Tổng quan về an toàn an ninh thông tin

Đại học Duy Tân

Đà Nẵng, 22/12/2012

NGƯỜI TRÌNH BÀY: LÊ TRUNG NGHĨA
VĂN PHÒNG PHỐI HỢP PHÁT TRIỂN
MÔI TRƯỜNG KHOA HỌC & CÔNG NGHỆ,
BỘ KHOA HỌC & CÔNG NGHỆ

Email: letrungnghia.foss@gmail.com
Blogs: http://vn.myblog.yahoo.com/ltnghia
http://vnfoss.blogspot.com/
Trang web CLB PMTDNM Việt Nam: http://vfossa.vn/vi/
HanoiLUG wiki: http://wiki.hanoilug.org/
Đăng ký tham gia HanoiLUG:
http://lists.hanoilug.org/mailman/listinfo/hanoilug/

Nội dung

A. Tổng quan tình hình an toàn an ninh thông tin.

B. Kiến trúc & an ninh hệ thống thông tin

C. Chuẩn hóa & an ninh hệ thống thông tin

D. Một số biện pháp & công cụ cho an ninh hệ thống thông tin

E. Nhu cầu giáo dục đào tạo về nguồn mở

Một số trích dẫn đáng lưu ý

- Barack Obama, 29/05/2009: “Sự thịnh vượng về kinh tế của nước Mỹ trong thế kỷ 21 sẽ phụ thuộc vào an ninh có hiệu quả của không gian mạng, việc đảm bảo an ninh cho không gian mạng là xương sống mà nó làm nền vững chắc cho một nền kinh tế thịnh vượng, một quân đội và một chính phủ mở, mạnh và hiệu quả”. “Trong thế giới ngày nay, các hành động khủng bố có thể tới không chỉ từ một ít những kẻ cực đoan đánh bom tự sát, mà còn từ một vài cái gõ bàn phím trên máy tính – một vũ khí huỷ diệt hàng loạt”. Văn bản gốc tiếng Anh. Video.

- TrendMacro: Nền công nghiệp chống virus đã lừa dối người sử dụng 20 năm nay. Khả năng chống virus hầu như là không thể với số lượng khổng lồ các virus hiện nay;

- McAfee: 80% tất cả các cuộc tấn công bằng phần mềm độc hại có động lực là tài chính..., 20% các cuộc tấn công còn lại có các mục đích liên quan tới tôn giáo, gián điệp, khủng bố hoặc chính trị.

Một số trích dẫn đáng lưu ý

Từ tài liệu về ANKGM, xuất bản tháng 02/2012

- Isaac Ben-Israel, cố vấn về ANKGM của Thủ tướng Israel Benjamin Netanyahu: "*Một cuộc CTKGM có thể giáng một thiệt hại y hệt như một cuộc chiến tranh thông thường. Nếu bạn muốn đánh một quốc gia một cách khốc liệt thì bạn hãy đánh vào cung cấp điện và nước của nó. Công nghệ không gian mạng có thể làm điều này mà không cần phải bắn một viên đạn nào*".

- Phyllis Schneck của McAfee: "*Công nghệ mới bây giờ được tập trung bên dưới các hệ điều hành. Nó giao tiếp trực tiếp với phần cứng máy tính và các con chip để nhận biết được hành vi độc hại và sẽ đủ thông minh để không cho phép hành vi độc hại đó... Giao tiếp với phần cứng là Hoàng Hậu trên bàn cờ - nó có thể dừng kẻ địch hầu như ngay lập tức hoặc kiểm soát được cuộc chơi dài hơn. Cách nào thì chúng ta cũng sẽ thắng*".

Thông điệp: An ninh hệ thống thông tin phụ thuộc trước hết vào kiến trúc của hệ thống thông tin đó, cả phần cứng lẫn phần mềm!

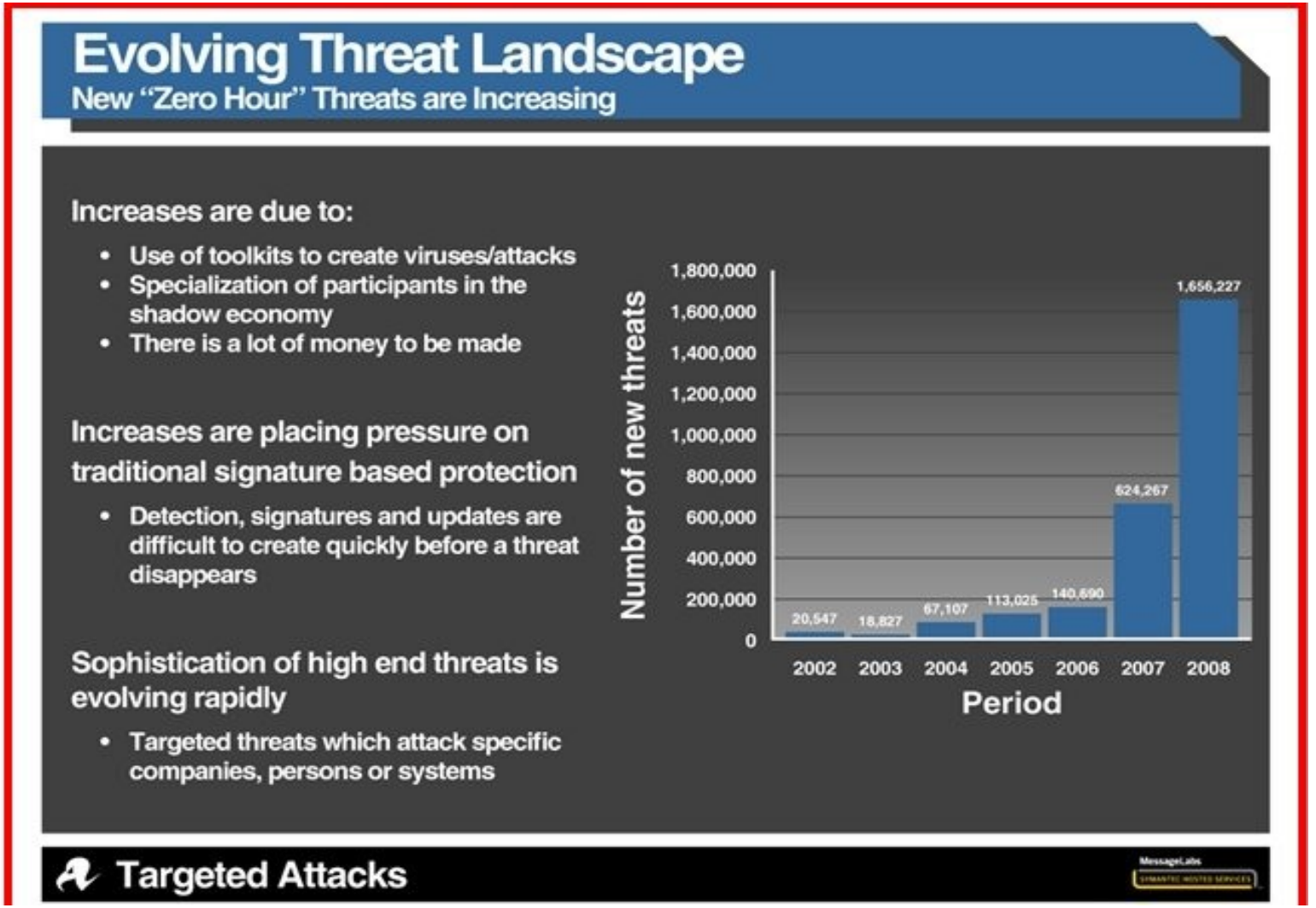
Lý do và mục đích tấn công

Về chính trị: không chỉ gián điệp thông tin, mà còn phá hoại cơ sở hạ tầng
- Xung đột giữa các nước: Israel <> Syria, Palestine; Mỹ - Liên quân <> Iraq; Nga <> Estonia, Georgia; Mỹ - Hàn <> Bắc Triều Tiên; Mỹ - Israel <> Iran.
- Vào hệ thống các lực lượng vũ trang: CIA, MI6, FBI, NATO, Hải quân Ấn...
- Vào các hệ thống an ninh nhất thế giới: LHQ, các bộ của nhiều nước.
- Stuxnet ra đời giữa năm 2010 sớm hơn dự báo.
- Tấn công vào các hệ thống cơ sở hạ tầng điện, nước, đường sắt, dầu khí... Tại Mỹ năm 2009 có 9 vụ → 198 vụ, có 17 vụ nghiêm trọng.
- Stuxnet, Duqu, Flame: vũ khí KGM không thể kiểm soát, nhà nước bảo trợ.
- WikiLeaks phơi các tài liệu mật của nhiều quốc gia
- Chạy đua vũ trang trong KGM

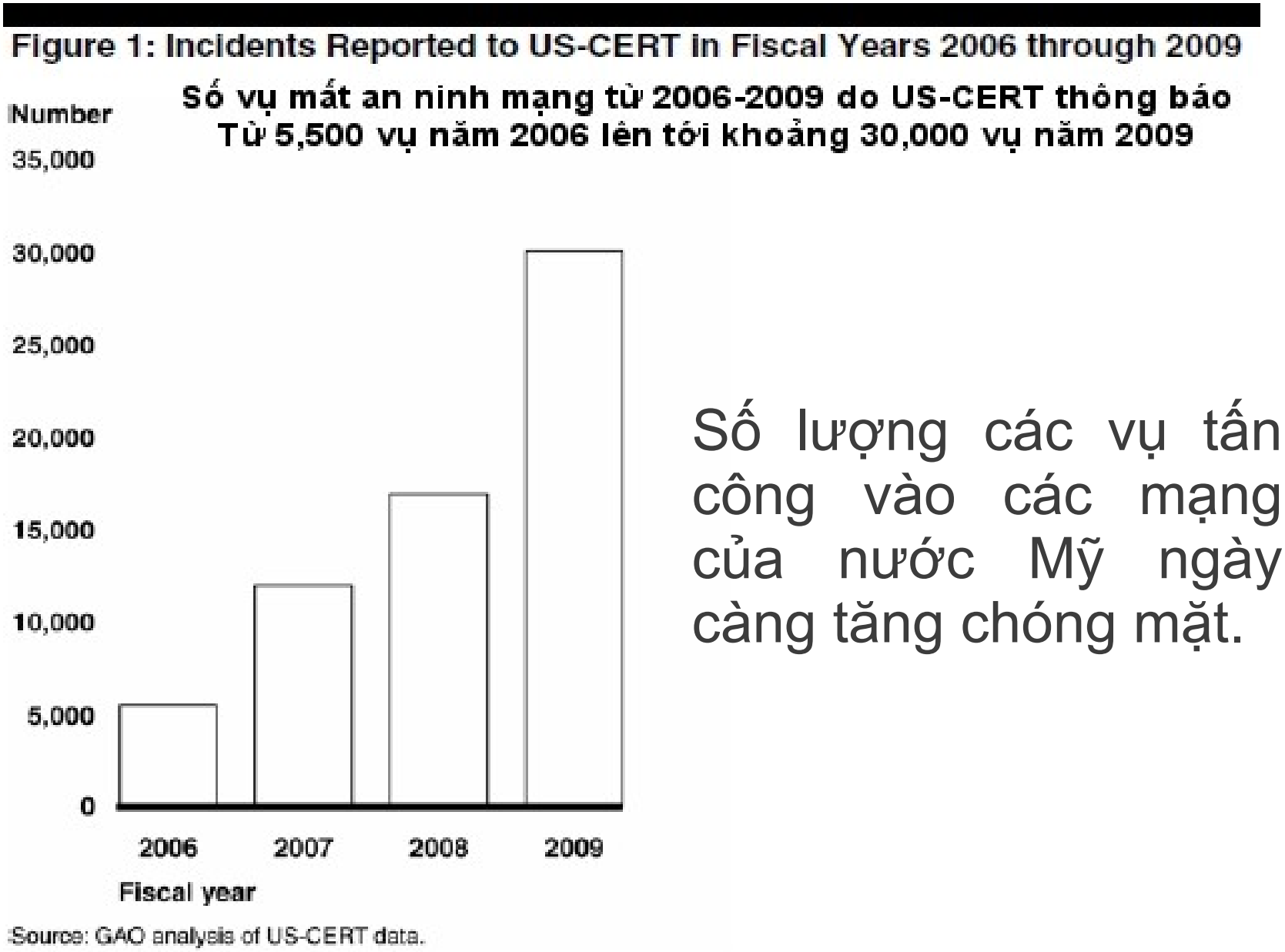
Về kinh tế: ăn cắp thông tin sở hữu trí tuệ, ăn cắp tiền, tống tiền...
- Các tập đoàn lớn bị tấn công: Sony, Honda, Lockheed Martin, Mitsubishi... Vụ Aurora với hơn 30 công ty Mỹ như Google, Adobe, …
- Gauss, có liên quan với Stuxnet-Duqu-Flame, chuyên giám sát các giao dịch, gián điệp, ăn cắp ủy quyền và dữ liệu các ngân hàng trực tuyến.
- Khu vực tài chính, ngân hàng: CitiBank, NASDAQ, Global Payments...
- Các cơ quan chứng thực số CA: Codomo, Diginotar, GlobalSign, StartSSL...
- Các công ty tư vấn an ninh: Startfor, Kaspersky, Symantec...
- Các dạng lừa đảo ăn cắp và tống tiền

Một vài hình ảnh minh họa

Số lượng các mối đe dọa tăng vọt gấp 5 lần trong năm 2008, bằng với 5 năm trước đó cộng lại.

