

Tren Spam 2016
Diskusi Publik:
RPM Surat Elektronik Bersifat Mengganggu
JAKARTA, 05 OKTOBER 2016

Ahmad Alkazimy
(Manajer ID-CERT)
ahmad@cert.or.id

Fingerprint PGP Key: 39B2 87BA 3DD6 7832 D56F 0344 FCE4 3A7C FE38 CC96

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



Pendahuluan ID-CERT

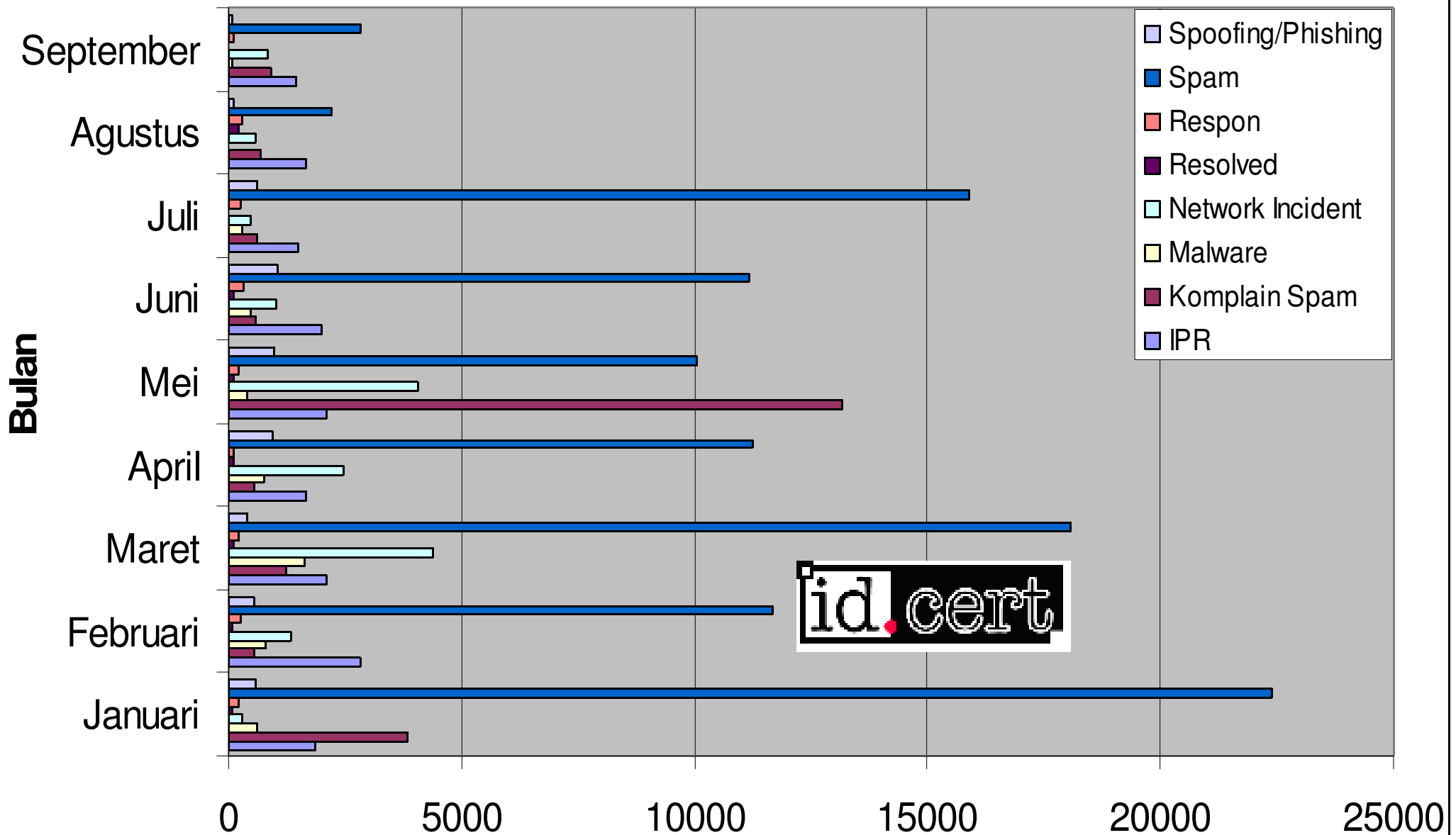
<http://www.cert.id/tentang-kami/id/>

- Tim Penanganan insiden komputer (CERT) yang terbentuk sejak 1 DES 1998
- Diketuai oleh Bpk. Budi Rahardjo, PhD, Wakil Ketua: Bpk. Andika Triwidada
- Merupakan tim CERT yang Independen, Non-Profit dan Non-Pemerintah
- Berbadan hukum: Perkumpulan sejak tahun 2013.
- Konstituen: terbuka untuk umum.
- Menangani ribuan aduan insiden per tahun.
- Menjadi penasehat untuk CSIRT lain: GovCSIRT/ DITKAMINFO-KEMKOMINFO, JabarProvCSIRT.

