

Peranan ID-CERT dalam penanganan insiden siber di Indonesia

Jakarta, 04 MAR 2017

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

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

Sejarah CERT

- CERT: Computer **Emergency Response** Team (1988) dibentuk oleh CMU (Carnegie Mellon University).
- CSIRT: Computer **Security Incident** Response Team (1998), dibakukan melalui kesepakatan bersama masyarakat internet dunia dibawah IETF/ICANN.

"Morris Worm"
(CMU - 1988)

"CERT"
(CMU - 1988)

"RFC 2350"
(IETF - 1998)

Sejarah ID-CERT

- ➔ Dimulai pada **01 Des 1998** sebagai respon terhadap kebutuhan pelaporan masalah **security** yang terkait dengan **internet Indonesia**;
- ➔ Bersifat **voluntir** (come and go)
- ➔ Memiliki domain dan situs web
- ➔ **Pendiri** forum regional APCERT (Asia Pacific Computer Emergency Response Team) pada 2001-2003, dengan status **Full Member**;
- ➔ **Kontak Utama** untuk Indonesia (**PoC**) di APCERT;

“ID-CERT”
(Budi Rahardjo - 1998)

“APCERT”
(ID-CERT
pendiri forum
2001-2003)

Visi - Misi

- (1) Visi: meningkatkan **awareness** keamanan Siber di Indonesia
- (2) Tujuan ID-CERT adalah untuk melakukan **koordinasi penanganan insiden** yang melibatkan pihak Indonesia dan luar negeri.
- (3) **Menginformasikan berbagai keluhan** atas **insiden jaringan keamanan internet**, serta bergantung sepenuhnya pada kerjasama dengan para pihak yang terlibat dalam insiden jaringan terkait.
- (4) Membangun **komunitas** CERT Indonesia.
- (5) Memasyarakatkan pentingnya **keamanan internet** di Indonesia.
- (6) Melakukan berbagai **penelitian di bidang keamanan Internet** yang dibutuhkan oleh komunitas Internet Indonesia

Voluntir:

- **Ketua**: Budi Rahardjo, PhD
- **Wakil Ketua**: Andika Triwidada
- Didukung oleh sejumlah **voluntir** lainnya.

Staf Profesional:

- **Manager Operasional**: Ahmad Alkazimy
- **Incident Response Officer – Helpdesk**: Rahmadian
- **Technical Editor**: Wayan Achadiana
- **Malware Analyst – Coordinator**: Setia Juli Irzal

➡ 3.4. Otoritas:

ID-CERT tidak memiliki otoritas secara operasional terhadap konstituensinya baik di Indonesia maupun luar negeri, melainkan hanya menginformasikan berbagai keluhan atas insiden jaringan, serta bergantung sepenuhnya pada kerjasama dengan para-pihak yang terlibat dalam insiden jaringan terkait.

Layanan:

5.1. Respon Insiden

5.1.1. Triage Insiden

5.1.2. Koordinasi Insiden

5.1.3. Resolusi Insiden

5.2. Aktivitas Reaktif

Aduan yang masuk: **Darimana** Informasi didapat?

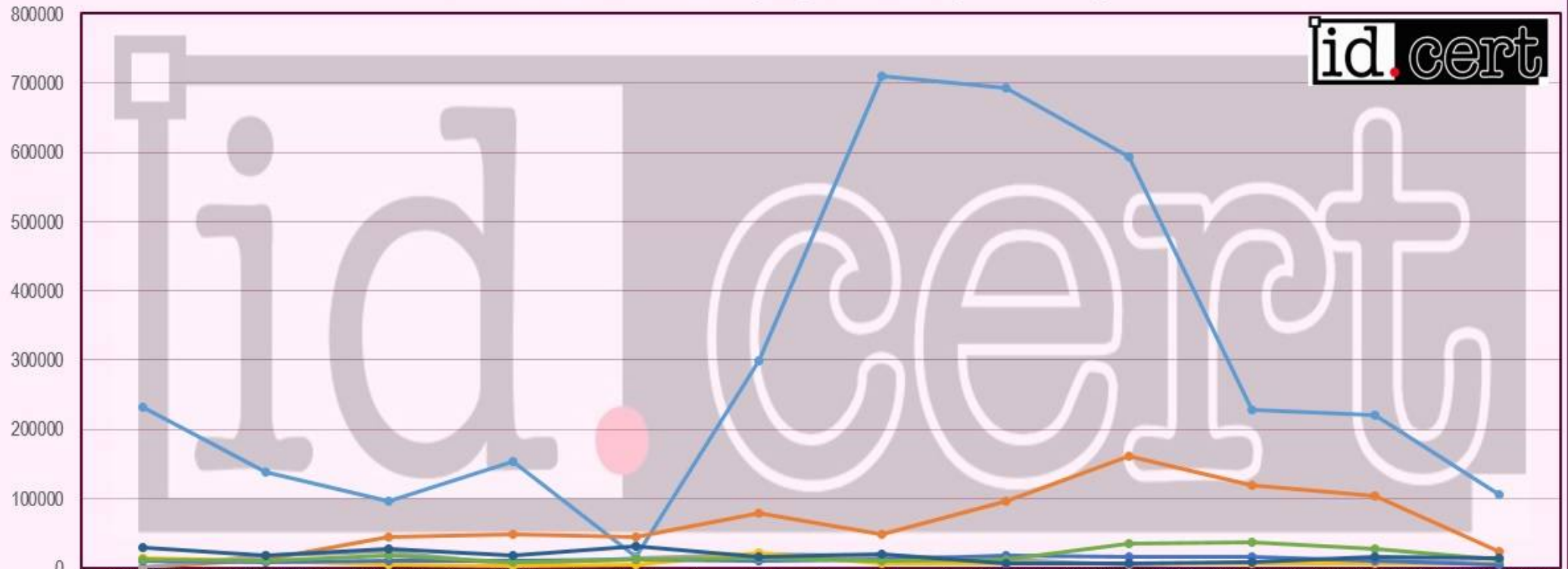
- ➔ Informasi dari aduan pengguna internet di dalam negeri yang mengetahui kelemahan tersebut;
- ➔ Informasi dari aduan pengguna internet diluar maupun komunitas tertentu yang mengetahui kelemahan yang ada;
- ➔ Informasi dari media online dan *mailing list*;

