INCIDENT MONITORING REPORT

2012

LAPORAN DWI BULAN-I TAHUN 2012

Bulan JANUARI dan PEBRUARI

Edisi: UMUM

06 APRIL 2012

Disusun oleh:

DIDUKUNG OLEH:

DAFTAR ISI

I. PENGANTAR

Keamanan berinternet merupakan salah satu faktor terpenting dalam menjalankan usaha maupun bisnis.

Selain bertujuan memberikan deskripsi tentang insiden keamanan informasi di Indonesia, laporan ini juga dapat dijadikan contoh agar Indonesia mempunyai data primer tentang salah satu indicator keamanan informasi di Indonesia.

Setiap lembaga sangatlah penting menindaklanjuti berbagai keluhan/pengaduan yang diterimanya terkait internet *abuse*. Sebagai analogi: bila kita berkeinginan agar setiap keluhan/pengaduan dari negara kita direspon dengan baik oleh negara lain, tentunya kita juga harus memperlakukan hal yang sama terhadap laporan yang masuk.

Keluhan/pengaduan yang terjadi menunjukkan betapa lemahnya sistem yang dibangun sehingga membutuhkan perbaikan kedepannya. Kita tentu tidak ingin, situs web yang kita bangun ditumpangi oleh *Malware* ataupun *Phishing* yang terkait dengan *Fraud* akibat lemahnya sistem yang kita bangun.

Tidak hanya sebatas menindaklanjuti keluhan/pengaduan, tetapi kita juga harus bisa lebih pro-aktif melaporkannya bila menjadi korban dari prilaku jahat di internet.

Dalam 2 bulan ini, ID-CERT sendiri menerima laporan pengaduan Phishing yang cukup unik, yaitu adanya aduan Phishing non-finansial.Bahkan phishing non-finansial ini merupakan kasus pertama di Dunia. Selama ini kita beranggapan bahwa Phishing selalu akan terkait dengan masalah finansial. Hal ini akan menjadi sorotan edisi Dwi Bulan 1 tahun 2012 ini.

Dalam penelitian ini, kami berhasil mengambil data dari tiga puluh tujuh (37) responden yang terdiri dari: **KEMKOMINFO**, **ID-CERT**, **PANDI**, **DETIK.NET, Zone-h dan Anti Fraud Command Center (AFCC), 3 Operator** Telekomunikasi, **7 NAP** dan **22 ISP**.

Statistik ini juga mendapatkan dukungan sponsor dari PANDI dan APJII.

II. Metodologi penelitian

Metodologi yang digunakan dalam penelitian ini adalah:

A. Pengambilan data dari sejumlah responden.

B. Metode analisis berdasarkan:

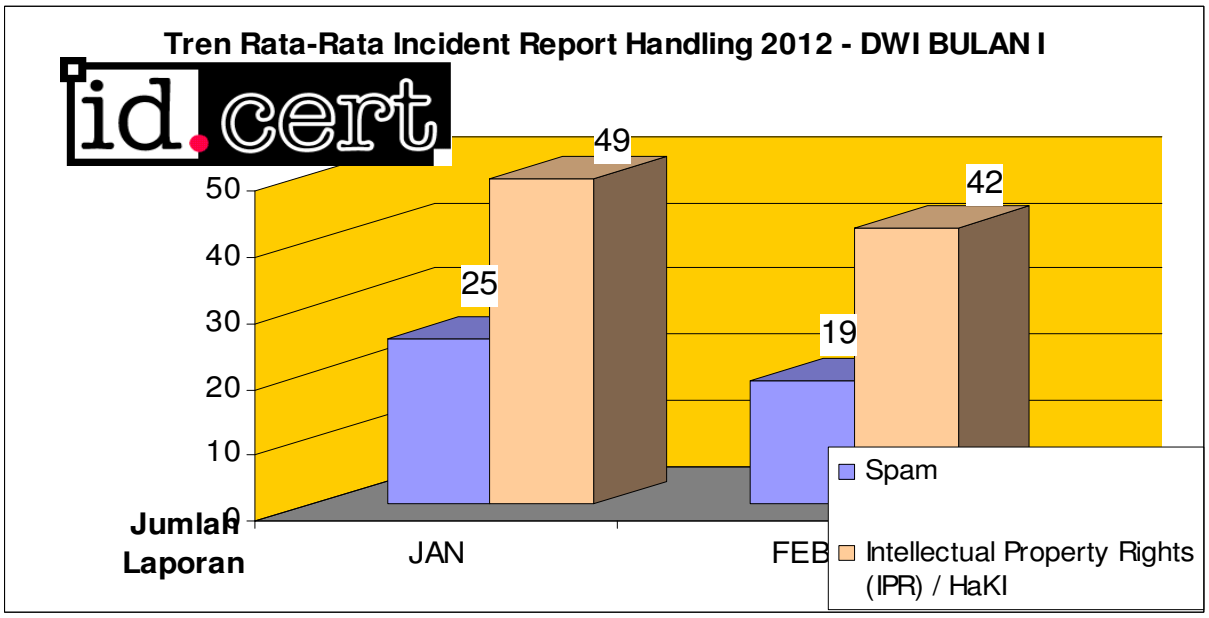
B.1. Tembusan laporan yang masuk via email akun abuse ISP/ Operator Telekomunikasi/lembaga non-ISP.

