

Cybersecurity Global status update

Dr. Hamadoun I. Touré
Secretary-General, ITU

Cybercrime takes a toll on the global economy

- Online fraud, identity theft, and lost intellectual property;
- On governments, companies and individuals around the world;
- Inflicting damage on the innocent, on the vulnerable, and on our children.




Some Major Attacks in 2011

January	<ul style="list-style-type: none">• Major cyber intrusion in Defense Research and Development in Canada. Finance Department and Treasury board forced to disconnect from the internet
March	<ul style="list-style-type: none">• Hackers penetrate French government computer network• South Korea Defense Network penetrated• RSA Secure ID compromised• Attacks at EU's Commission and External Action Service
June	<ul style="list-style-type: none">• Attacks at Sony. Millions of logins leaked• Attacks and NATO internal network• Attacks at International Monetary Fund (IMF)• Hackers disrupt 51 Malaysian government websites• UK Treasury under sustained cyberattack
October	<ul style="list-style-type: none">• Cyber-attacks on UK at disturbing levels• Japan under Heavy Cyber Attack
November	<ul style="list-style-type: none">• Hackers destroyed a pump used by a US water utility• Duqu computer virus Detected by Iran civil defense organization• More than 100 Pakistani Government Sites Under Malware attack• Thousands of United Nation (UNDP) logins leaked• Cyber attacks hit Fujitsu local government system in Japan• Largest DDOS attack hit Chinese company

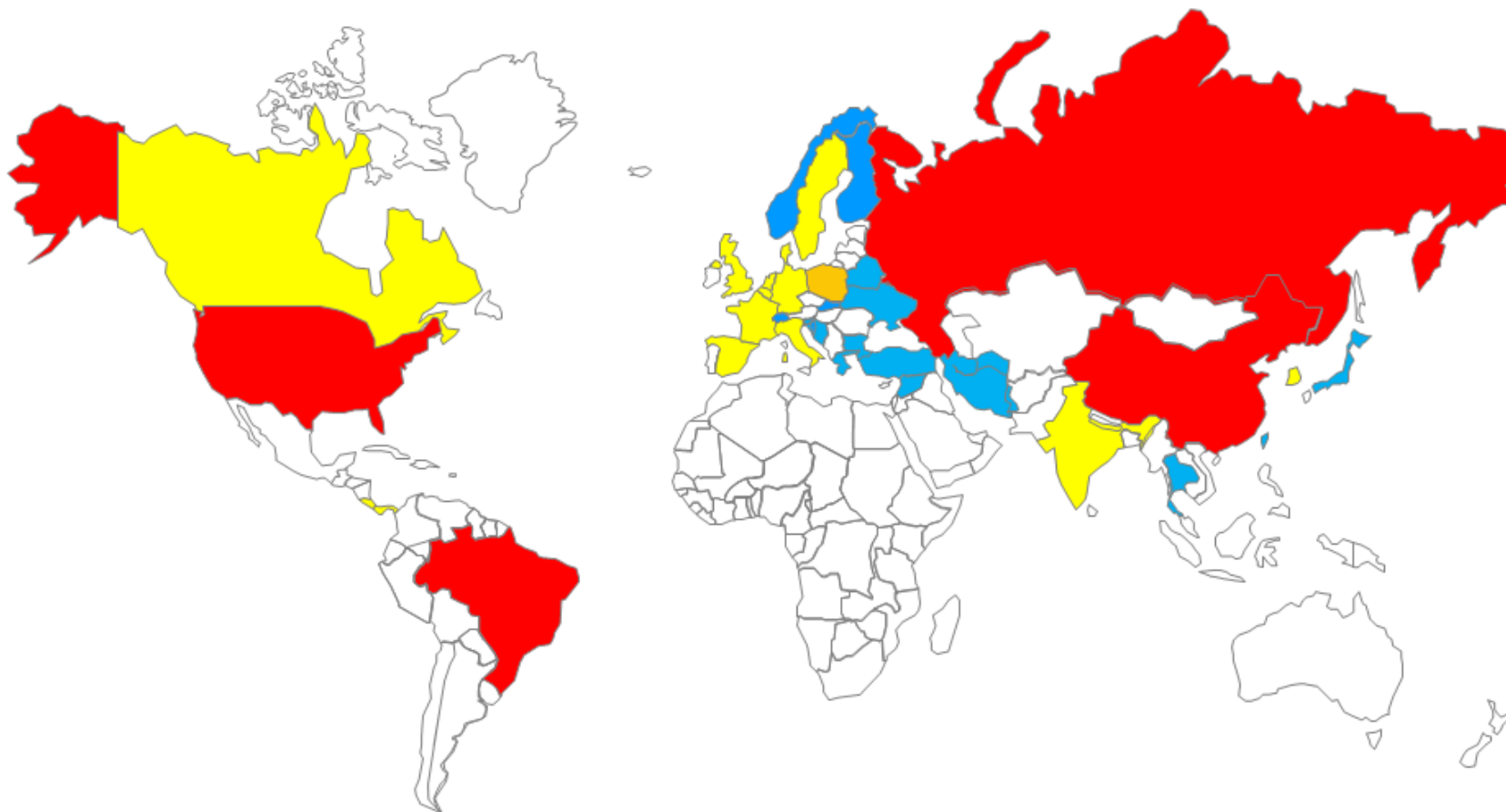
Many more have happened, and many more will...