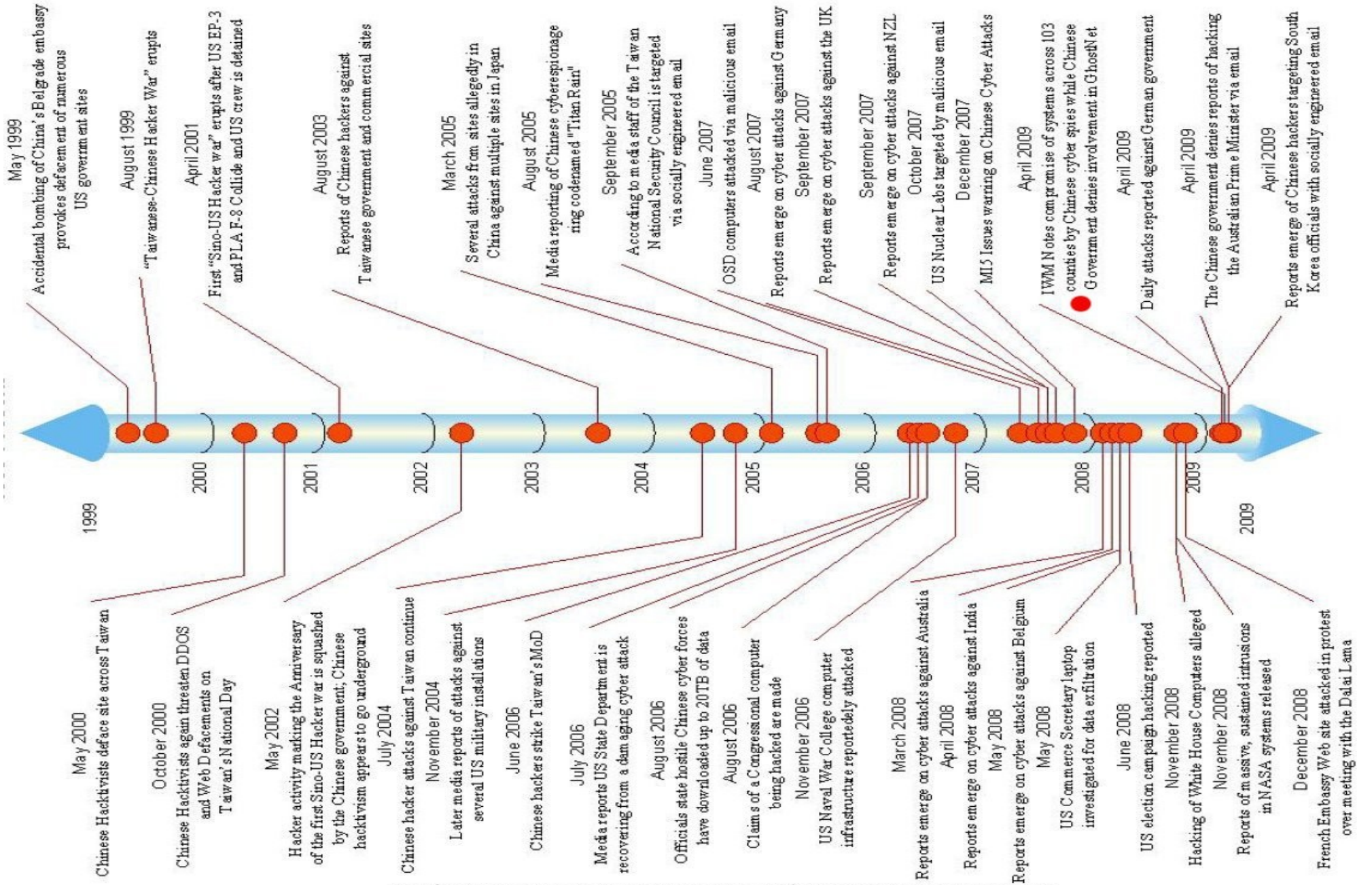


Một vài hình ảnh minh họa



Số lượng các vụ tấn công vào các mạng của nước Mỹ ngày càng tăng chóng mặt.

Các cuộc tấn công không gian mạng của Trung Quốc vào các quốc gia trên thế giới cho tới năm 2009.



Nguồn: Khả năng của CHND Trung Hoa tiến hành CTKGM và khai thác mạng máy tính, tập đoàn Northrop Grumman xuất bản ngày 09/10/2009.

An ninh không gian mạng năm 2009 qua các con số Báo cáo của Symantec tại Ngày An toàn Thông tin VN 2010 tại Hà Nội, 23/11/2010

The Problem

A Quick Look At Cyber Security 2009 By The Numbers

3,200,000,000

attacks blocked by Symantec in 2009

- 12 new 0day vulnerabilities
- 14 new public SCADA vulnerabilities
- 321 browser plug-in vulnerabilities
- 4,501 new vulnerabilities
- 17,432 new bot C&C servers
- 30,000 domains hosting malware
- 59,526 phishing hosts
- 2,895,802 new AV signatures
- 6,798,338 bot infected computers

240,000,000

million new malware variants

In the time it takes to give this presentation, we will block more than 540,000 attacks!

Số lượng các virus mới liên tục tăng thêm hơn 1 triệu loại sau mỗi 6 tháng, trong đó 99.4% - 99.8% là cho Windows. (G-Data).

	Platform	# 2010 H1	Share	# 2009 H2	Share	Diff. 2010 H1 2009 H2	# 2009 H1	Share	Diff. 2010 H1 2009 H1
1	Win32	1,001,902	98.5 %	915,197	99.0 %	+9 %	659,009	99.3 %	+52 %
2	MSIL[4]	9,383	0.9 %	2,732	0.3 %	+243 %	365	0.1 %	+2471 %

Σ

Σ: 1.017.208
W: 1.011.285
W: 99.4%

	Platform	# 2010 H2	Share	# 2010 H1	Share	Diff. 2010H2 2010H1	# 2009 H2	Share	Diff. 2010H2 2009H2
1	Win32	1,056,304	98.1%	1,001,902	98.5%	+5%	915,197	99.0%	+15%
2	.NET	15,475	1.4%	9,383	0.9%	+65%	2,732	0.3%	+466%

Σ: 1.076.236
W: 1.071.779
W: 99.5%

	Platform	# 2011 H1	Share	# 2010 H2	Share	Diff. 2011H1 2010H2	# 2010 H1	Share	Diff. 2011H1 2010H1
1	Win32	1.218.138	97,8 %	1.056.304	98,1 %	+15,3 %	1.001.902	98,5 %	+21,6 %
2	MSIL	21.736	1,7 %	15.475	1,4 %	+40,5 %	9.383	0,9 %	+131,7 %

Σ: 1.245.403
W: 1.239.874
W: 99.5%

	Platform	# 2011 H2	Share	# 2011 H1	Share	Diff. # 2011 H2 # 2011 H1		
1	Win	1,305,755	98.2%	1,218,138	97.8%	+7.2%	0,4 %	-20,8 %
2	MSIL	18,948	1.4%	21,736	1.7%	-12.8%	0,1 %	-9,8 %
							<0,1 %	+273,1 %
							<0,1 %	+39,1 %
							<0,1 %	+3,1 %

Σ: 1.330.146
W: 1.324.703
W: 99.6%

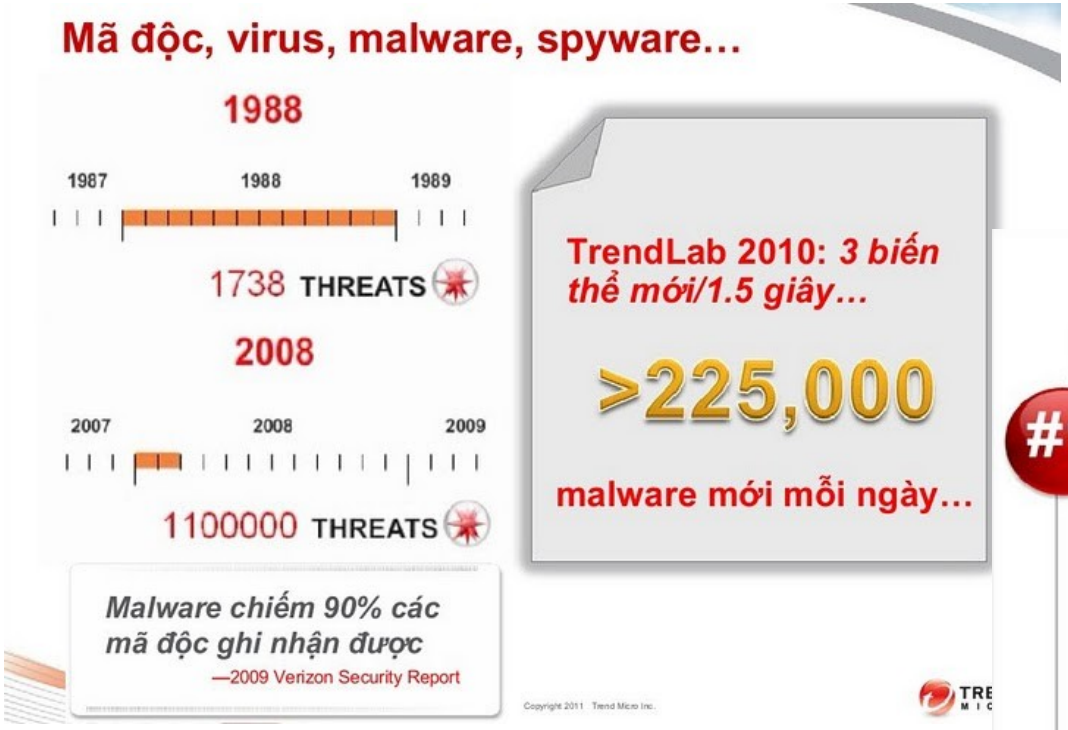
	Platform	#2012 H1	Share	#2011 H2	Share	Diff. #2012 H1 #2011 H2	Diff. #2012 H1 #2011 H1
1	Win	1,360,200	98.4%	1,305,755	98.2%	+4.2%	+11.7%
2	MSIL	18,561	1.4%[4]	18,948	1.4%	-2.0%	-14.6%
3	WebScripts	1,672	0.1%	2,402	0.2%	-30.4%	-46.5%
4	Java	662	<0.1%	244	<0.1%	+171.3%	+111.5%
5	Scripts[5]	483	<0.1%	626	<0.1%	-22.8%	-42.0%

Σ: 1.381.967
W: 1.378.761
W: 99.8%

Table 1: *Top 5 platforms of the last two six-month periods*

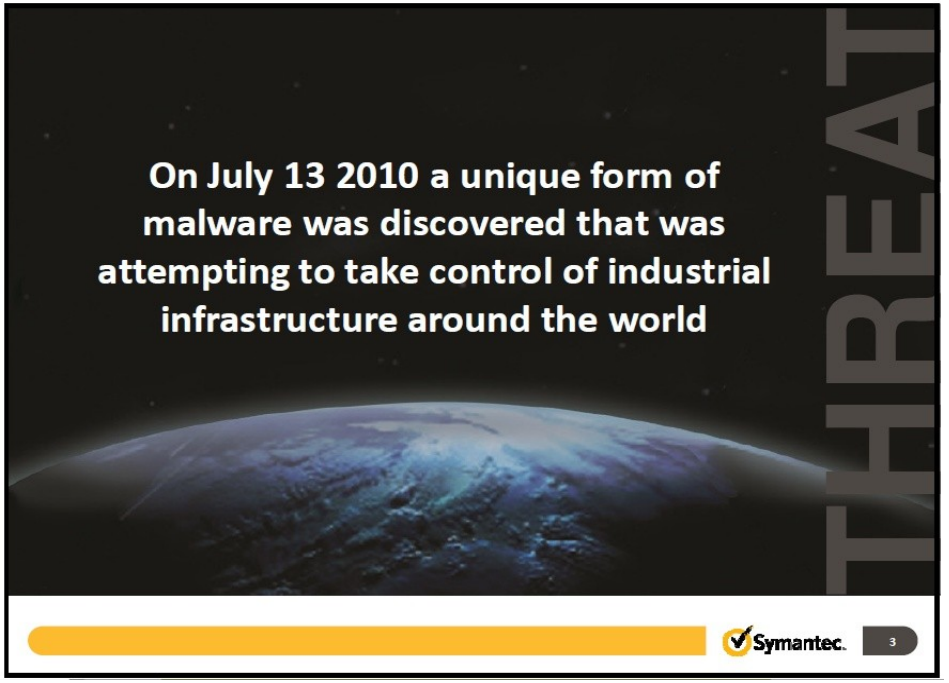
Σ: Tổng số
W: Windows

Năm 2010, mỗi giây có 2 phần mềm độc hại được sinh ra.
Nhanh nhất phải 3 giờ đồng hồ mới có được 1 bản vá.
Báo cáo của TrendMacro ngày 06/04/2011 tại Hà Nội
Hội thảo và triển lãm quốc gia về an ninh bảo mật



