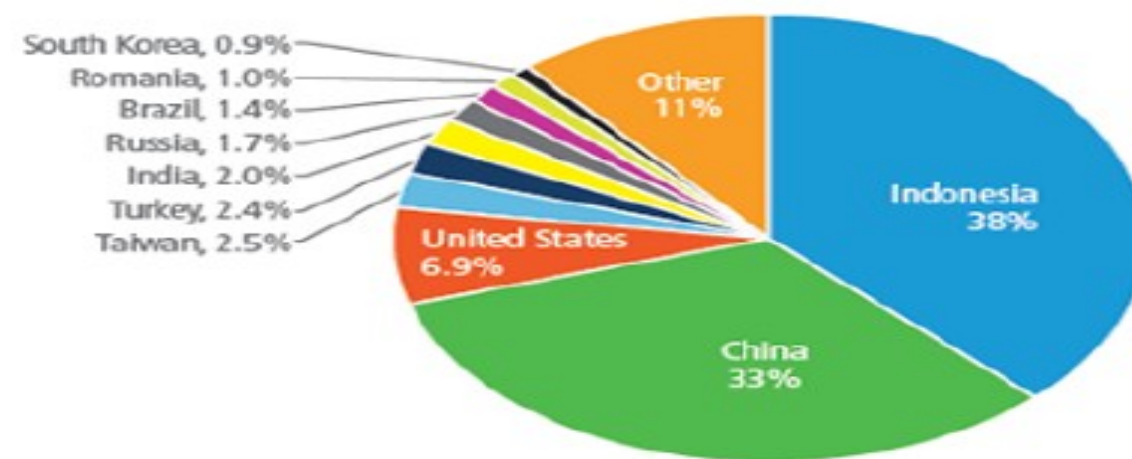


Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

Country	Q3 '13 % Traffic	Q2 '13 %
1 China	35%	33%
2 Indonesia	20%	38%
3 United States	11%	6.9%
4 Taiwan	5.2%	2.5%
5 Russia	2.6%	1.7%
6 Brazil	2.1%	1.4%
7 India	1.9%	2.0%
8 Romania	1.7%	1.0%
9 South Korea	1.2%	0.9%
10 Venezuela	1.1%	0.6%
— Other	17%	11%

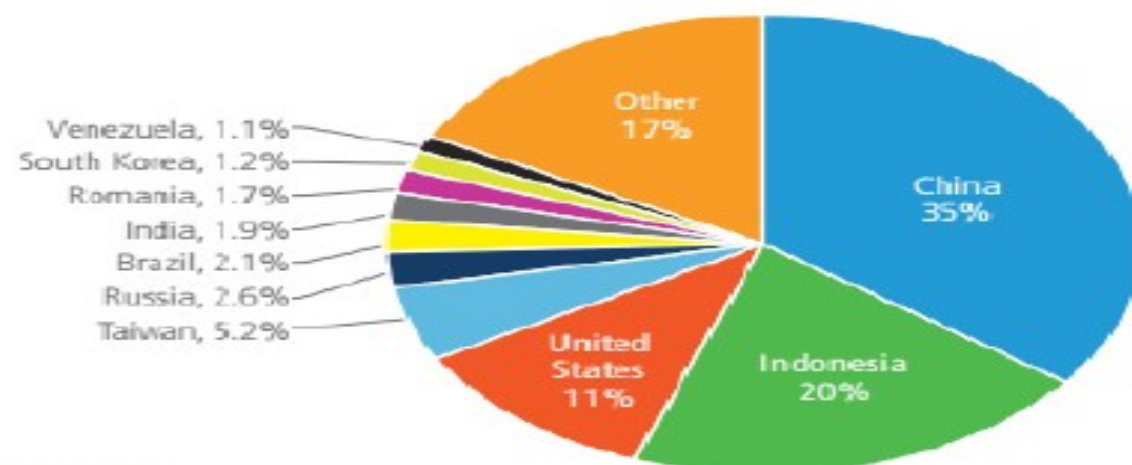


Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

Trend Serangan Internet Dunia

Kuartal 4 - 2013 dan 1 - 2014



	Country/Region	Q4 '13 Traffic %	Q3 '13 %
1	China	43%	35%
2	United States	19%	11%
3	Canada	10%	0.4%
4	Indonesia	5.7%	20%
5	Taiwan	3.4%	5.2%
6	Netherlands	2.7%	0.5%
7	Russia	1.5%	2.6%
8	Brazil	1.1%	2.1%
9	Romania	0.9%	1.7%
10	Germany	0.8%	0.9%
—	Other	12%	17%

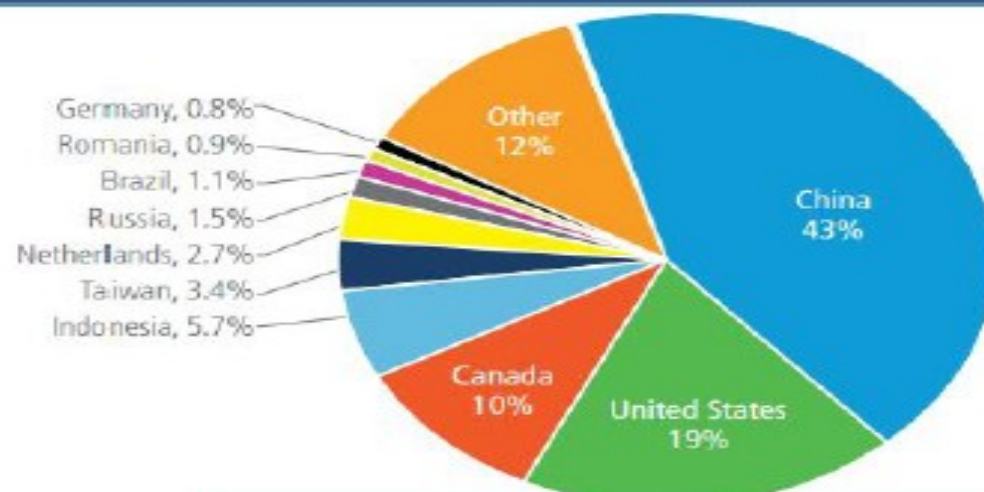


Figure 1: Attack Traffic, Top Originating Countries (by source IP address, not attribution)