B.2. Tabulasi yang dikeluarkan oleh sejumlah responden. Tabulasi yang dimaksud adalah: data-data yang telah dihitung dan dikategoriasi oleh responden tersebut.

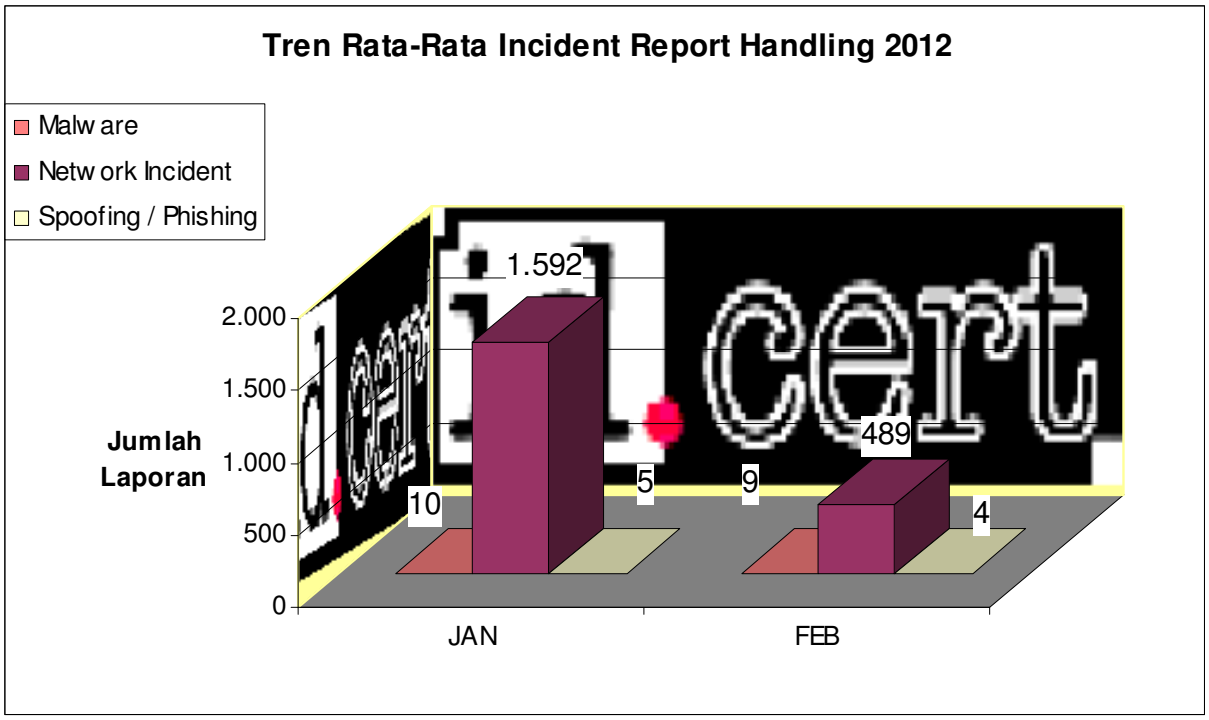
C. Dari laporan tersebut, kami melakukan pengkategorian laporan sebagai berikut:

C.1. Spam	transmisi pesan-pesan massal yang tidak diminta;
C.2. Spam Komplain	Keluhan/pengaduan email spam dari dalam negeri terhadap network di Indonesia dan luar negri.
C.3. Respon	Respon yang diberikan semua pihak terhadap laporan yang masuk.
C.4. Network Incident	Aktifitas yang dilakukan terhadap jaringan milik orang lain serta segala aktifitas terkait dengan penyalahgunaan jaringan.
C.5. Fraud	Laporan kepada penegak hukum/instansi terkait yang mengakibatkan kerugian finansial.
C.6. Spoofing/Phishing	Pemalsuan e-mail dan situs untuk menipu pengguna.
C.7. Malware	Sebuah program komputer yang dibuat dengan maksud jahat.
C.8. Lain-lain	Laporan penyalahgunaan yang diterima selain dari kategori yang ada diatas.

