Laporan Dwi Bulan I 2013

ID-CERT[1]

Ringkasan
Pada laporan Dua Bulan I Tahun 2013 ini disajikan hasil pengumpulan pengaduan selama dua bulan, Januari dan Februari 2013. Pelaporan tsb. diterima dalam bentuk email dan dikumpulkan sesuai kategori, sebagai bahan penyusunan statistik, dalam bentuk angka dan grafik. *Spam*, komplain *spam*, respon, *network incident*, Hak atas Kekayaan Intelektual, *fraud*, *spoofing*/*phising*, dan *malware* merupakan kategori yang dipilih untuk pengelompokan pengaduan yang masuk.

Kata kunci
Security – Pelaporan – Laporan Dwi Bulan

[1] *Diterbitkan 28 Apri 2013*

Daftar Isi

1. Pendahuluan

Internet menjadi bagian penting kegiatan sehari-hari dengan pemakaian meluas pada banyak aspek. Salah satu bagian penting yang perlu diperhatikan oleh pengguna adalah aspek keamanan Internet atau *Internet security*. Dengan kian banyak pengguna Internet dari berbagai lapisan dan latar belakang, mendengarkan peristiwa di lapangan, memahami laporan yang disampaikan, menelaah fenomena, dan menindaklanjuti kejadian tsb. menjadi sebagian dari aspek yang perlu dikerjakan secara khusus.

Laporan ini disusun sebagai paparan gambaran insiden keamanan (*security incident*) yang terjadi dalam kurun waktu dua bulan, Januari dan Februari 2013. Tujuan lain penyediaan laporan ini adalah sebagai contoh data primer keamanan teknologi informasi (TI) di Indonesia.

Perlu ditekankan pentingnya menindaklanjuti laporan tentang penyalahgunaan Internet (*Internet abuse*) sebagai respon positif dan langkah perbaikan keadaan. Hal ini juga tidak lepas dari interaksi yang sehat antara kita sebagai satu bangsa dengan pihak-pihak dari mancanegara perihal penanganan pelaporan. Pengaduan yang datang memberi gambaran bagian-bagian yang perlu diperbaiki, keterkaitan antarlembaga, dan dapat dijadikan awal dari rencana ke depan.

Hal yang menarik pada Laporan Dwi Bulanan I 2013 ini adalah jumlah laporan pengaduan *network incident* yang

sangat banyak. Disebut "sangat banyak" karena jumlah laporan *network incident* mencapai 72% dari keseluruhan laporan, sehingga boleh dikatakan periode Dwi Bulan I 2013 ini adalah "bulan-bulan *network incident*". Penjelasan tentang perkembangan *network incident* dalam dua bulan dan jenis gangguan ini diangkat di bagian Uraian.

Pada penelitian ini, data diambil dari tiga puluh tujuh (37) responden yang terdiri dari: Kominfo, ID-CERT, PANDI, Detik.net, Zone-h dan Anti Fraud Command Center (AFCC), tiga operator telekomunikasi, tujuh NAP, dan 22 Penyedia Jasa Interenet (PJI/ISP).

Statistik ini juga mendapat dukungan sponsor dari Pengelola Nama Domain Internet Indonesia (PANDI) dan Asosiasi Penyedia Jasa Internet Indonesia (APJII).

2. Metoda Penelitian

Laporan ini disusun dari beberapa sumber dalam bentuk laporan dengan melalui metoda-metoda berikut ini.

Metodologi yang digunakan pada penelitian ini:

1. Pengambilan data dari sejumlah responden.
2. Analisis berdasarkan:
   (a) Tembusan laporan yang masuk lewat alamat email pengaduan penyalahgunaan (*abuse*) PJI/operator telekomunikasi/lembaga non-ISP.
   (b) Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi yang dimaksud berupa data yang telah dihitung dan dikelompokkan oleh responden.

Dari laporan yang diterima, dilakukan pengelompokan sbb.:

Fraud Penipuan disengaja yang dibuat untuk keuntungan pribadi atau untuk merugikan individu lain[1].

Hak atas Kekayaan Intelektual Pengaduan tentang pelanggaran terhadap hasil karya yang terkait Undang Undang Hak atas Kekayaan Intelektual (HaKI) atau *Intellectual Property Rights* (IPR).

