id.cert

PERTEMUAN TAHUNAN XI

OUTLOOK KEAMANAN INFORMASI 2019

BLOCK71 BANDUNG
14 FEBRUARI 2019

DIDUKUNG OLEH:

INDOCISC

CBN

.id my entity

Qwords

AGENDA

- 13.00 Pembukaan Pertemuan Tahunan XI ID-CERT dan Doa
- 13.00 - 13.30 Pembukaan Acara dan Sejarah ID-CERT oleh DR Budi Rahardjo
- 13.30 - 14.00 Laporan kegiatan ID-CERT termasuk IMR, Membership oleh Ahmad Alkazimy
- 14.00 - 14.30 Presentasi Mitra
- 14.30 - 15.00 Outlook Keamanan Informasi 2019

Mengenai ID-CERT

- Berdiri pada 01 DES 1998
- Pendiri: DR. Budi Rahardjo
- Tugas dan Fungsi ID-CERT ada di RFC 2350 https://cert.id/rfc/id/
- Independen
- Non Profit
- Non Pemerintahan

Badan Hukum ID-CERT

- Tahun 2013 ID-CERT membuat Badan hukum untuk mempermudah kerjasama dengan berbagai pihak.
- Nama badan Hukum tertanggal 11 JULI 2013, no.31 dan telah didaftarkan di KEMENKUMHAM:

“PERKUMPULAN TIM TANGGAP DARURAT KEAMANAN KOMPUTER INDONESIA (PL. INDONESIA COMPUTER EMERGENCY RESPONSE TEAM -ID-CERT)”

Laporan Aktifitas 2019

- *Incident Handling*
- *Incident Monitoring Report*
- *Penambahan Staf*
- *Event Report Tools*
- Penasehat CERT/CSIRT
- Pertemuan Tahunan
- APCERT Drill
- Narasumber Pelatihan

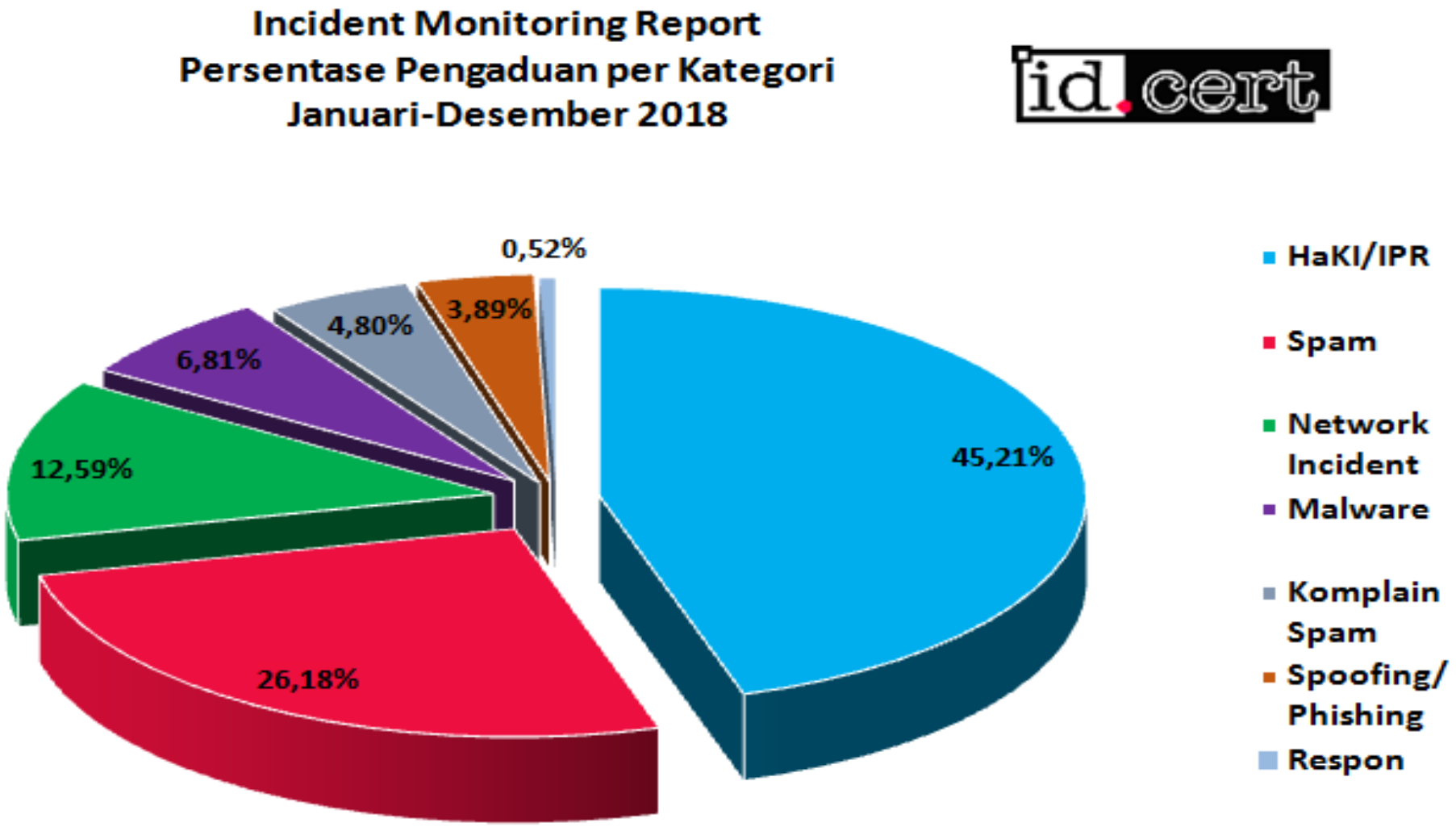
Incident Handling 2018

- Total Aduan: 144.620
- Ditangani: 748

Incident Monitoring Report (IMR)