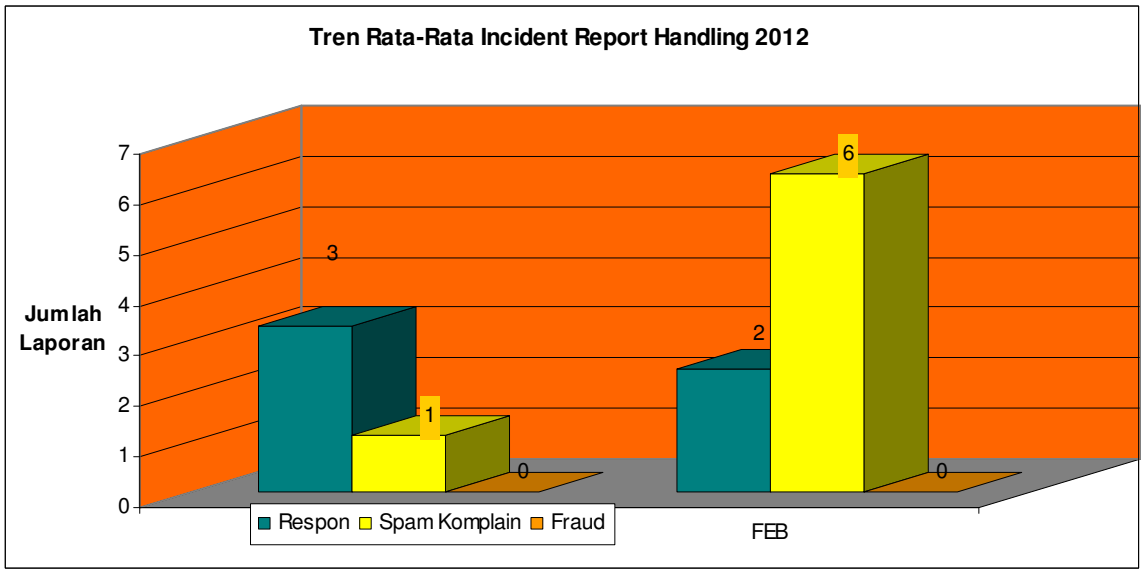
III. STATISTIK JANUARI – PEBRUARI



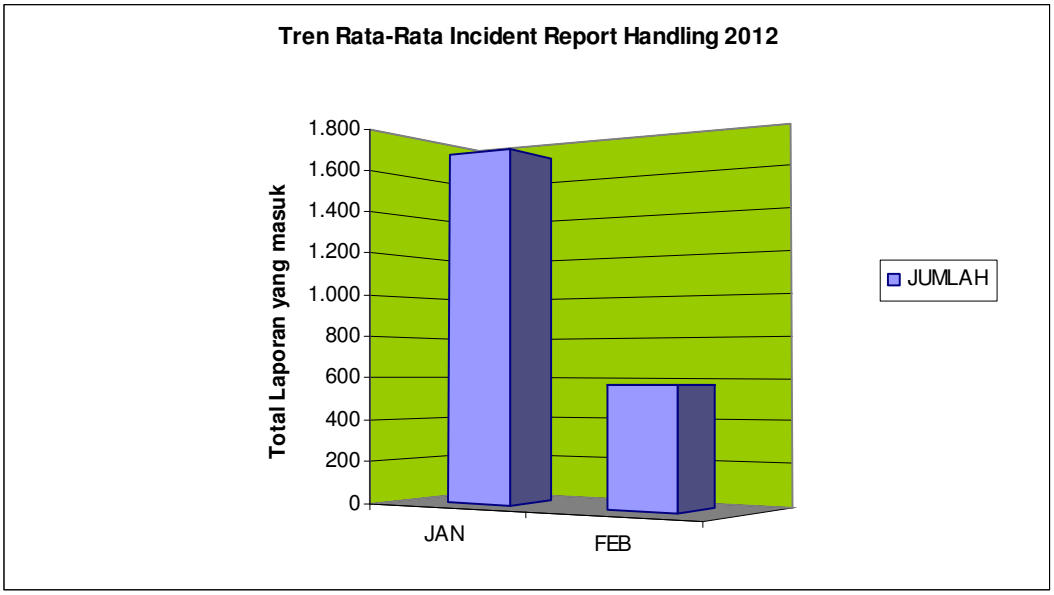
GRAFIK-I: Spam dan Intellectual Propterty Rights/IPR (Lain-Lain) – Dwi Bulan I



GRAFIK-II: Kategori MALWARE, NETWORK INCIDENT dan SPOOFING/PHISHING, Dwi Bulan - I



GRAFIK-III: Kategori RESPON, FRAUD dan SPAM KOMPLAIN, Dwi Bulan – I



GRAFIK-IV: JUMLAH LAPORAN RATA-RATA YANG MASUK PADA Dwi Bulan-I

IV. URAIAN

GRAFIK-V: TREN RATA-RATA DWI BULAN - I

A. NETWORK INCIDENT

Posisi pertama tertinggi adalah Network incident.

Laporan terbanyak yang diterima pada bulan Januari dan Pebruari 2011 ini umumnya adalah *3 failed login (Brute Force), deface* dan *DDoS attack*.

Network Incident mengalami penurunan dibulan Pebruari menjadi 489 laporan rata-rata dari sebelumnya 1.592 laporan rata-rata dibulan januari 2012.