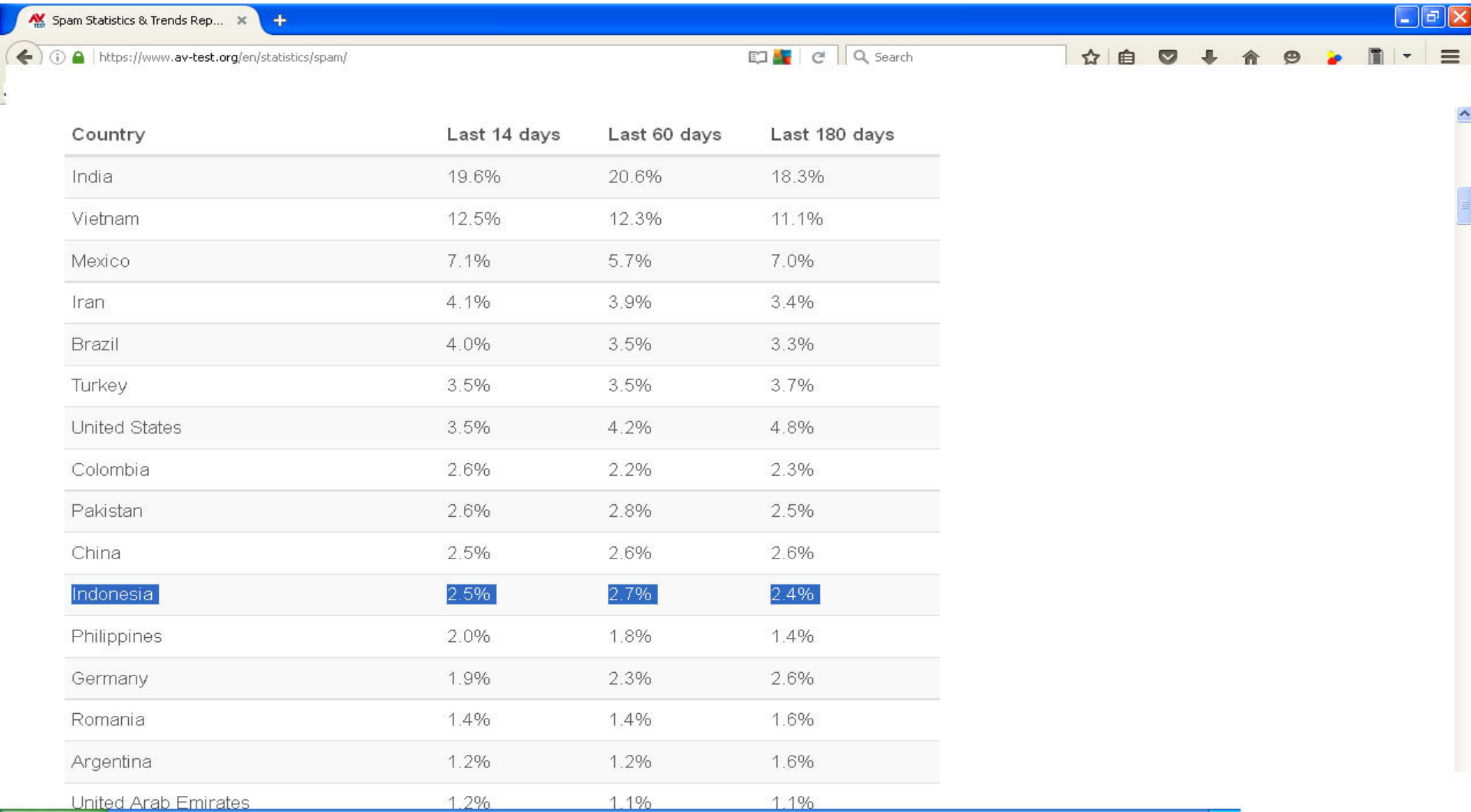
Statistik Spam ID-CERT tahun 2010-2016 (sampai dengan 30 SEP 2016)

TAHUN	ADUAN	PERINGKAT	JUMLAH RESPONDEN
2010	90,3 %	1	11
2011	17,40%	2	45
2012	4,78%	4	38
2013	40,40%	1	35
2014	51,78%	1	37
2015	28,01%	2	37
2016)*	60,83%	1	37