Jumlah Aduan

Statistik Jumlah Pengaduan dari tahun 2011 s/d 2016



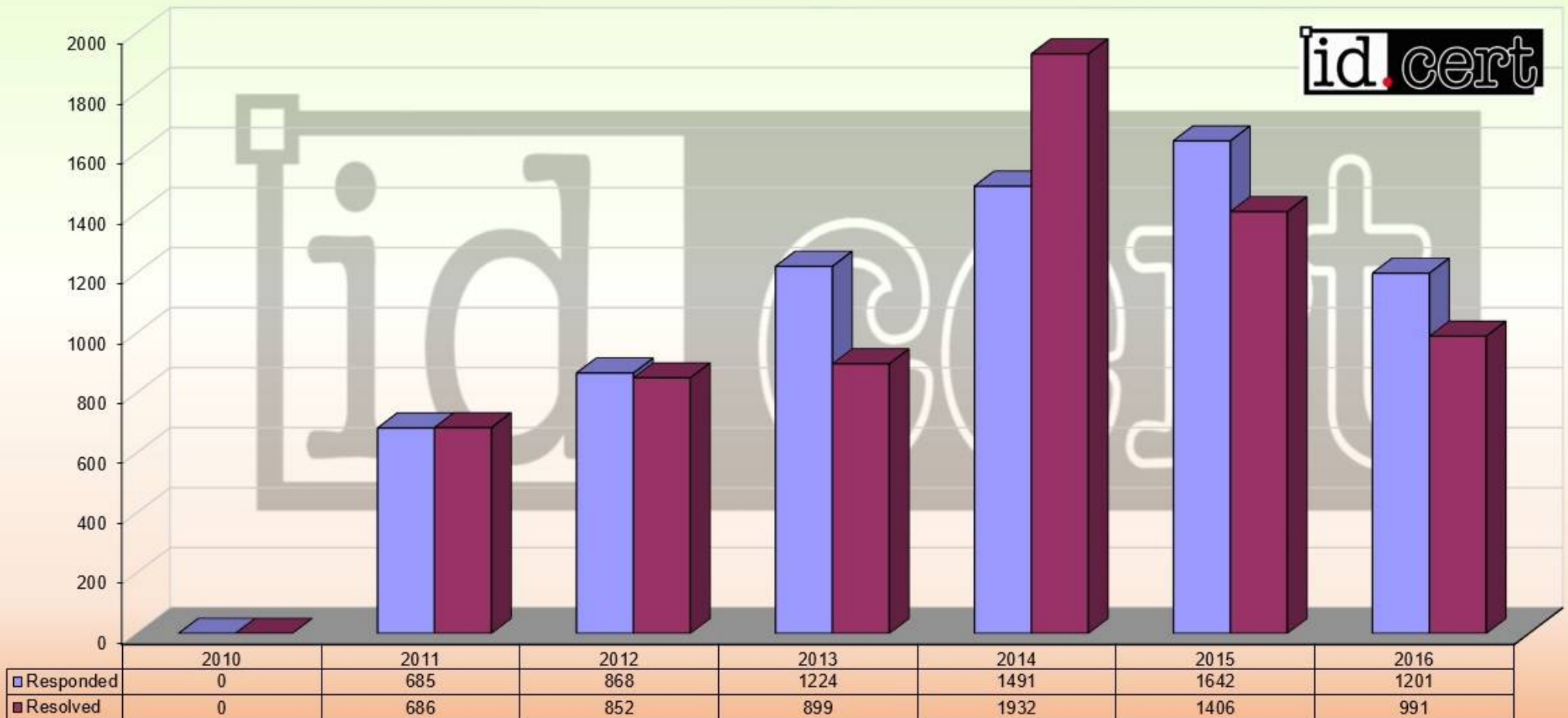
Statistik Jumlah Insiden yang diadukan (2010-2016)



	JANUARI	FEBRUARI	MARET	APRIL	MEI	JUNI	JULI	AGUSTUS	SEPTEMBER	OKTOBER	NOPEMBER	DESEMBER
2010	231411	139195	96693	Chart Area	15321	298578	709747	692570	593765	227810	220476	104945
2011	1	12849	44707		49294	44281	79449	48287	97228	160455	118788	103916
2012	1382	17276	23423	4913	13670	19779	18166	11777	3661	8442	12164	6963
2013	13788	9478	5211	1853	4947	20941	5927	6611	6369	5558	6224	7128
2014	10722	9269	11260	11015	11872	11239	11819	17829	15109	15975	10064	4115
2015	11550	10331	17802	8280	11579	14724	10148	11662	35661	37490	26667	11539
2016	29876	18045	28152	17854	31087	16743	19618	5764	6284	9060	15509	14453

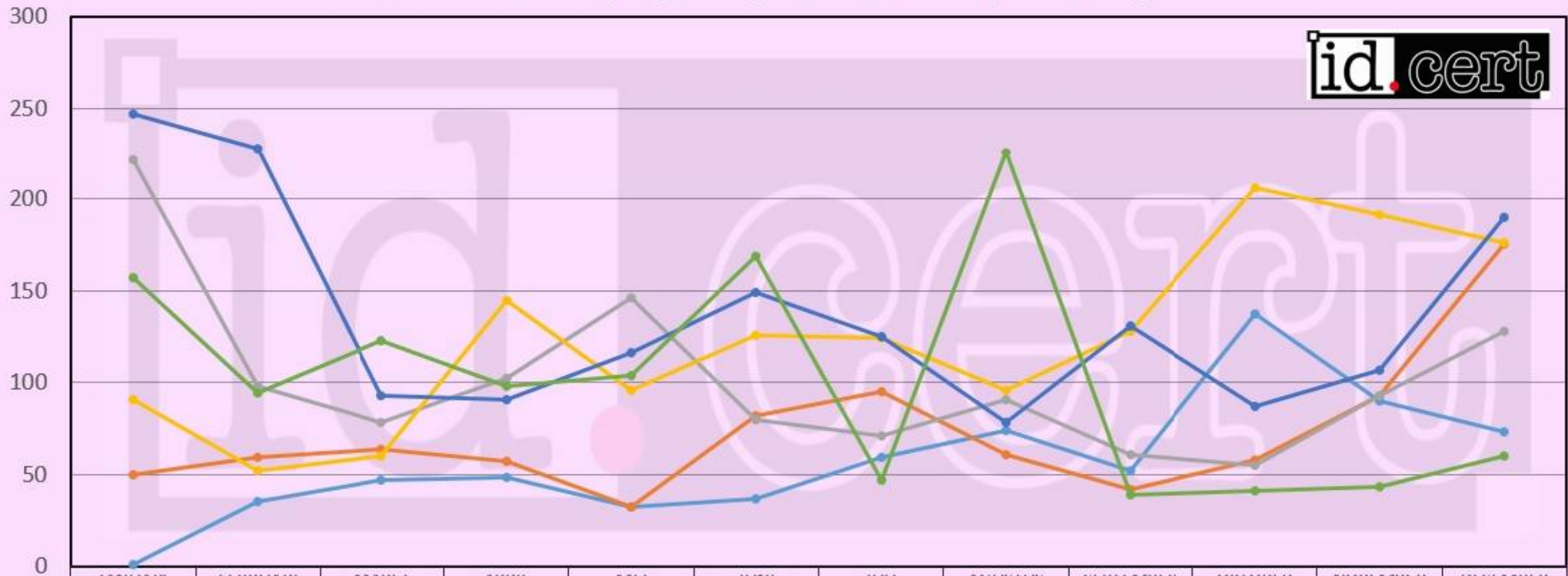
Jumlah Insiden yang direspon dan diselesaikan

Penanganan Insiden tahun 2010 - 2016



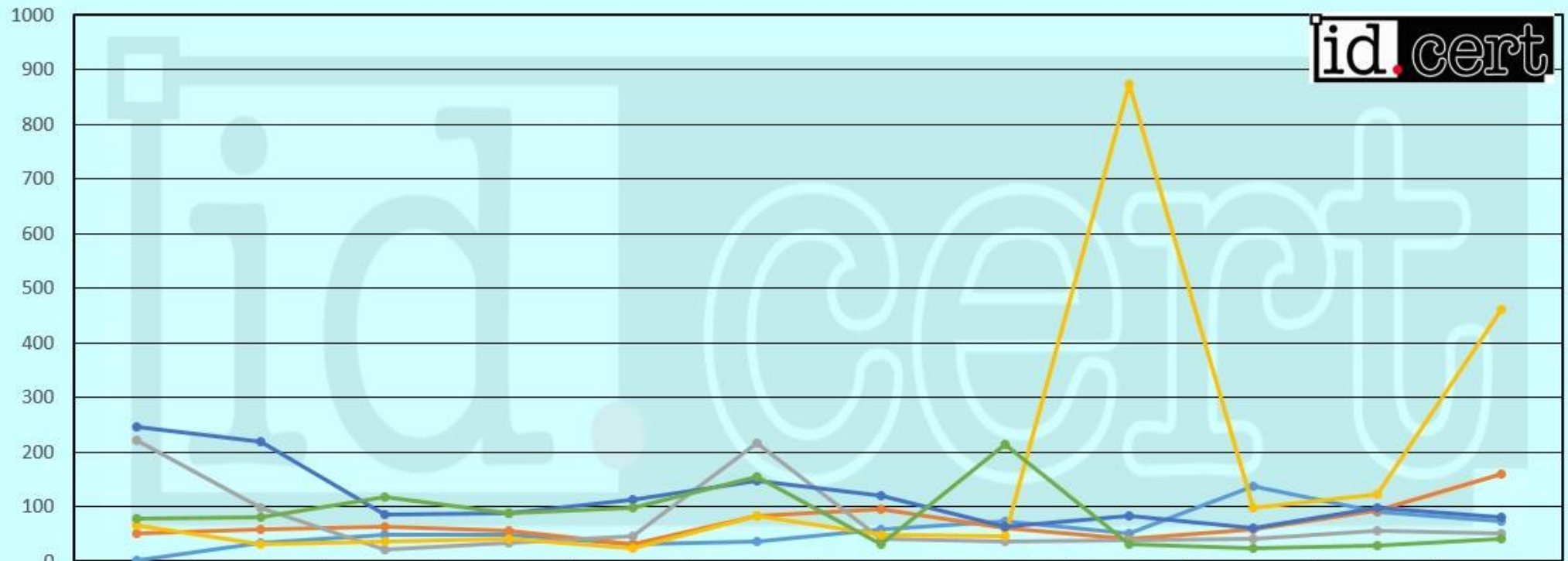
Jumlah Insiden yang direspon

Statistik Insiden yang ditangani oleh ID-CERT (2011-2016)