Terdapat dua ancaman besar yang akan terjadi dalam beberapa bulan kedepan, yaitu: Ancaman serangan ke DNS Root Server di Seluruh dunia. Bila ini terjadi, maka internet diperkirakan akan melambat atau bahkan tidak dapat terkoneksi sama sekali. Langkah antisipasi yang perlu dilakukan adalah: mengawasi aktifitas di port 53 UDP, bila terjadi anomaly, segeralah berkoordinasi dengan ID-CERT agar penanganan cepat dapat segera dilakukan. Hal ini juga telah menjadi perhatian seluruh CERT di Asia Pasifik. Artikel mengenai hal ini kami lampirkan bersama laporan ini.

Ancaman kedua adalah: rencana FBI (Federal Berau Investigation) mematikan jutaan DNS palsu yang menyebarkan Malware mulai **08 Mar 2012**. Kami lampirkan dalam laporan ini adalah rilis beserta solusi yang harus dilakukan bila hal ini terjadi.

B. Intellectual Property Rights (IPR)/HaKI

Posisi kedua tertinggi pada tahun ini adalah dengan kategori Intellectual Property Rights (IPR)/ HaKI. Dimana yang masuk dalam kategori ini adalah semuanya terkait dengan pelanggaran HaKI (Hak Atas Kekayaan Intelektual) baik itu untuk Piranti Lunak maupun Film.

Umumnya pengirim keluhan/pengaduan ini berasal dari luar negeri.

Komplain ini juga mengalami penurunan dari 49 laporan rata-rata pada bulan Januari menjadi 42 laporan rata-rata pada bulan Pebruari.

C. SPAM

Dari total laporan yang masuk, *SPAM* menduduki peringkat ketiga dari total laporan rata-rata yang diterima.

SPAM mengalami penurunan pada bulan Pebruari dengan jumlah rata-rata dari seluruh responden adalah 19 laporan komplain.

Sedangkan ditingkat global, berdasarkan data Messagelabs bulan Pebruari 2011, Negara-negara yang termasuk dalam negara paling banyak menerima spam adalah sebagai berikut:

Pebruari 2012			
Rating	**Negara**	**% Spam**	**Keterangan**
1	Saudi Arabia	76,2	Korban spam
2	Belanda	70	
3	USA	68,9	
4	Denmark	68,8	
5	Inggris	68,6	
6	Kanada	68,5	
7	Australia	68,3	
8	Hongkong	67,9	
9	Jerman	67,9	
10	Singapore	67	
11	Jepang	65,1	

Tabel – 1: Rating Spam Dunia (Messagelabs)

D. MALWARE

Posisi keempat tertinggi adalah MALWARE.Posisi ini turun dibandingkan tahun sebelumnya.

Kecenderungan Malware pada bulan Januari dan Pebruari 2012 ini adalah sedikit menurun.

Pada 13 Feb 2012, ID-CERT menerima aduan tentang adanya situs Indonesia yang didalamnya terdapat malware. Malware ini bekerja ketika seseorang mengunjungi web tersebut dan secara otomatis, link yang dikunjungi akan muncul di wall facebook tanpa seizin pengguna.

Berdasarkan data Messagelabs, malware secara global memiliki kecenderungan sedikit meningkat atau terjadi anomali dengan tren global dibulan Peb 2012 ini.

E. SPOOFING / PHISHING

Posisi kelima tertinggi adalah Spoofing/phishing.

Terdapat sejumlah situs Phishing yang menyebarkan *Malware.*

Laporan pada tahun ini mengalami sedikit penurunan dibandingkan Januari 2012 yang hanya 5 laporan rata-rata.

Kasus Phishing non-finansial merupakan kasus aduan pertama yang diterima ID-CERT. Adalah situs mafiahukum.org yang dilaporkan merupakan situs palsu dari http://www.satgas-pmh.go.id/. Bahkan ini merupakan kasus pertama didunia, dimana sebuah situs palsu tidak berisi informasi financial melainkan berisi informasi yang terkait dengan masalah hukum dan politik.

Dalam masalah Phishing Finansial, terdapat sejumlah aduan yang terkait dengan login bank palsu.

F. RESPON

Respon menduduki posisi keenam tertinggi.

Kecenderungan respon yang meningkat menunjukkan indikator yang cukup baik, karena pihak yang menerima komplain sudah mulai merespon laporan komplain yang masuk.

Sedangkan bila dibandingkan dengan jumlah komplain keseluruhan, respon masih terbilang rendah. Adapun penyebabnya: selain setiap keluhan/pengaduan yang masuk tidak/belum direspon, dimungkinkan pula bahwa respon dilakukan tanpa di tembuskan dalam proses riset ini.

G. SPAM KOMPLAIN dan FRAUD

SPAM KOMPLAIN menempati peringkat terakhir.

Yang masuk pada kategori ini adalah laporan korban spam dari network di Indonesia maupun luar negeri.

Untuk *Fraud*, kami belum berhasil mendapatkan data dari pihak penegak hukum tentang berapa besar kasus Fraud yang terjadi di Indonesia.