Komplain Spam Keluhan/pengaduan email *spam* dari dalam negeri terhadap jaringan di Indonesia dan luar negeri.

Lain-lain Laporan penyalahgunaan selain yang termasuk pada kategori di atas.

Malware Sebuah program komputer yang dibuat dengan maksud jahat.

Network Incident Aktivitas yang dilakukan terhadap jaringan milik orang lain dan semua aktivitas terkait dengan penyalahgunaan jaringan.

Respon Respon terhadap laporan yang masuk.

Spam Penggunaan sistem pengelolaan pesan elektronik untuk mengirim pesan-pesan tidak-diharapkan dalam jumlah banyak, terutama untuk pengiklanan, tanpa pilih-pilih[2].

Spoofing/Phishing Pemalsuan email dan situs untuk menipu pengguna.

3. Uraian perhitungan pelaporan

Dari email pengaduan yang diterima, dikumpulkan berdasarkan topik dan dicacah berdasarkan bulan. Hasil perhitungan tsb. disajikan dalam bentuk grafik batang dalam dua kelompok, Januari dan Februari 2013. Sebelum dibahas per topik, pada Gambar 1 di bawah ini ditampilkan keseluruhan laporan yang diterima.

Terlihat di sini bahwa empat besar laporan pengaduan yang masuk adalah: *network incident*, *malware*, *spam*, dan *Intellectual Property Rights*. Tiga sisanya, yaitu komplain tentang *spam*, *spoof*, dan respon, sangat sedikit sehingga tidak tergambarkan dengan baik pada diagram di Gambar 1.

3.1 *Network Incident* yang Mencolok

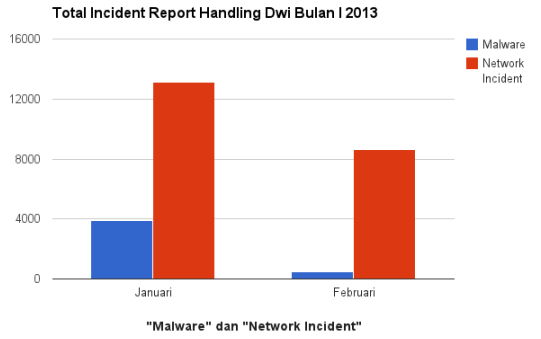
Network incident masih menempati posisi terbanyak, berjumlah total hingga 21.000-lebih email yang diterima.

[1] *Fraud*, `http://en.wikipedia.org/wiki/Fraud`

[2] *Spam (electronic)*, `http://en.wikipedia.org/wiki/Spam_(electronic)`

Gambar 1. Keseluruhan laporan yang diterima

Dari pengaduan, kejadian paling banyak berupa gangguan ke Postfix, salah satu produk server email. Laporan gangguan terbanyak ini berasal dari satu sumber di mancanegara dan ditujukan pada satu Penyedia Jasa Internet (PJI/ISP) di sini. Alamat IP yang dilaporkan berubah beberapa kali, sehingga kemungkinan besar insiden ini diawali dari komputer klien PJI tsb.



Gambar 2. *Malware* dan *network incident*

Kendati terjadi penurunan di bulan Februari, jumlah laporan *network incident* setelah penurunan tsb. tetap lebih tinggi dibanding masalah lain yang dilaporkan. Dari Januari ke Februari, *network incident* berkurang 34,12% dan malware berkurang 87,9% (Gambar 2). Tampak jelas pada grafik keseluruhan (Gambar 1): *network incident* seperti "menenggelamkan" topik aduan lain dari sisi jumlah.

Pada Gambar 3 ditampilkan contoh email pengaduan *network incident*, dihasilkan secara otomatis oleh sistem dan dikirimkan ke PJI yang menangani asal gangguan.

Network incident menempati peringkat pertama dengan

Hello Abuse-Team,

your Server with the IP: 202.[redacted] has attacked one of our server on the service:
"postfix" on Time: Thu, 31 Jan 2013 17:34:53 +0100
The IP was automatically blocked for more than 10 minutes. To block an IP, it needs
3 failed Logins, one match for "invalid user" or a 5xx-Error-Code (eg. Blacklist)!