Jumlah Insiden Yang di Selesaikan

Statistik Insiden yang dapat diselesaikan (2011-2016)



	JANUARI	FEBRUARI	MARET	APRIL	MEI	JUNI	JULI	AGUSTUS	SEPTEMBER	OKTOBER	NOPEMBER	DESEMBER
2011	1	35	48	48	32	37	59	74	52	137	90	73
2012	50	59	64	57	32	82	95	61	42	58	93	159
2013	221	98	22	33	46	216	41	36	38	42	56	50
2014	66	31	37	40	25	83	49	45	874	98	122	462
2015	245	218	85	89	114	148	120	64	83	61	99	80
2016	79	80	118	89	98	154	32	213	31	25	30	42

Beberapa Kasus Yang Sering Diadukan

- ➔ Pembajakan akun media sosial (FB, Twitter, dsb)
- ➔ Pembajakan pengelolaan nama domain
- ➔ Deface
- ➔ Pemalsuan Situs Web/Phishing
- ➔ HaKI
- ➔ Malware
- ➔ Insiden Jaringan
- ➔ Spam

Kendala yang dihadapi atas aduan yang diterima

- ➔ Email tidak valid;
- ➔ Nomer Telpon tidak valid;
- ➔ Alamat tidak valid/berubah;
- ➔ Kontak yang ada merupakan kontak pihak ketiga yang sudah tidak valid;
- ➔ Terkait masalah Hukum;

Aktifitas

- ➔ Riset Internet Abuse Indonesia, yang dimulai sejak 2010 dan 2011
 - ➔ Sejak Maret 2012, aktifitas ini berubah nama menjadi *Incident Monitoring Report* dan bersifat permanen;
- ➔ Koordinasi dengan tim CERT regional, (seperti: Malaysia CERT, Australian CERT, Japan CERT, dsb);
- ➔ Koordinasi dengan lebih dari 1.000+ organisasi/ perusahaan asing diseluruh dunia, seperti Google, Yahoo, FB, Twitter, Wordpress, Blogspot, dsb
- ➔ Koordinasi dengan berbagai organisasi didalam negeri termasuk Kementrian (KOMINFO, KEMENPOLHUKAM, DITJEN AHU, BPPT, KEMDIKBUD, dsb), APJII, PANDI, ISP, NAP , Hosting Provider, dsb
- ➔ Membangun kesadaran publik tentang pentingnya IT Security melalui Gathering dan Seminar publik.

Kegiatan

- ➔ Partisipasi dalam APCERT Drill Februari 2012, 2013, 2014, 2015, 2016.
- ➔ Menghadiri APCERT Annual General Meeting, 25 – 27 Maret 2012, BALI.
- ➔ Membantu pembentukan Roadmap CERT/CC, Regulasi CERT dan GovCERT yang diadakan oleh DITKAMINFO.
- ➔ Menghadiri forum IISF (Indonesia Information Security Forum) 14 Desember 2011 yang diadakan oleh DITKAMINFO.

Kegiatan: ID-Malware Summit

- Rangkaian acara pertemuan tingkat tinggi pimpinan komunitas Pemerhati Malware, termasuk AV, Peneliti, Industri, Korporasi, Pemerintahan, Perbankan.
- Tema: Indonesia Darurat Malware
- Membahas tren Malware dan isu spesifik malware.
- ID-Malware Summit I: di Bandung pada 5 MEI 2015, dihadiri 110 peserta dengan 12 pembicara.
- Hasil Pembahasan: Dukungan terhadap AV lokal, Sharing sampel malware, Monitoring malware bersama.



Kegiatan: ID-Malware Summit II

- Tema: Mobile & Fileless Malware
- Lokasi di Jakarta (tentative)
- Tanggal; 30 Maret 2017 (tentative)
- Saat ini tengah dalam proses pencarian sponsor untuk kegiatan ini.

Kegiatan: Gathering ID-CERT

- Rangkaian acara pertemuan komunitas yang adakan setahun sekali dengan konstituen ID-CERT
- Membahas laporan aktifitas ID-CERT serta Tren yang tengah terjadi.
- Umpan balik aktifitas
- Pertemuan berikutnya:
 - 13 APR 2017 di Bandung (tentative).
 - Agenda: Identity Theft & Mobile Security
 - Mengundang Sponsor untuk berpartisipasi membiayai aktifitas ini.

Kegiatan ID-CERT Lainnya

Survey Malware

<http://www.cert.or.id/index-berita/id/berita/49/>

- ➔ Melakukan Survey Malware dengan menggunakan USB.
- ➔ 1. Kirim email ke daftar@malware.cert.or.id dengan keterangan nama lengkap, kota tinggal dan email anda
- ➔ 2. Tunggu konfirmasi dari admin@malware.cert.or.id atau support@malware.cert.or.id untuk verifikasi akun anda
- ➔ 3. Untuk info lebih lanjut, harap hubungi support@malware.cert.or.id atau ahmad@cert.or.id

Survey Malware: Mekanisme Pelaporan

- ➔ 1. Jalankan start.exe yang terdapat pada folder Emsisoft Emergency Kit
- ➔ 2. Pilih Emergency Kit Scanner -> Scan PC
- ➔ 3. Pilih metode scan sesuai kebutuhan (Quick Scan, Smart Scan, Deep Scan, Custom Scan)
- ➔ 4. Tekan tombol 'Scan'
- ➔ 5. Tunggu sampai scan selesai
- ➔ 6. Tekan tombol 'View Report' dan folder log akan terbuka
- ➔ 7. Kirimkan melalui email file log tersebut ke lapor@malware.cert.or.id
<<mailto:lapor@malware.cert.or.id>> (dengan attachment file log)
 - ➔ (file report tersimpan pada folder /Run/Report/.....)
- ➔ 8. Pelaporan diharapkan dapat dilakukan secara periodik (tiap 1 minggu atau 1 bulan sekali, sesuai kebutuhan)
- ➔ 9. Scan dapat dilakukan pada komputer lain dengan memakai flashdisk (copy tool ke flashdisk), namun dipastikan untuk melakukan scan pada flashdisk tersebut setelah digunakan untuk melakukan scan pada komputer, hal ini diharapkan tidak terjadi penyebaran malware melalui flashdisk tersebut

Aplikasi Event Report Tools

- ➔ Merupakan aplikasi yang dibuat untuk memudahkan *Incident Handler* dalam mengolah data *raw* data/data mentah *bulk* log yang diterimanya.
- ➔ Input: log dari multi ISP / IP Address Indonesia, 1 file log sekitar 70 ribu baris setiap hari.
- ➔ Proses: melakukan pengelompokan berdasarkan IP Address atau AS Number untuk selanjutnya dapat dikirim ke ISP terkait.
- ➔ Output: PDF atau CSV untuk masing-masing ISP yang dituju.