Statistik Incident Monitoring Report ID-CERT 2016



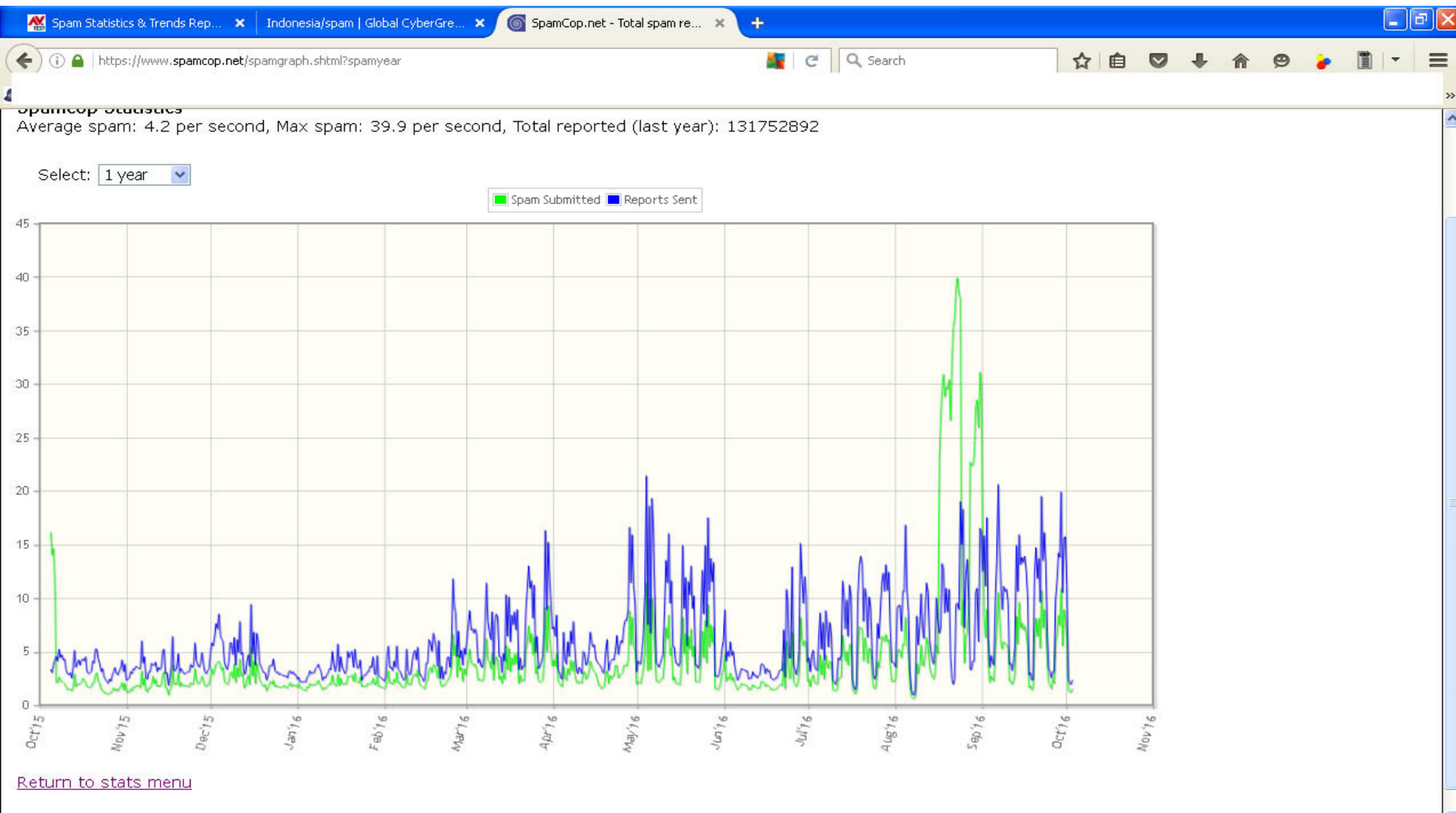
AV-TEST - <https://www.av-test.org/en/statistics/spam/>