Please check the machine behind the IP 202.[redacted] (unknown) and fix the problem.

real-time data for this day available at:

http://support.clean-mx.de/clean-mx/publog?ip=202.[redacted]

You can parse this Mail with X-ARF-Tools (1. attachment = Details, 2. attachment = Logs).
You found more Information about X-Arf under http://www.x-arf.org/specification.html

If you have a special x-arf email contact, please drop us a note.

In the attachment of this mail you can find the original protocols of our systems.

yours

[redacted]
(Geschaeftsfuehrer)

[redacted]

[redacted]

Gambar 3. Contoh pengaduan *network incident* lewat email

jumlah pelaporan hingga 72%, angka yang sangat tinggi, bahkan terhadap kategori kedua laporan, yakni *malware*, 14%. Dengan demikian bulan Januari dan Februari 2013 adalah "bulan-bulan *network incident*" jika dilihat dari laporan yang diterima.

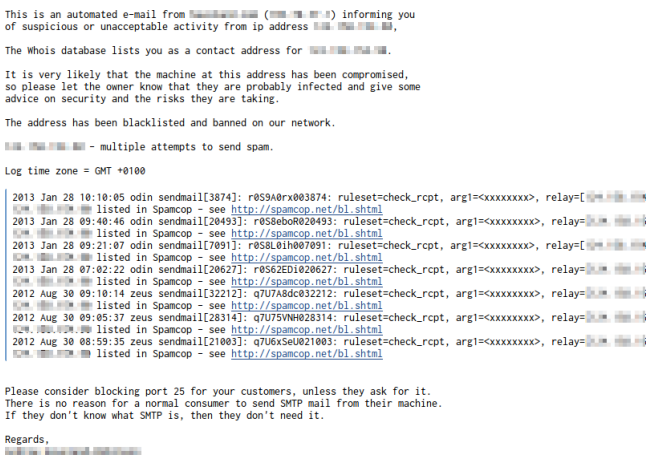
3.2 *Malware* gangguan kedua

Cukup jauh di bawah *network incident*, *malware* berada pada peringkat kedua dalam hal jumlah laporan yang masuk, sekitar 4.200. Seperti halnya *network incident*, terjadi penurunan jumlah laporan *malware* pada bulan Februari secara drastis, menjadi hanya 12% dari jumlah laporan bulan Januari. Menarik dicermati bahwa sekitar 3.300 laporan yang masuk – atau sekitar 78% – berisi laporan tentang Grum botnet, yang dijelaskan di Wikipedia sebagai [3]

> **Grum botnet**, juga dikenal dengan aliasnya Tedroo dan Reddyb, adalah *botnet* yang banyak berperan dalam mengirimkan email *spam* produk farmasi. Pernah sekali menjadi *botnet* terbesar di dunia, Grum dapat dilacak kembali pada awal 2008. Grum dilaporkan bertanggung jawab pada 18% lalu-lintas *spam* dunia, saat dihentikan pada 19 Juli 2012.

Contoh email pengaduan *malware* ditunjukkan di Gambar 4.

[3] Grum *botnet*, `http://en.wikipedia.org/w/index.php?title=Grum_botnet&oldid=545960797`



This is an automated e-mail from [redacted] ([redacted]) informing you
of suspicious or unacceptable activity from ip address [redacted],

The Whois database lists you as a contact address for [redacted].

It is very likely that the machine at this address has been compromised,
so please let the owner know that they are probably infected and give some
advice on security and the risks they are taking.

The address has been blacklisted and banned on our network.

[redacted] - multiple attempts to send spam.

Log time zone = GMT +0100

2013 Jan 28 10:10:05 odin sendmail[3874]: r0S9A0rx003874: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=[
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2013 Jan 28 09:40:46 odin sendmail[20493]: r0S8eboR020493: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2013 Jan 28 09:21:07 odin sendmail[7091]: r0S8L0ih007091: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=[
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2013 Jan 28 07:02:22 odin sendmail[20627]: r0S62ED1020627: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2012 Aug 30 09:10:14 zeus sendmail[32212]: q7U7A8dc032212: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2012 Aug 30 09:05:37 zeus sendmail[28314]: q7U75VNH028314: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml
2012 Aug 30 08:59:35 zeus sendmail[21003]: q7U6xSeU021003: ruleset=check_rcpt, arg1=<xxxxxxxx>, relay=
[redacted] listed in Spamcop - see http://spamcop.net/bl.shtml

