www.vncert.gov.vn

MINISTRY OF INFORMATION AND COMMUNICATIONS
VIET NAM EMERGENCY RESPONSE TEAM

INCIDENT RESPONSE DDOS ATTACKS IN VIETNAM

www.vncert.gov.vn

MINISTRY OF INFORMATION AND COMMUNICATIONS
VIET NAM EMERGENCY RESPONSE TEAM

Presenter: **Dang Hai Son**

Regional Director

GSEC | C|HFI Computer Hacking Forensic INVESTIGATOR | E|CSA EC-Council Certified Security Analyst | C|EH Certified Ethical Hacker | CompTIA Security+

About me

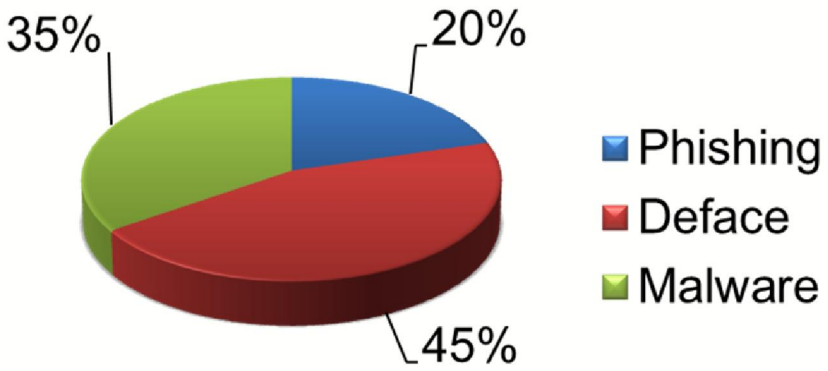
- Master of Computer Science
- Computer Hacking Forensic Investigator (CHFI)
- GIAC Security Essentials Certification (GSEC)
- EC-Council Certified Security Analyst (ECSA)
- Certified Ethical Hacker (CEH)
- Comptia Security+

Full Name: **Dang Hai Son**

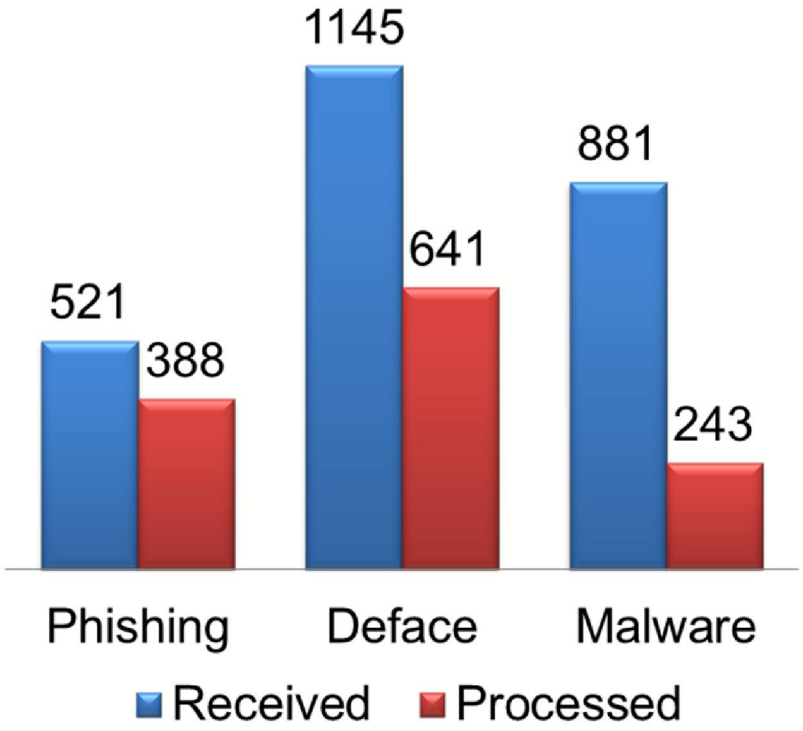
Dang Hai Son is currently in charge of VNCERT branch in central Vietnam (VNCERT is a unit of the Ministry of Information and Communications of the Socialist Republic of VietNam). Assisting Vietnam organizations and Internet users in implementing proactive measures to reduce the risks of computer security incidents and to assist them in responding to such incidents when they occur.