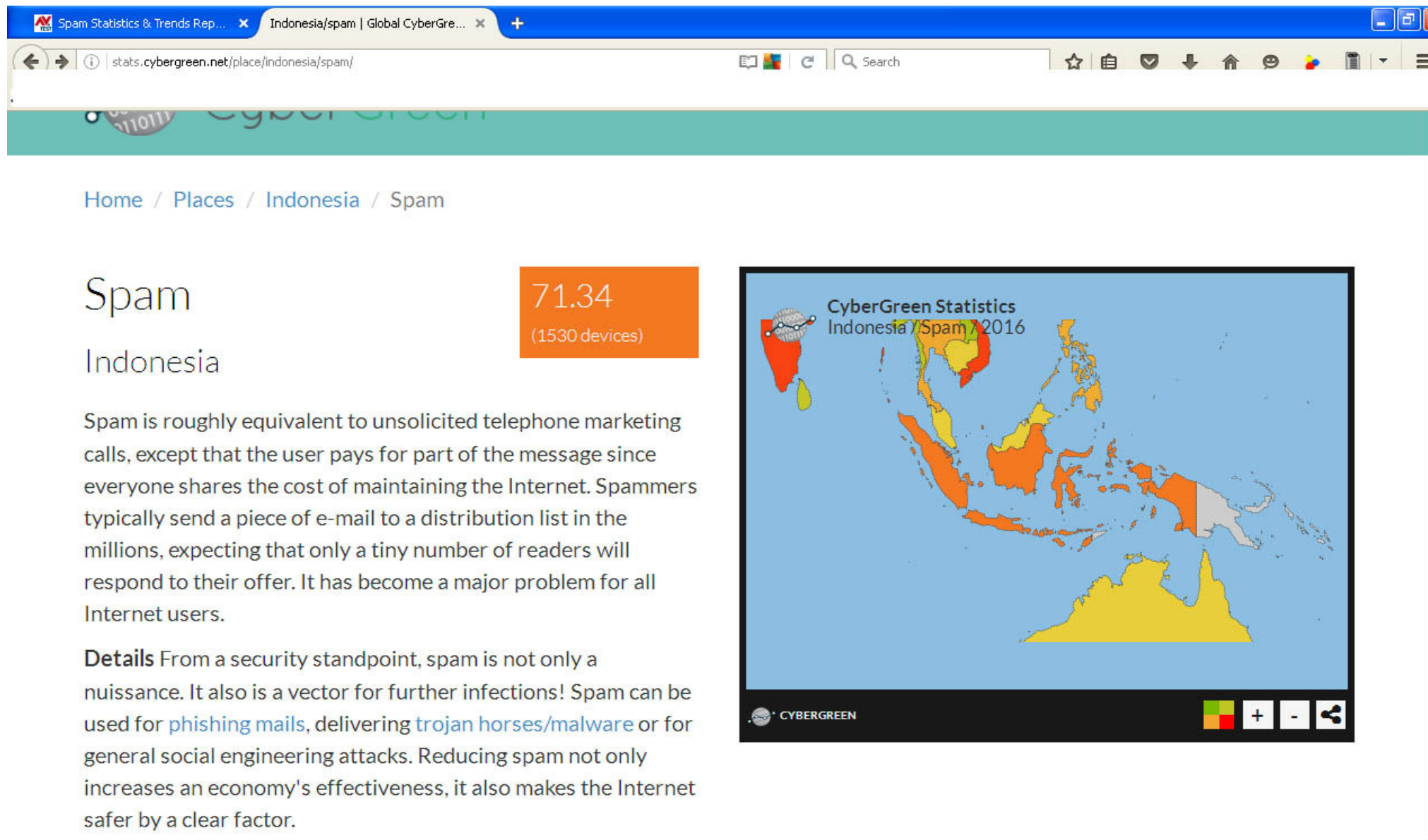
The screenshot shows a web browser displaying the AV-TEST spam statistics page. The browser's address bar shows the URL <https://www.av-test.org/en/statistics/spam/>. The page title is "Spam Statistics & Trends Rep...". The table lists countries and their spam percentages for the last 14, 60, and 180 days. Indonesia is highlighted in blue.

Country	Last 14 days	Last 60 days	Last 180 days
India	19.6%	20.6%	18.3%
Vietnam	12.5%	12.3%	11.1%
Mexico	7.1%	5.7%	7.0%
Iran	4.1%	3.9%	3.4%
Brazil	4.0%	3.5%	3.3%
Turkey	3.5%	3.5%	3.7%
United States	3.5%	4.2%	4.8%
Colombia	2.6%	2.2%	2.3%
Pakistan	2.6%	2.8%	2.5%
China	2.5%	2.6%	2.6%
Indonesia	2.5%	2.7%	2.4%
Philippines	2.0%	1.8%	1.4%
Germany	1.9%	2.3%	2.6%
Romania	1.4%	1.4%	1.6%
Argentina	1.2%	1.2%	1.6%
United Arab Emirates	1.2%	1.1%	1.1%