- Dimulai pada 2010 dengan Riset Internet Abuse
- Pada Maret 2012 menjadi *Incident Monitoring Report*
- Jumlah Responden hingga saat ini = 40 organisasi
- Cara partisipasi: CC email abuse@namadomain ke abuse@cert.or.id

Incident Monitoring Report



Laporan yang paling sering

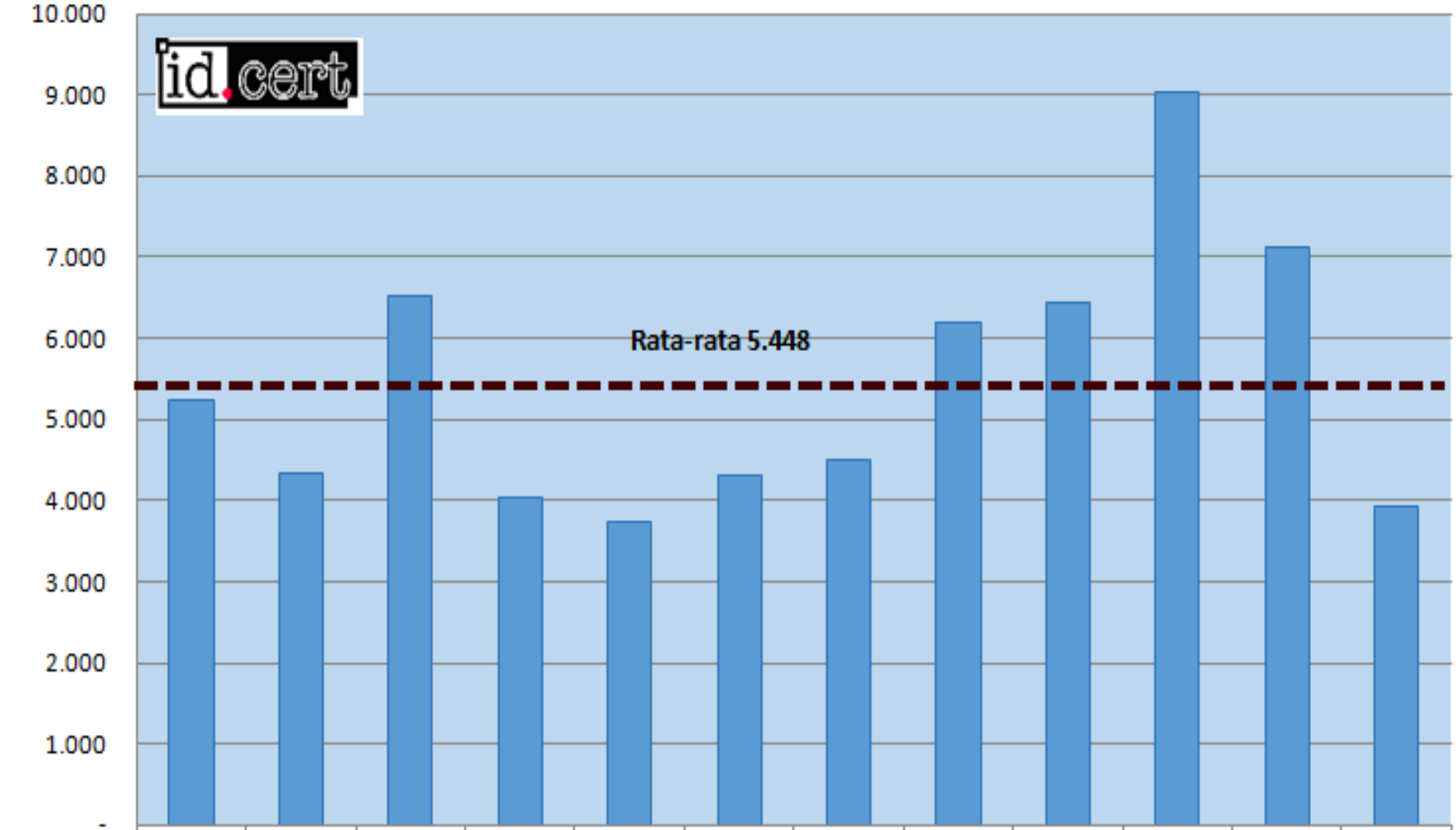
- Spoof/Phishing di IP/Domain Indonesia
- Network Incident:
  - Brute Force Attack
  - SQL injection
  - Hacked FTP Account
- Malware di IP/Domain Indonesia
- Intellectual Property Right
- Spam

Incident Monitoring Report 2018

2018	HaKI/IPR	Spam	Network Incident	Malware	Komplain Spam	Spoofing/ Phishing	Respon
Januari	5.247	3.789	1.877	520	562	991	82
Februari	4.345	2.810	583	416	130	533	65
Maret	6.513	2.880	1.435	517	212	366	81
April	4.040	2.376	1.066	632	250	310	83
Mei	3.744	2.221	1.421	754	388	491	74
Juni	4.309	2.012	1.279	1.007	374	572	70
Juli	4.493	2.846	1.199	1.088	561	358	53
Agustus	6.181	2.547	2.006	1.153	848	335	50
September	6.425	4.458	2.305	1.163	978	505	64
Oktober	9.039	4.205	2.357	1.387	492	489	55
November	7.123	3.667	1.354	562	1.274	368	36
Desember	3.922	4.050	1.328	656	868	310	35
Total	**65.381**	**37.861**	**18.210**	**9.855**	**6.937**	**5.628**	**748**
Rata-rata	**5.448**	**3.155**	**1.518**	**821**	**578**	**469**	**62**
%	**45,21%**	**26,18%**	**12,59%**	**6,81%**	**4,80%**	**3,89%**	**0,52%**