Statistics Cyber Attacks in Vietnam

Type of Cyber Attacks

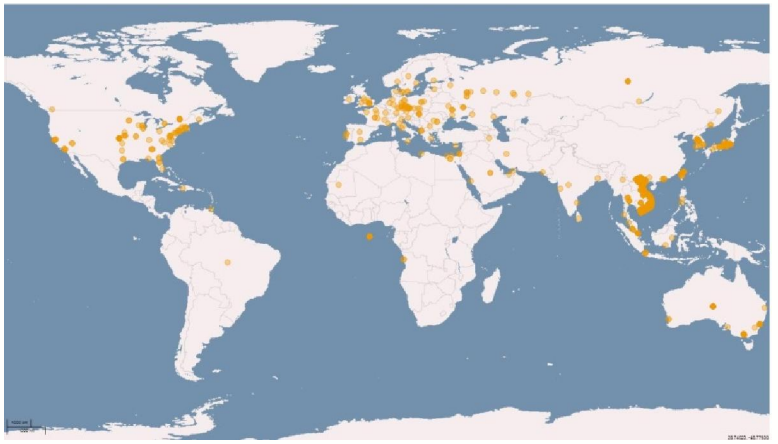


Total attacks VNCERT receive and process

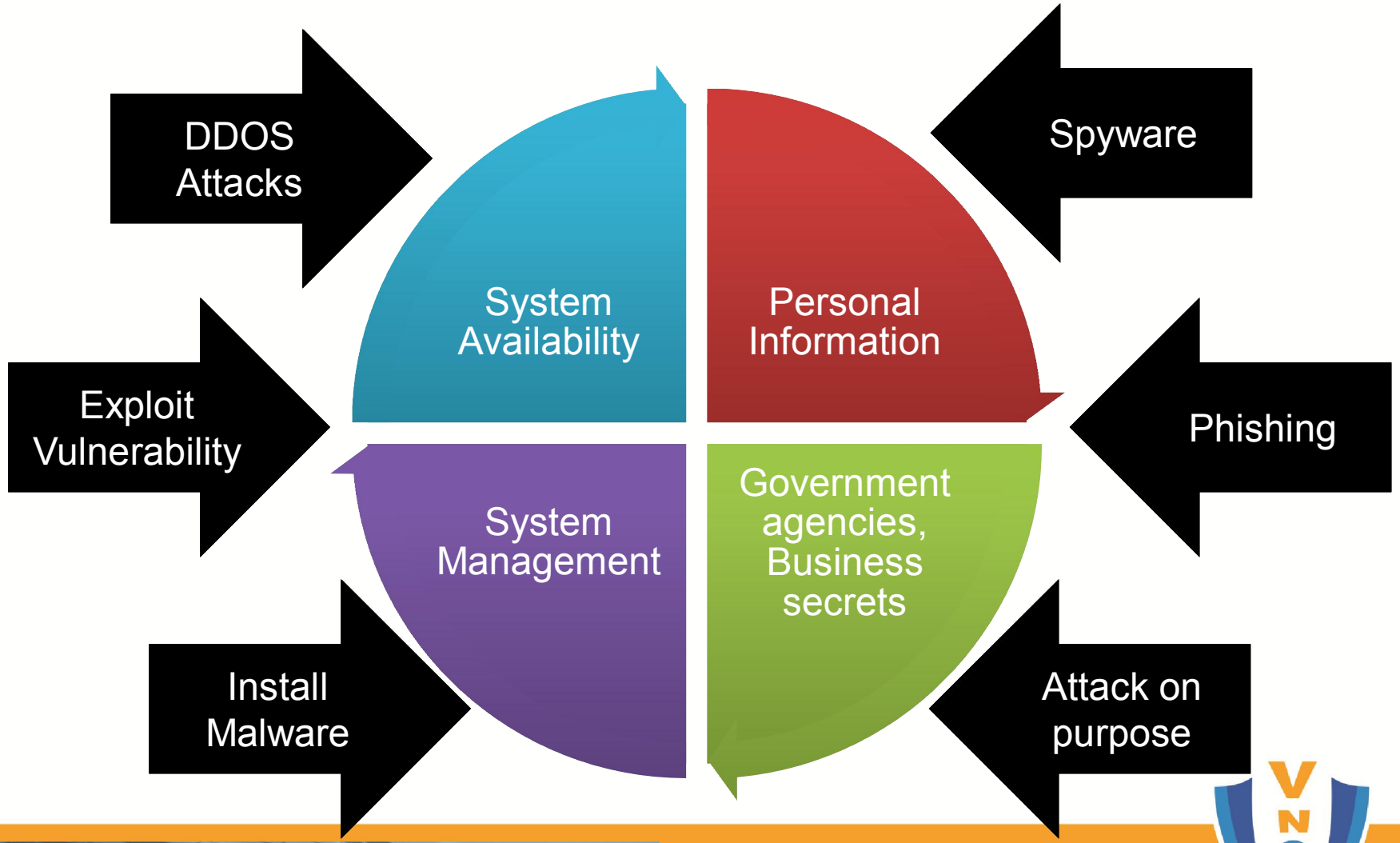


VNCERT Incident Response Report 2013

- Statistics botnets:
  - Zeus Botnet: **14075** IP addresses.
  - Sality Botnet, Downadup, Traffic-converter: **113273** IP addresses. Send warning information to **174** IP addresses (Government and State Agencies).
  - Brobot Botnet (request cooperation from US-CERT): malware removed from **335** sites (linked page **2373**).
  - Statistics Botnet DDoS attack: **~100.000 – 300.000** bots, **69** network addresses (Government and State Agencies), C&C Server: **7** IP addresses, **18** domains from **5** countries.



