



# Ministry of Information and Communications Vietnam Computer Emergency Response Team

Case study – Coordinate the Vietnam's largest cyber incident of the year

## DNS goes bad



Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam

# About me

- Do Ngoc Duy Trac (dntrac@vncert.vn).
  - Director of Operation.
  - Regional Director, Southern of Vietnam.
- Vietnam Computer Emergency Response Team (VNCERT).
- Ministry of Information and Communications (MIC).



# Agenda

- Case study – Coordinate the Vietnam's largest cyber incident of the year.
- A short introduction of Vietnam Antispam Law.



# When (1)

- 09 July: Dan Kaminsky officially confirmed about a bug in the global DNS system.
- But there is no details information, POC,...



## An Astonishing Collaboration

Wow. It's out. It's finally, finally out.

Sweet!

So there's a bug in DNS, the name-to-address mapping system at the core of most Internet services. DNS goes bad, every website goes bad, and every email goes...somewhere. Not where it was supposed to. You may have heard about this — the [Wall Street Journal](#), the [BBC](#), and some [particularly important people](#) are reporting on what's been going on. Specifically:

- 1) It's a bug in many platforms
- 2) It's *the exact same bug* in many platforms (design bugs, they are a pain)


### DNS CHECKER

Recently, a significant bug was discovered in the system that translates domain names into IP addresses (the system that trans can remember (such as www.doxpara.com) to the Internet can route (6... was discovered, that malicious people to in any website on the In companies across the quietly collaborated to release fixes for all a servers. To find out if you use is vulnerable

Check My DNS



# So there's a bug in DNS

A photograph of Dan Kaminsky, a man with dark hair, wearing a black t-shirt, speaking into a microphone. He is smiling slightly and gesturing with his hands. The background is a blurred white banner with some text and logos, including 'RED LAMPOA' and 'SCO'.

**"So there's a bug in DNS, the name-to-address mapping system at the core of most Internet services. DNS goes bad, every website goes bad, and every email goes...somewhere !!!"**

**Dan Kaminsky**

# DNS cache poisoning again? No way!



- Yes! That's the common sense when we all first heard about that bug.



# But .. Wait a minute

- All the giants seem so serious about this: Symantec, Cisco, Microsoft,...
- CERT teams around the world start raising awareness.



# Early warning

- In the same day (9 July), we decided to dispatch an early warning to more than 150 key stakeholders include: ISPs, govt agencies, banking sector,...



# When (2)

- 23 July: unofficial details information about DNS bug leaked on the Internet.
- We check the bug's theory side.
- We ask for opinions from specialists.
- We wrote a small tool for POC purpose.
- The result of POC is positive. We can poison unpatch Microsoft DNS server successful within 15 minutes.



# Urgent public warning

- We decided to dispatch an urgent public warning.
- This warning widespread on all local newspapers, online papers, television channels,...



# The third Urgent warning of the year



Trang chủ Giới thiệu FAQ Khảo sát Liên hệ



**VNCERT**

**TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM**

<http://vncert.gov.vn/canhbao/cbnd/CBND08-003.htm>

Tìm kiếm ...



Báo sự cố

Cập nhật

Hệ thống cảnh báo

Hội thảo & Sự kiện

Tài nguyên tham khảo

Hoạt động đào tạo

Tư vấn & hướng dẫn

Nghiên cứu - Phân tích

Các mục khác



## Hệ thống cảnh báo

CBND08-003

### Điểm yếu rất nghiêm trọng liên quan đến hệ thống phân giải tên miền DNS toàn cầu

**Cập nhật lúc 22h ngày 25/07/2008**

1. Công cụ tự động đang được phát tán rộng rãi trên Internet.
2. Đã xuất hiện một số vụ tấn công trên thế giới. Có dấu hiệu cho thấy hacker sử dụng mạng botnet vào việc tấn công DNS server khiến hiệu quả tấn công gia tăng