Incident Monitoring Report 2018

Rata-rata HaKI/IPR



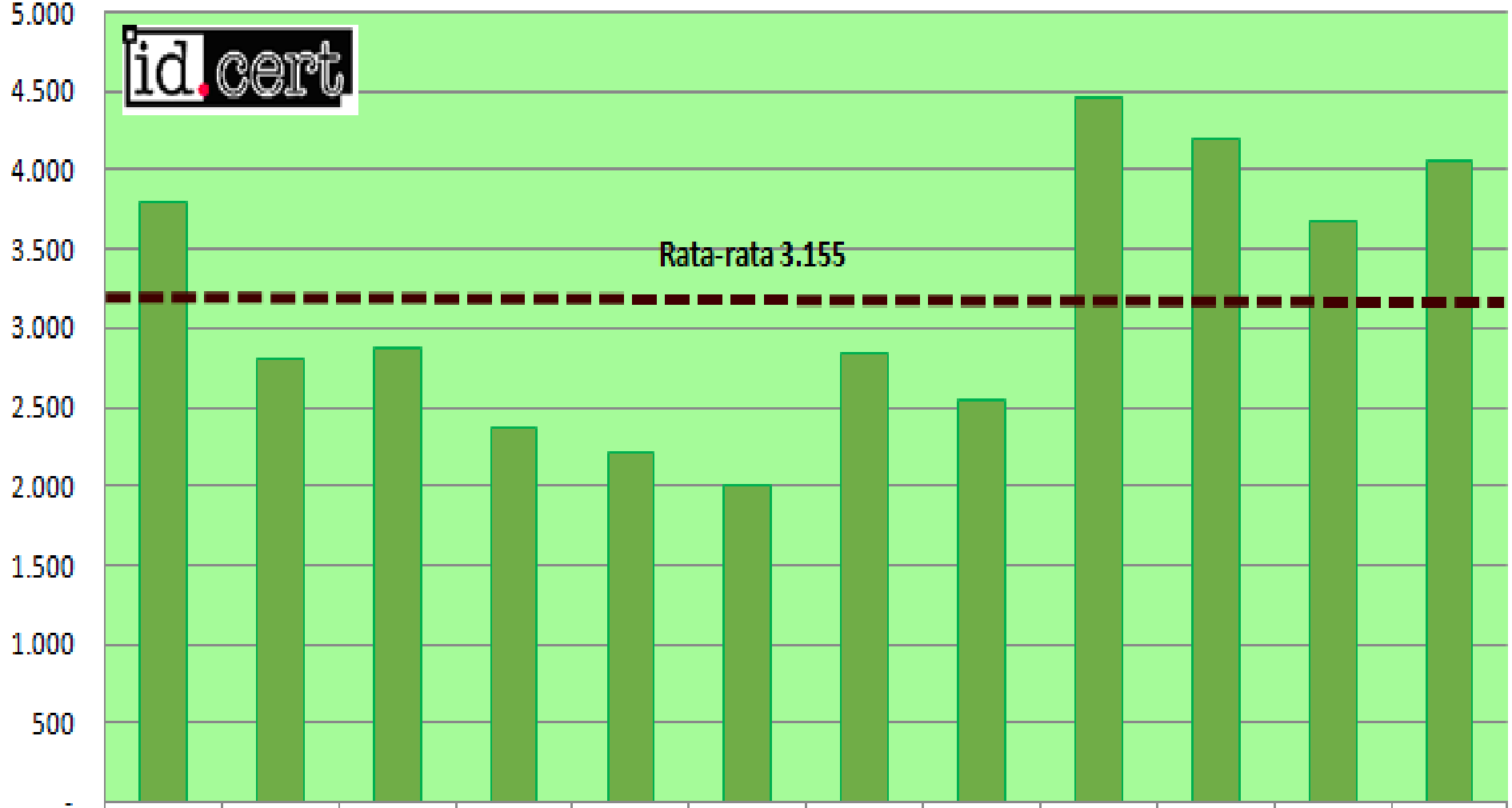
	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
HaKI/IPR	5.247	4.345	6.513	4.040	3.744	4.309	4.493	6.181	6.425	9.039	7.123	3.922

IPR/HaKI

- Sumber laporan 100% dari luar negeri
- Penyebaran Film dan Musik luar negeri di IP/Domain Indonesia menggunakan tools P2P
- Permintaan untuk menghapus file tsb
- Laporan IPR Indonesia belum ada.
  - Silahkan dilaporkan ke abuse@cert.or.id dan ipr@cert.or.id
- ID-CERT membutuhkan mitra external