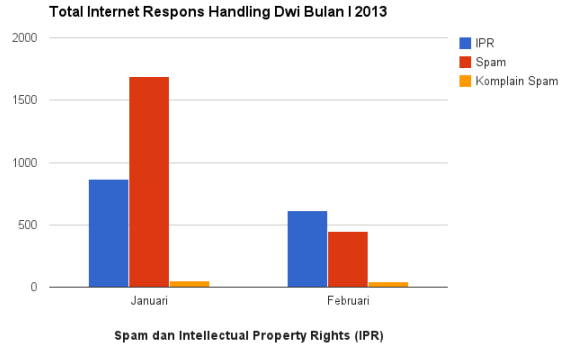
Please consider blocking port 25 for your customers, unless they ask for it.
There is no reason for a normal consumer to send SMTP mail from their machine.
If they don't know what SMTP is, then they don't need it.

Regards,
[redacted]

Gambar 4. Contoh pengaduan *malware* lewat email

3.3 *Spam* dan Komplain *Spam*

Laporan aktivitas *spam* secara umum dihasilkan secara otomatis oleh sistem *anti-spam*, sedangkan "komplain *spam*" merupakan laporan atas gangguan *spam*, sehingga terlihat bersifat insidental – sehingga berjumlah sedikit, yakni jika pengguna merasa perlu melaporkan.



Gambar 5. *Spam*, komplain-*spam* dan *Intellectual Property Rights* (IPR)

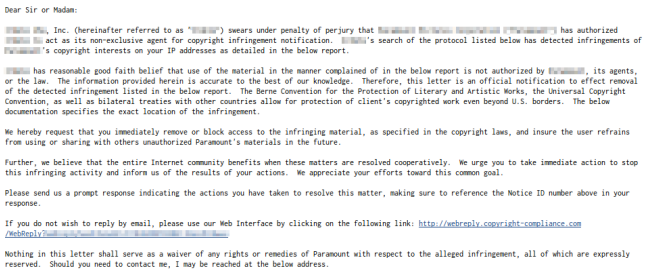
Terjadi penurunan jumlah laporan aktivitas *spam* dari bulan Januari ke Februari, cukup drastis hingga angka untuk Februari sekitar 25% dari Januari. Akan halnya komplain *spam* dalam dua bulan berjumlah sedikit dan relatif tidak berubah, yaitu rata-rata 45 laporan/bulan. Jika *spam* berada di urutan ketiga pada laporan dua bulan pertama ini, komplain *spam* tertinggal di belakang, sangat sedikit. Dari beberapa kemungkinan fenomena ini, dua poin yang perlu dipertimbangkan:

1. Media pelaporan seperti IDCERT tidak dipertimbangkan oleh penerima *spam*.

2. Pengguna Internet "menyelesaikan sendiri" urusan *spam*, baik menggunakan fasilitas pelaporan yang sudah disediakan layanan (sebagai misal hampir semua layanan email berbasis web sudah menyediakan penandaan "pesan sebagai *spam*") atau membiarkan *spam* ini dengan cukup menghapusnya.

3.4 Intellectual Property Rights (IPR)

Persoalan Hak atas Kekayaan Intelektual (HaKI/IPR), seperti ditampilkan pada grafik di Gambar 5, secara umum disampaikan oleh pemegang/pengelola hak tsb. atas kemungkinan penyalahgunaan bahan-bahan yang dilindungi HaKI. Jumlah laporan IPR berada pada peringkat terakhir dari "grup empat besar" laporan. Terjadi sedikit penurunan pada jumlah laporan IPR bulan Januari ke Februari, menghasilkan kisaran 730 laporan/bulan.



Dear Sir or Madam:

[redacted], Inc. (hereinafter referred to as "[redacted]") swears under penalty of perjury that [redacted] has authorized [redacted] to act as its non-exclusive agent for copyright infringement notification. [redacted]'s search of the protocol listed below has detected infringements of [redacted]'s copyright interests on your IP addresses as detailed in the below report.

[redacted] has reasonable good faith belief that use of the material in the manner complained of in the below report is not authorized by [redacted], its agents, or the law. The information provided herein is accurate to the best of our knowledge. Therefore, this letter is an official notification to effect removal of the detected infringement listed in the below report. The Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention, as well as bilateral treaties with other countries allow for protection of client's copyrighted work even beyond U.S. borders. The below documentation specifies the exact location of the infringement.