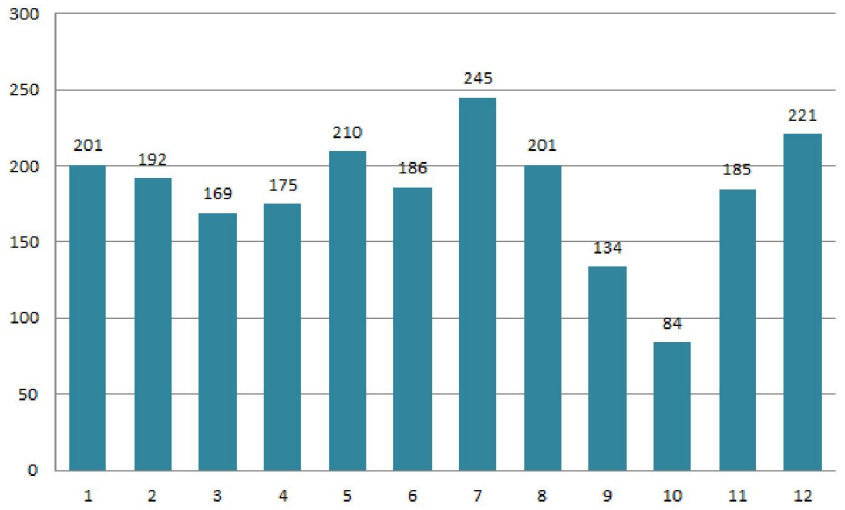
The common types of attacks



Statistics Website Attacked

Date	Notifier	H	M	R	L	Domain	OS
2013/09/12	sy.t	H	M	R		soyte.baria-vungtau.gov.vn	Linux
2013/09/12	copres-dz	H	M	R		soytebrvt.gov.vn	Linux
2013/09/09	M4STER 1T4LI4N H@CKERS TE4M					stnmt.gialai.gov.vn/admin/	Win 2008
2013/09/07	AnonGhost	H				tinhdoanbg.gov.vn	Linux
2013/09/07	SultanHaikal		M	R		vnca.molisa.gov.vn/x.htm	Win 2003
2013/09/07	SultanHaikal		M	R		phapluatlaodong.molisa.gov.vn/...	Win 2003
2013/09/07	SultanHaikal	H	M	R		thanhnien.molisa.gov.vn	Win 2003
2013/09/07	SultanHaikal			R		nccd.molisa.gov.vn/x.htm	Win 2003
2013/08/23	TurkHackArmy	H				www.congankhanhhoa.gov.vn	Unknown
2013/08/22	Hmei7			R		daitruyenhinh.hoabinh.gov.vn/i...	Linux
2013/08/22	Hmei7		M	R		buonmathuot.gov.vn/indonesia.gif	Linux
2013/08/22	越南邻国宰相	H	M			mohaids.gov.vn	Win 2003
2013/08/21	CrashBandicot69		M	R		congbao.laocai.gov.vn/Crash.htm	Win 2008
2013/08/21	CrashBandicot69		M	R		thutuchanhchinh.laocai.gov.vn/...	Win 2008
2013/08/21	CrashBandicot69		M	R		doankhoiccq.laocai.gov.vn/Cras...	Win 2008
2013/08/21	CrashBandicot69			R		lcitp.laocai.gov.vn/Crash.htm	Win 2008
2013/08/21	Ali TOOFAN			R		www.phuongkhuongmai.gov.vn/z0n...	Win 2003
2013/08/20	RainsevenDotMy			R		www.caugiay.hanoi.gov.vn/image...	Win 2003
2013/08/16	RainsevenDotMy			R		www.cphud.danang.gov.vn/images...	Linux
2013/08/13	ArTiN FUCKING LAMER			R		kstthc.moit.gov.vn/index.htm	Win 2008
2013/08/13	RainsevenDotMy			R		congtacxahoi.molisa.gov.vn/en/...	Win 2003
2013/08/10	Dr.SHA6H	H	M			www.hoichuthapdoquangbinh.gov.vn	Win 2003
2013/08/10	Dr.SHA6H	H	M			www.hoikhuyenhocqb.gov.vn	Win 2003
2013/08/10	Dr.SHA6H	H	M	R		www.congthuongquangbinh.gov.vn	Win 2003
2013/08/10	M3QD4D		M			vpdt.sonhoa.gov.vn/m3.htm	Win 2008

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30



Identify trends attacks