SpamCop – <https://www.spamcop.net/spamgraph.shtml?spamyear>

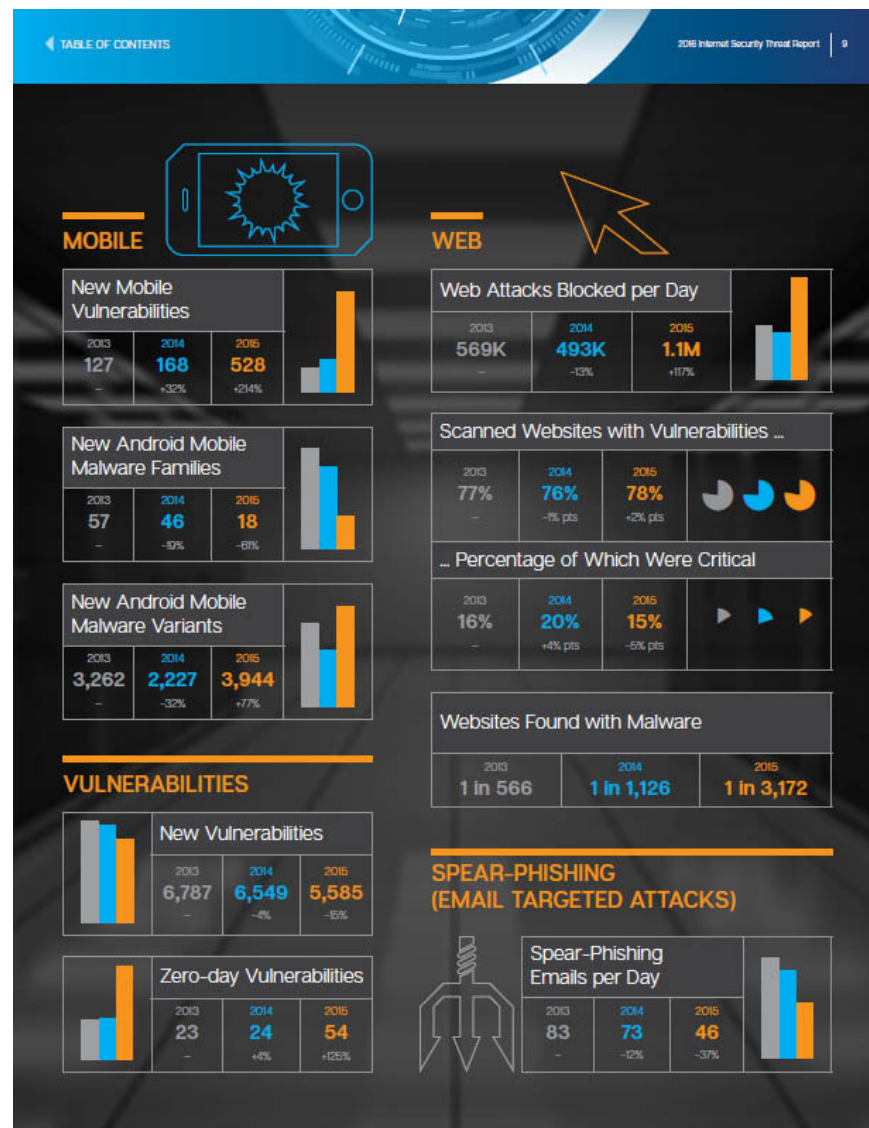
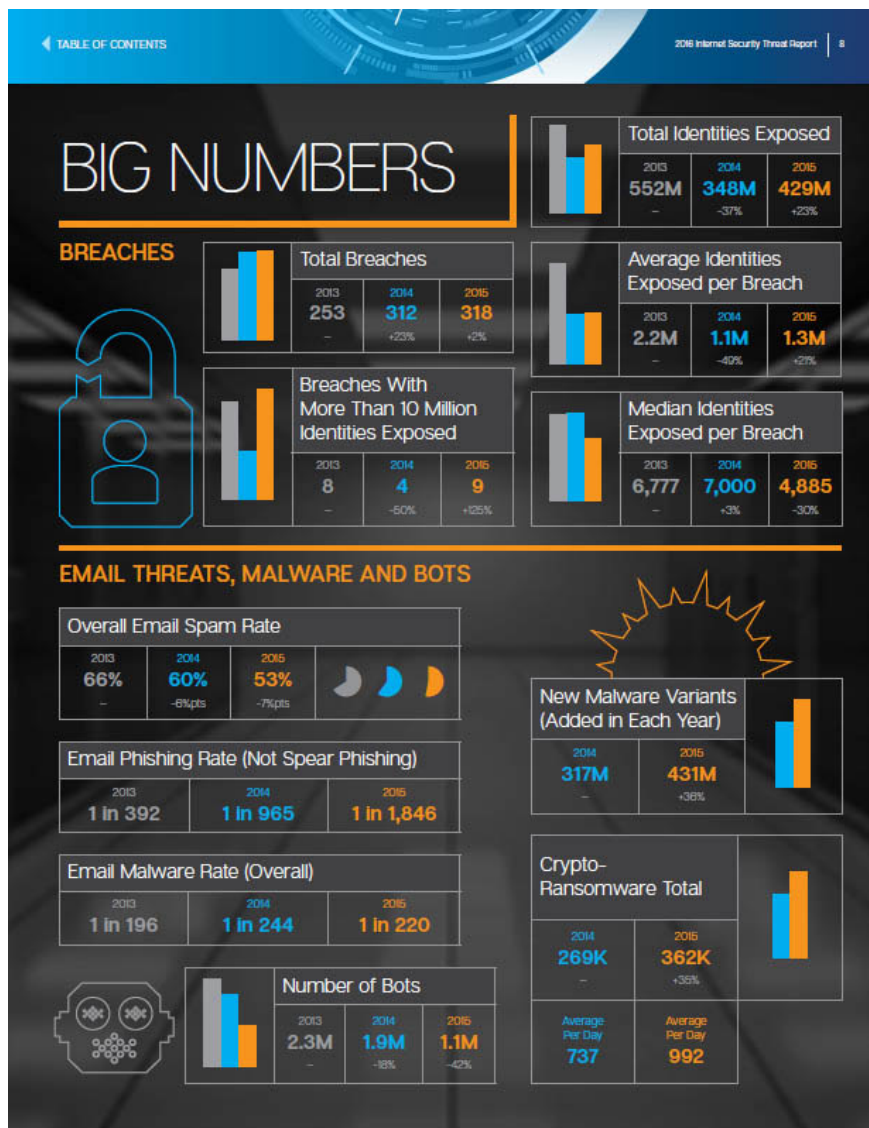