Top 26 attack destination countries

Attack Percentage Scale

	High	4.00 % – 25.0%
	Med	1.01 % – 3.99%
	Low	0.11% – 1.00%

Rank	Country	Percentage	Rank	Country	Percentage	Rank	Country	Percentage
1	United States	24.01	10	South Korea	2.21	19	UAE	0.63
2	China	22.81	11	Panama	2.08	20	Taiwan	0.59
3	Brazil	17.29	12	Japan	1.60	21	Finland	0.56
4	Russia	6.05	13	Sweden	1.51	22	Hungary	0.39
5	Denmark	2.94	14	Spain	1.43	23	Turkey	0.36
6	India	2.77	15	Italy	1.33	24	Norway	0.24
7	United Kingdom	2.73	16	France	1.27	25	Lebanon	0.13
8	Canada	2.72	17	Poland	1.08	26	Luxembourg	0.11
9	Netherlands	2.43	18	Romania	0.7			

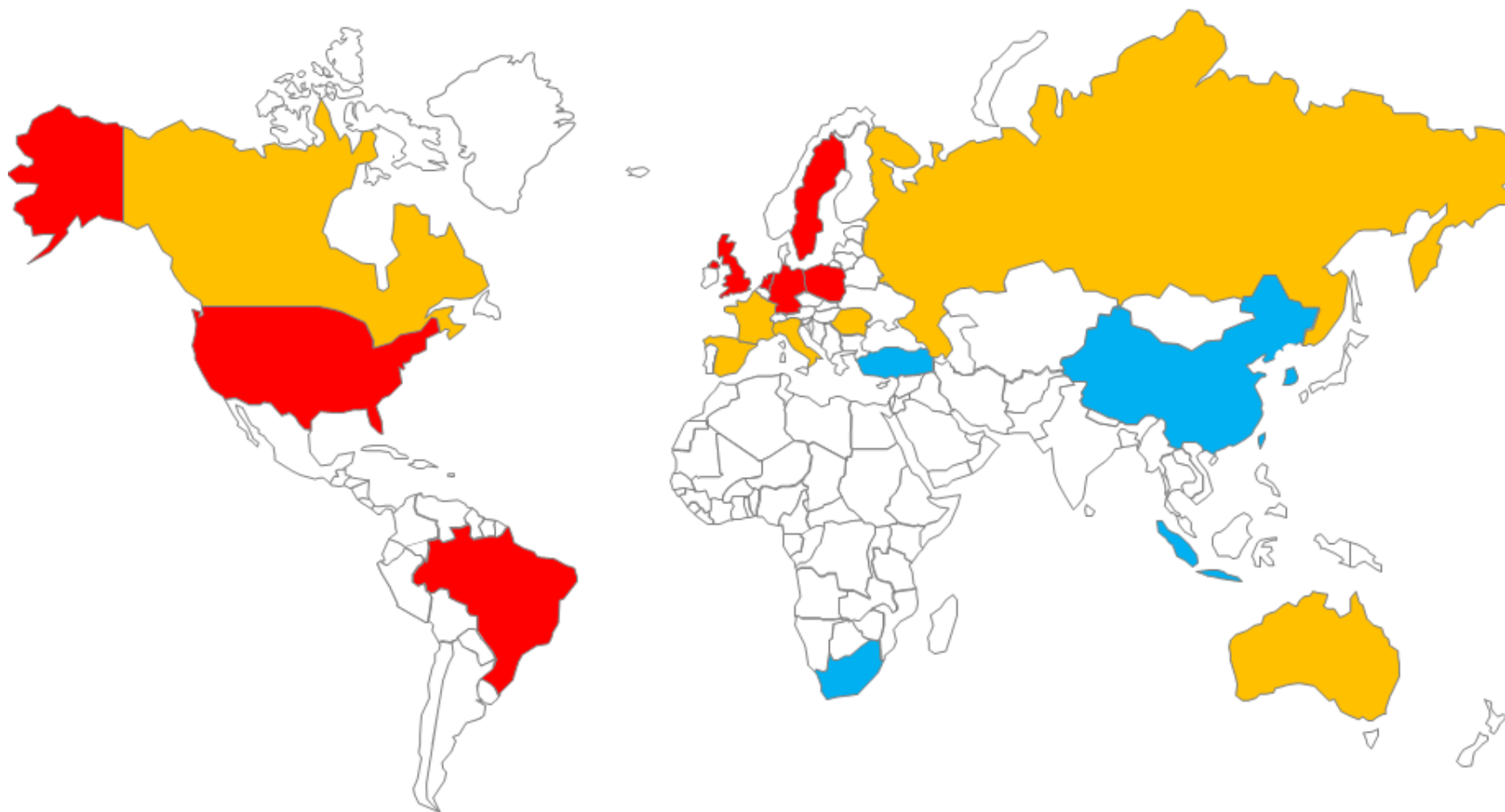


Top 20 attack source countries

Attack Percentage Scale

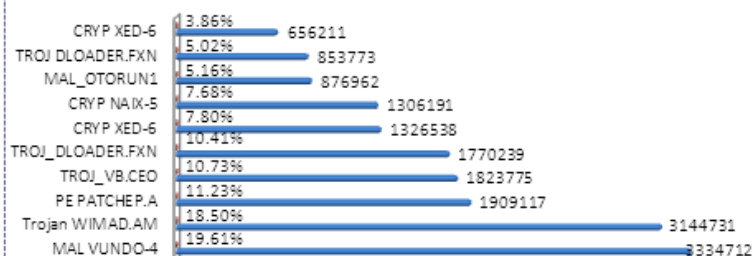