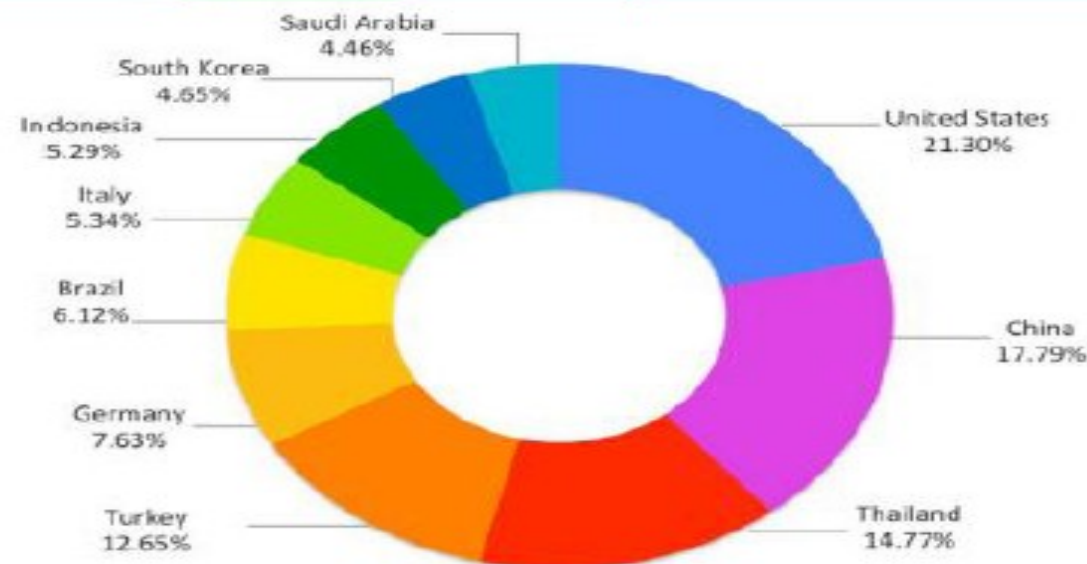


Figure 6: Top 10 source countries for non-spoofed DDoS attacks in Q1 2014

Tingkat Keamanan Internet Nasional

- 
- Januari - Februari 2014 : SEDANG
 - Maret - April 2014 : BURUK
 - Mei 2014 : SANGAT BURUK
 - Juni - Agustus : BURUK

	Bulan Ini	Bulan Lalu	Rata-Rata Tahun Lalu
Pemantauan Trafik Nasional	Meningkat 25.905.063	4.086.353	3.474.728,00
Aktifitas <i>Malware</i>	Meningkat 24.271.700	2.501.300	445.186,33
Insiden <i>Website</i>	Menurun 921	1.702	792,23
Informasi Celah Keamanan	Menurun 2.398	2.737	N/A
Aktivitas Manipulasi dan Kebocoran Data	Meningkat 1.223	832	N/A
Pelaporan Insiden	Menurun 115	118	58,75