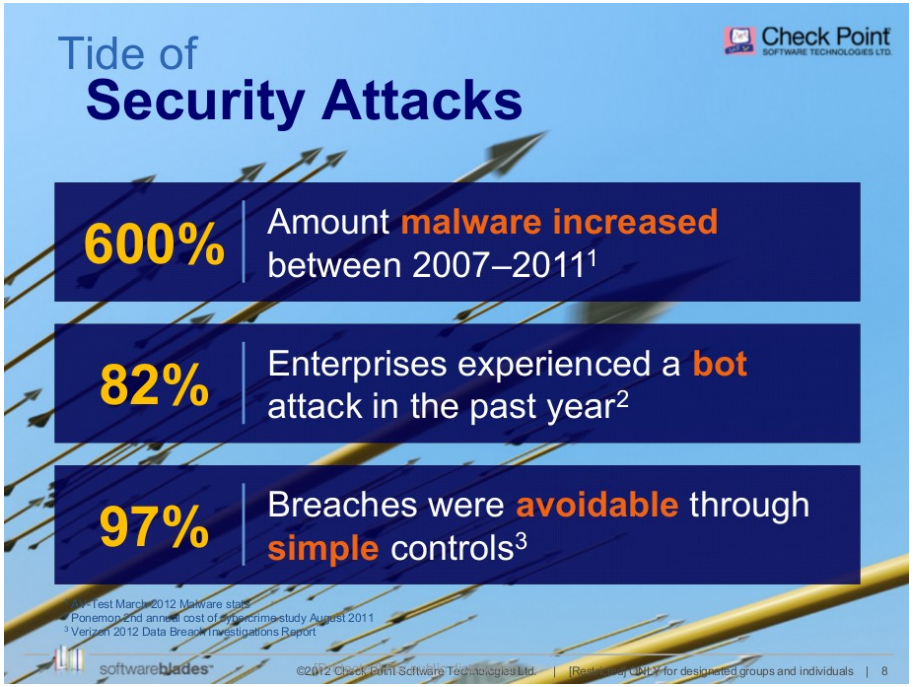
Ngày 13/07/2010 dạng phần mềm độc hại độc nhất vô nhị đã định chiếm quyền kiểm soát hạ tầng công nghiệp
Báo cáo của Symantec ngày 23/11/2010 tại Hà Nội.

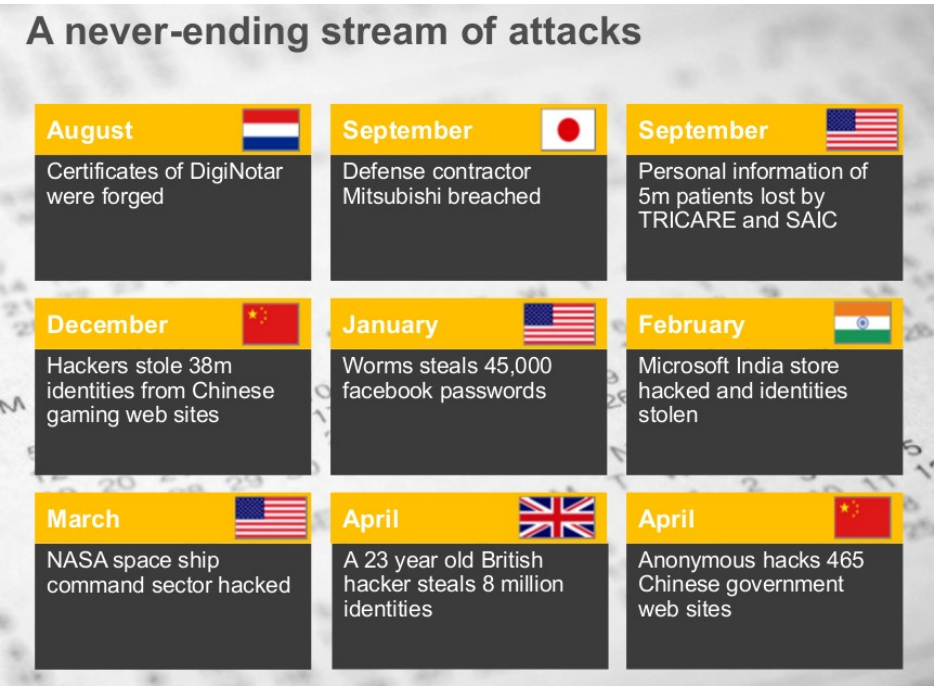
- Kỷ nguyên của Stuxnet, sử dụng 4 lỗi ngày số 0 trong Windows; 2 chứng thực số bị ăn cắp và các lỗi trong SCADA của Siemens để đánh què chương trình hạt nhân của Iran.
- Không chỉ là gián điệp thông tin mà còn là phá hoại các cơ sở hạ tầng sống còn của mọi quốc gia như dầu/ khí/ điện/ hóa/ dược/ nguyên tử/giao thông...



- Lần lượt Stuxnet;Trojan Duqu (9/2011); Flame (5/2012); Gauss (8/2012); Narilam (11/2012). Các phần mềm diệt virus chịu!
- Đánh cơ sở hạ tầng: trước 2010 có 9 vụ; tới 2011 có 198 vụ, 17 vụ nghiêm trọng.
- WikiLeaks!
- Hàng loạt các cơ quan chứng thực (CA) bị tấn công, DigiNotar phá sản.

Báo cáo của CheckPoint ngày 23/11/2012 tại Hà Nội.





- 600%: số lượng phần mềm độc hại tăng từ 2007-2011; 82% doanh nghiệp lớn bị botnet tấn công năm 2011.
- 50% công ty trong Fortune 100 đã bị lây botnet Mariposa và ăn cắp dữ liệu; 80% tất cả các spam là gửi từ các botnet.
- Các cuộc tấn công bất tận vào mọi quốc gia năm 2011: Mỹ, Anh, Trung Quốc, Ấn Độ, Nhật, Hà Lan.

Một số hình ảnh về Việt Nam

Số 1 thế giới về tỷ lệ địa chỉ IP quốc gia bị nhiễm Conficker là 5%. (Shadowserver Foundation).

Conficker-VN

Position	ASN	Country	AS Name AS	Description	Routed Space	Unique A+B IPs	A+B Chart	Unique C IPs	C Chart	Unique Aggregate IPs	Aggregate Chart
4	7643	VN	VNN-AS	AP Vietnam Posts and	2,573,122	143,949		3,550		145,429	
24	18403	VN	FPT-A								
43	7552	VN	VIETEL-								
126	45899	VN	VNPT-A								
168	24086	VN	ETC-A								
318	7602	VN	SPT-A								
501	45543	VN	SCTV-A								
1640	38246	VN	SFONE-								
2924	24085	VN	QTSC-A								

Tháng ↑ 11/2009

Conficker-VN

Position	ASN	Country	AS Name AS	Description	Routed Space	Unique A+B IPs	A+B Chart	Unique C IPs	C Chart	Unique Aggregate IPs	Aggregate Chart
3	45899	VN	VNPT-AS	VN VNPT Corp	1,929,970	127,407 (6.6%)		0 (0%)		127,407 (6.6%)	
18	18403	VN	FPT-AS	AP The Corporation for Financing & Promot							
30	7552	VN	VIETEL-AS	AP Vietel Corporation							
156	24086	VN	ETC-AS	VN Electric Telecommunication Co							
250	45543	VN	SCTV-AS	VN SaiGon Tourist cable Television (							
353	7602	VN	SPT-AS	VN Saigon Postel Corporatio							
461	45903	VN	CMCTI-AS	VN CMC Telecom Infrastructure Co							
503	7643	VN	VNPT-AS	VN Vietnam Posts and Telecommunicat							
2656	45538	VN	ODS-AS	VN Online data services							
2919	55322	VN	NPC-AS	VN North Power Company							
2964	24085	VN	QTSC-AS	VN Quang Trung Software City Developm							
3376	45557	VN	VNTT-AS	VN Vietnam Technology and Telecomm							
3605	24173	VN	NETNAM-AS	AP Netnam Company							
3814	38727	VN	HUT-AS	VN Ha Noi University of Techno							
4055	24175	VN	VINAREN-AS	AP VietNam Research and Education							
4730	24176	VN	NETNAMHCMC-AS	AP Branch of Netnam Company in Ho C							

Tháng 06/2011 ↑
Tháng 04/2012 →

Conficker-VN

Position	ASN	Country	AS Name AS	Description	Routed Space	Unique A+B IPs	A+B Chart	Unique C IPs	C Chart	Unique Aggregate IPs	Aggregate Chart
2	45899	VN	VNPT-AS	VN VNPT Corp	2,330,474	93,803 (4.03%)		247 (0.01%)		93,910 (4.03%)	
18	7552	VN	VIETEL-AS	AP Vietel Corporation	18,441,064	27,669 (0.15%)		65 (0%)		27,707 (0.15%)	
20	18403	VN	FPT-AS	AP The Corporation for Financing & Promoting Technology	3,430,506	25,906 (0.76%)		101 (0%)		25,953 (0.76%)	
244	45903	VN	CMCTI-AS	VN CMC Telecom Infrastructure Company	84,538	1,299 (1.54%)		4 (0%)		1,301 (1.54%)	
279	24086	VN	ETC-AS	VN Electric Telecommunication Company	3,139,706	1,097 (0.03%)		8 (0%)		1,101 (0.04%)	
302	45543	VN	SCTV-AS	VN SaiGon Tourist cable Television Company	589,700	993 (0.17%)		2 (0%)		995 (0.17%)	
398	7602	VN	SPT-AS	VN Saigon Postel Corporation	352,388	730 (0.21%)		5 (0%)		730 (0.21%)	
407	7643	VN	VNPT-AS	VN Vietnam Posts and Telecommunications (VNPT)	266,652	702 (0.26%)		13 (0%)		707 (0.27%)	
1118	55322	VN	NPC-AS	VN North Power Company	12,284	150 (1.22%)		0 (0%)		150 (1.22%)	

Một số hình ảnh về Việt Nam (tiếp)

Table 2.1 Biggest botnets in 2009 **Những botnet lớn nhất trong năm 2009**

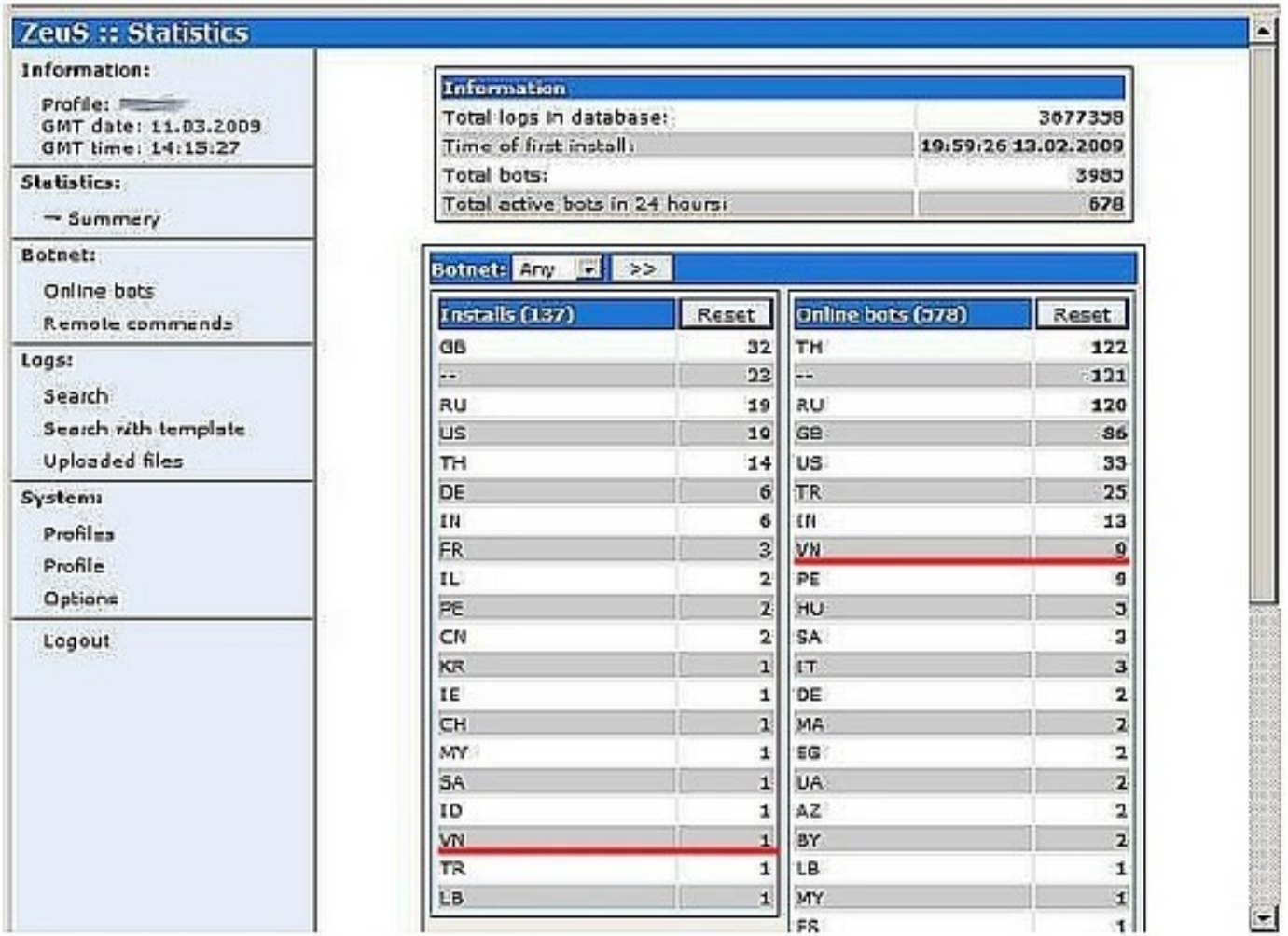
botnet	estimated botnet size	Country of Infection
Rustock	540k to 810k	Brazil (21%), USA (9%), Poland (7%)
Cutwail	100k to 1600k	Vietnam (17%), RepKorea(12%), Brazil (10%)
Bagle	520k to 780k	Brazil (12%), Spain (9%), USA (9%)
Bobax	100k to 160k	Spain (12%), Italy (7%), India (7%)
Grum	580k to 860k	Vietnam (18%), Russia (17%), Ukraine (8%)
Maazben	240k to 360k	Romania (17%), Brazil (11%), Saudi Arabia (7%)
Festi	140k to 220k	Vietnam (31%), India (11%), China (5%)
Mega-D	50k to 70k	Vietnam (14%), Brazil (11%), India (6%)
Xarvester	20k to 36k	Brazil (15%), Poland (11%), USA (10%)
Gheg	50k to 70k	Brazil (15%), Poland (8%), Vietnam (8%)
Unclassified Botnets	120k to 180k	
Other, smaller botnets	130k to 190k	

Source MessageLabs, *Message Labs Intelligence: 2009 Annual Security Report*, MessageLabs, December 2009, p.8.