Incident Monitoring Report 2018

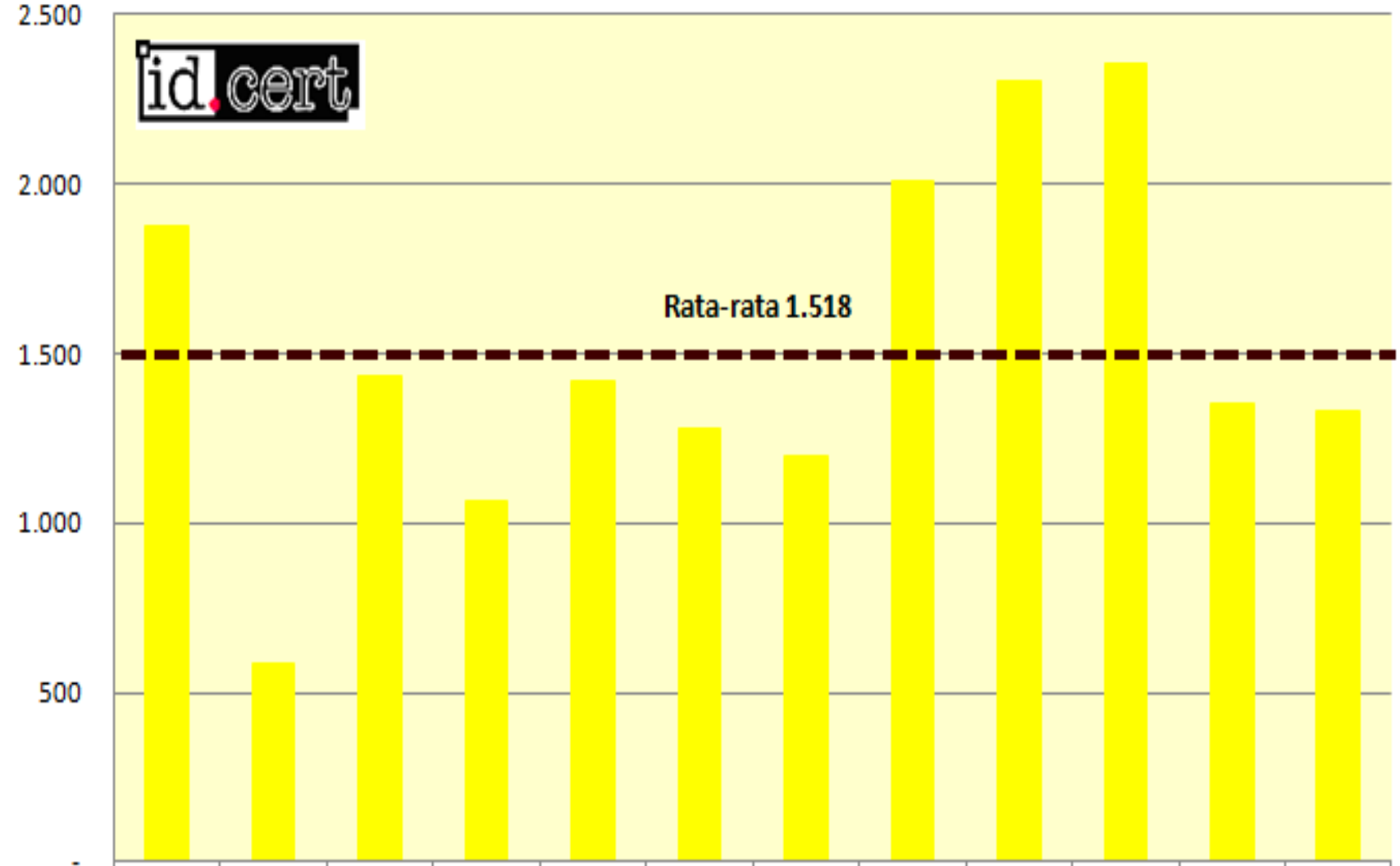
Rata-rata SPAM



	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Spam	3.789	2.810	2.880	2.376	2.221	2.012	2.846	2.547	4.458	4.205	3.667	4.050