Pemantauan Trafik Nasional (Jumlah Serangan) Tahun 2013

Jumlah serangan : 72.225.360, atau 200.626/hari

Serangan terbesar terjadi pada bulan November : 26 Juta

82% serangan kategori SQL, Malware, Web Base & Botnet

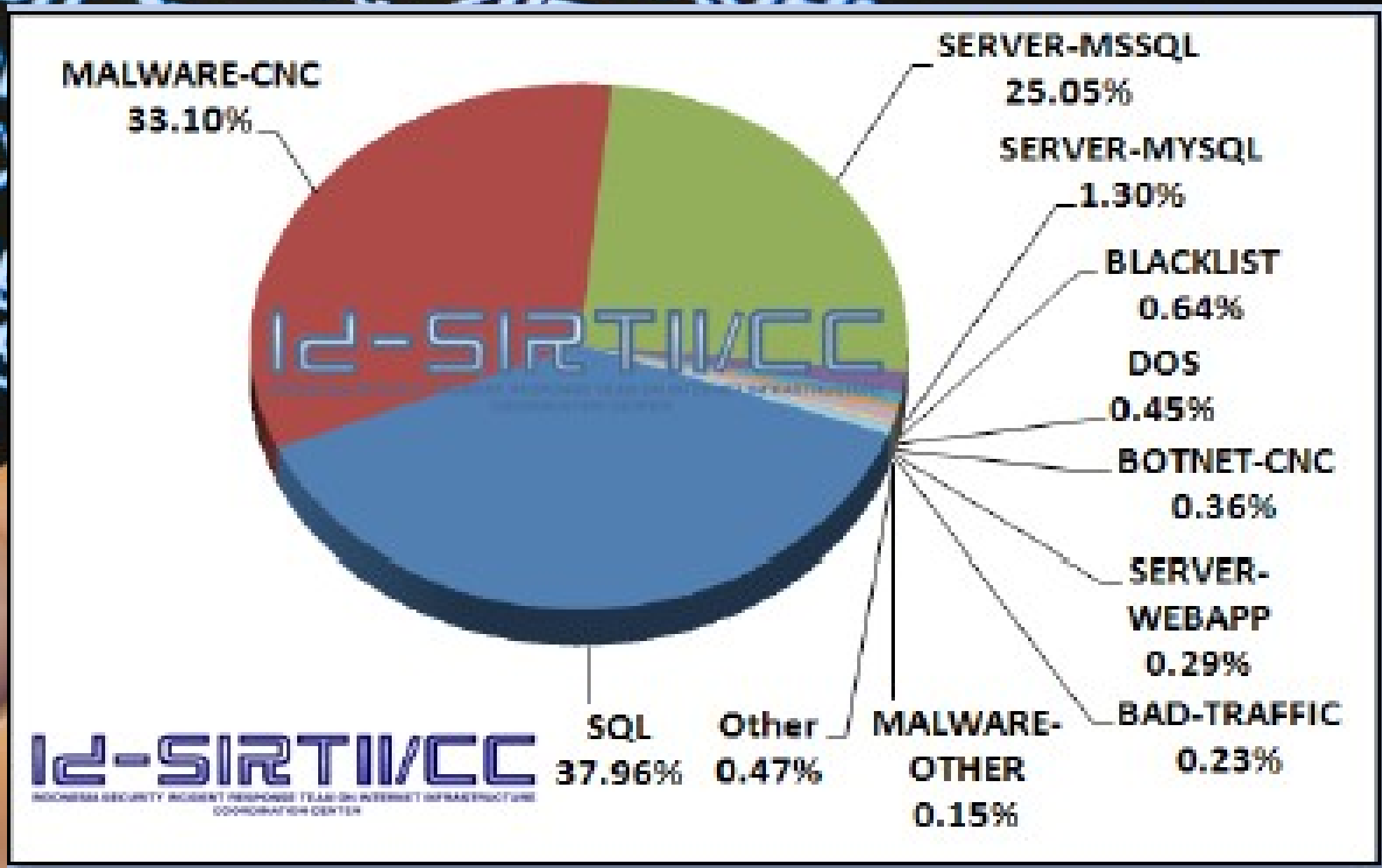
Jumlah insiden website terbesar terjadi pada bulan Mei 2013, 3.126 insiden website