Việt Nam đứng số 1 thế giới ở 4/5 trong tổng số 10 botnet lớn nhất thế giới năm 2009.

Một số hình ảnh về Việt Nam (tiếp)

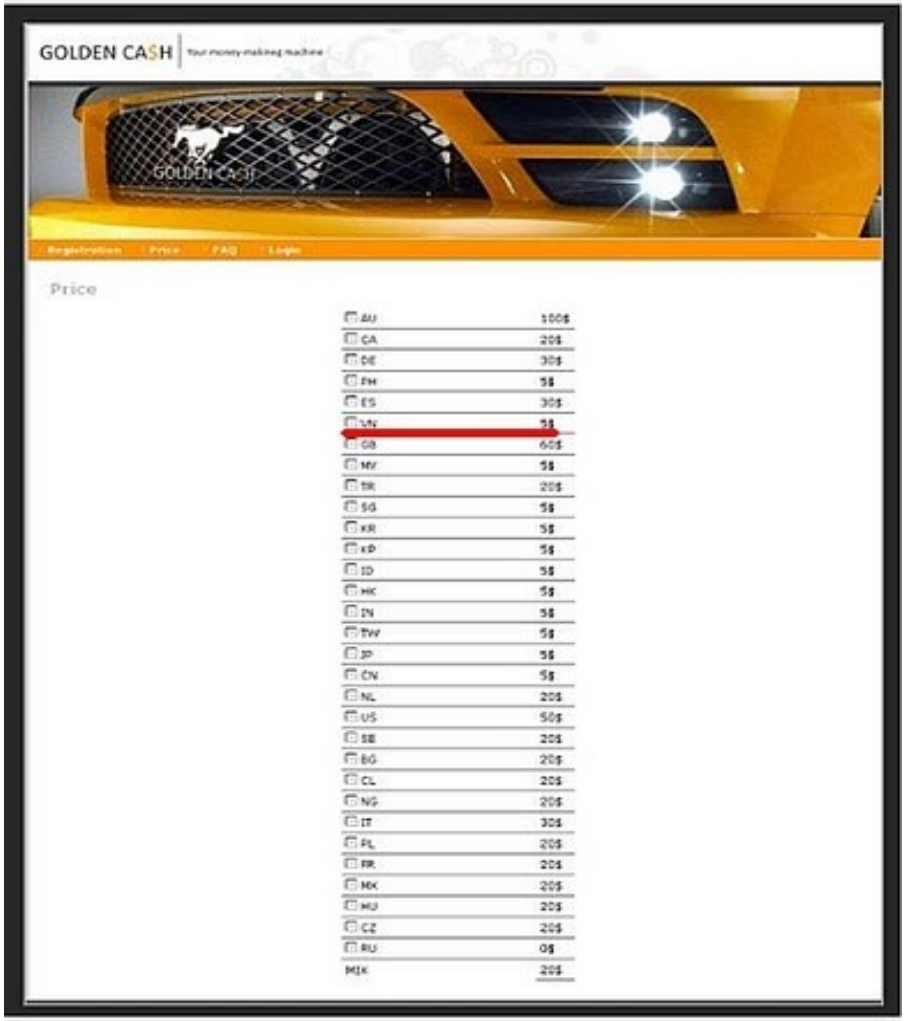
Figure 2.5 Screenshot of 'Zeus Crimeware Toolkit' Bộ công cụ phần mềm tội phạm Zeus



Việt Nam đã có các botnet được sinh ra từ bộ công cụ phần mềm tạo botnet số 1 thế giới - Zeus.

Source P Coogan, *Zeus, King of the underground crimeware toolkits*, blog post, Symantec Security Blogs, Symantec Corporation, 25 August 2009, viewed 14 January 2009 ,<http://www.symantec.com/connect/blogs/zeus-king-underground-crimeware-toolkits>.

Một số hình ảnh về Việt Nam (tiếp)



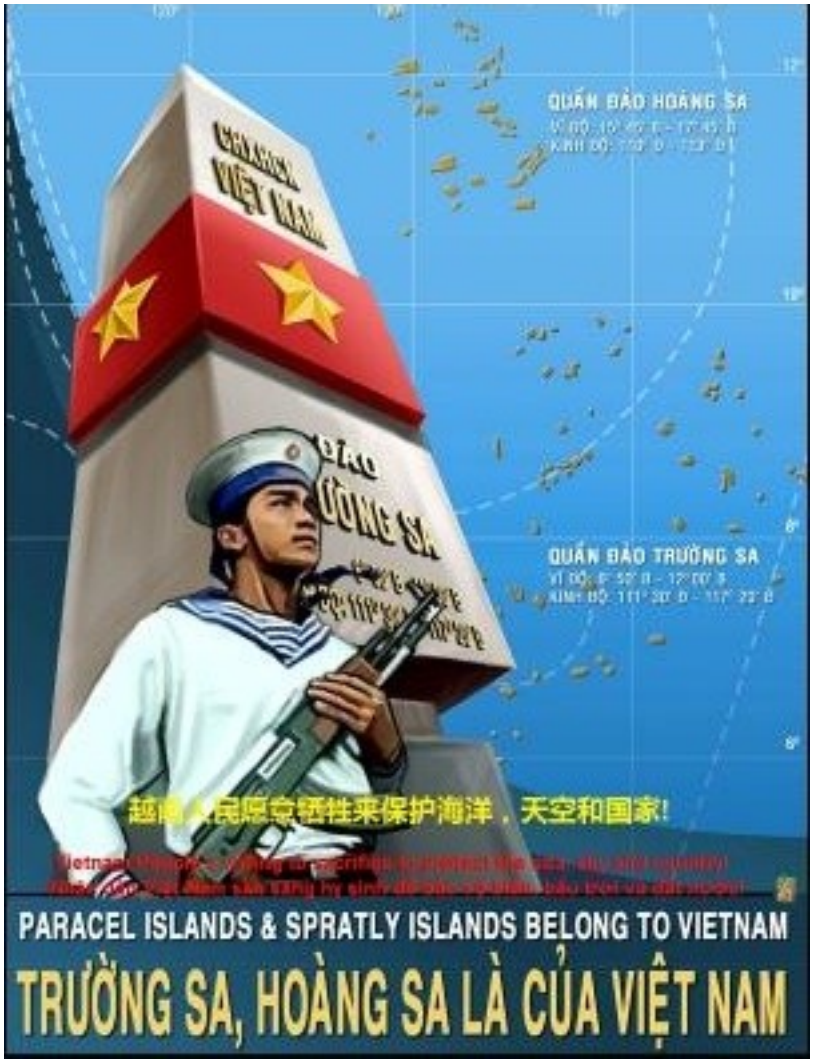
Pricelist for batches of 1,000 malware-infected PCs per country

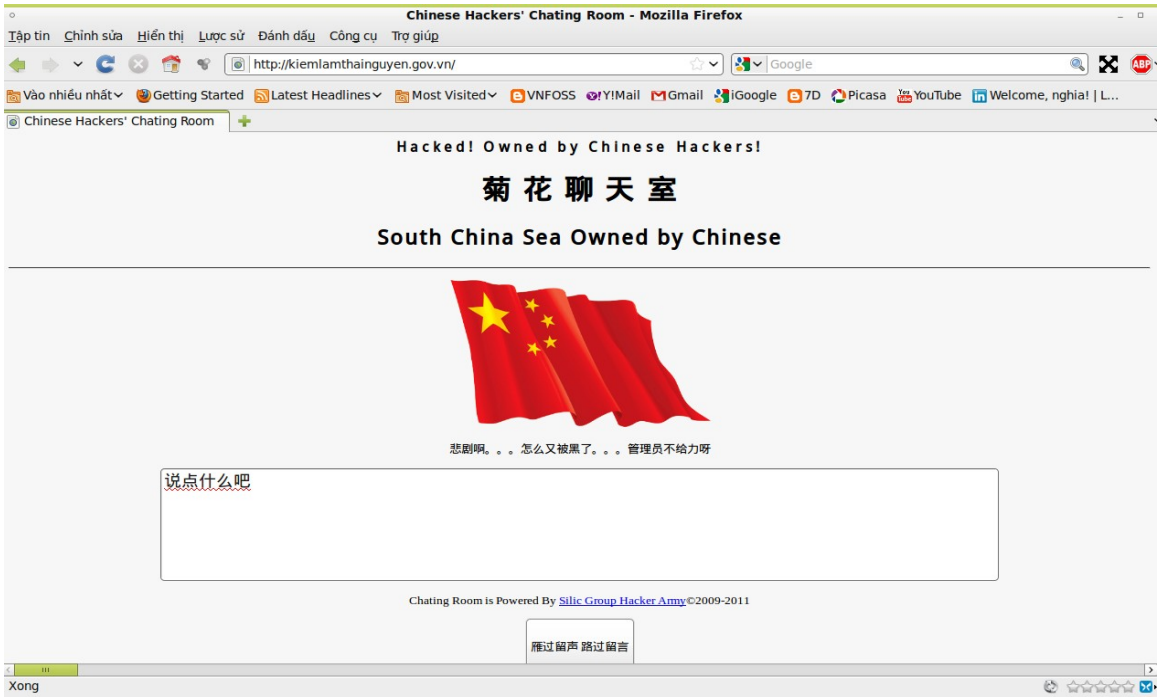
Botnet:

Mua vào: 5USD/1000 ch Bán ra: 25USD/1000 chiếc

Báo cáo của Finjan "Cybercrime Intelligence" số 2 năm 2009.

Cuộc chiến hacker TQ-VN lần thứ nhất 02-07/06/2011





1. Hàng trăm (ngàn) website của 2 bên bị tấn công bôi xấu mặt, trong đó có cả các site của Chính phủ.
2. Cuộc chiến của cộng đồng tự phát?

Chừng nào còn xung đột Biển Đông, chừng đó còn chiến tranh không gian mạng ở VN!

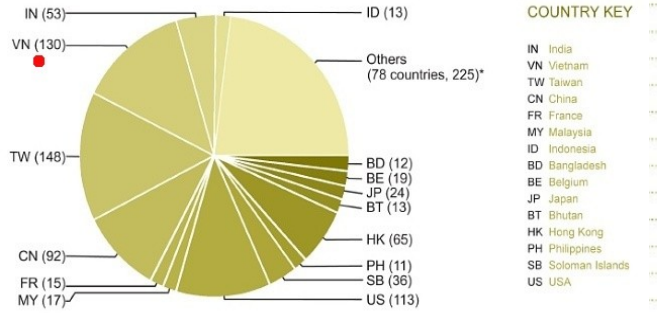
Lịch sử và hiện tại

Việt Nam đứng thứ 2/103 quốc gia bị tấn công với 130/1295 máy bị tấn công trên toàn thế giới. Vụ GhostNet 05/2007 - 03/2009.