# Here come cowboys

## Websense reports China Netcom DNS cache poisoning

Posted by Ryan Naraine @ 12:43 pm

**Categories:** [Patch Watch](#), [Browsers](#), [Responsible disclosure](#), [Botnets](#), [Exploit code](#), [Data theft](#), [Google](#), [Firefox](#), [Adobe](#), [Flash](#), [Arbitrary Code Execution](#), [Anti Virus](#), [Malware](#)

**Tags:** [China Netcom](#), [DNS](#), [DNS Server](#), [Internet Service Provider](#), [Websense Inc.](#), [Internet Service Providers \(ISPs\)](#), [Domain Names](#), [Servers](#), [Internet](#), [Hardware](#)

 **TalkBack** ADD YOUR OPINION |  SHARE |  PRINT |  E-MAIL |  WORTHWHILE? **+1** 1 VOTES



The DNS server of one of China's largest ISPs has been poisoned to redirect typos to a malicious site rigged with drive-by exploits.

According to a [warning](#) from Websense Security Labs, the DNS poisoning attacks are affecting customers of China Netcom (CNC) and are using a malicious iFrame to launch exploits for known vulnerabilities in RealNetworks'



# Now everybody is on the run

## COMPUTERWORLD



MONASH University  
Information Technology



Networking eBusiness Open Source Security Servers SW Dev Storage Unified Comms Mobility & Wireless

- Home
- + Events
- News
- Reviews
  - Notebooks
  - Mobile Phones
  - Projectors
- Features
- Interviews
- Opinions
- Case Studies
- Tutorials
- + Knowledge Centres
- + Jobs
- PHP Developer's Guide
- Quickstudy
- Whitepapers

### Hackers start DNS attacks, researcher says

They're using an unknown exploit, says HD Moore, who posted different attack code last week.

[Gregg Keizer](#) 31/07/2008 08:12:24

Hackers are now actively exploiting a critical flaw in the Domain Name System, but they're not using any of the already known exploits, said a researcher who crafted the first attack code to go public.

"We're seeing an entirely new technique," said HD Moore, the creator of the Metasploit penetration testing framework, who with a hacker identified as "l)ruid," published exploits last week for the vulnerability in the Internet's routing system.



Print this story

Digg this story

More by [Gregg Keizer](#)

**Computerworld Buyer's Guide - Vendors Matched to this Article**

[HAL Data Services](#) , [Dimension Data](#) , [Trend Micro](#) , [GFI](#) , [SonicWALL](#) , [Secure Computing](#) , [MessageLabs](#) , [CA](#)

Top Reviews

Most Popular

- Related Article
- [DH](#)
- [Re](#)
- [W](#)  
[im](#)

# Now you better watch out

July 30th, 2008

## HD Moore pwned with his own DNS exploit, vulnerable AT&T DNS servers to blame

Posted by Dancho Danchev @ 8:08 am

**Categories:** [Hackers](#), [Exploit code](#), [Black Hat](#), [Metasploit](#)

**Tags:** [Google Inc.](#), [DNS](#), [DNS Server](#), [AT&T Corp.](#), [Server](#), [Domain Names](#), [Networking](#), [Internet](#), [Dancho Danchev](#)


**14** TalkBacks ADD YOUR OPINION
 SHARE
 PRINT
 E-MAIL
 WORTHWHILE?
**+8** 12 VOTES

A week after |)ruid and HD Moore release part 2 of DNS exploit, HD Moore's company [BreakingPoint](#) has suffered a traffic redirection to a rogue Google site, thanks to the already poisoned cache at AT&T servers to which his company was forwarding DNS traffic :



"It happened on Tuesday morning, when Moore's company, BreakingPoint had some of its Internet traffic redirected to a fake Google page that was being run by a scammer. According to Moore, the hacker was able to do this by launching what's known as a cache poisoning

### Essential Topics

Think your data is safe? It's time to Outthink eBook now.