- Attacks intended to steal information, malicious code inserted, with the form: E-mail spoofing, phishing site (Phishing), Hack site (defacements), ... especially targeting state agencies and government.
- Spreading malicious increasing (the site for the cracked software or free, sex websites, games, social networking, ...) and the fake e-mail attachments.
- Malware on 3G mobile platforms has increased rapidly.

E-newspapers in Vietnam DDOS attack (July 2013)

Incident response DDOS attacks (1)

1. VNCERT received a assistance request prevent DDOS attacks from the E-newspapers
2. VNCERT require system administrators to send information related to the incident DDOS attack (Webserver, Firewall, ... log files, network activities *.pcap files).
3. Analysis DDOS attack (strength, speed packets sent, packet type, the number of IP addresses is sent to the destination, …).
4. Based on these factors (speed, package type, ...) to build a set of addresses likely infected computer malware.
5. VNCERT require ISPs to provide information about static IP addresses for conducting malware samples.

Incident response DDOS attacks (2)

6. Analysis malicious code and send malware samples to antivirus organizations, companies requirements analysis support.
7. VNCERT implement sum information malware analysis results.
8. VNCERT coordinating ISPs implementation shutdown the C&C server if they are in Vietnam.
9. Coordinate with other CERT if C&C server located outside Vietnam.
10. Send malware samples and simultaneously require the antivirus vendors to update database to remove malware in computer users.
11. Awareness activities to users on how to check your computer is infected with malicious perform DDOS attack or not? Provides links tool for users to download and remove malware (e-newspapers, forums, social networking)

Thank you !

Address: Ministry of Information and Communications
VIET NAM EMERGENCY RESPONSE TEAM (VNCERT)
18 Nguyen Du, Ha Noi, Viet Nam
Tel: (84) 4 36404 424
Fax: (84) 4 36404 425
Email:dhson@vncert.vn