Table 2: Selected infections (cont'd)

Organization	Confidence	Location	Infections
Embassy of Romania, Norway			
Embassy of Romania, PRC			
Embassy of Thailand, Philippines			
Embassy of the Republic of Korea, China			
Government Integrated Telecommunicat			
High Commission of India, Cyprus			
High Commission Of India, United Kingdo			
Institute for Information Industry, Taiwa			
International Campaign for Tibet			
International Chamber of Shipping, Unite			
Lanka Education and Research Network,			
Malta External Trade Corporation Ltd.			
Maritime Police, Solomon Islands			
Ministry of Communications, Brunei			
Ministry of Education, Solomon Islands			
Ministry of Foreign Affairs, Bangladesh			
Ministry of Foreign Affairs, Barbados			
Ministry of Foreign Affairs, Bhutan			
Ministry of Foreign Affairs, Brunei			
Ministry Of Foreign Affairs, Iran			
Ministry of Foreign Affairs, Latvia	H	LV	2
Ministry of Industry and Trade, Vietnam	L	VN	30
Ministry of Labour and Human Resources, Bhutan	H	BT	1
National Informatics Centre, India	L	IN	12
NATO, (SHAPE HQ)	H	NL	1
Net Trade, Taiwan	H	TW	1
New Tang Dynasty Television, United States	L	US	1
Office of the Dalai Lama, India	H	IN	2
Pakistan Mission to The United Nations	L	US, JP	4
Permanent Delegation of Cyprus to the European Union	L	BE	1
Permanent Mission of Cuba to the United Nations	L	US	1
PetroVietnam	L	VN	74
Prime Minister's Office, Laos	H	LA	5
Public Service Division, Solomon Islands	H	SB	1
Russian Federal University Network, Russian Federation	H	RU	1

Fig. 12
The geographic location of infected hosts.



Petrotimes.vn bị hacker tấn công xóa dữ liệu

Cập nhật lúc 10/06/2011 12:36:48 PM (GMT+7)

- Tờ báo điện tử đưa tin đầu nguồn về các vụ tàu Trung Quốc xâm phạm lãnh hải, cắt cáp thăm dò địa chấn của các tàu Petrovietnam vừa bị tấn công làm tê liệt tối qua, 9/6.

>Hơn 1.500 trang web Việt bị tấn công
>Nguy cơ chiến tranh mạng đang tăng
>Hàng loạt website Việt Nam bị tấn công

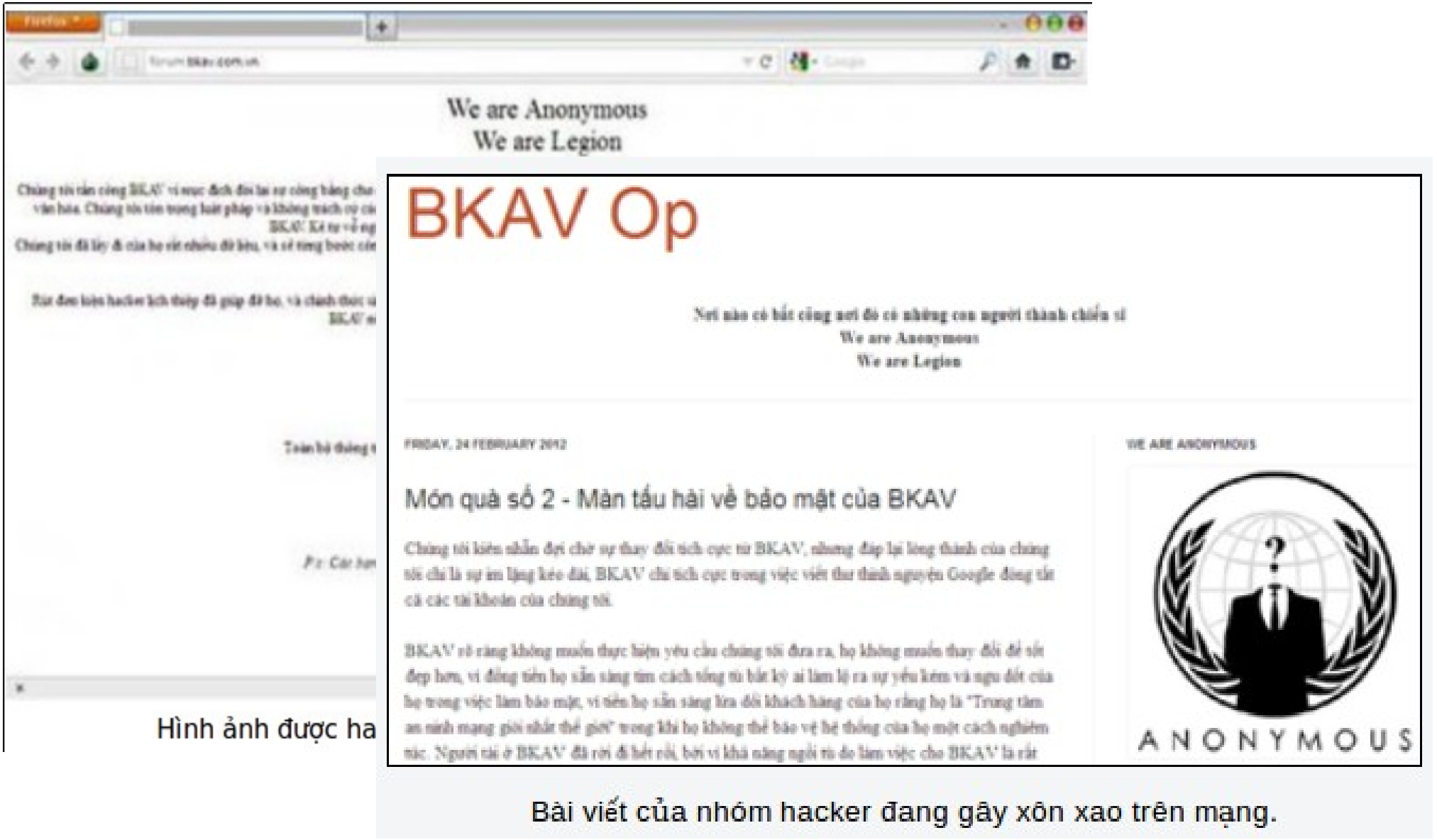
Dữ liệu website Petrotimes.vn cũng bị hacker xóa sạch nhưng rất may đã được sao lưu đầy đủ nên không gây thiệt hại nào đáng kể.

Trả lời phóng viên VietNamNet, ông Nguyễn Như Phong, Tổng biên tập Báo điện tử Tin nhanh Năng Lượng Mới – PetroTimes.vn, cho biết: Vào lúc hơn 20h tối qua (9/6), một lượng truy cập khoảng trên 600 ngàn kết nối đồng thời đã dồn vào websie petrotimes.vn khiến website bị ngừng hoạt động vì quá tải.

Tuyên bố của Bộ TTTT: Vẫn chưa tìm ra thủ phạm tấn công Vietnamnet!
22/11/2010 - 22/11/2011

Một số hình ảnh về Việt Nam (tiếp)

BKAV BỊ TẤN CÔNG, THÁNG 02/2012



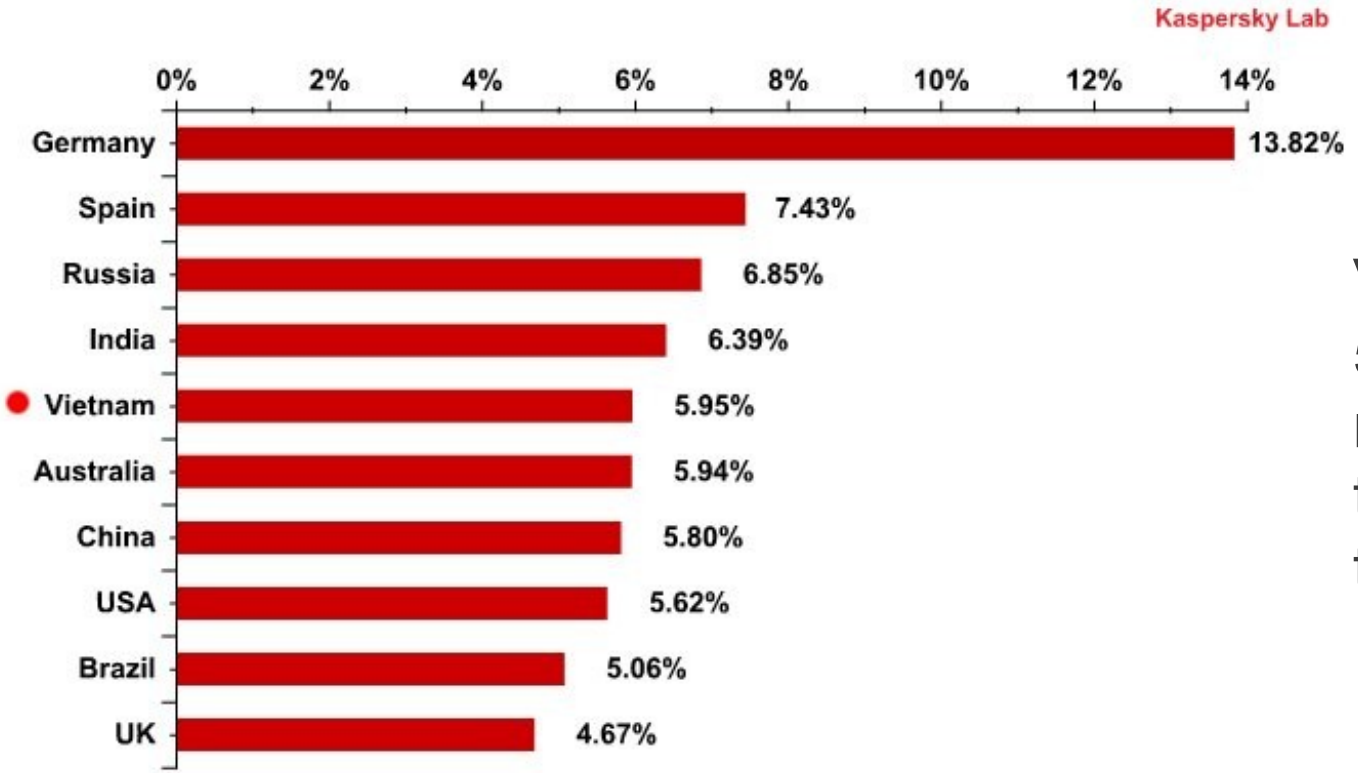
Bài viết của nhóm hacker đang gây xôn xao trên mạng.

Một số hình ảnh về Việt Nam (tiếp)

THE H

Germany gets the most malicious spam

Back to *Germany gets the most malicious spam*



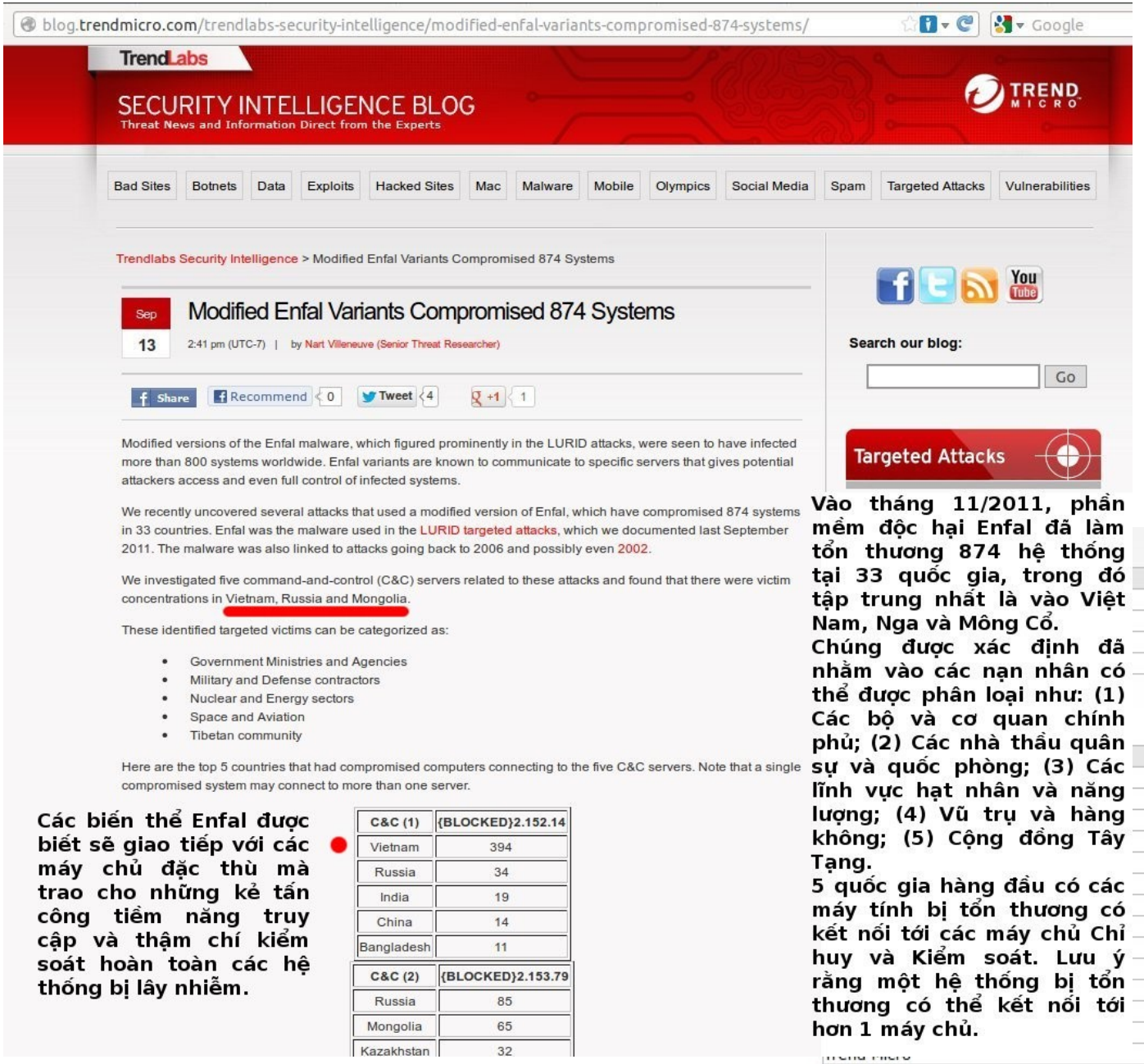
Share of malicious email by country

Back to *Germany gets the most malicious spam*

Số liệu tháng 09/2012 từ Kaspersky Lab

Việt Nam đứng số 5 thế giới về thư rác độc hại vào tháng 09/2012 với tỷ lệ là 5.95%.