Ad Fee

**At the Whiteboard**

Leading Virtualization Performance



Find out more about Intel's processor platform

Adesh Gupta

Adesh Gupta  
Marketing Manager  
Intel

### Sponsored Links

→ **The DDOS Spe**  
Identify and block DDOS automatically and in  
[www.riorey.com](http://www.riorey.com)

That's not the most interesting  
part of my story!

# Who

WELCOME TO PA VIETNAM

VNNIC has named **P.A Vietnam Ltd** the domain registrar for ccTLD (.VN) Vietnam

**P.A Vietnam Ltd** 's a partner of Enom who is accredited the Internet Corporation for Assigned Names and Numbers (ICANN).



WEBDESIGN \$159



- [Home](#)
- [Company](#)
- [Order](#)
- [Vietnam Domain](#)
- [Domain](#)
- [Web/Mail Hosting](#)
- [Servers](#)
- [Reseller](#)
- [Webdesign](#)
- [Support](#)
- [Services](#)
- [Transfer Domain](#)
- [Renew Services](#)

<b>Personal</b> \$1  30 Mb 300 MB Transfer 5 Emails	<b>Business</b> \$10  1000 Mb 5000 MB Transfer 80 Emails	<b>Reseller</b> \$20  500 Mb 10000Mb Transfer
---	--	--

**Search domain**

www.

<input type="checkbox"/> .com	<input type="checkbox"/> .net	<input type="checkbox"/> .org	<input type="checkbox"/> .info
<input type="checkbox"/> .biz	<input type="checkbox"/> .ws	<input type="checkbox"/> .us	<input type="checkbox"/> .vn
<input type="checkbox"/> .com.vn	<input type="checkbox"/> .net.vn	<input type="checkbox"/> .org.vn	<input type="checkbox"/> .edu.vn

**Việt Nam Hosting Windows (from 05-10-2006) NEW**



Windows Hosting Server is located in Việt Nam with very fast speed. It's very good for connections from Vietnam. You can switch to Vietnam if you are hosting in US.

ORDER LOGIN

# What



**NEWS**

- Politics
- Business
- Sci-Tech
- Social
- Lifestyle
- Sports
- International
- Education
- Travel

**IN DEPTH**

**LIFE IN VIETNAM**

**PHOTOGALLERY**

**RESOURCES**

- STOCK MARKET
- EXCHANGE RATES
- WEATHER

**WEEK IN FOCUS**

**SEARCH**

Go

## Pavietnam hacked, nearly 8,000 .vn websites crippled

16:58' 28/07/2008 (GMT+7)

*VietNamNet Bridge – The domain server of PAVietnam, a large hosting service provider in Vietnam, was controlled by hackers in the morning on July 27, which deadlocked around 8,000 websites based on PAVietnam's server.*

Hackers converted access to PAVietnam.com to Vnexpress online newspaper. Access to 5giay.com, an online market based on PAVietnam server, was also transferred to yahoo.com.vn.

Three major domain names of PAVietnam, PAVietnam.net, PAVietnam.com and dotvndns.com were also controlled by hackers.

Around 8,000 websites based on the PAVietnam domain server (ns\*pavietnam.net) were paralysed because of the attack.

Around 1,155 websites are based on PAVietnam.com domain server and 5,456 others on PAVietnam.net server. Most of the websites have .com.vn and .vn domain names, which belong to businesses and organisations in Vietnam.

PAvietnam reported the case to the Vietnam Computer Emergency Response Team (VNCERT) to ask for assistance. It instructed clients to



### EDITOR'S CHOICE

VFF willing to spend over \$2.4 million to get MU

Sotheby's denies selling fake Thai paintings

- ▶ Official suspended in connection to PCI scandal
- ▶ Prime rate continues going down

### Politics

President gets to work at APEC meetings

→ Ambassador: One UN Initiative works in Vietnam

→ POLITICS IN BRIEF 23/11

→ Vietnam, Venezuela vow to build comprehensive partnership

→ Party Vietnam-China links start at local level

# How's it happened?

## **.vn Websites Hacked**

*July 29th, 2008 · 1 Comment*

---

“It’s believed the hackers broke in through a hole in DNS to control the administration,” said VNCERT Technical Branch Chief Do Ngoc Duy Trac.