We hereby request that you immediately remove or block access to the infringing material, as specified in the copyright laws, and insure the user refrains from using or sharing with others unauthorized Paramount's materials in the future.

Further, we believe that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to stop this infringing activity and inform us of the results of your actions. We appreciate your efforts toward this common goal.

Please send us a prompt response indicating the actions you have taken to resolve this matter, making sure to reference the Notice ID number above in your response.

If you do not wish to reply by email, please use our Web Interface by clicking on the following link: http://webreply.copyright-compliance.com
/WebReply?[redacted]

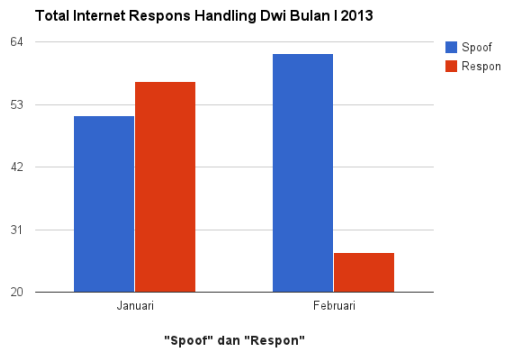
Nothing in this letter shall serve as a waiver of any rights or remedies of Paramount with respect to the alleged infringement, all of which are expressly reserved. Should you need to contact me, I may be reached at the below address.

Gambar 6. Contoh pengaduan *Intellectual Property Rights* (IPR) lewat email

Persoalan terkait IPR menyangkut ranah hukum berkaitan dengan aspek legal hak kekayaan intelektual dan dapat menjadi sulit dipantau karena baru diketahui setelah materi (*content*) diperiksa. Untuk kemudahan PJI/ISP mengawasi hal ini, perlu adanya prosedur standar yang dijadikan acuan kebolehan pemasangan materi di Internet.

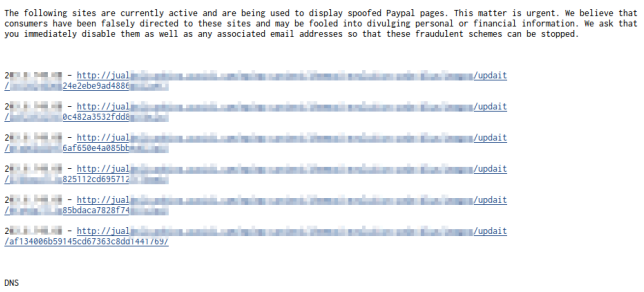
3.5 *Spoofing*

Laporan *spoofing* atau gangguan dengan cara "menyaru sebagai pihak lain" berjumlah sedikit dalam dua bulan ini, dengan kisaran 55 laporan/bulan. Bersama dengan komplain *spam* yang dibahas pada uraian sebelumnya, laporan *spoofing*



Gambar 7. *Spoof* dan Respon

tidak signifikan dalam hal jumlah dibanding jenis laporan-laporan lain.


The following sites are currently active and are being used to display spoofed Paypal pages. This matter is urgent. We believe that consumers have been falsely directed to these sites and may be fooled into divulging personal or financial information. We ask that you immediately disable them as well as any associated email addresses so that these fraudulent schemes can be stopped.

2[redacted] - http://jual[redacted]/updait
/[redacted]24e2ebe3ad4486[redacted]

2[redacted] - http://jual[redacted]/updait
/[redacted]0c482a3532fdd6[redacted]

2[redacted] - http://jual[redacted]/updait
/[redacted]6af650e4a085bb[redacted]

2[redacted] - http://jual[redacted]/updait
/[redacted]825112cd695712[redacted]

2[redacted] - http://jual[redacted]/updait
/[redacted]85bdaca7828f74[redacted]

2[redacted] - http://jual[redacted]/updait
/af134006b59145cd67363c8dd1441/69/

DNS

Gambar 8. Contoh pengaduan *spoof* lewat email

4. Rangkuman

Dengan pertimbangan jumlah gangguan berupa *network incident* yang banyak, perlu menjadi perhatian para administrastor jaringan, baik jaringan lokal atau Penyedia Jasa Internet (PJI), agar mempertimbangkan tindakan preventif mengurangi penyalahgunaan akses keluar dari pengguna di dalam jaringan. Hal ini sesuai dengan pendapat sebagian ahli keamanan jaringan bahwa “gangguan dapat muncul dari dalam, pengguna jaringan itu sendiri”, baik dilakukan dengan sengaja atau ketidaksengajaan seperti penyusupan bot di komputer.