Một số hình ảnh về Việt Nam (tiếp)



blog.trendmicro.com/trendlabs-security-intelligence/modified-enfal-variants-compromised-874-systems/

TrendLabs

SECURITY INTELLIGENCE BLOG

Threat News and Information Direct from the Experts

TREND MICRO

Bad Sites | Botnets | Data | Exploits | Hacked Sites | Mac | Malware | Mobile | Olympics | Social Media | Spam | Targeted Attacks | Vulnerabilities

Trendlabs Security Intelligence > Modified Enfal Variants Compromised 874 Systems

Sep 13

Modified Enfal Variants Compromised 874 Systems

2:41 pm (UTC-7) | by Nart Villeneuve (Senior Threat Researcher)

Share | Recommend 0 | Tweet 4 | +1 1

Modified versions of the Enfal malware, which figured prominently in the LURID attacks, were seen to have infected more than 800 systems worldwide. Enfal variants are known to communicate to specific servers that gives potential attackers access and even full control of infected systems.

We recently uncovered several attacks that used a modified version of Enfal, which have compromised 874 systems in 33 countries. Enfal was the malware used in the LURID targeted attacks, which we documented last September 2011. The malware was also linked to attacks going back to 2006 and possibly even 2002.

We investigated five command-and-control (C&C) servers related to these attacks and found that there were victim concentrations in Vietnam, Russia and Mongolia.

These identified targeted victims can be categorized as:

- Government Ministries and Agencies
- Military and Defense contractors
- Nuclear and Energy sectors
- Space and Aviation
- Tibetan community

Here are the top 5 countries that had compromised computers connecting to the five C&C servers. Note that a single compromised system may connect to more than one server.

C&C (1)	{BLOCKED}2.152.14
Vietnam	394
Russia	34
India	19
China	14
Bangladesh	11

C&C (2)	{BLOCKED}2.153.79
Russia	85
Mongolia	65
Kazakhstan	32

Search our blog: Go

Targeted Attacks

Các biến thể Enfal được biết sẽ giao tiếp với các máy chủ đặc thù mà trao cho những kẻ tấn công tiềm năng truy cập và thậm chí kiểm soát hoàn toàn các hệ thống bị lây nhiễm.

Vào tháng 11/2011, phần mềm độc hại Enfal đã làm tổn thương 874 hệ thống tại 33 quốc gia, trong đó tập trung nhất là vào Việt Nam, Nga và Mông Cổ.
Chúng được xác định đã nhằm vào các nạn nhân có thể được phân loại như: (1) Các bộ và cơ quan chính phủ; (2) Các nhà thầu quân sự và quốc phòng; (3) Các lĩnh vực hạt nhân và năng lượng; (4) Vũ trụ và hàng không; (5) Cộng đồng Tây Tạng.
5 quốc gia hàng đầu có các máy tính bị tổn thương có kết nối tới các máy chủ Chỉ huy và Kiểm soát. Lưu ý rằng một hệ thống bị tổn thương có thể kết nối tới hơn 1 máy chủ.

	Property Values
	Enfal
	57344 bytes
	543c17d4da5d23527c8a854953d953fa
	6a7274ce41dd3fcfff77f327d17981657e3960d5

	Detection Names
	Trojan-Spy.Win32.Agent.M!IK
	Win32:Malware-gen
	Win32/DH.FF8203B0{40008000-10000000-00000000} (sus
	TR/Hijacker.Gen
	Gen:Trojan.Heur.JP.dmW@aa9LcRl
	Trojan.Spy-87634
	BackDoor.Tiblue.37
	W32/Heuristic-431!Eldorado
	W32/Pincav.GRW!tr
	trojan:win32/malagent
	Win32/Spy.Agent.M trojan (variant)
	W32/Suspicious_Gen2.TMONT
	Troj/Mkmoo-Gen
	TROJ_GEN.R01C7KT
vba32	Trojan-Spy.Agent.8
V-Buster	TrojanSpy.Agent!xbCIFIKBTtA (trojan)

Other brands and names may be claimed as the property of others.

- Việt Nam đứng số 1 thế giới về lây nhiễm virus Enfal, với 394/874 (45%) hệ thống bị lây nhiễm tại 33 nước.

- Enfal có thể kiểm soát hoàn toàn hệ thống bị lây nhiễm.

- Một hệ thống bị tổn thương có thể kết nối tới hơn 1 máy chủ.

- Trend Macro, tháng 09/2012.

Cảnh giác với tấn công dạng Stuxnet ở Việt Nam!
(1) Windows + (2) SCADA + (3) Stuxnet = THẢM HỌA!
Phát hiện 2 dạng SCADA của TQ có lỗi - có thể bị tấn công DDoS hoặc chạy chương trình tùy ý.

* SCADA: Supervisory Control And Data Acquisition

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-167-01—HEAP OVERFLOW VULNERABILITIES IN SUNWAY FORCECONTROL AND PNETPOWER

June 16, 2011

OVERVIEW

ICS-CERT has received a report from Security researcher Dillon Beresford of NSS Labs[a] concerning vulnerabilities affecting Sunway ForceControl and pNetPower SCADA/HMI applications. The reported vulnerabilities are heap-based buffer overflows[b] that could result in a denial of service or the execution of arbitrary code.

ICS-CERT has coordinated with the researcher, China National Vulnerability Database (CNVD), and Sunway to ensure full remediation of the reported vulnerabilities. Sunway has issued two patches that address both vulnerabilities. CNVD has confirmed the effectiveness of the patches issued by Sunway. Neither ICS-CERT nor the researcher has validated these patches. Sunway has issued a security bulletin describing their response.[c]

AFFECTED PRODUCTS

According to the researcher, these vulnerabilities affect Sunway ForceControl 6.1 (SP1, SP2, and SP3) and pNetPower Version 6.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to perform a remote denial of service or to remotely execute arbitrary code against the ForceControl and pNetPower server applications. This action can result in adverse application conditions and ultimately impact the production environment on which the SCADA system is used.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

products are also deployed in Europe, the Americas, Asia, and Africa. Sunway products are deployed across a wide variety of industries including petroleum, petrochemical, defense, railways, coal, energy, pharmaceutical, telecommunications, water, manufacturing, and others.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The following two vulnerabilities have been identified:

1. The heap-based buffer overflow affecting ForceControl 6.1 WebServer can be exploited if an attacker makes a request to the httpsvr.exe process with a specially crafted HTTP URL. Successful exploitation results in a denial of service and the possible execution of arbitrary code.
2. The heap-based buffer overflow affecting pNetPower AngelServer can be exploited if an attacker sends specially crafted UDP packets to the AngelServer.exe process. Successful exploitation results in a denial of service and the possible execution of arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

Remote exploitability of this vulnerability could be possible.

EXISTENCE OF EXPLOIT

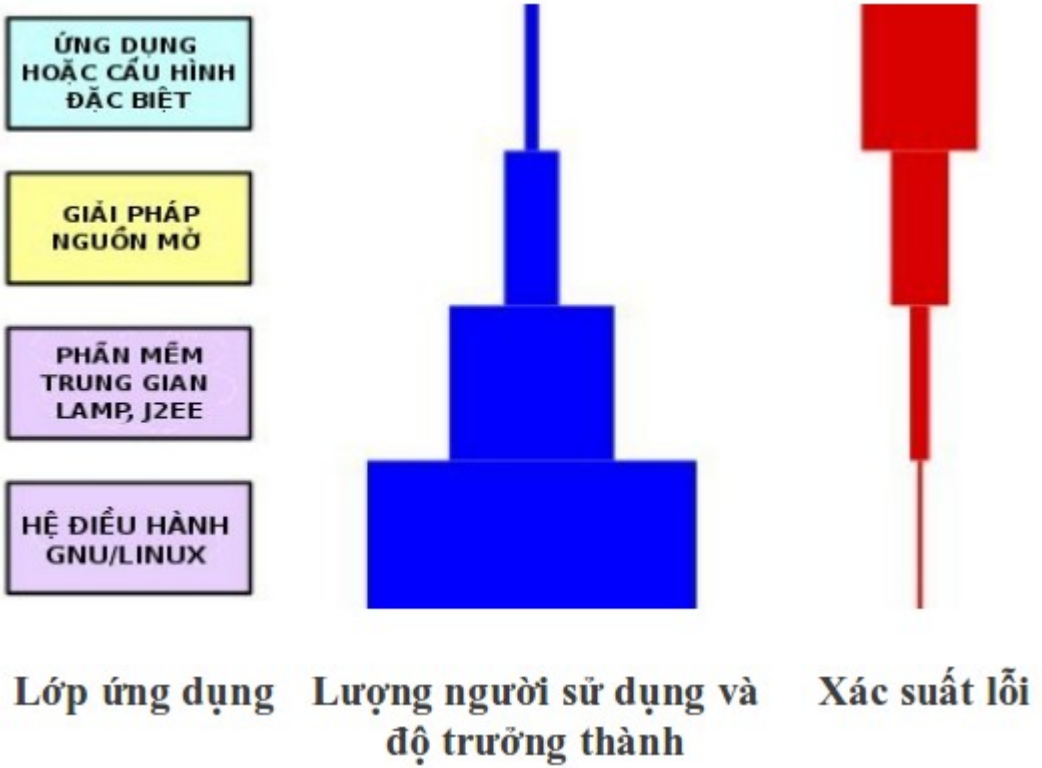
No known exploits specifically target this vulnerability.

Công cụ được sử dụng để tấn công

Phần cứng và thiết bị

- Chip, BIOS, RAM, USB & bàn phím: Cấy mã độc và BIOS - Stoned Bootkit, vào USB, nạo vét RAM - Cold Boot, nghe bàn phím (KeyLogger).
- Thiết bị viễn thông: Lo ngại của Mỹ, Anh, Ấn về Hoa Vĩ (Huwei) và ZTE.
- Hệ thống nhúng: máy in, photocopy đa năng của Canon, Ricoh, Xerox, HP...
- Các thiết bị di động: phần mềm độc hại gia tăng nhanh.
- Thẻ và đầu đọc thẻ thông minh: Bộ Quốc phòng & Bộ An ninh nội địa Mỹ.

Phần mềm



Lỗi có tính sống còn trong RHEL 4.0 và RHEL 5.0 bằng 0.

Công cụ được sử dụng để tấn công

Phần mềm (tiếp)

- Cửa hậu gài trong Windows, các OS thương mại khác; và cả Lotus Notes.
- Sử dụng các lỗi của phần mềm để tấn công: Windows, Exchange Server, MS SQL Server, MS Office, IE, Wordpad, Windows Update... Adobe Reader - Flash, QuickTime, Firefox, AutoCAD... FaceBook, Twitter... SCADA – ICS...
- Tạo ra các botnet từ vài trăm tới hàng chục triệu máy bị lây nhiễm
- Mua bán các máy tính bị lây nhiễm theo vùng địa lý
- Sử dụng không đúng dẫn tới mất an ninh: Sidekick.

Liên quan

- Pháp nhân đứng ra tấn công là đủ loại, cao nhất là các quốc gia như Mỹ, Israel, Trung Quốc, Nga, Anh... → chạy đua vũ trang KGM → vùng chiến sự.
- Tần suất cực lớn, phạm vi rộng khắp, mọi lĩnh vực, mọi tổ chức
- Virus ngày càng tinh vi phức tạp hơn: Stuxnet – Duqu – Flame – Gauss...
- Thiệt hại lớn: Stuxnet đẩy lùi chương trình hạt nhân của Iran 2 năm; Mỹ mất hàng Terabyte dữ liệu; chỉ trong 6 tháng Conficker gây hại tới 9.1 tỷ USD, Barack Obama: 2008-2009 riêng Mỹ thiệt hại do tội phạm KGM là 8 tỷ USD...

Đối phó của các quốc gia

Chính sách chiến lược, tổ chức và nhân sự

- Có chiến lược, học thuyết, kế hoạch về ANKGM, cả tấn công và phòng thủ.
- Củng cố các tổ chức, hợp tác các CERT, diễn tập chung các quốc gia.
- Đầu tư nghiên cứu về ANKGM, các vũ khí KGM, cả tấn công và phòng thủ.
- Chính phủ có quyền không giới hạn với mã nguồn phần mềm/ hệ thống.
- Phát triển các công nghệ mở - Cộng đồng trước, công nghệ sau!
- Tuyển nhân tài về ANKGM, lập các đội quân chuyên về ANKGM
- Nhiều hoạt động và sáng kiến mới...

Khu vực dân sự

- Chuyển sang các hệ thống mở → các thị trường chứng khoán hàng đầu.
- Khuyến cáo không sử dụng Windows khi giao dịch ngân hàng trực tuyến → Viện công nghệ SAN, bang New South Wale - Úc, chuyên gia an ninh...
- Khuyến cáo chuyển đổi sang PMTDNM, nhưng nếu phải sử dụng Windows, hãy tuân theo 10 lời khuyên về an ninh.