High	2.62 % – 50.09 %
Med	0.33 % – 2.19 %
Low	0.02 % – 0.20 %

Rank	Country	Percentage	Rank	Country	Percentage	Rank	Country	Percentage
1	US (United States)	50.09	8	CA (Canada)	2.19	15	TR (Turkey)	0.20
2	SE (Sweden)	10.41	9	FR (France)	2.13	16	KR (South Korea)	0.15
3	NL (Netherlands)	9.82	10	RU (Russian Federation)	1.45	17	CN (China)	0.15
4	BR (Brazil)	9.81	11	IT (Italy)	0.90	18	TW (Taiwan)	0.11
5	DE (Germany)	4.40	12	AU (Australia)	0.72	19	ID (Indonesia)	0.11
6	PL (Poland)	3.56	13	RO (Romania)	0.70	20	ZA (South Africa)	0.02
7	GB (Great Britain)	2.62	14	ES (Spain)	0.33			

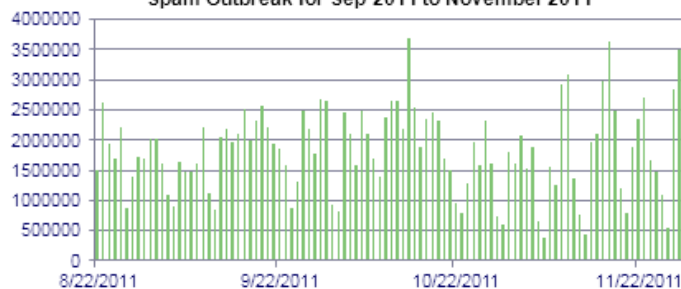


Threats Report: November 2011

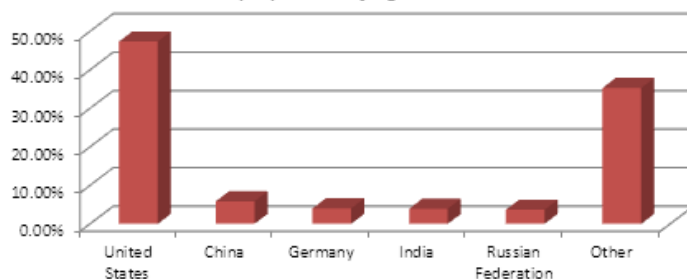
Global Top 10 Malwares with Number of Systems Affected