CyberGreen – <http://stats.cybergreen.net/place/indonesia/spam/>



Symantec ISTR 2016 – halaman 8 dan 9

<https://www.symantec.com/security-center/threat-report>



Regulasi Antispam Dunia

→ CASL (Kanada):

- Menganut sistem OPT-IN
- Adanya ketentuan tentang Konsen
- Mencakup semua jenis pesan elektronik (SMS, instant messaging, OTT)
- Adanya ketentuan sanksi berupa denda tinggi bagi yang melanggar.
 - Individu: 1 juta dollar kanada
 - Bisnis: 10 juta dollar Kanada

→ Can Spam Act (Amerika):

- Menganut OPT-OUT
- Selama tidak ada komplain terhadap spam, maka dianggap setuju menerima spam.
- Bila tidak setuju, laporkan sebagai spam.
- Sanksi denda melanggar: USD 16.000

Implikasi CASL terhadap perkembangan Spam

<http://www.michaelgeist.ca/2015/04/study-reports-big-drop-in-spam-following-canadian-anti-spam-law-implementation/>

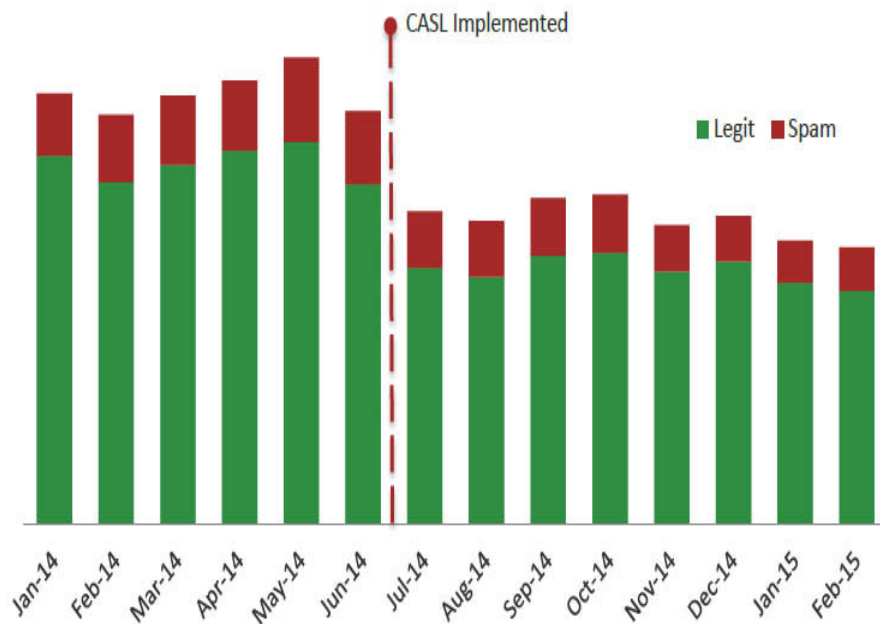


Fig. 2: Email Received in Canada

The monthly average volume for all email received by Cloudmark customers in Canada went down by 29% after CASL. This was split evenly between spam and legitimate email. The average percentage of email that was spam increased by an insignificant amount, from 16.5% to 16.6%.

Why did CASL have such an impact on legitimate email? Most likely because it enforces far more stringent requirements for obtaining consent for marketing emails. Practices for adding a consumer

Spam is an international phenomenon, but the US is both one of the biggest sources and the biggest targets for spammers. It's not a surprise, then, that 53% of spam that Canadians receive is from the US, and 78% of spam that is sent from Canada goes to the US. However, the amount of spam outbound from Canada went down noticeably when CASL was implemented.