V. RANGKUMAN

Yang perlu menjadi perhatian adalah ancaman terhadap DNS Root Server dalam beberapa bulan kedepan dan juga DNS Changer / DNS palsu penyebar Malware yang berpotensi berimbas pada lambatnya akses internet diseluruh dunia terutama di Indonesia.

Berikut ini sejumlah rekomendasi :

A. Gunakan piranti lunak anti virus dan piranti lunak tambahan untuk mengurangi resiko *spam* ;
B. Hindari pencantuman alamat email ditempat umum seperti disitus web, forum, dsb. Gantikan dengan formulir isian;
C. Laporkan kepada ID-CERT bila menjadi korban dari tindakan *abuse* internet, terutama dalam kasus DNS Root Server. Bila menemukenali adanya anomali dari jaringan XL terutama port 53 UDP, agar segera berkoordinasi dengan ID-CERT;
D. ISP dan Operator Telekomunikasi disarankan menyediakan tombol pelaporan khusus untuk *abuse* internet yang memudahkan user untuk melapor;
E. Cantumkan formulir pengaduan Internet Abuse disetiap website.
F. Terkait dengan HaKI, sebaiknya pemerintah menyiapkan aturan hukum yang jelas mengenai konten yang melanggar HaKI, karena ISP maupun penyelenggara konten memerlukan landasan hukum yang jelas untuk menurunkan suatu konten yang bermasalah;
G. Semua pihak wajib menindaklanjuti setiap laporan keluhan/pengaduan yang diterimanya. Bila menyangkut pelanggaran hukum, sebaiknya dilaporkan kepada pihak penegak hukum;

VI. UCAPAN TERIMA KASIH

Dalam kesempatan ini, saya ingin mengucapkan terima kasih kepada berbagai pihak atas dukungan yang diberikan sehingga riset ini dapat terlaksana dengan baik dan lancar.

Ucapan terima kasih kami sampaikan kepada seluruh responden yang telah berpartisipasi dalam riset ini, yang terdiri dari:

[A] – Kementrian Komunikasi dan Informatika [KEMKOMINFO]

[B] – Pengelola Nama Domain Internet Indonesia [PANDI]

[C] – APJII

[D] – DETIK.NET

[E] – 3 Operator Telekomunikasi, 7 NAP dan 22 ISP.

VII. DAFTAR PUSTAKA

[1] – Statistik Internet Abuse 2010:
http://ahmadkaz.wordpress.com/riset-abuse/

[2] – DNS Changer: https://www.hkcert.org/my_url/en/blog/12022901

[3] – APCERT Annual Reports 2009
http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2009.pdf

[4] – CERT Vulnerability Reporting forms; https://forms.cert.org/VulReport/

[5] – Messagelabs
http://www.symanteccloud.com/globalthreats/overview/r_mli_reports

[6] – RFC 5039, SIP and SPAM: http://tools.ietf.org/html/rfc5039

VIII. LAMPIRAN-I: ANCAMAN SERANGAN KE ROOT DNS

---------- Forwarded message ----------
From: Ahmad ID-CERT <ahmad@cert.or.id>
Date: Mon, 20 Feb 2012 13:28:18 +0700
Subject: [WASPADA] Rencana Serangan ke DNS Root
To: diskusi <diskusi@cert.or.id>
Cc: responden <responden@cert.or.id>

Kepada Yth,
Konstituen ID-CERT

Dihimbau kepada semua pihak untuk mewaspadai Serangan Anonymious terhadap DNS Root Server.

Bila terjadi anomali, mohon agar menginformasikan hal ini ke ID-CERT <ahmad@cert.or.id> atau <cert@cert.or.id> agar dapat segera kami koordinasikan langkah antisipasinya dengan CERT yang lain.

Hal ini telah menjadi perhatian Anggota APCERT.

Terima kasih,
Ahmad Alkazimy
--

SEND YOUR INCIDENT REPORTS TO: <cert@cert.or.id>

KIRIMKAN KOMPLAIN INTERNET ABUSE YANG TERJADI,KE: <cert@cert.or.id>

AHMAD KHALIL ALKAZIMY,ST
INCIDENT RESPONSE TEAM
INDONESIA COMPUTER EMERGENCY RESPONSE TEAM (ID-CERT)
email: <ahmad@cert.or.id>
http://www.cert.or.id/
SKYPE/YM ID: ahmadkaz
HP: (+62)83-874-9292-15
==========

---------- Forwarded message ----------
From: "ZHOU, Yonglin" <zyl@cert.org.cn>
Date: Mon, 20 Feb 2012 10:04:54 +0800
Subject: [APCERT Teams] Watching UDP53 -- Anonymous attack plan
To: apcert-teams@apcert.org

Dear team,

May you notice the the announcement of 'anonymous' who is planning to attack the 13 DNS roots. They are going to use DNS reflection attack. A interesting thing is that recently, CNCERT has handled several serious DDOS of this type. Although those cases had nothing to do with the

'anonymous' announcement, it does worth paying more attention on UDP/53 these day.