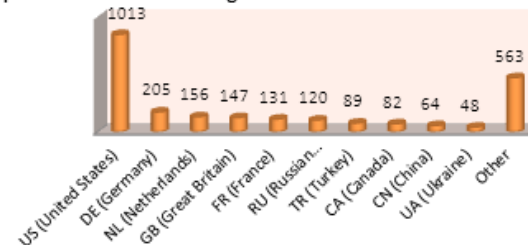
Spam Outbreak for Sep 2011 to November 2011



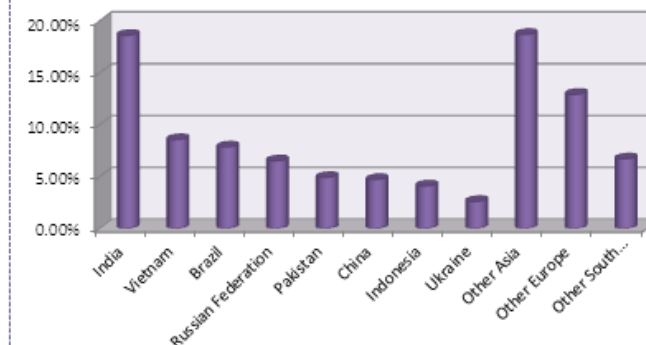
Top Spam Relaying Countries



Top 10 C&C Server Hosting Countries with Number of Servers



Global Zombie Distribution



Legend

Malware: Hostile, intrusive, or annoying software or program code designed to infiltrate a computer system (virus/worms/Trojans/root-kit/backdoors/spyware).

Botnets: Software agents/bots that run autonomously and automatically under a common command-and-control structure and perform malicious activities.

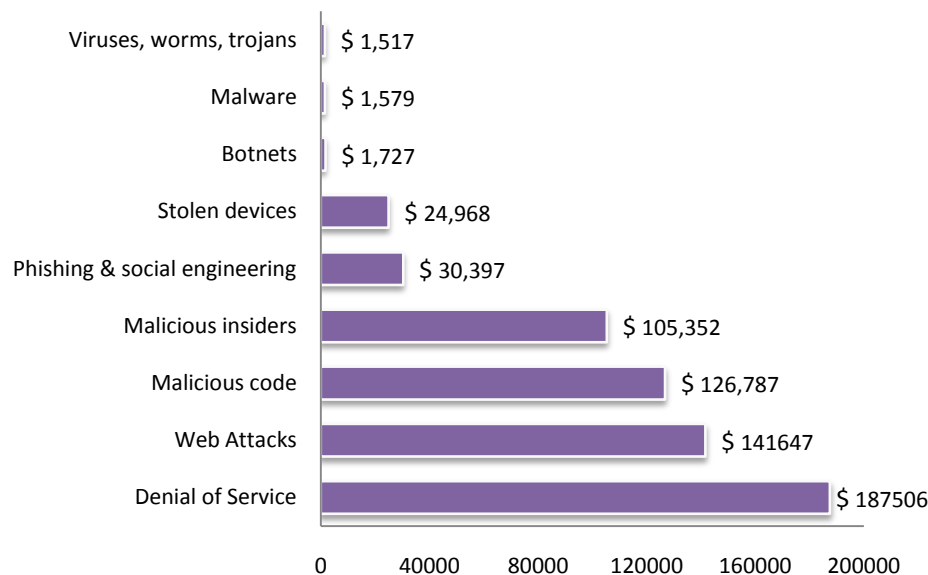
Phishing: Fraudulent process of attempting to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.

Spamming: Abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately in the form of e-mail, instant messaging etc.

Statistical Information Sources: Shadowserver, Symantec, Kaspersky, McAfee, Sophos, Commtouch, Trendmicro, Securiylab, Atlas Arbor, ThreatExpert
Aggregator: ITU-IMPACT