Rata-rata 67% tingkat serangan

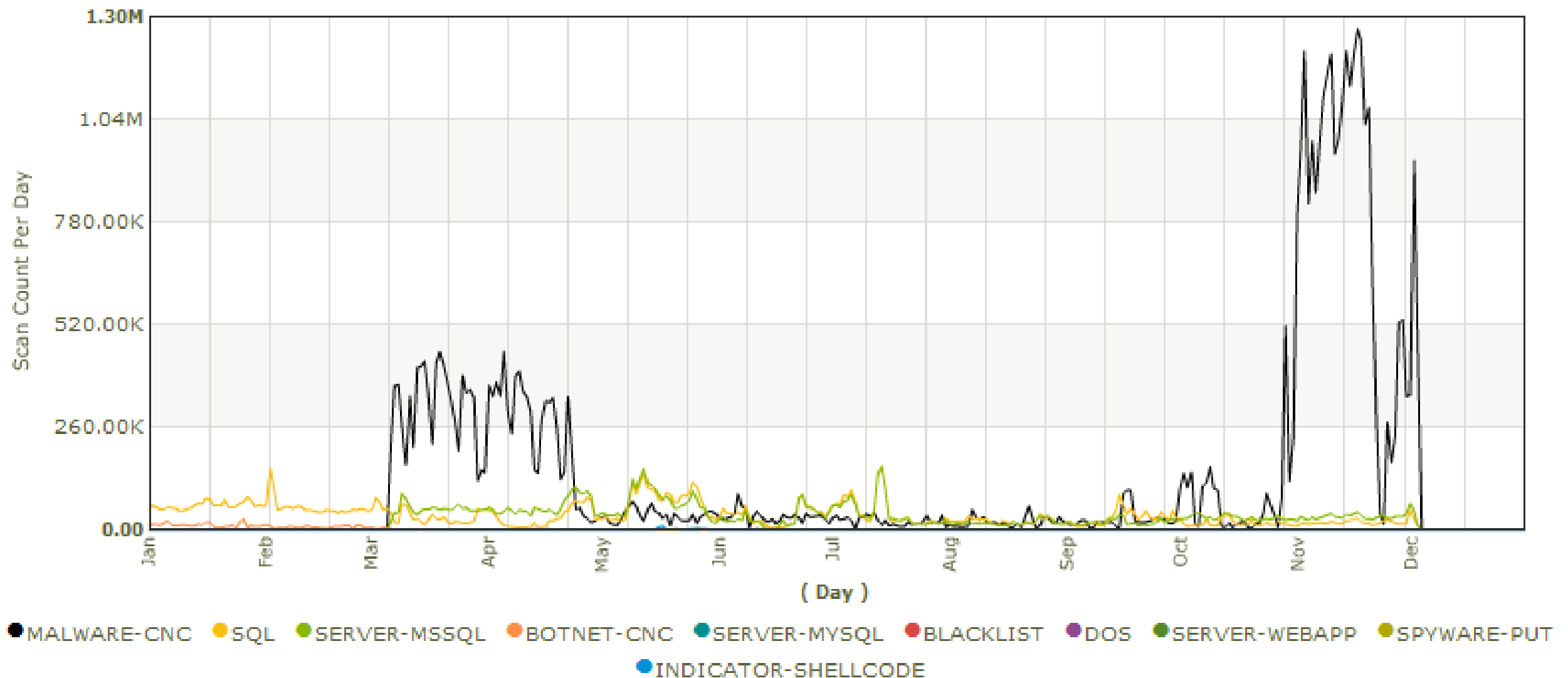
Negara sumber serangan : CN, ID, BR

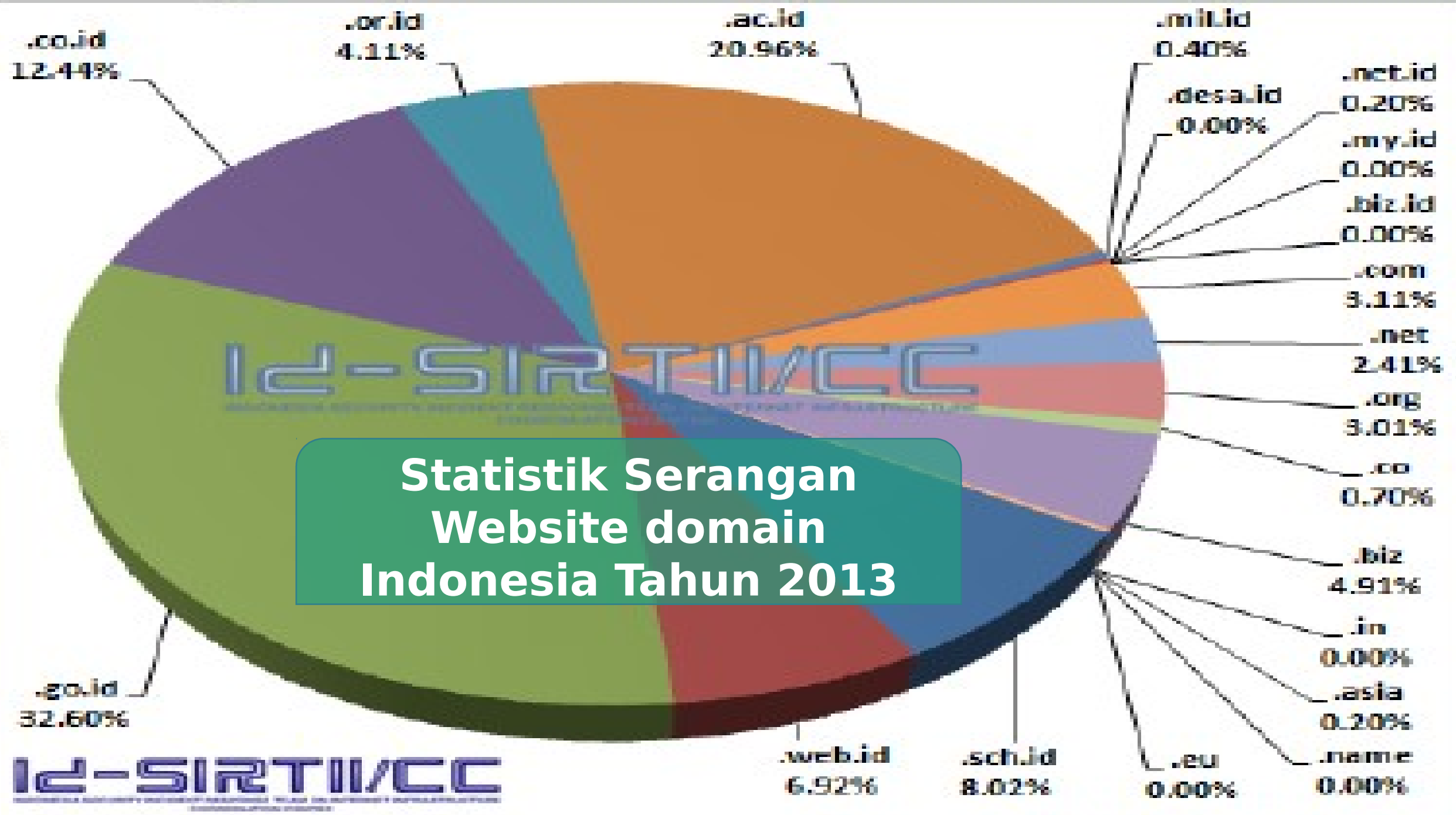
Negara target serangan : ID, US, CN, JP

Pemantauan Trafik Nasional (Jumlah Serangan) Tahun 2013



Statistik Serangan Website domain Indonesia Tahun 2013