Here I suggest APCERT teams to watch more on UDP/53 flow and relative DDOS. And share the abnormal trend timely.

Yonglin.

```
------------------------------------------------------------------------
01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
01101110  01000111 01101100 01101111 01100010 01100001 01101100
01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
------------------------------------------------------------------------
```

```
  ___                        _   _                ___ _      _            _
 / _ \ _ __   ___  _ _  ___ _| |_(_)___ _ _ _     / __| |___ | |__  ___ _| |
| (_) | '_ \/ -_)| '_/ _ `  |  _| / _ \ ' \ | | (_ | / _ \ '_ \/ _ `  | |
 \___/| .__/\___||_| \__,_|\__|_\___/_||_|  \___|_\___/_.__/\__,_|_|_|
      |_|
 ___ _              _                _
| _ ) |__ _ __| |_____ _  _| |_
| _ \ / _` / _| / / _ \ || |  _|
|___/_\__,_\__|_\_\___/\_,_|\__|
```

```
------------------------------------------------------------------------
01001111 01110000 01100101 01110010 01100001 01110100 01101001 01101111
01101110  01000111 01101100 01101111 01100010 01100001 01101100
01000010 01101100 01100001 01100011 01101011 01101111 01110101 01110100
------------------------------------------------------------------------
```

"The greatest enemy of freedom is a happy slave."

To protest SOPA, Wallstreet, our irresponsible leaders and the beloved bankers who are starving the world for their own selfish needs out of sheer sadistic fun, On March 31, anonymous will shut the Internet down.

In order to shut the Internet down, one thing is to be done. Down the 13 root DNS servers of the Internet. Those servers are as follow:

A	198.41.0.4
B	192.228.79.201
C	192.33.4.12
D	128.8.10.90
E	192.203.230.10
F	192.5.5.241
G	192.112.36.4
H	128.63.2.53
I	192.36.148.17
J	192.58.128.30
K	193.0.14.129
L	199.7.83.42

M 202.12.27.33

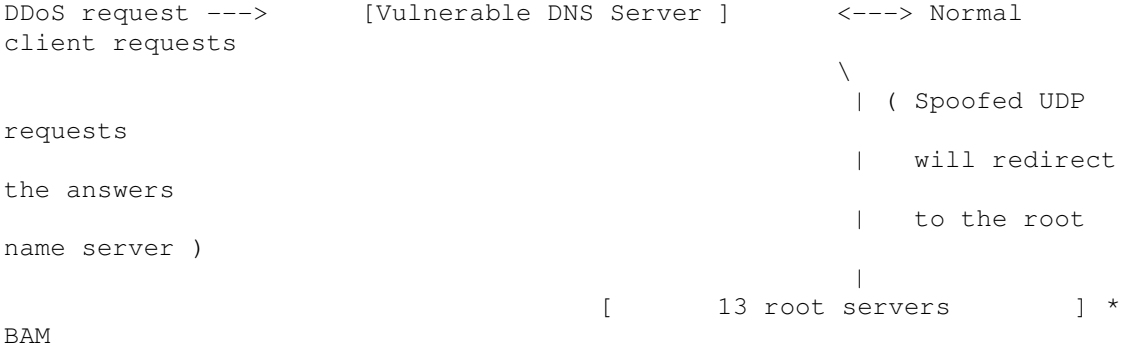
By cutting these off the Internet, nobody will be able to perform a domain name lookup, thus, disabling the HTTP Internet, which is, after all, the most widely used function of the Web. Anybody entering "http://www.google.com" or ANY other url, will get an error page, thus, they will think the Internet is down, which is, close enough. Remember, this is a protest, we are not trying to 'kill' the Internet, we are only temporarily shutting it down where it hurts the most.

While some ISPs uses DNS caching, most are configured to use a low expire time for the cache, thus not being a valid failover solution in the case the root servers are down. It is mostly used for speed, not redundancy.

We have compiled a Reflective DNS Amplification DDoS tool to be used for
this attack. It is based on AntiSec's DHN, contains a few bugfix, a different dns list/target support and is a bit stripped down for speed.

The principle is simple; a flaw that uses forged UDP packets is to be used to trigger a rush of DNS queries all redirected and reflected to those 13 IPs. The flaw is as follow; since the UDP protocol allows it, we can change the source IP of the sender to our target, thus spoofing the source of the DNS query.

The DNS server will then respond to that query by sending the answer to the spoofed IP. Since the answer is always bigger than the query, the DNS answers will then flood the target ip. It is called an amplified because we can use small packets to generate large traffic. It is called
reflective because we will not send the queries to the root name servers,
instead, we will use a list of known vulnerable DNS servers which will attack the root servers for us.



Since the attack will be using static IP addresses, it will not rely on name server resolution, thus enabling us to keep the attack up even while the Internet is down. The very fact that nobody will be able to make new requests to use the Internet will slow down those who will try to stop the attack. It may only lasts one hour, maybe more, maybe even

a few days. No matter what, it will be global. It will be known.