Trac also said VNCERT recommended Vietnam Internet Network Information Center (VNNIC) and other internet service providers (ISPs) assist the recovery work.

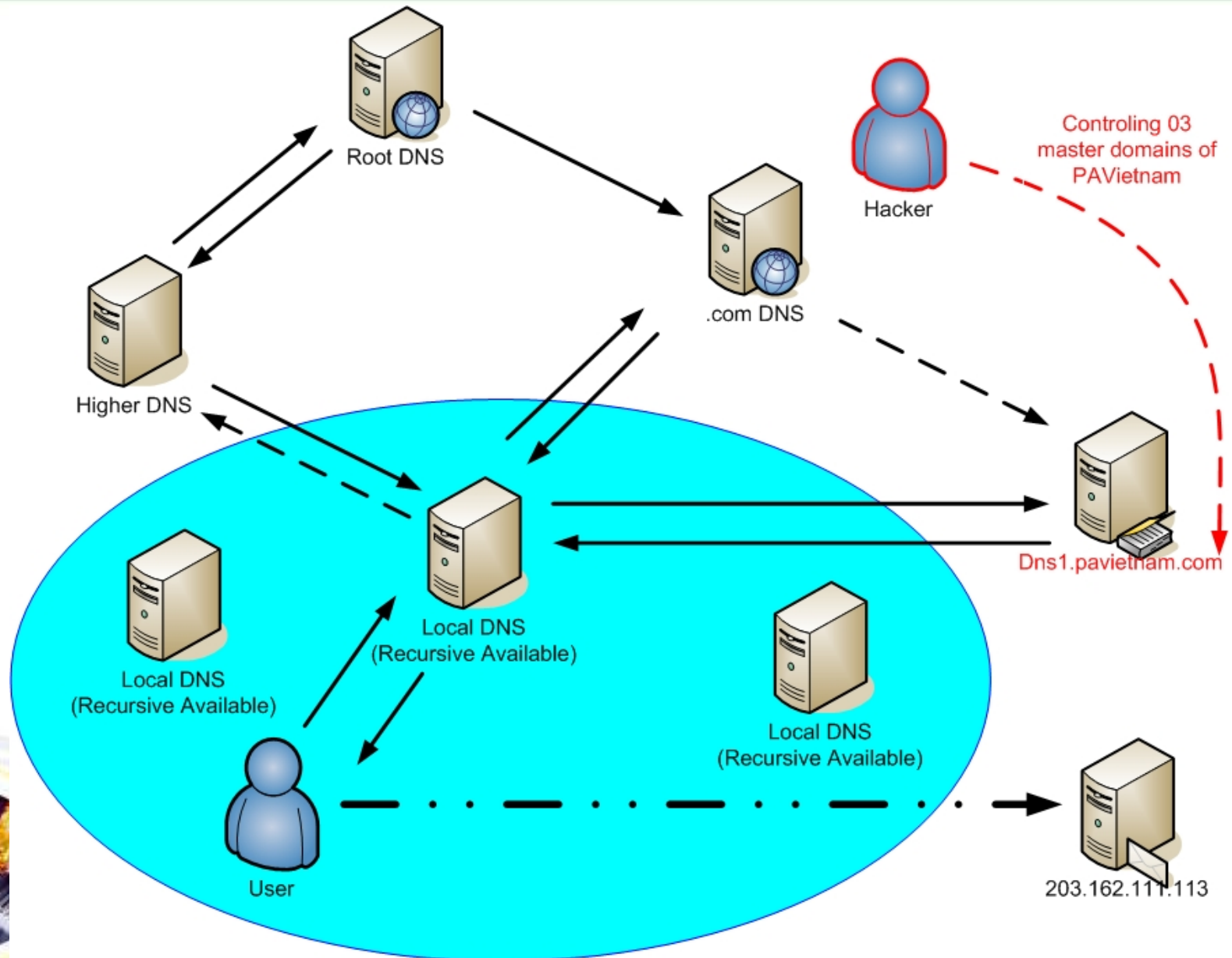
PA Vietnam Ltd, which is affiliated to the Ministry of Information and Communication’s National Domain Center, is one of the computers that provides the “.vn” domain.