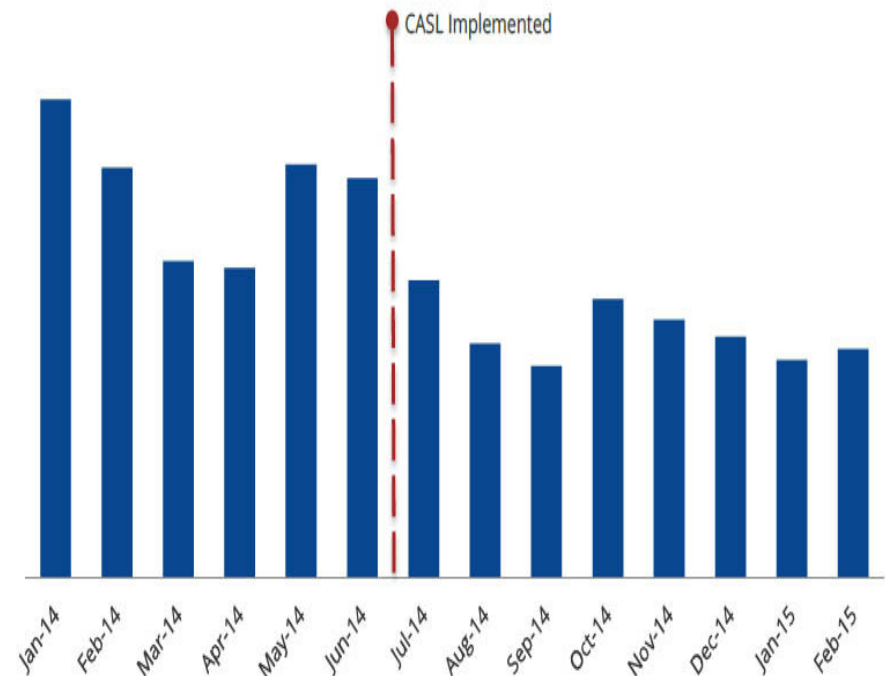
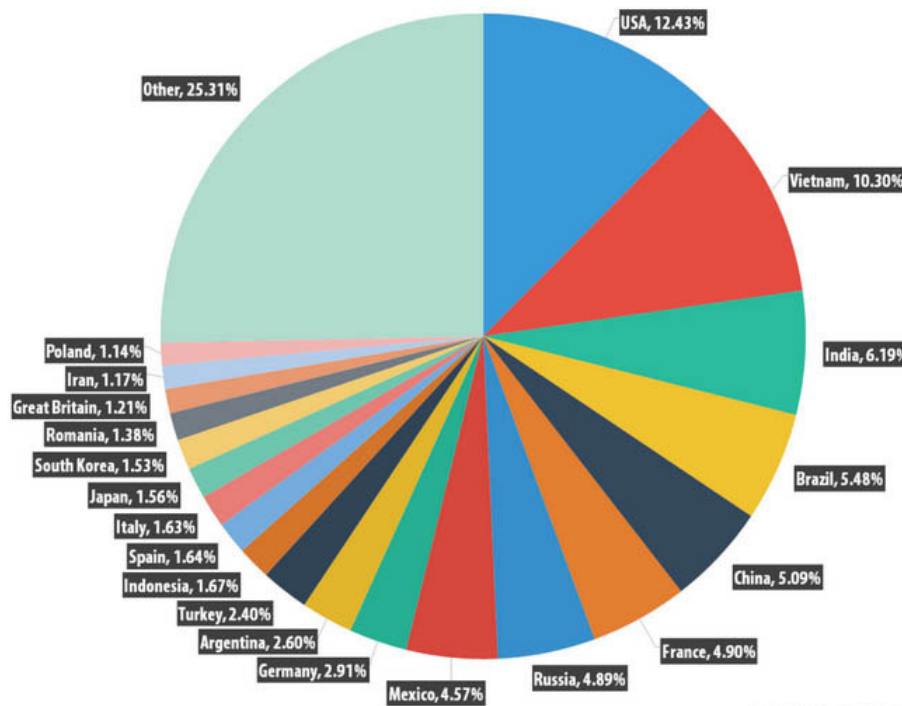


Fig. 1: Spam Originating in Canada

Implikasi regulasi Can Spam Act

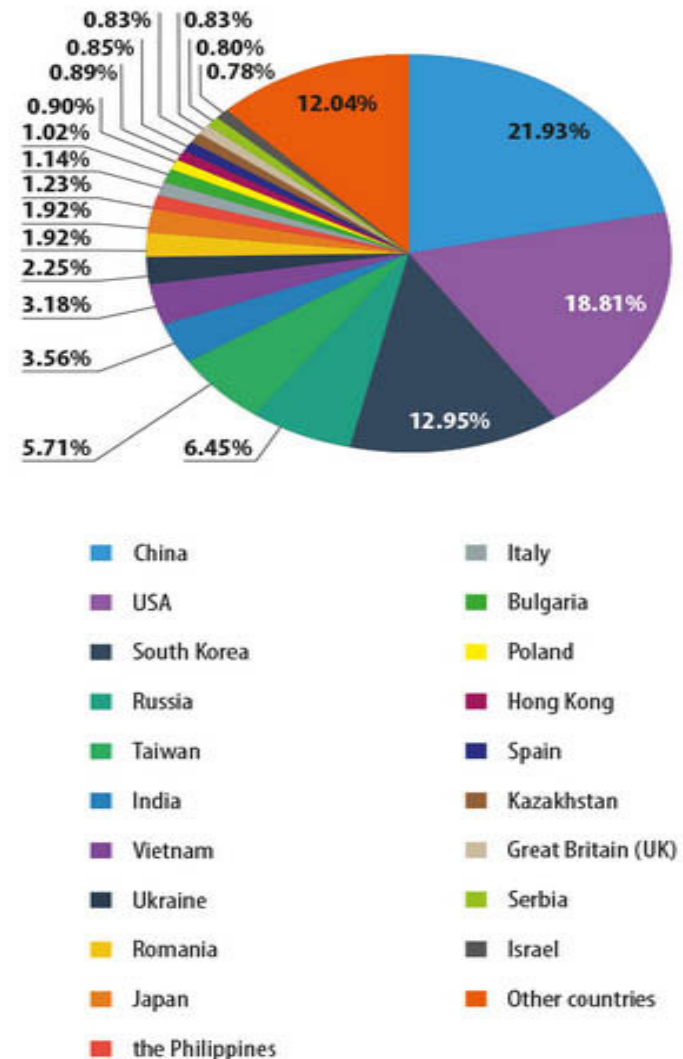
- Kuartal I tahun 2016,
<https://securelist.com/analysis/quarterly-spam-reports/74682/spam-and-phishing-in-q1-2016/>