Financial impact

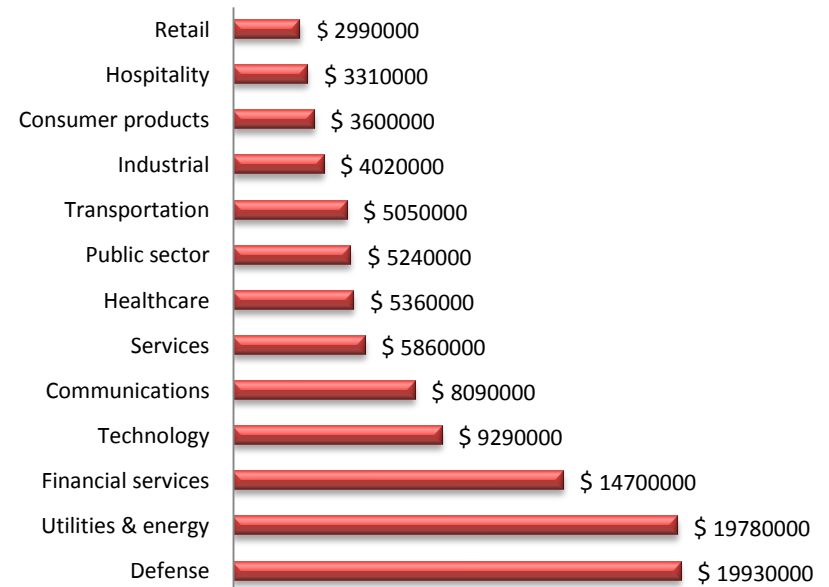
- It is estimated that overall cost of cybercrime is as much as \$1 trillion on a global basis.
- The estimated average cost to an individual US organization was \$3.8 million per year in 2010.
- In 2011 the estimated average cost to an individual US organization is \$5.9 million per year, with a range from \$1.5 million to \$36.5 million per organization.
- The most costly cyber crimes are those caused by malicious code, denial of service, stolen or hijacked devices and malicious insiders.



Average annual cyber crime cost weighted by the frequency of attack incidents

Source:

http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf



Average annual cost by sector for sample of 50 US organizations for 2011

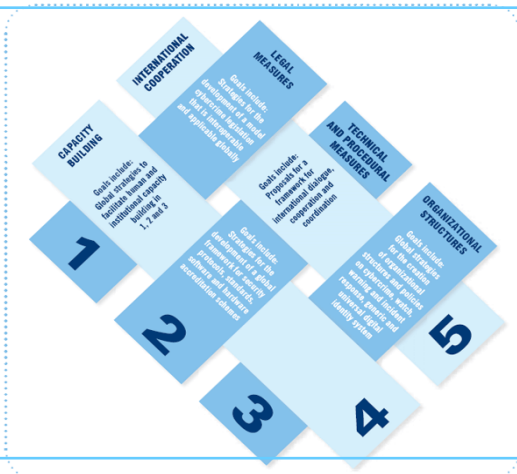
Source:

http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

ITU and Cybersecurity



2003 – 2005
WSIS entrusted ITU as sole facilitator for WSIS Action
Line C5
“Building Confidence and Security in the use of ICTs”



2007
ITU Secretary-General launched the Global Cybersecurity
Agenda (GCA)
A framework for international cooperation in
cybersecurity



2008 - 2010
ITU Membership endorsed the GCA as the ITU-wide
strategy on international cooperation; launch of ITU Child
Online Protection initiative

The world's foremost cybersecurity alliance!

- Within GCA, ITU and the International Multilateral Partnership Against Cyber Threats (IMPACT) are pioneering the deployment of solutions and services to address cyberthreats on a global scale.
- ITU-IMPACT's endeavor is the first truly global multi-stakeholder and public-private alliance against cyber threats, staging its state-of-the-art facilities in Cyberjaya, Malaysia.
- ITU-IMPACT supports Member States and others with the expertise, facilities and resources to effectively enhance the global community's capability and capacity to prevent, defend against and respond to cyber threats.



UN Delivering-As-One

- United Nations Chief Executive Board (CEB) has given high priority to Cybersecurity, following a proposal from the ITU Secretary General, on a UN-wide strategy.
- ITU and UNODC have been identified as lead UN Agencies to facilitate the review of the policy and technology implications of cyber-crime and cyber-threats for the UN system and are co-chairing a Working Group
- ITU is facilitating the process towards a UN common framework on Cybersecurity that would address the issue of Cybersecurity at national, regional and global level.



ITU – UNODC MoU

Legal Measures

Capacity Building and Technical Assistance

Intergovernmental and expert meetings

Joint Study

Sharing knowledge and information



Cyberpeace

The potential of the internet



*"There is a real hunger to address the need
for a safe and secure future in cyberspace.
All governments need to respond to this
demand;
not just some governments, in some regions
of the
world, but across the globe."*

UK Foreign Secretary, William Hague, London
Cyberspace Conference, November 2011

Cybersecurity: a global issue requiring a global solution

- Every government should commit itself to giving its people access to communications.
- Every government should commit itself to protecting its people in cyberspace.
- Every country should commit itself not to harbour terrorists / criminals in its own territories.
- Every country should commit itself not to be the first to launch a cyber attack on other countries.
- Every country should commit itself to collaborate with others within an international framework of co-operation to ensure that there is peace in cyberspace.

For further information
www.itu.int/cybersecurity
cybersecurity@itu.int