AndroScan

- ➡ Aplikasi yang dibuat untuk mengecek apakah .APK mengandung malware atau tidak?
- ➡ Pengecekan dapat dilakukan secara online

Wiki Malware

- ➔ Membuat eBook tentang Malware
- ➔ Diinisiasi oleh Pak Budi Rahardjo bersama Pak Setia Juli Irzal

Review Antivirus

- ➔ Beberapa vendor Antivirus lokal menginginkan agar ID-CERT dapat melakukan review terhadap produk mereka.
- ➔ Diperlukan SOP dan mekanisme review

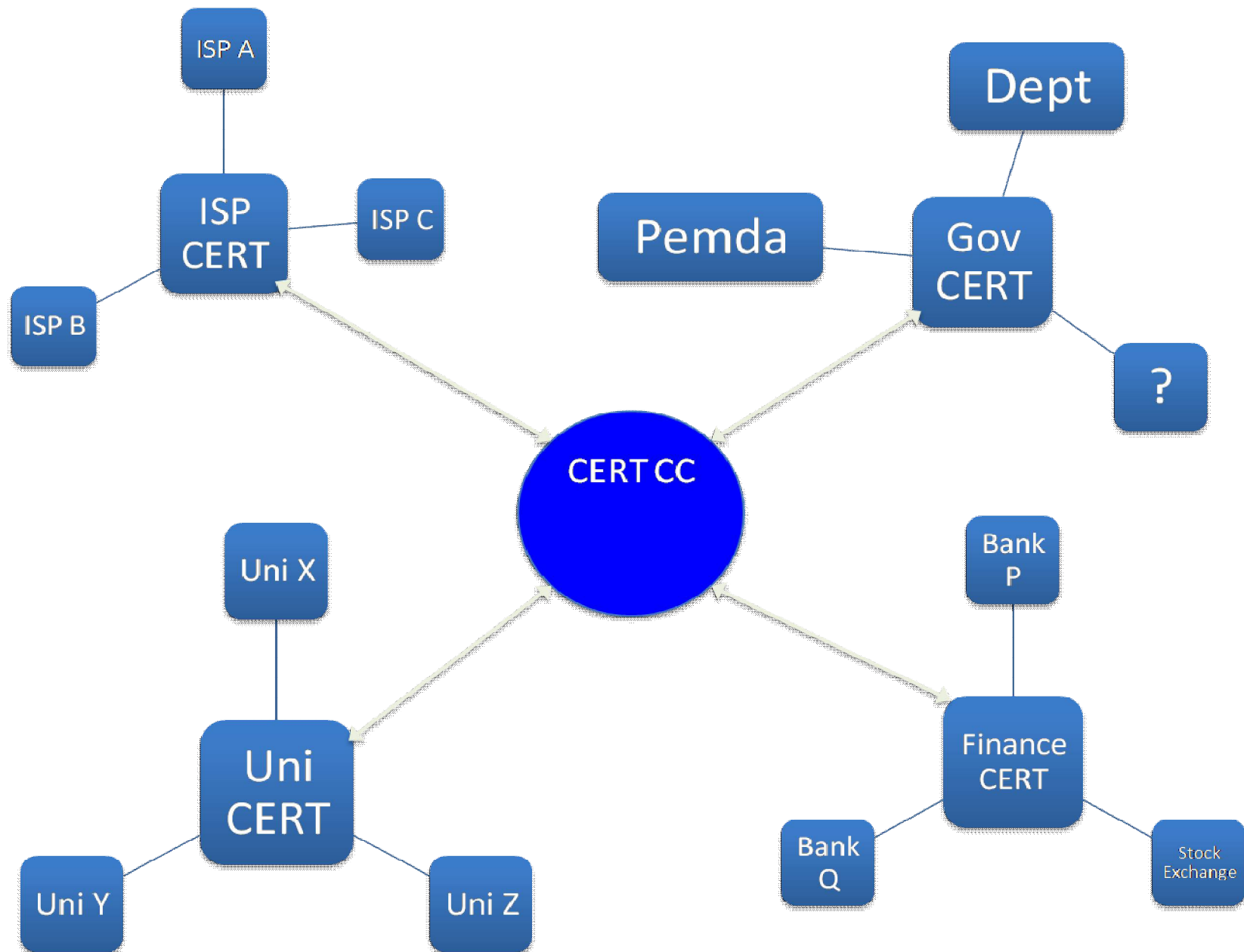
Layanan ID-CERT

- ➔ 21 Desember 2011: ID-CERT mulai mengirimkan feed/**berita harian** tentang **situs pemerintah** yang terkena aksi Deface/Phishing.
- ➔ 01 Juni 2012: ID-CERT meluncurkan Nomor kontak Desk **0889-1400-700**.
- ➔ Nopember 2013: Penerbitan Security Advisory dalam format “resmi”.
- ➔ Kerjasama Penanganan Insiden dengan PANDI
- ➔ Kerjasama Penanganan Insiden dengan APJII

CERT/CSIRT di Indonesia

<http://cert.id/index-berita/id/berita/65/>

- ID-CERT (1998), sektor umum dan berbasis aduan;
www.cert.or.id
- ID-SIRTII (2007), berbasis monitoring log dan memberikan bukti Digital bila diminta penegak hukum;
www.idsirtii.or.id
- Acad-CSIRT (2010), sektor Akademik, berbasis aduan;
<http://www.acad-csirt.or.id/>
- GovCSIRT / KAMINFO (2012), sektor Pemerintahan, berbasis aduan dan Monitoring log.
[Http://www.govcsirt.go.id/](http://www.govcsirt.go.id/)
- CSIRT BPPT, 2014, sektor terbatas dibawah BPPT
<https://csirt.bppt.go.id/>

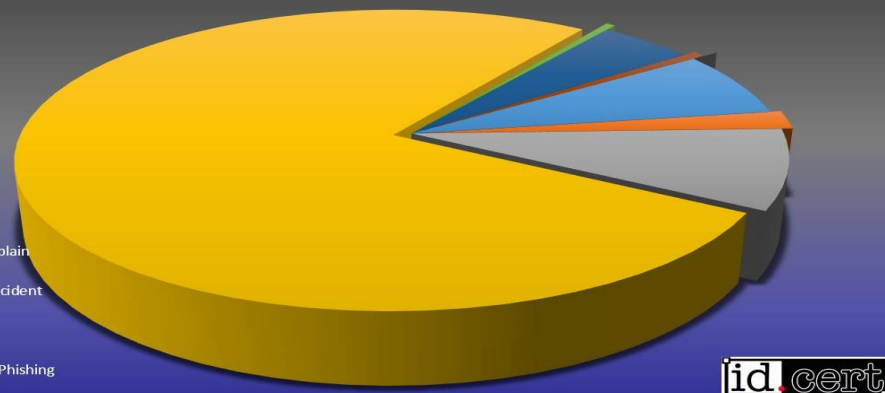


Layanan ID-CERT

- Incident Handling
- Incident Monitoring Report (IMR)
- Peringatan Keamanan

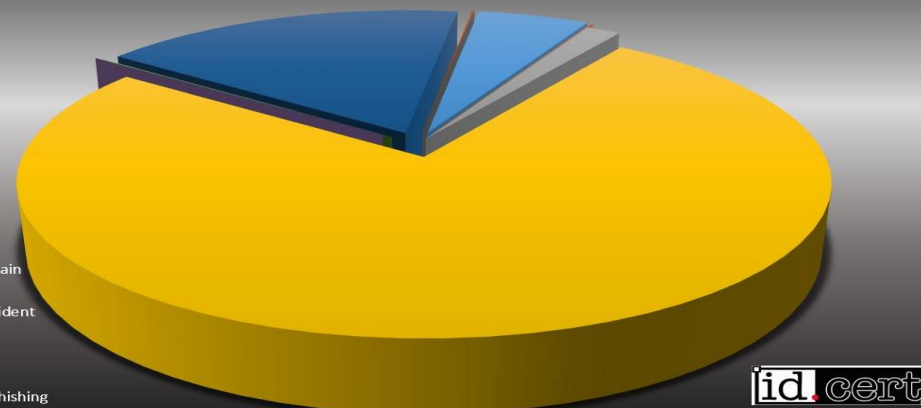
Insiden tahun 2012

IPR
Spam Komplain
Malware
Network Incident
Resolved
Respon
Spam
Spoofing / Phishing
Fraud
LAIN-LAIN