Incident Monitoring Report 2018

Rata-rata NETWORK INCIDENT



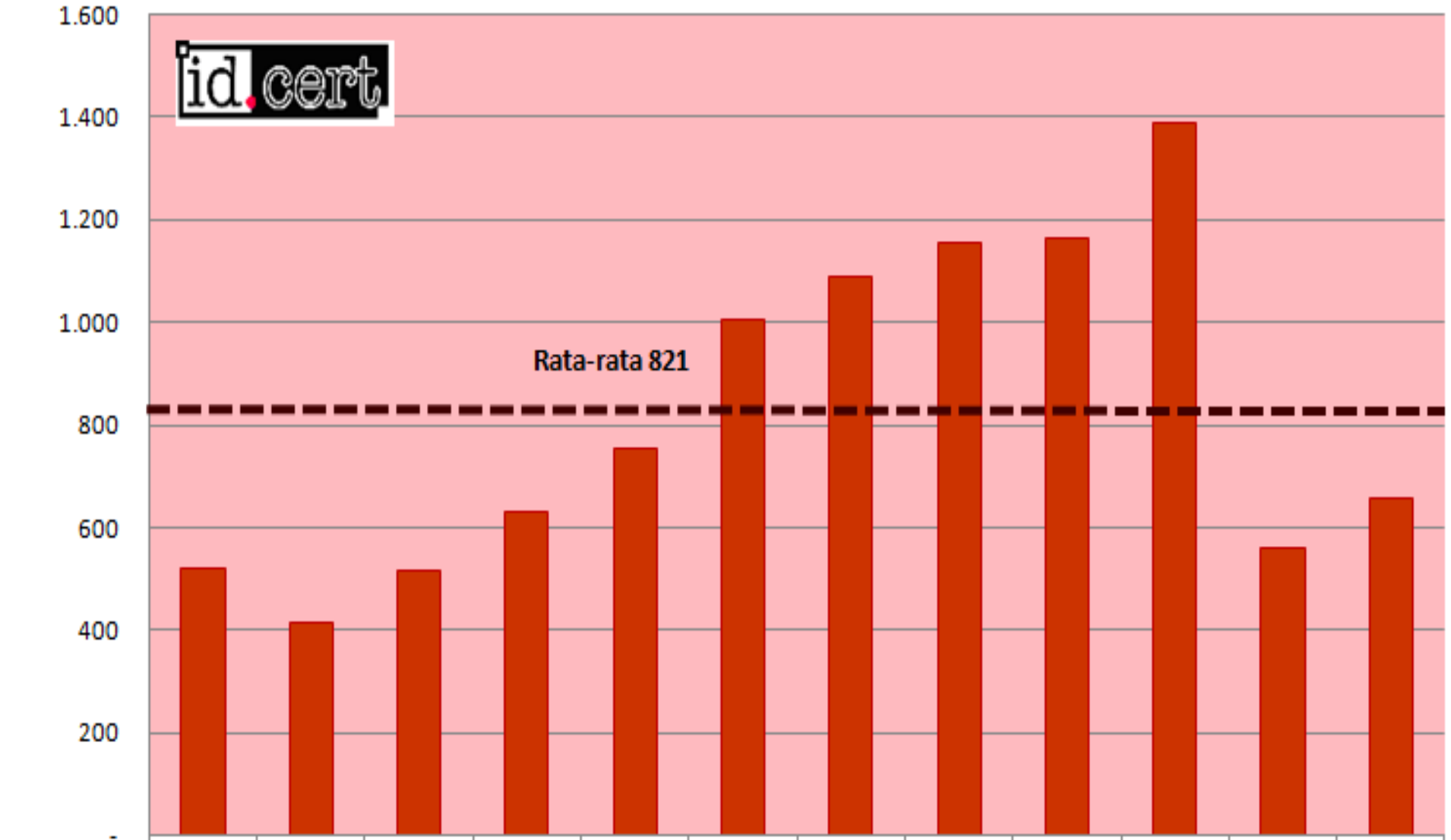
	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Network Incident	1.877	583	1.435	1.066	1.421	1.279	1.199	2.006	2.305	2.357	1.354	1.328

Network Incident: Brute Force

- Bila login berhasil:
  - Web/IP disusupi Malware
  - Web/IP disusupi hacking tools
  - Web/IP dijadikan C&C
  - Pencurian data web maupun identitas lainnya dengan menerobos sistem yang ada
  - Mengganti halaman tampilan (Hacking/Deface)
- Paling sering jadi target: Pemerintah