“Mở thì mới an ninh!!!” →

Mở thì mới an ninh!!!

Ứng dụng và phát triển các công nghệ mở cho quốc phòng

"Mil-OSS kết nối và trang bị cho một cộng đồng tích cực các lập trình viên phần cứng và phần mềm nguồn mở dân sự và quân sự khắp nước Mỹ. Phong trào của những người dân thường này là một tập hợp những người yêu nước đa dạng khác nhau làm việc vì và với BQP và tin tưởng vào việc áp dụng các triết lý sáng tạo của CNM để bảo vệ có hiệu quả dân tộc chúng ta".

Mở thì mới an ninh!!! (2)

Các thành phần của phát triển công nghệ mở:

1. Chuẩn mở và giao diện mở
2. Phần mềm tự do nguồn mở và thiết kế mở
3. Công cụ trực tuyến cộng tác và phân tán
4. Sự lanh lẹ về công nghệ

Tham khảo: Định nghĩa một số khái niệm mở.

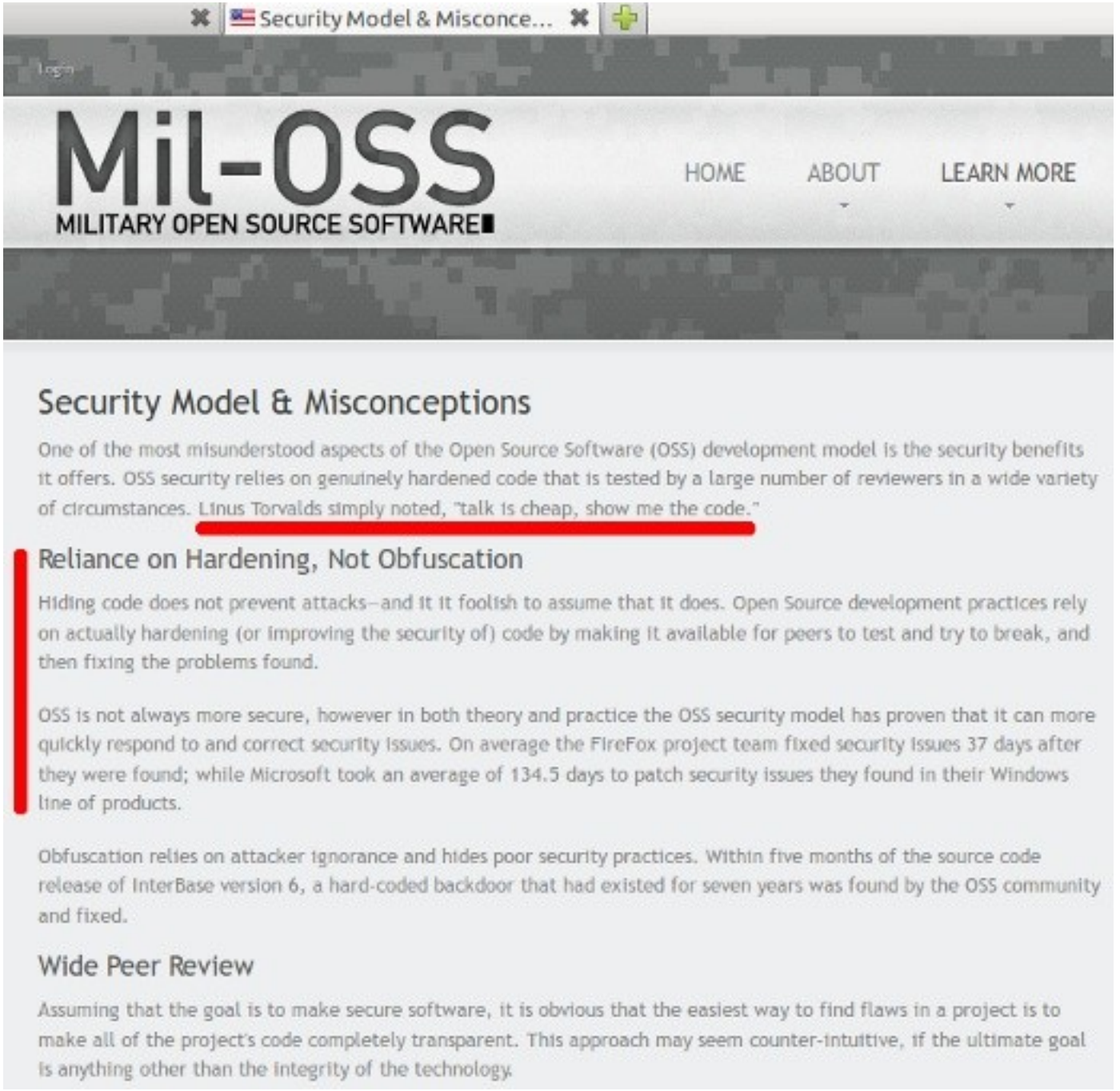
Mở thì mới an ninh!!! (3)

1. Mất ANAT trong các ứng dụng phần mềm xảy ra cả với các PMTDNM và PMSHĐQ.

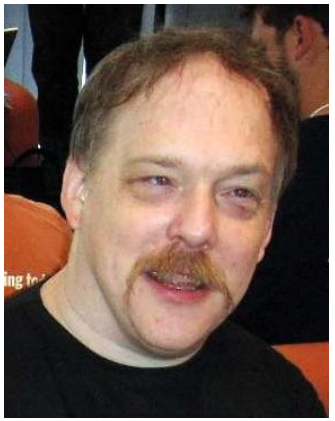
2. Mã nguồn yếu là điểm mấu chốt gây mất ANAT cho PM.

3. Site của Bộ Quốc phòng Mỹ:

- "Tin cậy vào sự cứng cỏi, không tin cậy vào sự tối tăm" (về mã nguồn).
- Trung bình để khắc phục 1 lỗi phần mềm, Mozilla cần 37 ngày, Microsoft cần 134,5 ngày



Mở thì mới an ninh!!! (4)



Eric Raymond, đồng sáng lập phong trào nguồn mở, tác giả cuốn sách "Nhà thờ lớn và cái chợ": "Given enough eyeballs, all bugs are shallow" - "**Nhiều con mắt soi vào thì lỗi sẽ cạn**"
- 1 trong 2 tuyên bố của Luật Linus.

Linus Torvalds, nhà phát minh ra nhân Linux: "Talk is cheap, show me the code" - "**Nói thì ít giá trị, hãy cho tôi xem mã nguồn**"
Trích Site nguồn mở của Bộ Quốc phòng Mỹ

Một trong những giá trị lớn nhất của phát triển nguồn mở là cho phép truy cập từ một cộng đồng rộng lớn tới mã nguồn. Theo cách này các lỗi sẽ ít và dễ tìm ra hơn. Truy cập rộng rãi hơn tới mã nguồn phần mềm cũng là chìa khóa để hình thành và duy trì vị thế an ninh cho phần mềm vì có khả năng rà soát lại mã nguồn phần mềm để xem điều gì thực sự hiện diện bên trong phần mềm đó.

Mở thì mới an ninh!!! (5)

06/2001, Steve Ballmer: "Linux là bệnh ung thư gắn bản thân nó vào ý thức sở hữu trí tuệ tới bất kỳ thứ gì nó động tới".

- 05/2002, Bill Gates so sánh giấy phép GPL với chủ nghĩa chống tư bản tại một Hội nghị các lãnh đạo của Chính phủ tại Seattle, Mỹ.

- Con lợn biết bay?

Bức tranh phát triển nhân Linux kể từ phiên bản 2.6.36 (20/10/2010):

Tên công ty	Số thay đổi	% tổng số	Tên công ty	Số thay đổi	% tổng số
Không	11,413	16.2%	Academia	882	1.3%
Red Hat	7,563	10.7%	Fujitsu	854	1.2%
Intel	5,075	7.2%	Pengutronix	733	1.0%
Novell	3,050	3.3%	Atheros Communications	726	1.0%
Không rõ	2,998	4.3%	Freescale	712	1.0%
IBM	2,638	3.7%	**Microsoft**	**688**	**1.0%**
Texas Instruments	2,124	3.0%	ST Ericsson	663	0.9%
Consultant	1,859	2.6%	Wind River	645	0.9%
Broadcom	1,780	2.5%	MiTAC	632	0.9%
Nokia	1,367	1.9%	Soc. Francaise de Radiotelephone	614	0.9%
Samsung	1,195	1.7%	Analog Devices	611	0.9%
Oracle	1,102	1.6%	tglx PITA	591	0.8%
Google	1,054	1.5%	Linaro	527	0.7%
Wolfson Microelectronics	1,005	1.4%	QLogic	526	0.7%
AMD	980	1.4%	Marvell	465	0.7%

Nguồn: Phát triển nhân Linux, Quỹ Linux xuất bản, tháng 01/2012

Nhân Linux là GPL!

Mở thì mới an ninh!!! (6)

Open GOTS: Phần mềm mở sử dụng được ngay của Chính phủ
Closed GOTS: Phần mềm đóng sử dụng được ngay của Chính phủ
GOTS: Phần mềm sử dụng ngay được của Chính phủ
COTS: Phần mềm thương mại sử dụng ngay được
PMNM: Phần mềm nguồn mở
PMSHĐQ: Phần mềm sở hữu độc quyền

- Tài liệu Bộ Quốc phòng Mỹ, xuất bản 16/05/2011:
Với phát triển công nghệ mở → sẽ không tồn tại phần mềm sở hữu độc quyền trong quân đội / Chính phủ.
- Chính phủ có quyền trí tuệ không hạn chế đối với phần mềm & hệ thống.
- Nhóm An ninh Điện tử Truyền thông Anh CESG: PMNM nên được sử dụng để đảm bảo an ninh cho các hệ thống khu vực nhà nước.

Mở thì mới an ninh!!! (7)

Bài học thành công với phát triển công nghệ mở của quân đội Mỹ:

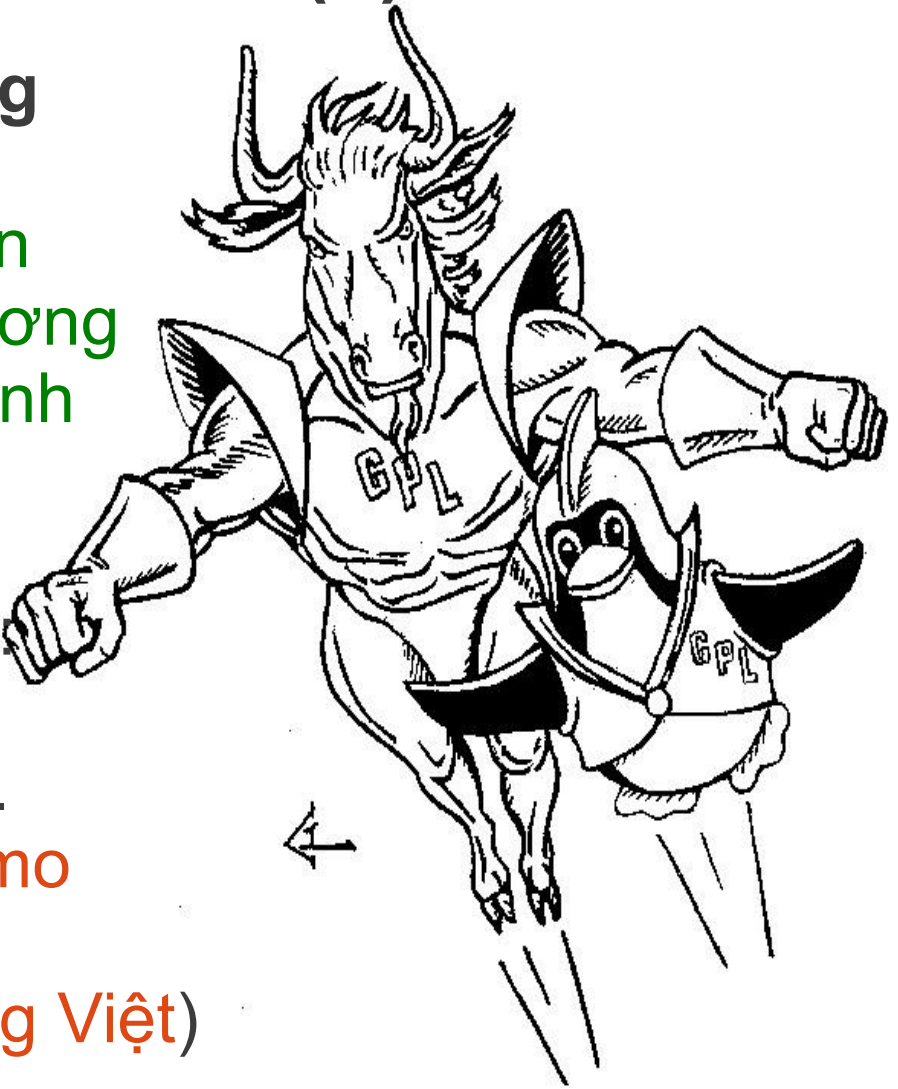
1. Cộng đồng trước, công nghệ sau
2. Mặc định là mở, đóng chỉ khi cần
3. Chương trình của bạn không có gì đặc biệt, kể cả là trong quân sự.
4. Lập cơ chế chia sẻ mã nguồn PM vận hành được trong chính phủ.
5. Quyền trí tuệ. Sử dụng các giấy phép PMTDNM.
6. Thương thảo yêu cầu các quyền không hạn chế mã nguồn phần mềm.
7. Không tạo ra các giấy phép mới, mất thời gian tranh luận pháp lý.
8. Loại bỏ việc cấp vốn lẫn lộn nhà nước - tư nhân cho PM, module.
9. Tách bạch các PM, module bí mật và công khai → cơ chế cài cắm.
10. Không kết hợp thành phần sở hữu độc quyền, tránh chi phí cấp phép
11. Có kế hoạch cấp vốn cho việc quản lý cộng đồng và duy trì mã nguồn.
12. Khuyến khích tranh luận trong cộng đồng các lập trình viên và NSD.
13. Xây dựng tài liệu: sử dụng, cài đặt, quản trị, thiết kế.
14. Quản lý cấu hình chặt chẽ.
15. Quản lý dự án như một phường hội, người sử dụng có thể đóng góp

→ mô hình phát triển theo kiểu 'cái chợ'.