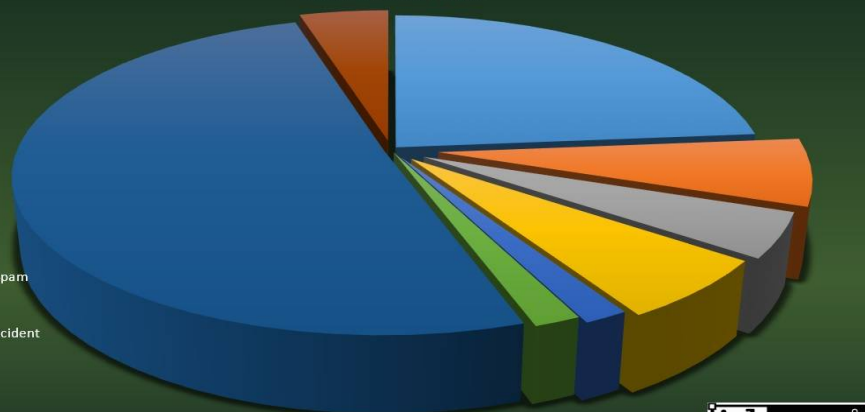
Total Insiden tahun 2011

IPR
Spam Komplain
Malware
Network Incident
Resolved
Respon
Spam
Spoofing / Phishing
Fraud



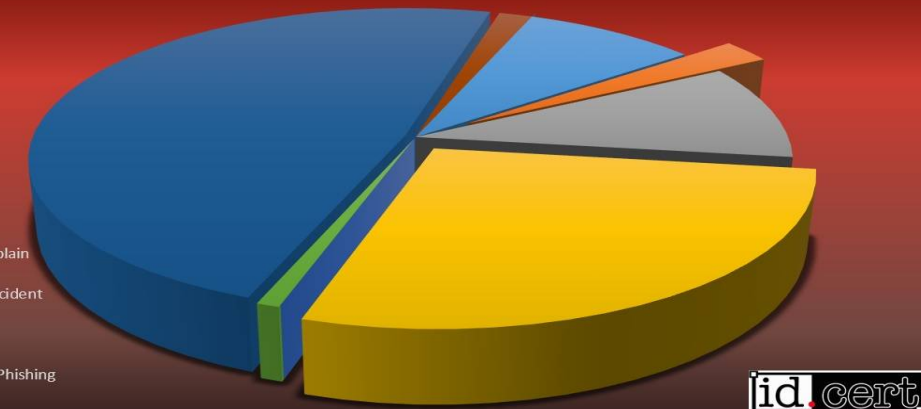
Insiden tahun 2014

IPR
Komplain Spam
Malware
Network Incident
Resolved
Respon
Spam
Spoofing/Phishing



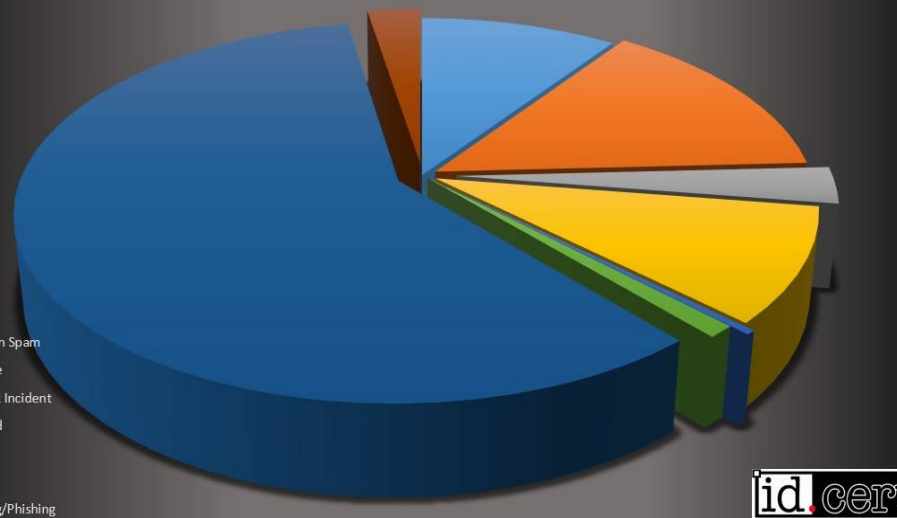
Insiden tahun 2013

IPR
Spam Komplain
Malware
Network Incident
Resolved
Respon
Spam
Spoofing / Phishing
Fraud
LAIN-LAIN



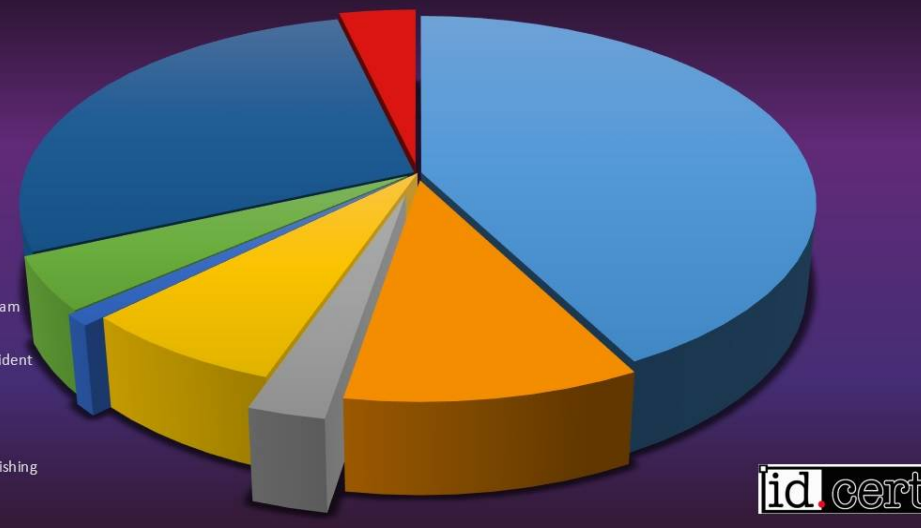
Insiden tahun 2016

IPR
Komplain Spam
Malware
Network Incident
Resolved
Respon
Spam
Spoofing/Phishing