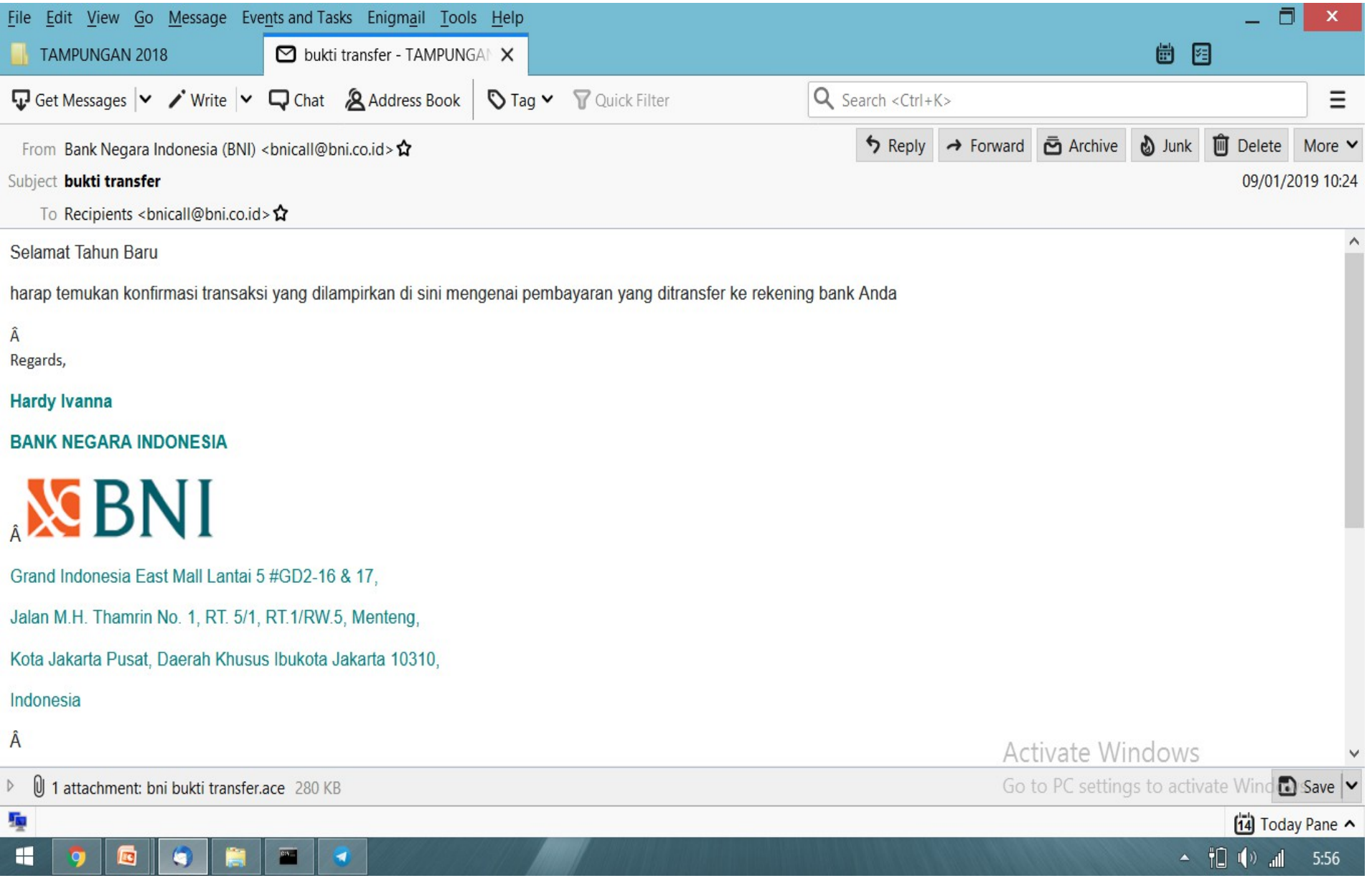
Incident Monitoring Report 2018

Rata-rata MALWARE

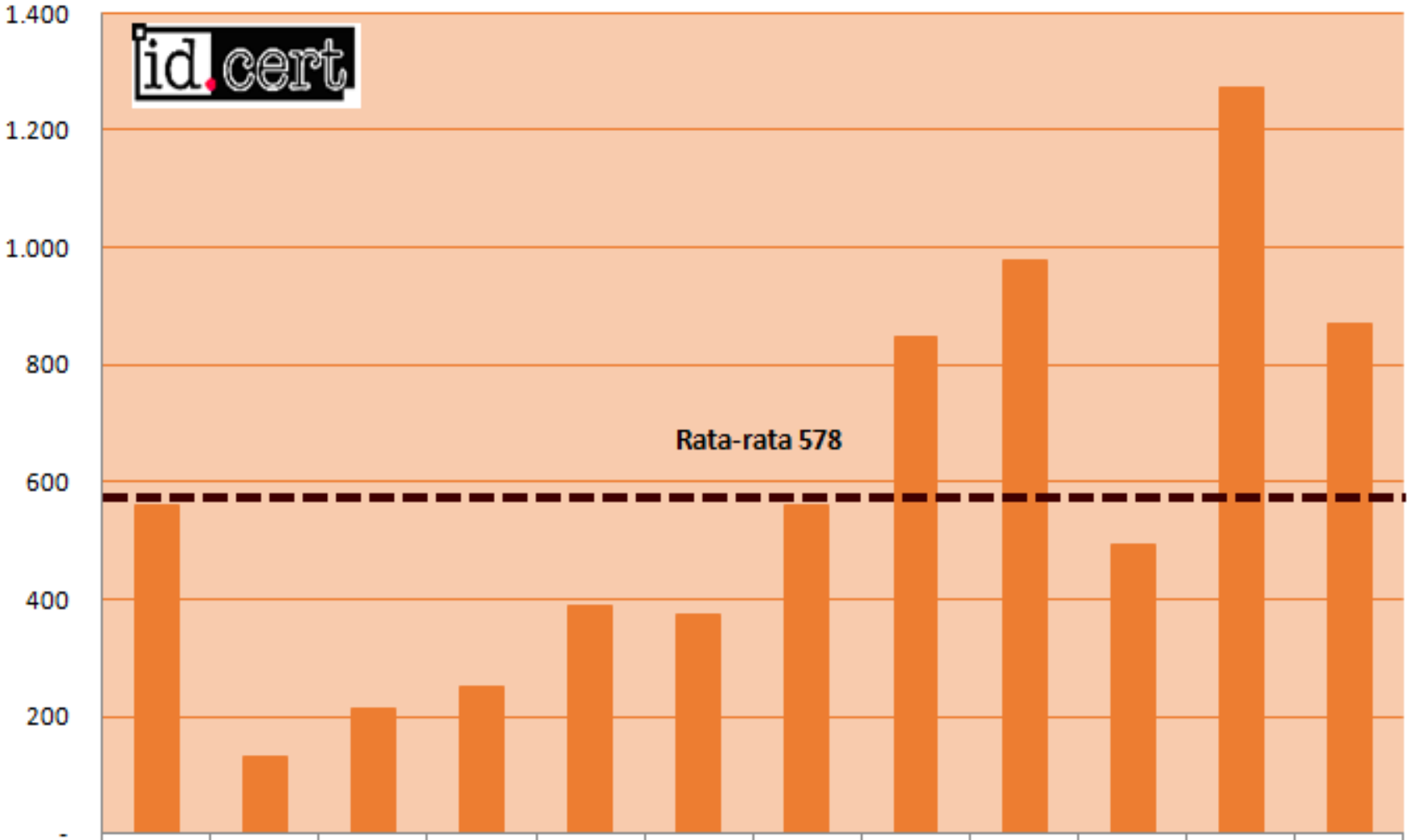


	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Malware	520	416	517	632	754	1.007	1.088	1.153	1.163	1.387	562	656