Statistics from VNNIC showed PA Vietnam was hosting 9,738 active domains, accounting for 14.39 percent of the domestic market, making it the second biggest among the 16 companies offering such services in Vietnam.

---

**Tags:** Uncategorized

# Coordinate activities



# How bad is it ?

- Thousands of website and email systems stop working for at least one week.
- Hacker ability to deface thousands of website (Thank God he didn't!)
- He also can intercept biz emails.
- Redirect millions of end-user to malicious websites.
- ...
- Reason ? He want to keep low profile.



# Lessons learned for CERTs (1)

- Don't underestimate early warning even if it look like very old one!
- A good relationship with multiform partners will help CERT made right decision in critical situation.
- Don't hesitate issue "very early warning" in un-clear conditions.
- Newspapers, televisions,... is more effective than email and website in this emergency response case.



# Lessons learned for CERTs (2)

- DNS is very critical because it affect all other services and need more protection in the near future.
- International legal proceeding related to domain is very complicated and take very long time.
- Quality of response (QoR) must be a mandatory requirements for ISPs.



# Vietnam Antispam Law

- Vietnam's Antispam Decree promulgated on 13 August 2008 by the Prime Minister.
- Became effective as from 13 September.
- Stakeholders have 60 days to prepare.
- Begin of 2009 will start inspect program for the compliance of related companies (zero milestone).



# Spam classification

- 1. Emails, mobile messages aiming to cheat, disturb or spread computer harmful virus and malicious softwares or to breach clause 2, Article 12 of the Law on Information Technology.
- 2. Advertising emails and advertising mobile messages breach the principles of sending advertising emails and advertising mobile messages as prescribed in Article 7, Article 9 and Article 13 of this Decree.