---

download link in #opGlobalBlackout

The tool is named "ramp" and stands for Reflective Amplification. It is located in the \ramp\ folder.

----------> Windows users

In order to run "ramp", you will need to download and install these two applications;

WINPCAP DRIVER - http://www.winpcap.org/install/default.htm
TOR - http://www.torproject.org/dist/vidalia-bundles/

The Winpcap driver is a standard library and the TOR client is used as a proxy client for using the TOR network.

It is also recommended to use a VPN, feel free to choose your own flavor
of this.

To launch the tool, just execute "\ramp\launch.bat" and wait. The attack
will start by itself.

----------> Linux users

The "ramp" linux client is located under the \ramp\linux\ folder and needs a working installation of python and scapy.

"He who sacrifices freedom for security deserves neither."
Benjamin Franklin

We know you wont' listen. We know you won't change. We know it's because
you don't want to. We know it's because you like it how it is. You bullied
us into your delusion. We have seen you brutalize harmless old womans who were
protesting for peace. We do not forget because we know you will only use
that
to start again. We know your true face. We know you will never stop. Neither
are we. We know.

We are Anonymous.
We are Legion.
We do not Forgive.
We do not Forget.
You know who you are, Expect us.

-- -------[CNCERT/CC]----------
Zhou, Yonglin ã€‚å‘¨å‹‡æ–ã€‘ CNCERT/CC, P.R.China
ã€‚å›½å®¶è„”ç½‘å°”æ€¥ä¸å¿ƒã€‘ Tel: +86 10 82990355 Fax: +86 10
82990399 Web: www.cert.org.cn Finger Print: 9AF3 E830 A350 218D BD2C
2B65 6F60 BEFB 3962 1C64
----------[CNCERT/CC]-------

IX. LAMPIRAN-II: DAMPAK TERMINASI DNS CHANGER PADA 08 MAR 2012

Diambil dari https://www.hkcert.org/my_url/en/blog/12022901

Harap mewaspadai dan melakukan pengecekan rutin.

DAMPAK TERMINASI DNS SERVER DARI DNSCHANGER
Tanggal rilis: 29 Februari 2012

Baru-baru ini, Information Security News melaporkan bahwa FBI (Federal Bureau Investigation) Amerika akan menutup DNS (Domain Name Server – Note 1) yang berhubungan dengan DNSChanger Botnet pada tanggal 8 Maret. Apa dampak dari insiden ini pada para pengguna Internet? HKCERT (Hong Kong Computer Emergency Response Team Coordination Center) akan memberikan informasi latar belakang DNSChanger, metode untuk mendeteksi apakah komputer terkena atau tidak, dan solusi bagi pengguna yang terkena untuk bagaimana cara mengatasinya tepat pada waktunya.

Latar Belakang

Malware botnet DNSChanger memiliki lebih dari 2000 varian (Ref 1). Diperkirakan sekitar 4 juta lebih komputer di seluruh dunia yang terkena
virus ini pada lebih dari 100 negara. Botnet ini diyakini dioperasikan oleh sebuah perusahaan IT bernama Rove Digital di Estonia sejak tahun 2007, sampai kelompok pelaku cyber crime ini ditahan/dipenjara pada tahun 2011 (Ref 2).

Apa Dampaknya bila terkena DNSChanger ini?

Malware DNSChanger ini terutama akan tersebar saat seorang user mengakses situs web tertentu atau men-download software viewer video online dan kemudian akan terkena malware ini. Malware DNSChanger diam-diam akan mengubah setting-an DNS pada komputer yang terkena, mengarahkan ke DNS server yang dibuat oleh kelompok pelaku cyber crime agar mereka bisa sepenuhnya mengontrol DNS untuk diarahkan ke IP address
yang diinginkan. Kelompok pelaku cyber crime ini dapat menggunakan botnet DNSChanger untuk mengarahkan user mengakses situs web tertentu yang tidak dikenal, termasuk mengganti iklan-iklan pada situs-situs web yang dituju pengguna untuk men-generate click-fraud atau memasang/menyusupkan software jahat lainnya.

Mengapa 8 Maret?

Pada November 2011, dalam "Operasi Ghost Click" (Ref 3), FBI berhasil menutup Botnet DNSChanger. Menurut perintah pengadilan, untuk menghindari komputer-komputer yang terkena malware itu kehilangan koneksi internet secepatnya, FBI diberi kuasa penuh untuk men-set sejumlah DNS server sementara untuk menjaga layanan-layanan DNS bagi para korban untuk menyelesaikan masalah ini dalam waktu 120 hari. Perintah pengadilan ini akan berakhir pada 8 Maret 2012. Apabila FBI

memutuskan untuk menutup DNS server sementara ini sesuai jadwal, maka beberapa juta bot DNSChanger di seluruh dunia akan terputus koneksi internetnya. Untuk menangani masalah ini dengan benar dan tepat, kita harus membantu korban-korban tersebut untuk membersihkan malware itu secepat mungkin.

Apakah (Komputer) Saya terkena?