Celah Keamanan Pada TLD .ID Tahun 2013

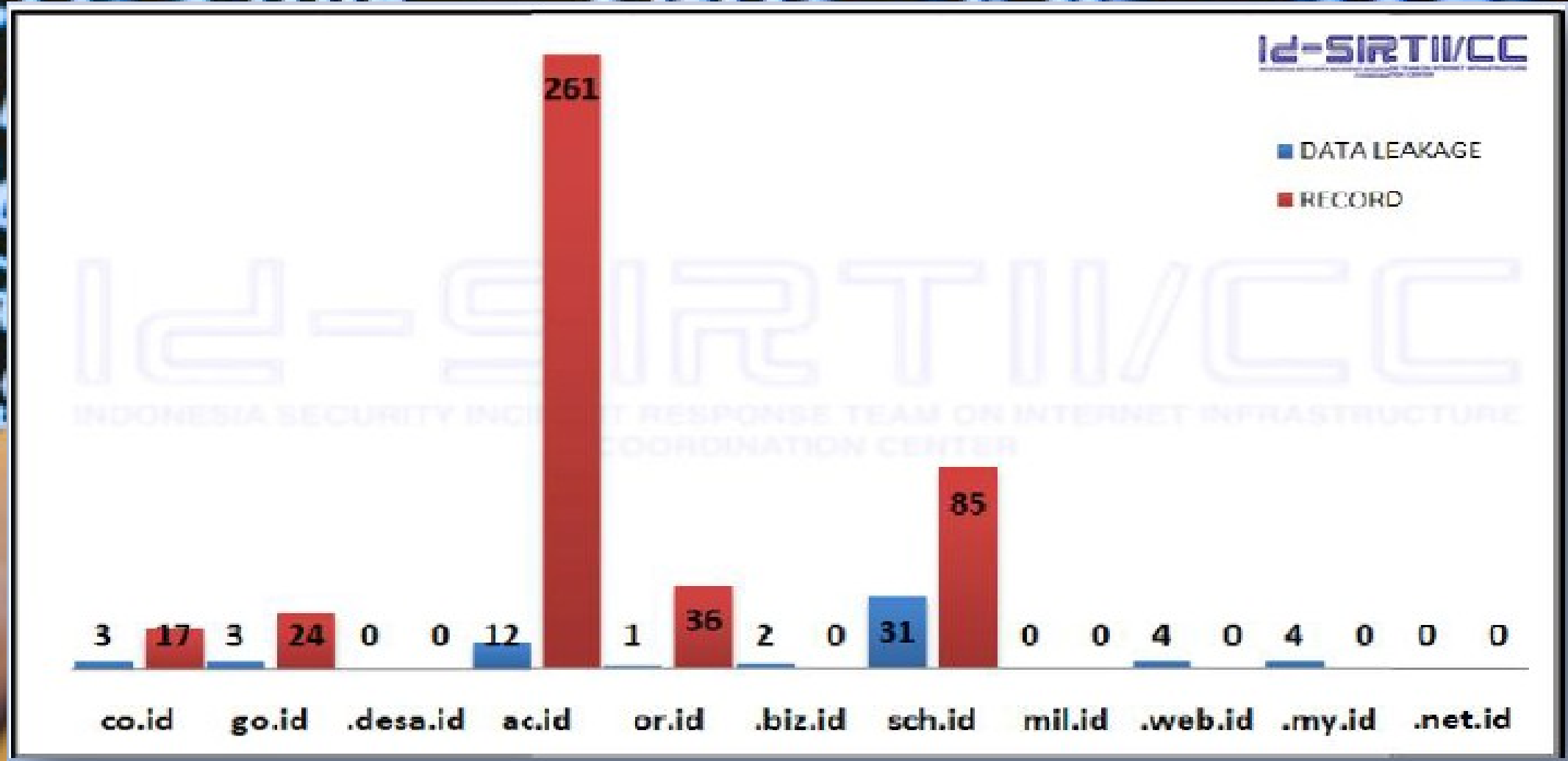
Rata-rata 2300/bulan ditemukan website yang rentan

Domain yang paling rentan : ac.id, .sch.id, .go.id, .co.id



Data Leaked

Terdapat 60 website dan 423 record data yang dibocorkan di internet



**Mengapa semua
ini bisa terjadi?**

Salah siapa?