Dilihat dari volume pengaduan yang masuk – yang menggambarkan kepedulian para pelapor terhadap isu keamanan Internet – menjadi tanggung jawab pihak-pihak terkait dengan bahan laporan tsb. untuk menindaklanjuti dalam bentuk respon atau aksi yang diperlukan. Dengan demikian, prosedur standar yang menjadi acuan dapat dijalankan dengan baik dan kepercayaan pihak pelapor terjaga atau meningkat.

4.1 Rekomendasi

Sejumlah rekomendasi yang dapat dipertimbangkan:

1. Perangkat lunak anti virus dan perangkat lunak keamanan dipasang untuk mengurangi risiko terinfeksi *malware*. Pemutakhiran terhadap aplikasi dan basis data yang terkait dengan aplikasi dilakukan secara teratur.

2. Administrator jaringan perlu melakukan pemantauan terhadap aksi yang mencurigakan, semisal akses ke *port* email/Postfix[4] secara intensif dalam periode lama atau berulang-ulang.

3. Administrator jaringan memblokir semua *port* akses ke Internet, kecuali untuk *port* yang dianggap diperlukan.

4. Penyedia Jasa Internet (PJI/ISP) dan operator telekomunikasi disarankan menyediakan tombol pelaporan khusus penyalahgunaan Internet (*Internet abuse*) guna kemudahan pelaporan.

5. Formulir pengaduan penyalahgunaan Internet (*Internet abuse*) dicantumkan di setiap situs web.

6. Terkait Hak atas Kekayaan Intelektual (HaKI), sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai materi (*content*) yang dianggap melanggar HaKI, karena PJI atau penyedia materi memerlukan landasan hukum yang jelas untuk menurunkan materi yang bermasalah.

7. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada penegak hukum.

[4] Terkait jumlah pengaduan *network incident* yang sangat banyak.

5. Ucapan terima kasih

Ucapan terima kasih disampaikan kepada seluruh responden yang telah berpartisipasi pada riset ini, yakni:

1. Kementrian Komunikasi dan Informatika (Kominfo).
2. Pengelola Nama Domain Internet Indonesia (PANDI).
3. Asosiasi Penyelenggara Jasa Internet Indonesia (APJII).
4. Detik (Detik.net).
5. Tiga operator telekomunikasi, tujuh NAP, dan dua puluh dua PJI/ISP.

6. Lampiran

6.1 Ancaman DDoS dan Langkah Antisipasi

Artikel ini dipublikasikan di situs web IDCERT, `http://www.cert.or.id/indeks_berita/berita/32/`.

Sumber terjemahan: `http://dns.measurement-factory.com/surveys/openresolvers.html`.

6.1.1 Pendahuluan

Kami sedang melakukan survei untuk mencari *DNS resolver* terbuka. Sebuah *DNS resolver* dinyatakan *terbuka* jika disediakan resolusi nama rekursif untuk klien di luar domain administrasifnya. *DNS resolver* terbuka adalah ide yang buruk karena beberapa alasan:

1. Mereka memungkinkan pihak luar mengonsumsi sumber daya bukan milik mereka.
2. Penyerang mungkin dapat meracuni tembolok (*cache*) *resolver* terbuka.
3. *Resolver* terbuka yang digunakan dalam serangan DDoS luas dengan alamat sumber palsu dan pesan balasan DNS yang besar.

Seperti relai SMTP terbuka, *DNS resolver* terbuka sekarang disalahgunakan oleh pengacau untuk lebih mencemari Internet.

6.1.2 Metodologi pengujian

Berdasarkan survei yang dilakukan oleh *DNS Expertise: The Measurement Factory* dengan mengirimkan permintaan DNS ke alamat IP target untuk nama dalam domain `test.openresolvers.org`. Jika server otoritatif domain milik kami menerima permintaan yang sama, alamat-IP target menjalankan *resolver* terbuka (*open resolver*).

Target alamat IP yang diuji tidak lebih dari sekali setiap tiga hari.