Sources of spam by country



- Kuartal I tahun 2014:
https://usa.kaspersky.com/internet-security-center/threats/spam-statistics-report-q1-2014#.V_NgTxJnDNk

Global Spam Statistics



Penyelenggara Antispam RBL/RWL

➔ Penyelenggara RBL:

- ➔ Menyenggarakan layanan Daftar Hitam;
- ➔ Badan Hukum: non-profit hingga komersil
- ➔ Belum ada Penyelenggara RBL di Indonesia
- ➔ Beberapa Penyelenggara RBL: Spamcop, Spamhaus, Barracuda
- ➔ Blocklist umumnya terbuka dan sering menjadi rujukan didalam maupun luar negeri.

➔ Penyelenggara RWL:

- ➔ Menyenggarakan layanan Daftar Putih
- ➔ Badan Hukum: non-profit hingga komersil
- ➔ Belum ada Penyelenggara RWL di Indonesia
- ➔ Beberapa penyelenggara RWL: Spamhaus
- ➔ Whitelist umumnya terbatas dan dilakukan dalam lingkup hubungan terbatas.

Harapan dengan adanya Regulasi Antispam

- Melindungi konsumen dari ancaman *spam surel*
- Tumbuhnya industri Antispam di Indonesia
- Daftar Hitam/Putih Induk yang mudah diakses didalam negeri.

Langkah ID-CERT dalam mengurangi Spam

→ Penyebab penyebaran Spam Surel:

1. Membuka surel yang mengandung Malware.
2. Membuka surel yang mengandung Phishing
3. Kerentanan aplikasi yang tidak diperbaiki
4. Kerentanan sistem operasi yang tidak diperbaharui.
5. Antivirus yang tidak diperbaharui

→ Langkah yang telah dilakukan:

1. Menerbitkan Peringatan Keamanan
2. Menghubungi organisasi yang diketahui memiliki kerentanan, untuk segera melakukan perbaikan.
3. Memberikan saran-saran khusus bila diminta.

KESIMPULAN

1. *Spam Surel* merupakan ancaman serius saat ini, dimana untuk Indonesia dalam beberapa tahun terakhir selalu menempati peringkat 1 dari total aduan *spam* yang diterima ID-CERT.
2. Indonesia tidak hanya menjadi penyebar *spam Surel*, tetapi juga turut menjadi korban *Spam Surel* yang dikirim dari luar negeri.
3. Dalam sejumlah kasus, *Spam Surel* juga turut menyebarkan *Malware* dan *Phishing*.
4. Perlu adanya regulasi Antispam yang dapat melindungi konsumen.

BAHAN BACAAN

- PDF Presentasi ini dapat diunduh di:
<http://www.cert.id/bahan-bacaan/id/konten/30/>
- Mengenai ID-CERT:
<http://www.cert.id/tentang-kami/id/>
- Laporan Berkala IMR:
<http://www.cert.id/bahan-bacaan/id/>
- Cakupan Kerja ID-CERT, RFC2350:
<http://www.cert.id/rfc/id/>
- AV Test project: <https://www.av-test.org/en/statistics/spam/>
- CyberGreen Project:
<http://stats.cybergreen.net/place/indonesia/spam/>
- Spamcop Statistics:
<https://www.spamcop.net/spamgraph.shtml?spamyear>

- Symantec ISTR:

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM



<https://www.symantec.com/security-center/threat-report>

PERTANYAAN, SARAN & MASUKAN?

Kontak Desk ID-CERT:

www.cert.or.id

Telpon: (+ 62)889-1400-700

Ahmad Alkazimy (Manajer ID-CERT)

cert@cert.or.id

Rahmadian L. Arbianita (Helpdesk ID-CERT)

rahmadian@cert.or.id

Mailing List:

diskusi@MILIS.cert.or.id

INDONESIA COMPUTER EMERGENCY RESPONSE TEAM