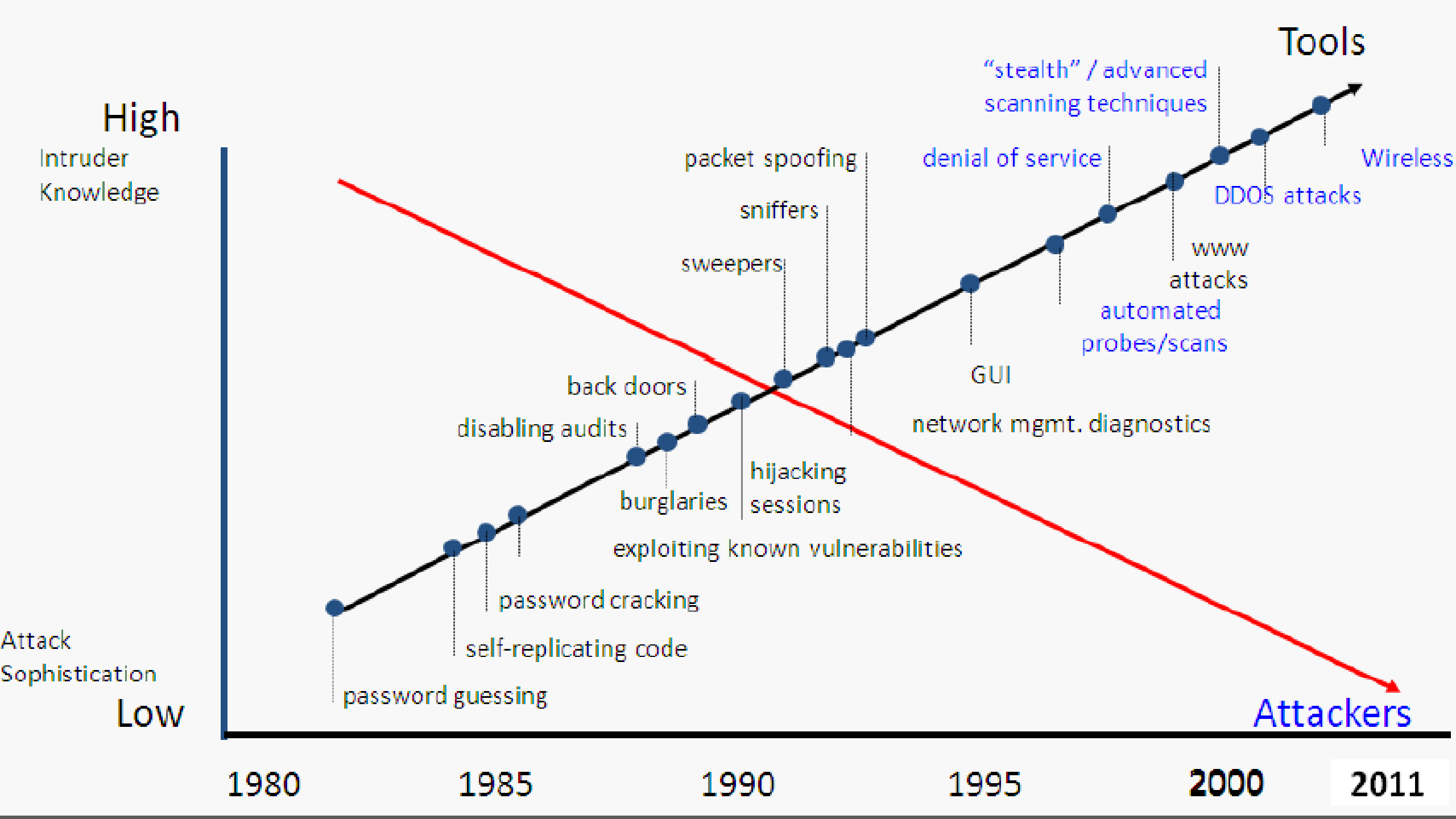
PENYEBAB BANYAKNYA SERANGAN

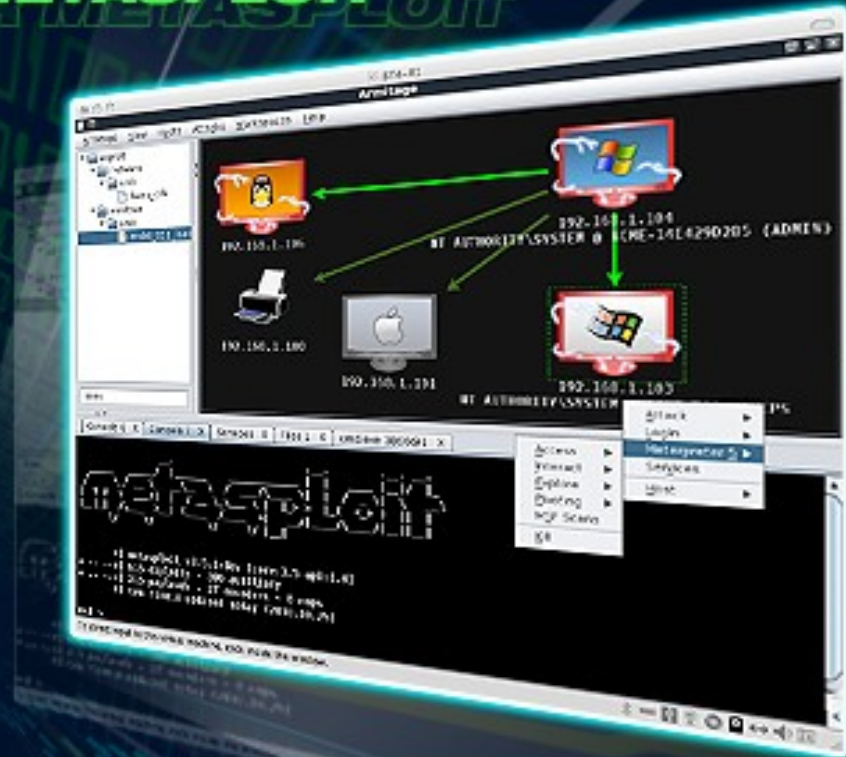
Kurangnya kesadaran keamanan informasi, dari sisi personal sampai dengan kelembagaan.

Manusia, sisi keamanan terlemah - social engineering, phishing & malicious code (tools)

Hacking Tools sangat mudah didapat dan mudah digunakan (Click Kiddies)

Hacker semakin nyaman dalam melakukan aksinya.