Malware DNSChanger dapat menjangkiti sistem operasi Microsoft Windows dan Apple Mac OS X. Malware ini juga mencoba untuk menggunakan login name dan password default pada router di kantor kecil atau broadband di rumah untuk menyusup dan mengubah setting DNS-nya. Untuk mengecek apakah
komputer anda atau router broadband anda terkena malware ini atau tidak,
anda dapat menggunakan 2 metode berikut ini:

Metode 1 - Gunakan DCWG EyeChart:
Buka web browser (misalnya Internet Explorer, Firefox, Chrome, atau Safari) untuk mengakses situs testing yang disediakan oleh Kelompok Kerja DNS Changer (DCWG: DNS Changer Working Group) (Ref 3):

- http://dns-ok.us
- http://dns-ok.de
- http://dns-ok.ax/index_en.html
- http://dns-ok.fi/index_en.html

Apabila hasil test berwarna hijau, maka komputer anda normal.

Apabila hasil test berwarna merah, maka setting DNS server dari komputer
anda atau router broadband anda diarahkan ke server jahat yang dikenal. Direkomendasikan untuk mengikuti instruksi pada "Bagaimana mengatasi/menangani komputer dan broadband router yang terjangkiti" untuk pemeriksaan lebih detil.

Metode 2 - Cek Manual:
1. Cari IP address-nya DNS server

Komputer:
Ikuti instruksi pada halaman web DCWG di bawah ini, pilih sistem operasi-mu dan ikuti langkah-langkahnya untuk cek IP address dari DNS server-mu saat ini.
http://www.dcwg.net/checkup.html

Broadband Router:
Untuk cek IP address-nya DNS server yang digunakan oleh broadband router-mu, silahkan merujuk pada dokumentasi yang disediakan oleh vendor.

2. Cek apakah IP address-nya DNS server digunakan oleh DNSChanger
Masukkan IP address yang ditemukan pada pengecekan sebelumnya pada halaman web tool checking online yang disediakan oleh FBI.
https://forms.fbi.gov/check-to-see-if-your-computer-is-using-rogue-DNS

Bila hasilnya adalah "IP anda terhubung pada satu DNS server jahat yang dikenal", artinya setting DNS server komputer atau broadband router anda
diarahkan ke server jahat yang dikenal. Direkomendasikan untuk mengikuti
instruksi pada "Bagaimana mengatasi/menangani komputer dan broadband router yang terjangkiti" untuk pemeriksaan lebih detil.

Bagaimana mengatasi/menangani komputer dan broadband router yang terjangkiti?

Komputer

1. Disarankan untuk me-restore setting DNS komputer yang terjangkiti untuk mendapatkan settingan lama dengan otomatis. Silahkan kontak ISP atau admin IT kantor anda untuk mendapatkan bantuan.
2. Selama komputer terjangkiti malware DNSChanger usahakan untuk tidak meng-update sistem dan database software security. Malware ini memperlemah perlindungan security-nya dan dapat menyebabkan terjangkiti dengan malware lainnya, jadi anda harus melakukan scanning malware yang menyeluruh pada komputer anda.
   i. Microsoft Windows

Anda dapat menggunakan Malware Scanner yang free (edisi online) via URL yang tercantum pada situs web HKCERT untuk pengecekan dan membersihkan komputer anda.
https://www.hkcert.org/security-tools

   ii. Apple Mac OS X

Anda dapat meng-install malware scanner yang free berikut ini untuk pengecekan dan membersihkan komputer anda.
http://download.cnet.com/mac/antivirus-software/?filter=licenseName%3DFree
3. Setelah dibersihkan, gunakan lagi metode test di atas untuk meyakinkan apakah setting DNS server sudah normal atau belum.

Broadband Router

Disarankan untuk mengikuti dokumentasi yang disediakan oleh vendor untuk
me-reset setting-an DNS server dan mengubah password akun admin yang default.

Referensi:
1. http://www.paloaltonetworks.com/researchcenter/2012/02/dnschanger-rogue-dns-servers-taken-down/
2. http://blog.trendmicro.com/esthost-taken-down-biggest-cybercriminal-takedown-in-history/
3. http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911 09113
4. http://www.dcwg.net

Catatan:
1. DNS (Domain Nama System) - Suatu database terdistribusi dari nama-nama domain dan IP address yang saling terpetakan, membuat orang lebih nyaman mengakses Internet, tanpa perlu mengingat IP address yang rumit dan tidak mudah.

--

SEND YOUR INCIDENT REPORTS TO: <cert@cert.or.id>

KIRIMKAN KOMPLAIN INTERNET ABUSE YANG TERJADI,KE: <cert@cert.or.id>

AHMAD KHALIL ALKAZIMY,ST
INCIDENT RESPONSE TEAM
INDONESIA COMPUTER EMERGENCY RESPONSE TEAM (ID-CERT)
email: <ahmad@cert.or.id>
http://www.cert.or.id/
SKYPE/YM ID: ahmadkaz
HP: (+62)83-874-9292-15