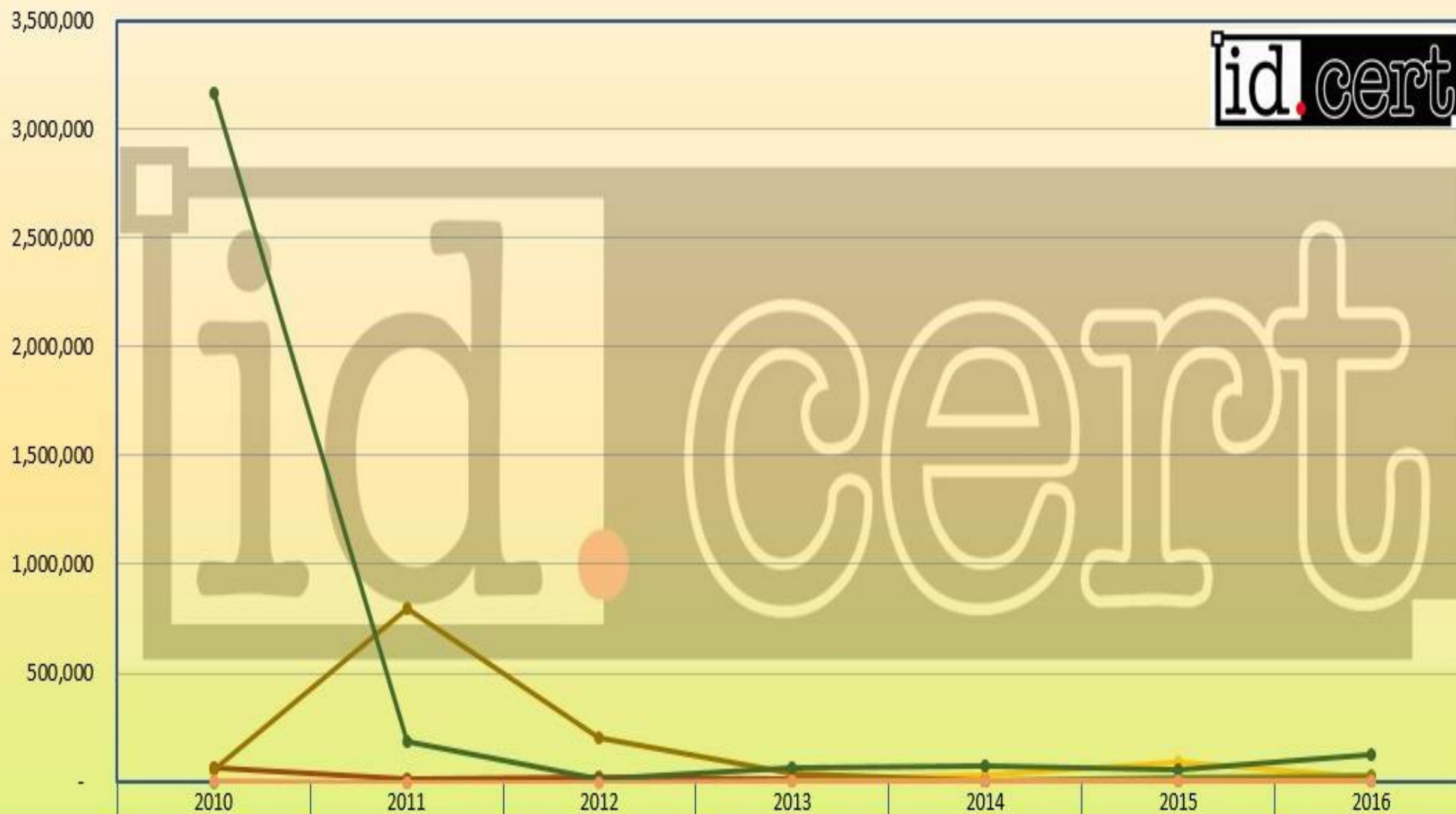
Insiden tahun 2015

IPR
Komplain Spam
Malware
Network Incident
Resolved
Respon
Spam
Spoofing/Phishing
Fraud
Lain-lain



TOTAL INSIDEN TAHUNAN 2010 - 2016

id.cert



IPR			18,538	11,606	33,912	88,098	20,728
Komplain Spam	287	352	5,146	3,335	9,790	21,553	30,734
Malware	68,059	17,168	22,894	13,426	6,568	5,624	6,644
Network Incident	60,617	797,712	202,963	37,071	9,048	15,218	20,868
Spam	3,164,133	183,932	12,672	64,514	72,874	58,337	124,838
Spoofing/Phishing	1,807	1,111	1,686	2,204	6,541	7,677	5,637

Information For**Control System Users**

Information for industrial control systems owners, operators, and vendors.

Government Users

Resources for information sharing and collaboration among government agencies.

Home and Business

Information for system administrators and technical users about latest threats.

GRIZZLY STEPPE – Russian Malicious Cyber Activity

Original release date: December 29, 2016



Overview

On October 7, 2016, the Department Of Homeland Security (DHS) and the Office of the Director of National Intelligence (DNI) issued a [joint statement](#) on election security compromises. DHS has released a Joint Analysis Report (JAR) attributing those compromises to Russian malicious cyber activity, designated as GRIZZLY STEPPE.

The JAR package offers technical details regarding the tools and infrastructure used by Russian civilian and military intelligence services (RIS). Accompanying CSV and STIX format files of the indicators are available here:

- [GRIZZLY STEPPE Indicators \(CSV\)](#)
- [GRIZZLY STEPPE Indicators \(STIX xml\)](#)

DHS recommends that network administrators review [JAR-16-20296.pdf](#) below for more information and implement the recommendations provided.

Revisions

- December 29, 2016: Initial release
- December 29, 2016: Updated CSV and STIX xml files with additional indicators
- December 29, 2016: Replaced JAR-16-20296 with JAR-16-20296A, which contains corrected NCCIC contact information

View Publication



[JAR_16-20296A_GRIZZLY STEPPE-2016-1229.pdf](#)

Malware Penyandera/Ransomware


<http://www.cnnindonesia.com/teknologi/20150123074005-185-26742/malware-penyandera-komputer-beredar-di-indonesia/>

- ➔ Eksensi: .SCR
- ➔ Media: Attachment email
- ➔ Meminta tebusan melalui rekening di Bitcoin
- ➔ Saran keamanan:
 - Lakukan Backup data secara rutin
 - Jangan membuka attachment yang tidak dikenal

Info Lowongan Kerja Bank Dana...

lokerkita.com/info-lowongan-kerja-bank-danamon-terbaru-mei-2014/

bank yang pertama memelopori pertukaran mata uang asing di tahun 1976 dan sahamnya tercatat di bursa sejak tahun 1989.



Lowongan Kerja Bank Danamon

Di akhir bulan Mei 2014 ini Bank Danamon membuka lowongan kerja bagi tenaga kerja terbaik untuk menempati posisi sebagai :

Officer Development Program Trainee – Transaction Banking

Persyaratan :

1. S1 dari segala jurusan
2. IPK minimal 2,75
3. Usia maksimum 28
4. Lulusan baru atau profesional dari bidang terkait (maksimal 2 tahun pengalaman kerja)
5. Bersedia untuk melakukan perjalanan
6. Baik kemampuan analisis dan pemecahan masalah
7. Baik penulisan laporan dan presentasi keterampilan
8. Baik tingkat kemampuan bahasa Inggris (lisan) lebih disukai

Ketentuan Melamar Lowongan Kerja Bank Danamon
Jika Anda tertarik dan memenuhi persyaratan diatas, silahkan mengirimkan lamaran kerja dan CV lengkap ke alamat :

PT. Bank Danamon Indonesia
Jl. Panglima Sudirman 11-17,
Surabaya 60271 Jawa Timur

atau melalui email :
heru.ramlan@danamon.co.id / sony.febrian@danamon.co.id

Lowongan ditutup 30 Mei 2014.

Pura Support Mei 2014

- Info Loker Bogor Terbaru PT Duta Cendana Adimandiri Juni 2014
- Loker SMA SMK BUMN Januari 2014 PT. Pertamina Retail
- Lowongan Kerja Bekasi Terbaru Juni 2014

Lowongan Kerja Terbaru

- Lowongan Kerja Ganut Terbaru PT Jasamedika Saranatama
- Info Loker Bank Tebaru Juni 2014 Bank Danamon
- Info Loker Depok Terbaru PT Pro Car International Juni 2014
- Info Loker BUMN Terbaru PT Pertamina Hulu Energi Juni 2014
- Info Loker Cirebon Terbaru Juni 2014 Eva Group Hotel Management