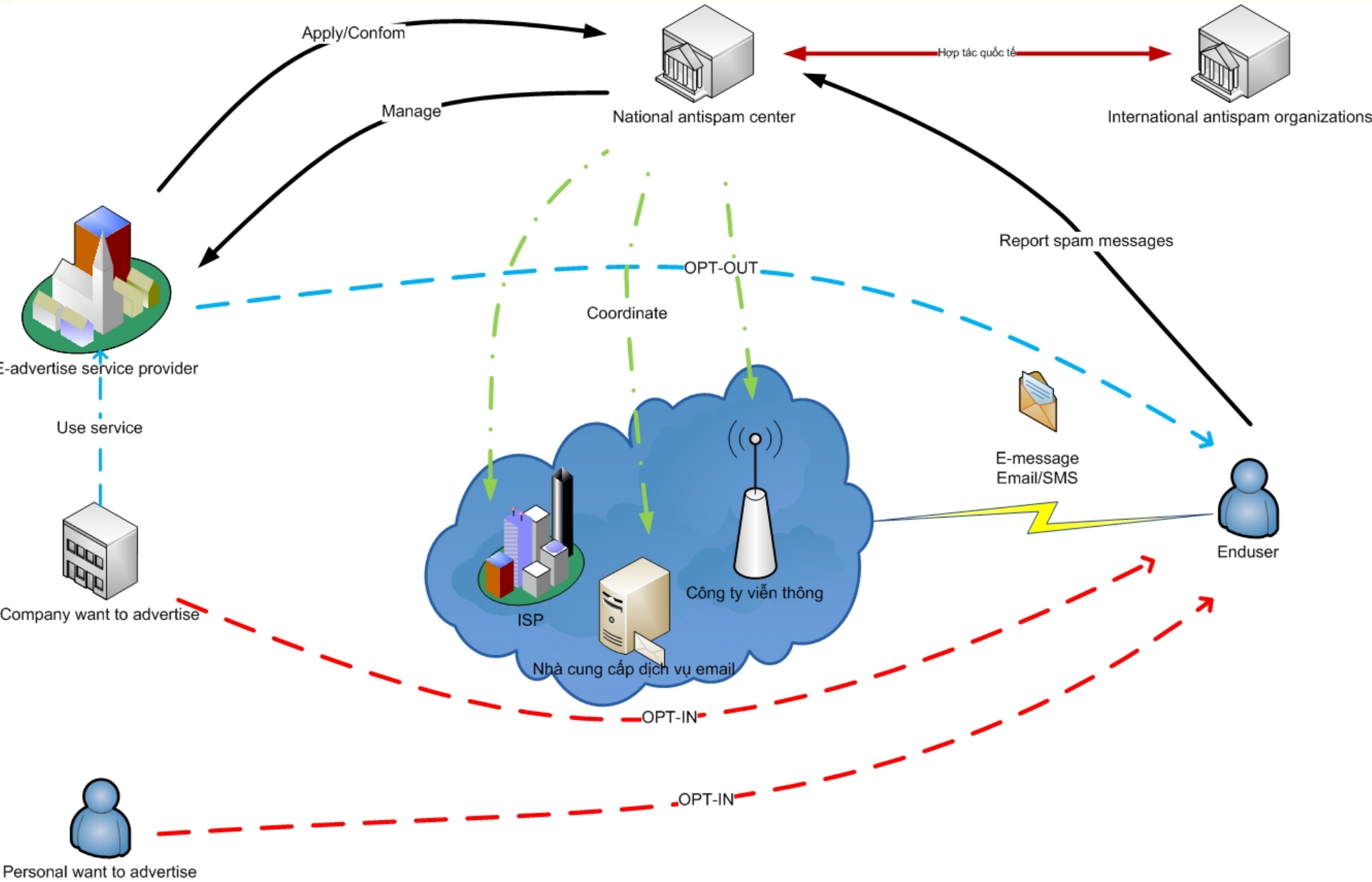


# Prohibited acts

- 1. Sending spam.
- 2. Misinforming between email subject and email content for spam purpose.
- 3. Helping, allowing other people to use your electronic equipments for sending or transiting spam.
- 4. Exchanging, trading or disseminating softwares to collect email addresses or copyright to use such softwares.
- 5. Using softwares to collect email addresses without permission of owners of those emails.
- 6. Exchanging and trading email lists or right to use email lists for spam purpose.



# Management model



# Mandatory requirements to advertising emails



- 1. **Subject must be suitable for content** and advertising content must comply with law stipulations on advertising.
- 2. Advertising emails **must be labeled** per prescribed in Article 10 of this Decree.
- 3. There must be **information on advertiser** per clause 1 and clause 3, Article 11 of this Decree.
- 4. In case of advertising emails send out by EASP, there must be **information on EASP** per clause 2 and clause 3, Article 11 of this Decree.
- 5. There is **refusal function** per Article 12 of this Decree.

EASP – Email Advertising Service Provider



# Mandatory requirements to advertising message



- 1. Advertising mobile messages **must be labeled** per prescribed in Article 14 of this Decree.
- 2. In case of advertising mobile messages send out by MASP, there must be **information on MASP** per Article 15 of this Decree.
- 3. There is **refusal function** per Article 16 of this Decree.

MASP – Mobile Advertising Service Provider



# Vietnam Antispam Law

- English version is ready!
- Would love to exchange antispam experiences and cooperation with other partners.
- Contact:
  - Do Ngoc Duy Trac.
  - dntrac@vncert.vn.



# Coordination for a better cyberspace!



**Thank you!!!**