Contoh Phishing dengan attachment Malware



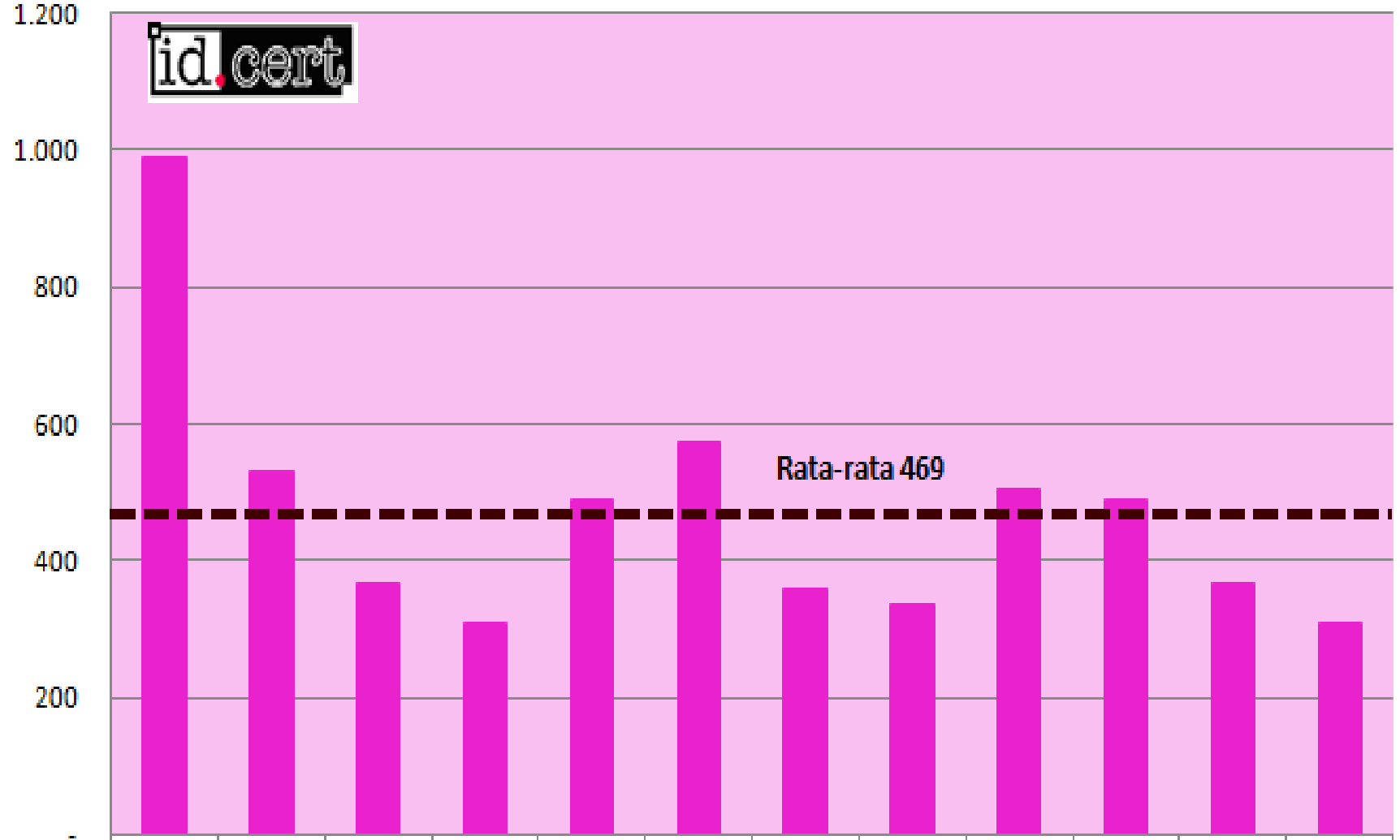
Incident Monitoring Report 2018
Rata-rata KOMPLAIN SPAM



	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Komplain Spam	562	130	212	250	388	374	561	848	978	492	1.274	868