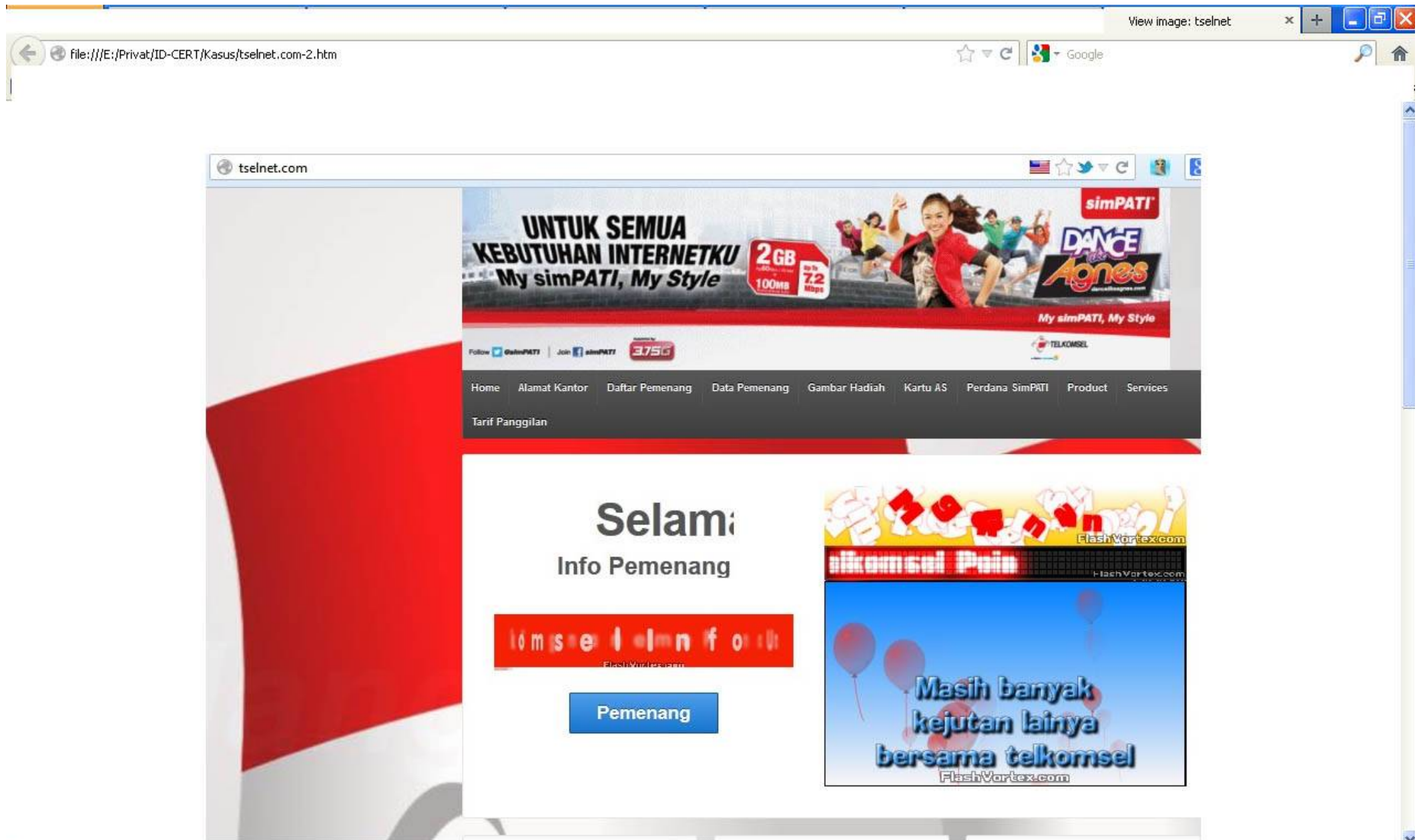
Loker Berdasarkan Lulusan

- Lowongan Kerja SMA SMU Terbaru
- Lowongan Kerja SMK Terbaru
- Lowongan Kerja D1 Terbaru
- Lowongan Kerja D3 Terbaru
- Lowongan Kerja S1 Terbaru
- Lowongan Kerja S2 Terbaru

Lowongan Kerja BUMN

- Lowongan Kerja Pertamina Terbaru
- Lowongan Kerja PLN Terbaru
- Lowongan Kerja Telkom Terbaru
- Lowongan Kerja Garuda Indonesia

Advertisements



Firefox XL Axiata: Cara Pengambilan Hadiah x New Tab

www.gebyar-xlaxiata.blogspot.com/p/blog-page_3058.html
















https://www.faceboo... Most Visited Maahir Al-Mu'ayqali Beasiswa Unggulan Alkazimy's-Family Mail ... Koneksikita.com Mail - ... Grant Recipients APNIC - Query the AP... Welcome to Korean Air >> Bookmarks

Selamat Bagi Pelanggan yang telah terpilih sebagai Pemenang Kami.
Tata Cara pengambilan Hadiah :

1. Pemenang bisa datang langsung di Kantor Kami untuk mengambil langsung hadiahnya (tidak boleh diwakili), sekaligus menandatangani SURAT SERAH TERIMA HADIAH dari kantor kami.
2. Hadiah Anda bisa kami antarkan langsung ke alamat melalui Jasa Penerbangan, dengan menggunakan Pesawat Kargo / Hercules menuju ke Bandara atau Lapangan Penerbangan yang terdekat di daerah Anda. Selanjutnya Kami antarkan langsung ke Alamat lengkap Anda.
3. Batas pengambilan Hadiah tergantung dari keputusan kami. Apabila Pemenang tidak mengurus Hadiah sampai batas pengambilan yang sudah kami tentukan, maka Hadiah akan dialihkan pada kandidat pemenang yang lain, dan kewajiban Kami kepada pemenang sudah tidak ada.
4. Syarat & ketentuan berlaku.

Untuk Melaporkan Alamat dan Identitas Anda, Silahkan Hubungi Nomor Pelayanan Kantor Kami.

Atas nama Bpk. Drs. H. HERIANTO
Contact Center: 0819-9836-8333



Adapun ke 34 situs yang teridentifikasi oleh Vaksincom sebagai toko online palsu adalah sebagai berikut:

1. <http://allsalam-elektronik.hourb.com/>
2. <http://andika77shop.blogspot.com/>
3. <http://anitaphoneshop.com/> (lihat gambar 2)



Gambar 2: Anita Phoneshop situs onlineshop fiktif

4. <http://anugerahelektronik.com/page/10/>
5. <http://aulaelectroshop.com>
6. <http://batamzentralelektronik.com/>
7. <http://batarashoping.com/>
8. <http://graha-shop.com/page/11/>

TOKO LAZADA 07

Saatnya Berbelanja Online Dgn Aman.
Hanya Di Toko Lazada 07.
Murah dan Terpercaya Se-Indonesia

[HOME](#)[POSTS RSS](#)[COMMENTS RSS](#)[EDIT](#)

MENU HANDPHONE

BlackBerry
Nokia
Samsung HP
Sony Ericsson
Apple Iphone
Apple Ipad
Sony Xperia
Motorola
Huawei
LG HP
HTC HP

LAPTOP & NOTEBOOK

ASUS
ACER
TOSHIBA
SONY VAIO
DELL
LAPTOP HO
APPLE LAPTOP

PRODUCK TERLARIS

BlackBerry Z10 Rp.3,9jt

CARA ORDER BARANG VIA SMS SILAKAN KETIK FORMAT DI BAWA INI :

Nama Lengkap # Alamat Lengkap # Nama Barang # Type Barang # Warna Barang #
No.Hp.Anda # Kota Tujuan # Kode Pos # Jumlah Pesanan # Bank Pembayaran #
Kirim melalui sms ke: **089-6013-222-02**
Kemudian tunggu sms konfirmasi Rekening Pembayaran dari kami.

INFORMASI

TENGTTANG KAMI
CARA PEMBAYARAN
JAMINAN GARANSI
SYARAT DAN KONDISI



--- Hotline 24 jam ---

089-6013-222-02

JL.lintas timur NO.757
pangkalan kerinci PROVINSI
riau pekan baru

Rek Pembayaran

PEMBAYARAN
DITRANSFER KE Rek:



TRANSAKSI PENGIRIMAN BARANG DAN PEMBAYARAN :

1). Barang dapat kami kirim melalui TIKI JNE untuk pembeli yg diluar daerah,

Sektor di Indonesia yang pernah diadukan - Phishing

- ➔ Operator Telekomunikasi
- ➔ Perbankan
- ➔ Universitas/Sekolah/Madrasah/Pendidikan
- ➔ Penerbangan
- ➔ Korporat
- ➔ Pemerintahan

PERINGATAN KEAMANAN:

Kelemahan Joomla

<http://www.cert.or.id/index-berita/id/berita/16/>

- ➔ Pada 22 Des 2012, ID-CERT kembali mendapatkan informasi dari NCCIC tentang adanya kelemahan sistem yang melibatkan sejumlah IP Address Indonesia. Sebelumnya, pada 14 Desember yang lalu, ID-CERT juga telah menerima laporan tentang hal yang sama.
- ➔ Sejak Agustus 2012, sejumlah situs terkontaminasi dan digunakan untuk menyimpan dan melakukan Distributed Denial of Service (DDoS).
- ➔ Kelemahan pada Joomla versi 1.6 hingga 2.5.4 telah teridentifikasi dan telah digunakan untuk menyerang
- ➔ Solusi:

Developer.joomla.org/security/news/470-20120601-core-privilege-escalation.html

Developer.joomla.org/security/news/395-20120303-core-privilege-escalation.html

PERINGATAN KEAMANAN: OpenSSL Heartbleed

<http://www.cert.or.id/index-berita/id/berita/47/>

- ➔ Pada 13 APRIL 2014: ID-CERT menerima informasi dari sumber yang valid mengenai kerentanan yang ada pada versi OpenSSL 1.0.1 hingga 1.0.1f yang dapat mengungkapkan informasi sensitif milik pengguna ke penyerang .
- ➔ Dampak dari kerentanan ini adalah remote , penyerang yang tidak berkepentingan mungkin dapat mengambil informasi sensitif , seperti kunci rahasia . Dengan menggunakan informasi sensitif , penyerang mungkin dapat mendekripsi , spoof , atau melakukan serangan man-in- the-middle pada lalu lintas jaringan yang seharusnya dapat dilindungi oleh OpenSSL .
- ➔ Solusi:
 - a. Menerapkan update
 - b. Nonaktifkan dukungan detak jantung OpenSSL
 - c. Rekomendasi lain adalah untuk mengkompilasi ulang OpenSSL dengan -DOPENSSL_NO_HEARTBEATS FLAG .

Peringatan Keamanan Tentang **BASH**

<http://www.cert.or.id/index-berita/id/berita/50/>

- ➔ 25 SEP 2014, ID-CERT menerima informasi tentang adanya kelemahan pada Bash.
- ➔ Dampak: menjalankan kode / Perintah remote / Unauthenticated / Akses tidak sah - dari akun yang ada
- ➔ Resolusi: Patch / upgrade

PERINGATAN KEAMANAN I: Malware ZEUS

- ➔ **Juli 2007:** Virus ini pertama kali teridentifikasi saat digunakan mencuri informasi dari Departemen Transportasi Amerika Serikat.
- ➔ **Mar 2009:** virus ini makin tersebar.
- ➔ **Juni 2009,** perusahaan keamanan Prevx menemukan bahwa Zeus telah menembus lebih dari **74,000 akun FTP**
- ➔ **1 Oktober 2009,** FBI mengumumkan bahwa telah ditemukan satu jaringan/network besar cyber crime internasional yang telah menggunakan Zeus to untuk meng-hack komputer2 di Amerika Serikat.
- ➔ **Oktober 2011** versi terbaru source code Zeus bocor. blog abuse.ch melaporkan mengenai satu trojan baru yang telah dikostumasi yang mengandalkan pada kemampuan peer-to-peer yang lebih canggih.
- ➔ **April 2012** versi terbaru Malware Zeus teridentifikasi menyerang Indonesia.
- ➔ Contoh-contohnya termasuk **otorisasi login** untuk online **social network, e-mail account, online banking** atau **layanan keuangan online lainnya**.
- ➔ Situs-situs yang tercuri otorisasi loginnya, menurut laporan Netwitness adalah Facebook, Yahoo, Hi5, Metroflog, Sonico dan Netlog.

Tips bagi Pengguna

- ➔ Cek URL situs tersebut disitus Antivirus
- ➔ Ciri-ciri situs palsu:
 - ➔ Menggunakan nama domain di tempat hosting gratis
 - ➔ Mencantumkan kontak personal untuk komunikasi
 - ➔ Mencantumkan nomor telpon pribadi
 - ➔ Mencantuman email gratisan dan atasnama pribadi
- ➔ Selalu mengunjungi situs asli untuk mendapatkan informasi mengenai program tertentu atau dapat menghubungi Call Center resmi Operator/Bank/Perusahaan tersebut.

Tips bagi Instansi

- ➔ Segera laporkan situs palsu yang dijumpai kepada ID-CERT (email pengirim harus email resmi instansi).
- ➔ Sangat disarankan pihak instansi ybs juga melaporkan masalah ini kepada Penegak Hukum;
 - ➔ Beberapa ISP/hosting kerap meminta surat dari penegak hukum sebagai dasar untuk menutup situs/aktifitas ilegal tersebut.
- ➔ Berkolaborasi dengan CERT/CSIRT untuk memudahkan kontak dimasa yang akan datang.

Tips di Media Sosial

- ➔ Pentingnya menjaga kredensial yang ada
 - ➔ Email
 - ➔ User Media Sosial
- ➔ Hal-hal yang perlu diperhatikan dalam proses pemulihan akun di Media Sosial:
 - ➔ Pastikan email tidak ikut dibajak
 - ➔ Bila email terbajak, maka pulihkan terlebih dahulu akun email
 - ➔ Umumnya Media Sosial memiliki tahapan untuk proses pemulihan akun terbajak.
- ➔ Bila Media Sosial digunakan untuk kepentingan yang serius, seperti perdagangan atau sosialisasi program pemerintah, maka sebaiknya akun yang didaftarkan di Media Sosial adalah akun email organisasi/instansi pemerintahan:
 - ➔ Memotong jalur pemulihan email, karena server email ada pada organisasi/instansi pemerintah.
- ➔ Pentingnya menjaga Prilaku ---> Terkait UU ITE
 - ➔ Misal: jangan update status ketika sedang marah.

READING ROOM: Saran Keamanan

- ➔ 1. Lakukan pemeriksaan kesehatan sistem, misal dengan menggunakan Antivirus untuk memastikan bahwa sistem anda tidak disusupi Malware.
- ➔ 2. Tempatkan seluruh aset sistem kontrol dibelakang firewall, terpisah dari jaringan yang digunakan untuk bisnis.
- ➔ 3. Membangun metode remote akses yang aman, seperti penggunaan Virtual Private Networks (VPN) untuk remote akses.
- ➔ 4. Singkirkan, disable atau rename seluruh akun system default (bila memungkinkan)
- ➔ 5. Implementasikan aturan penguncian akun untuk menghindari upaya coba-coba misal melalui brute force.
- ➔ 6. Implementasikan aturan penggunaan password yang kuat.
- ➔ 7. Lakukan pemantauan pembuatan akun administrator oleh pihak ketiga/vendor.

Reading Room

- Peringatan Keamanan 5-2012 tentang Kerentanan Sistem:
http://www.cert.or.id/index_berita/berita/15/
- Peringatan Keamanan 4-2012 tentang Celah Keamanan Joomla
http://www.cert.or.id/index_berita/berita/13/
- Peringatan Keamanan 3-2012 tentang Saran Pengamanan Sistem
http://www.cert.or.id/index_berita/berita/11/
- Peringatan Keamanan 2-2012 tentang Malware Grumbot
http://www.cert.or.id/index_berita/berita/8/
- Peringatan Keamanan 1-2012 tentang Malware Zeus dan target yang dicari:
http://www.cert.or.id/index_berita/berita/5/
- DNS Changer https://www.hkcert.org/my_url/en/blog/12022901
- Malware Zeus http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29
- Penelitian dan Incident Handling Report ID-CERT:
http://www.cert.or.id/incident_handling/

READING ROOM: cara melapor ke ID-CERT

- ➔ Konsultasikan dengan ID-CERT melalui email: cert@cert.or.id (sangat direkomendasikan via email) atau telpon di **0889-1400-700**;
- ➔ Sertakan informasi penting terkait hal yang diadukan, seperti:
 - ➔ **Log file**
 - ➔ **URL / Link bermasalah?**
 - ➔ **Surat Keterangan** dari instansi (untuk situs palsu)
- ➔ Bila merupakan masalah hukum atau lainnya, ID-CERT akan mengarahkan/mengkonsultasikannya kepada pihak yang tepat.

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

MedSos:

FanPage FB: IDCERT