ARMITAGE

DOWNLOAD

FAST AND EASY HACKING

MEDIA

MANUAL

FAQ

CONTACT

<http://www.fastandeasyhacking.com>

1

Port Scanning



Found Port 80,22,21 etc

2

Port Scanner

```

# http://www.10-4.com/secure.asp?org=10-4
# 10-4 security.org

Starting Step 4 (200000) (http://www.10-4.com/
2000-10-05 13:29:00
Initiating Parallel 000 replication of 1 host. at 13:29
Completed Parallel 000 replication of 1 hosts. at 13:29.
0.00% elapsed
Initiating 1st Ping Scan at 13:29
Scanning other (1 port)
Completed 1st Ping Scan at 13:29. 0.00% elapsed
(1 total hosts)
Initiating Parallel 000 replication of 1 host. at 13:29
Completed Parallel 000 replication of 1 host. at 13:29.
0.00% elapsed
Initiating 1st Scanline Scan at 13:29
Scanning 1 hosts (1000 ports/line)
Discovered open port 22/tcp on 209.217.155.55
Discovered open port 21/tcp on 209.217.155.57
Discovered open port 80/tcp on 209.217.155.55
Discovered open port 80/tcp on 209.217.155.57
Discovered open port 23/tcp on 209.217.155.57
Discovered open port 23/tcp on 209.217.155.55
Completed 1st Scanline Scan against 209.217.155.55 in
25.96s (1 host left)
Completed 1st Scanline Scan at 13:29. 25.96% elapsed
(100 total ports)
Initiating Service Scan at 13:30
Scanning 4 services on 1 hosts
Completed Service Scan at 13:30. 25.96% elapsed
(0 services on 1 hosts)
Initiating 2nd Detection (try #1) against 1 hosts
Scanning 40 detection (try #1) against 1 hosts
Initiating gpt 05 detection against 209.217.155.55 in
41.876s
For 05000 scanning port 22 is open, 70 is closed, and

```

Nmap

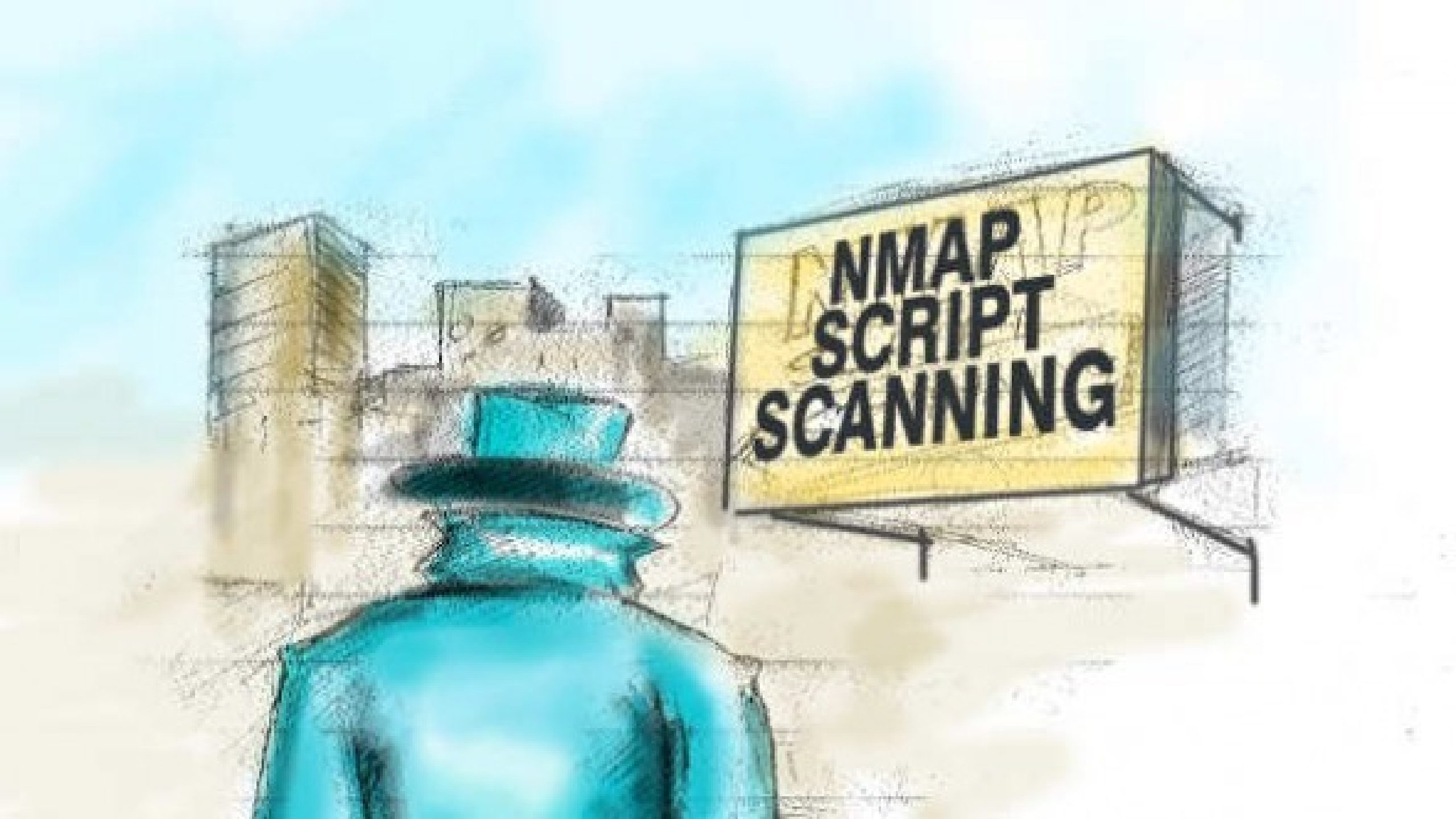
Metasploit


Port Scanning : Matrix Reloaded

```
Port      State      Service
22/tcp    open       ssh

No exact OS matches for host

Nmap run completed -- 1 IP address (1 host up) scanned
# sshnuke 10.2.2.2 -rootpw="210N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "210N0101".
System open: Access Level <9>
# ssh 10.2.2.2 -
```

A close-up photograph of a baby with light brown hair and blue eyes, sitting on a sandy beach. The baby has a grumpy or determined expression, with a slightly furrowed brow and a small frown. They are wearing a green long-sleeved shirt with a white collar. Their right hand is raised towards their mouth, with some sand visible on the fingers. The background is a blurred view of the ocean waves and the beach.