Incident Monitoring Report 2018

Rata-rata SPOOFING/PHISHING



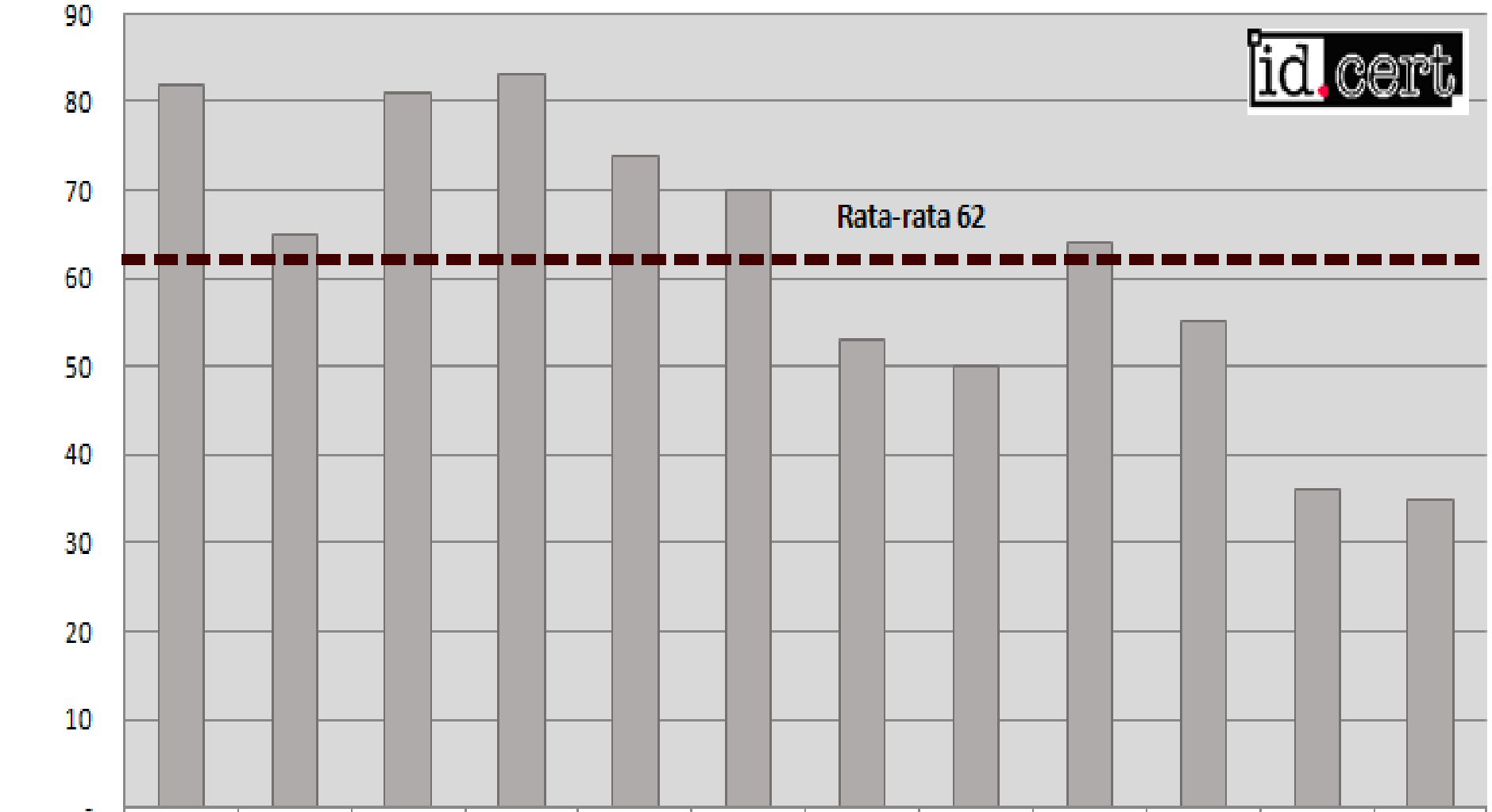
	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Spoofing/Phishing	991	533	366	310	491	572	358	335	505	489	368	310

Phishing

- Phishing disitus Sekolah Indonesia terkait login palsu ke universitas diluar negeri
- Phishing situs perbankan asing di IP Indonesia
- Phishing situs perbankan Indonesia di IP Indonesia maupun luar negeri
- Situs pemerintah disusupi Phishing

Incident Monitoring Report 2018

Rata-rata RESPON



	Jan	Feb	Mar	Apr	Mei	Juni	Juli	Agt	Sept	Okt	Nov	Des
Respon	82	65	81	83	74	70	53	50	64	55	36	35

Incident Monitoring Report (IMR)

- IMR Edisi Umum: Dwi Bulan

- IMR Edisi Khusus: Dwi Bulan dan Tahunan

Tim Operasional ID-CERT

- Manajer Operasional: Ahmad Alkazimy
- Incident Response Helpdesk: Rahmadian L. Arbianita
- Technical Editor: Emil Yakhya
- Technical Editor: Bainul

Event Report Tools

- Tools untuk mengolah data Feed log
- Dikostumasi dan dibuat khusus oleh volunteer dan mahasiswa magang untuk ID-CERT
- Dapat diterbitkan sesuai permintaan

Penasehat CERT/CSIRT

- Memberikan masukan kepada BSSN terkait Tata Kelola Penanganan Insiden di Indonesia
- Berkontribusi dalam penyusunan regulasi terkait Tata Kelola di BSSN

Pertemuan Tahunan

- 20-22 MARET 2018: DR Budi Rahardjo (ID-CERT) hadir sebagai Keynote dan Pembicara di *Cyber Intelligence Asia V* di Singapura.
- 13 APRIL 2017: Pertemuan Tahunan IX ID-CERT di GMP Telkom, Bandung
- 6 DES 2017: Pertemuan Tahunan X ID-CERT di Kolla Space, Jakarta
- 21-24 OKT 2018: Pertemuan Tahunan APCERT AGM di Shanghai. Diwakili oleh

APCERT Drill

- ID-CERT berpartisipasi sebagai peserta bersama dengan lebih dari 20 CSIRT se Asia Pasifik dan sejumlah CSIRT anggota OIC CERT.
- Kegiatan Tahunan penanganan insiden Siber yang dilaksanakan secara virtual diwaktu yang bersamaan.

Narasumber Pelatihan

- ID-CERT diundang sebagai pembicara di ITB dan Telkom University.
- ID-CERT diundang sebagai pembicara di BSSN.

MAGANG

- Kami juga telah menerima sejumlah mahasiswa Magang ditempat kami sejak beberapa tahun terakhir
- Lokasi kerja: Bandung
- Informasi umum magang dapat dilihat di: https://cert.id/index-berita/id/8/
- Informasi lowongan/topik magang:

https://cert.id/index-berita/id/berita/101/

TOPIK MAGANG 2018

1. Mengubah CSS dari CMS Web statis.

2. Malware Advisory

~~3. Security Advisory~~

4. Malware Scanner multi AV.

5. Metode dan Software untuk Crowling web/IP

id.cert

PERTEMUAN TAHUNAN XI

OUTLOOK KEAMANAN INFORMASI 2019

BLOCK71 BANDUNG
14 FEBRUARI 2019

DIDUKUNG OLEH:

INDOCISC

CBN

.id my entity

Qwords