Daftar alamat IP target berasal dari beberapa sumber:

1. *Nameserver* rekursif yang sudah dikenal. Jika *nameserver* rekursif Anda mengirim *query* satu dari empat *nameserver* otoritatif kami, kami akan mengujinya. Sila hubungi kami (`info@measurement-factory.com`) jika Anda tertarik menyediakan alamat IP target dari *nameserver* otoritatif Anda sendiri.
2. *Nameserver* otoritatif yang sudah dikenal.
3. Antarmuka web untuk basis data.

6.1.3 *Database lookup*

Berbasis web

Silakan lihat antarmuka Open Resolver Check[5]. Anda dapat memasukkan alamat IP Anda sendiri (atau IP pihak lain) untuk segera diuji.

Anda juga dapat menggunakan alat bantu kami, Network Query[6] untuk melihat daftar *resolvers* terbuka di jaringan Anda.

[5] `http://dns.measurement-factory.com/cgi-bin/openresolvercheck.pl`

[6] `http://dns.measurement-factory.com/cgi-bin/openresolverquery.pl`

Berbasis DNS

Anda juga dapat mengirim *query* DNSBL[7] kami menggunakan zona `dnsbl.openresolvers.org`. Sebagai contoh:

```
$ dig + short 2.2.2.4.dnsbl.openresolvers.org
127.0.0.2
```

Respon dari `127.0.0.2` berarti bahwa alamat yang ditanyakan tadi terbuka secara rekursif. Suatu respon "NXDOMAIN" berarti alamat yang yang tidak terbuka atau belum diselidiki.

Kami juga memiliki cara mudah untuk mengetahui apakah server *DNS resolver* lokal Anda bersifat terbuka. Jika Anda memiliki perintah `dig` pada sistem, jalankan:

```
$ dig + short amiopen.openresolvers.org TXT
```

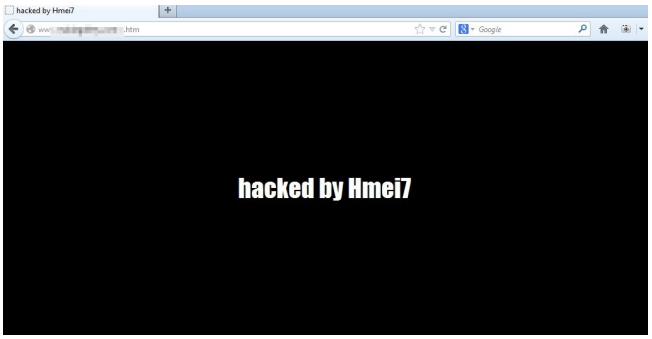
Jika Anda terbiasa dengan `nslookup`, coba ini:

```
$ nslookup
> set type = TXT
> amiopen.openresolvers.org
```

Kami memiliki arsip laporan harian[8] menunjukkan jumlah *resolver* terbuka untuk setiap nomor Autonomous System. Berikut laporan terbaru: `http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/latest.html`.

6.2 Tampilan situs web korban *defacement*

Website defacement adalah serangan terhadap situs web dalam bentuk mengubah tampilan situs atau halaman web tsb.[9]. Kasus *defacement* ini tampak meningkat dalam periode terakhir ini dan terlihat seperti "adu ketangkasan" yang dilakukan secara sporadis atau terorganisasi. Serangan dapat dilakukan pada situs web yang bersangkutan secara langsung atau dengan pembelokan alamat IP lewat pengubahan di server DNS secara ilegal. Beberapa tampilan korban *defacement* terlihat di bawah ini.



Gambar 9. "Hacked by Hmei7"

Gambar 10. "Stop Korupsi dan Suap"

Defacement menjadi perhatian karena dalam hal serangan terhadap situs web, cara ini sering dijadikan "permainan" atau bahan awal kegiatan meretas. Selain cara yang digunakan dianggap dapat dilakukan dengan mudah, perubahan tampilan di halaman web cepat menarik perhatian publik dan media massa. Beberapa kelompok peretas melakukan aksi *defacement* ini hanya sebagai aksi gagah-gagahan dan "permainan bersama" di antara anggota.

[7] DNS-based Blackhole List

[8] `http://dns.measurement-factory.com/surveys/openresolvers/ASN-reports/`

[9] *Website defacement is an attack on a website that changes the visual appearance of the site or a webpage.*, `http://en.wikipedia.org/wiki/Website_defacement`