**Yes, aku berhasil
masuk ke sistemnya,
haha!**

Update status dulu . .

**Terus gimana
caranya Agar **aman**?**



You can't **secure the
system**





You can **slow down** the performance of **hackers**

Kippo SSH Honeypot

The background of the slide features a dark blue globe with lighter blue landmasses. Overlaid on the globe is a magnifying glass with a silver rim and a black handle. The magnifying glass is positioned in the lower-left quadrant, with its lens focused on the text 'Mencatat Semua Perbuatan Dosa Si Attacker'.

Membuat Sistem Palsu

Seolah-olah Attacker Berada Dalam Sistem Yang Sebenarnya

Mencatat Semua Perbuatan Dosa Si Attacker

Berkreasi Sesuka Anda!

Download :
code.google.com/p/kippo/

Konfigurasi

Lokasi : kippo/kippo.cfg

Start Kippo SSH Honeypot!

```
kippo@mrrwx:~/kippo$ ls
chmod  doc      kippo      kippo.tac      public.key      txtcmds
data   fs.pickle  kippo.cfg      log             start.sh        utils
dl     honeyfs    kippo.cfg.dist private.key      stop.sh
kippo@mrrwx:~/kippo$ ./start.sh
Starting kippo in background...kippo@mrrwx:~/kippo$
```

Portspoof

Menyamarkan Port

Dialihkan ke Port 4444

Memperlambat Kinerja Attacker

Mengaktifkan 65 Ribu Port





**“Portspooftakes more than 8 hours
and 200MB of sent data in order to
properly go through the reconessaince
phase for your system”**

@drk1wi

Starting Nmap 6.25 (<http://nmap.org>) at 2013-07-16 10:48 CEST

Nmap scan report for 172.16.37.145

Host is up (0.00097s latency).

PORT	STATE	SERVICE	VERSION
1/tcp	open	pop3	Eudora Internet Mail Server X pop3d 870
2/tcp	open	honeypot	Network Flight Recorder BackOfficer Friendly http honeypot
3/tcp	open	smtp	Postfix smtpd (Debian)
4/tcp	open	ssh	(protocol 7)
5/tcp	open	X11	XFree86 9 patch level g (Connectiva Linux)
6/tcp	open	imap	Kerio imapd 4539 patch 4
7/tcp	open	ftp	Sambar ftpd
8/tcp	open	unknown	
9/tcp	open	http	Cisco VPN Concentrator http config
10/tcp	open	ssh	(protocol 3)
11/tcp	open	ms-wbt-server	Microsoft NetMeeting Remote Desktop Service
12/tcp	open	scalix-ual	Scalix UAL
13/tcp	open	smtp	Small Home Server smtpd
14/tcp	open	telnet	Dreambox 500 media device telnetd (Linux kernel t; PLi image Jade, based on Dk)
15/tcp	open	ftp	ProFTPD (German)
16/tcp	open	ftp	Lexmark K series printer ftpd (MAC: k)
17/tcp	open	ftp	ProFTPD
18/tcp	open	irc-proxy	muh irc proxy
19/tcp	open	ftp	ProFTPD
20/tcp	open	hp-gsg	IEEE 1284.4 scan peripheral gateway
21/tcp	open	desktop-central	ManageEngine Desktop Central DesktopCentralServer
22/tcp	open	ssh	OpenSSH 5.3p1 Debian 3ubuntu7 (Ubuntu Linux; protocol 2.0)
23/tcp	open	telnet	Blue Coat telnetd
24/tcp	open	hp-gsg	IEEE 1284.4 scan peripheral gateway
25/tcp	open	ftp	Polycom VSX 7000A VoIP phone ftpd
26/tcp	open	vnc	Ultr@VNC 1.0.8.0
27/tcp	open	ssh	(protocol 133038)
28/tcp	open	telnet	Blue Coat telnetd
29/tcp	open	printer	VSE lpd
30/tcp	open	ssh	SSHTools J2SSH (protocol 0740)
31/tcp	open	telnet	Lantronix MSS100 serial interface telnetd 8469697
32/tcp	open	pop3	Dovecot pop3d
33/tcp	open	telnet	Control DeviceMaster RTS ethernet to serial telnetd (Model 4; NS-Link DqX; MAC Q)
34/tcp	open	smtp	WebShieldet smtpd
35/tcp	open	telnet	HP switch telnetd
36/tcp	open	upnp	MiniDLNA MJsUCeP (Dk; UPnP YT)

Portsentry

Mendeteksi Port Scanner

Banned IP Secara Otomatis

Membuat Port Palsu

Fun With Custom Banner



Port Sentry

Config > /etc/portentry/portentry.conf

Log > /var/log/syslog

History > /var/lib/portentry/portentry.history

Custom Banner

```
mrrwx@mrrwx:~$ telnet 192.168.0.101 1
Trying 192.168.0.101...
Connected to 192.168.0.101.
Escape character is '^]'.
V
** UNAUTHORIZED ACCESS PROHIBITED *** YOUR CONNECTION ATTEMPT HAS BEEN LOGGED. C
O AWAY.Connection closed by foreign host.
mrrwx@mrrwx:~$
```

THANK YOU!

 @aabdullahfath

 doel@mc-crew.or.id

 <http://forum.mc-crew.or.id>