Mở thì mới an ninh!!! (8)

Chính sách về công nghệ mở trong quân đội Mỹ:

1. PMNM được phép và được ưu tiên
2. PMNM được coi là phần mềm thương mại theo Luật liên bang và các qui định mua sắm của quân đội.



Chính sách nguồn mở - quân đội Mỹ:

- 2003 Stenbit Memo
- 2006 OTD Roadmap - (Tiếng Việt) .
- 2009 OSS Clarifying Guidance Memo
- 2010 Carter Memo
- 2011 OTD Lessons Learned - (Tiếng Việt)

Tham khảo:

Chính sách nguồn mở trong quân đội.

Mở thì mới an ninh!!! (9)

1. Bộ Quốc phòng: 3
2. Cơ quan các hệ thống thông tin: 6
3. Bộ Tổng tham mưu Liên quân: 3
4. Lục quân: 3
5. Hải quân: 8
6. Cảnh sát đường thủy: 5
7. Không quân: 8

Ngoài ra:
8. NASA: 2
9. Bộ An ninh Nội địa: 2

Quân đội Trung Quốc:
Tất cả các máy tính cá nhân đều được cài đặt hệ điều hành an ninh Kylin có nguồn gốc từ FreeBSD.

Một số dự án của giới công nghiệp được sử dụng trong quân đội Mỹ: Apache, Drupal, Eclipse, James Mail, JBoss, Joomla!, Linux, Lucene, ModSecurity, Nagios, OpenStack, Plone, Postgresql, Red Hat Enterprise Linux (RHEL), Subversion, Tomcat, TransVerse, Zope.

Tham khảo: Các dự án PMTDNM trong Chính phủ và quân đội Mỹ

Mở thì mới an ninh!!! (10)

1. Chính phủ Canada tuyên bố chuyển sang nguồn mở sau khi các tin tặc tấn công vào một số bộ của Chính phủ.

2. Thủ tướng Nga Putin ra lệnh cho các cơ quan chính phủ Nga chuyển đổi hết sang PMTDNM. Bắt đầu quý II/2012, kết thúc quý III/2014.

3. Chính phủ Anh đưa ra hàng loạt các văn bản chính sách để chuyển đổi sang PMTDNM và chuẩn mở (có hiệu lực từ 01/11/2012).

4. Chính phủ Mỹ với: "Phát triển công nghệ mở - những bài học học được và những thực tiễn tốt nhất cho các phần mềm – hệ thống trong quân sự - chính phủ". Nhà Trắng khẳng định sự đổi mới sáng tạo khổng lồ của PMTDNM đối với nước Mỹ.

5. Các chính phủ khác: Báo cáo quốc tế về tình hình phát triển nguồn mở trên thế giới năm 2010: 5 quốc gia hàng đầu trong phát triển PMTDNM và xã hội thông tin: Mỹ, Đức, Pháp, Tây Ban Nha và Úc.

6. Quốc hội Ý đã phê chuẩn luật, từ 12/08/2012, tất cả các phần mềm mới xây dựng trong các cơ quan nhà nước đều phải dựa vào PMTDNM.

Mở thì mới an ninh!!! (11)

Một số hệ thống PMTDNM trong tài chính thương mại

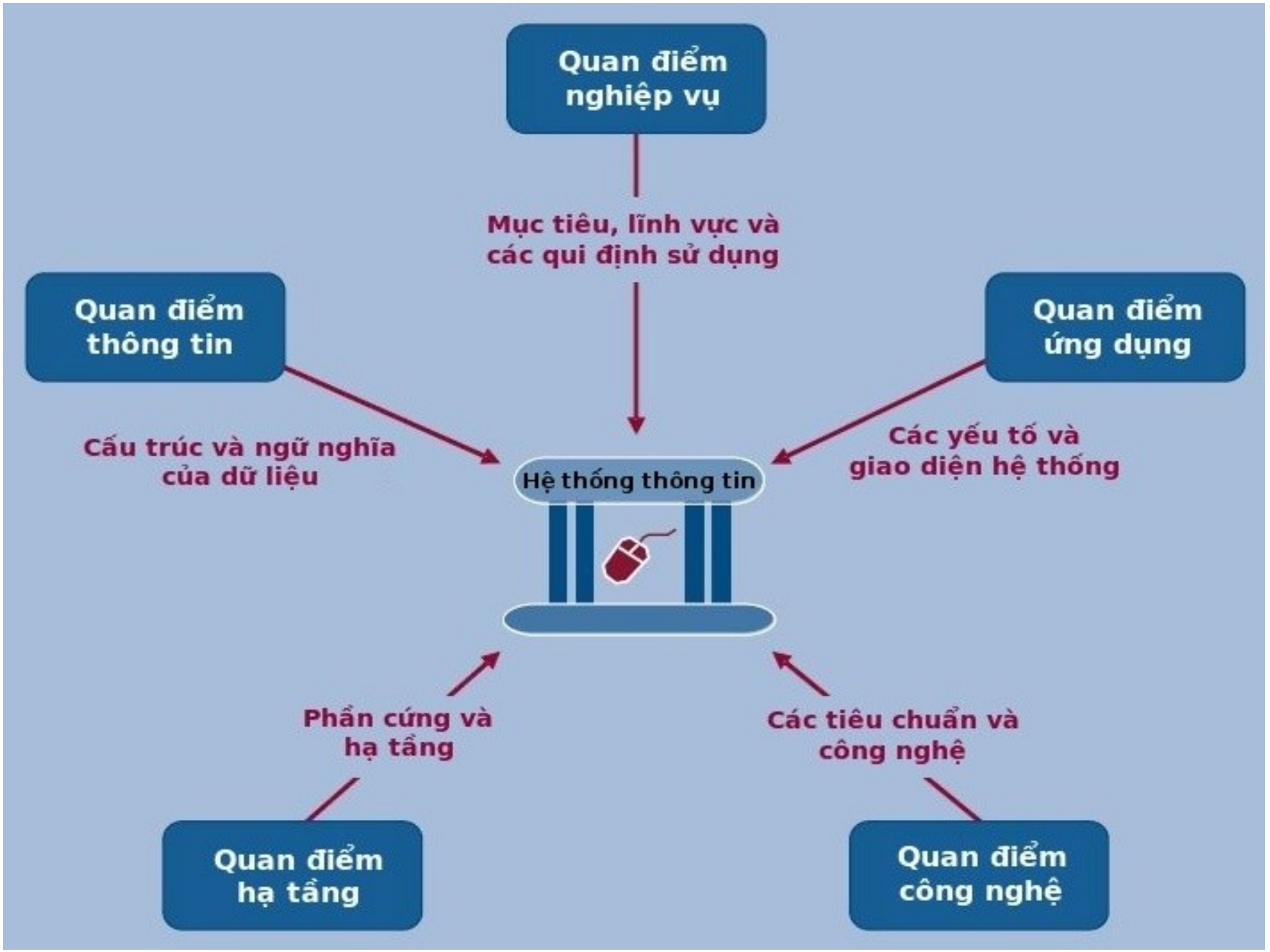
1. Thị trường chứng khoán New York, Tokyo, Luân Đôn, ... và 75% các hệ thống chứng khoán trên toàn thế giới là chạy trên nền tàng hệ điều hành PMTDNM GNU/Linux như RHEL.
2. Nhiều ngân hàng có các phần mềm nghiệp vụ cốt lõi được xây dựng trên các PMTDNM
3. Sử dụng các PMTDNM để xây dựng các website TMĐT: 15 nền tảng TMĐT là PMTDNM tốt nhất thế giới: (1) Magento; (2) osCommerce; (3) OpenCart; (4) Spree Commerce; (5) PrestaShop; (6) VirtueMart; (7) Ubercart; (8) Zeuscart; (9) AFCommerce; (10) Zen Cart; (11) Simple Cart js; (12) Tomato Cart; (13) CuberCart; (14) RokQuickCart; (15) StoreSprite;

Tại Việt Nam:

http://www.magentovietnam.com/; http://opencart.vn/
http://www.oscommerce.com/community/contributions,3960
http://viet-cntt.com/Thiet-ke-web/Prestashop/;
http://www.iwayvietnam.com/dong-gop-PMTDNM.html
http://www.mycounter.net/site/zen-cart.vn.html

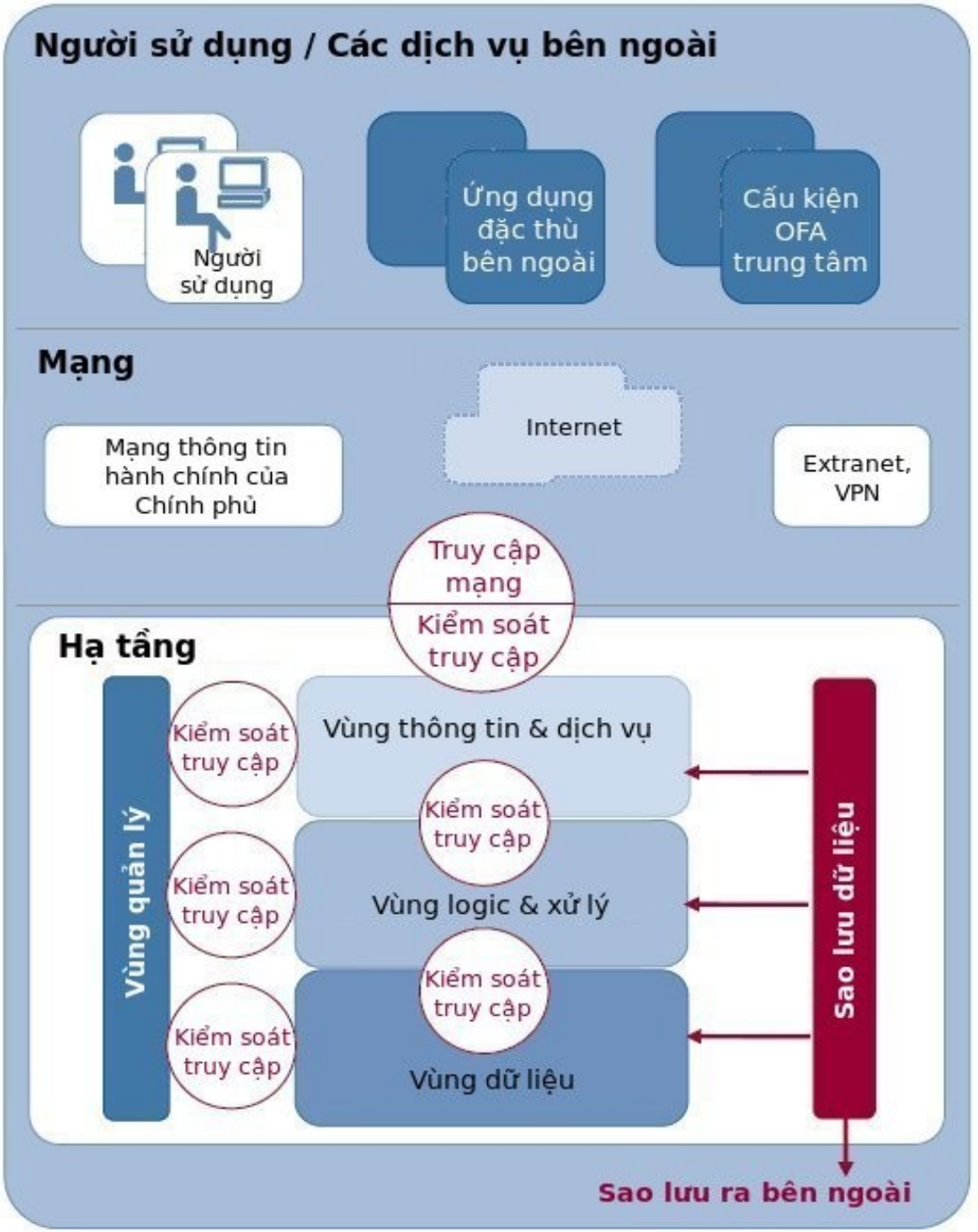
B. Kiến trúc & an ninh hệ thống thông tin

An ninh hệ thống thông tin phụ thuộc trước hết vào kiến trúc của nó.

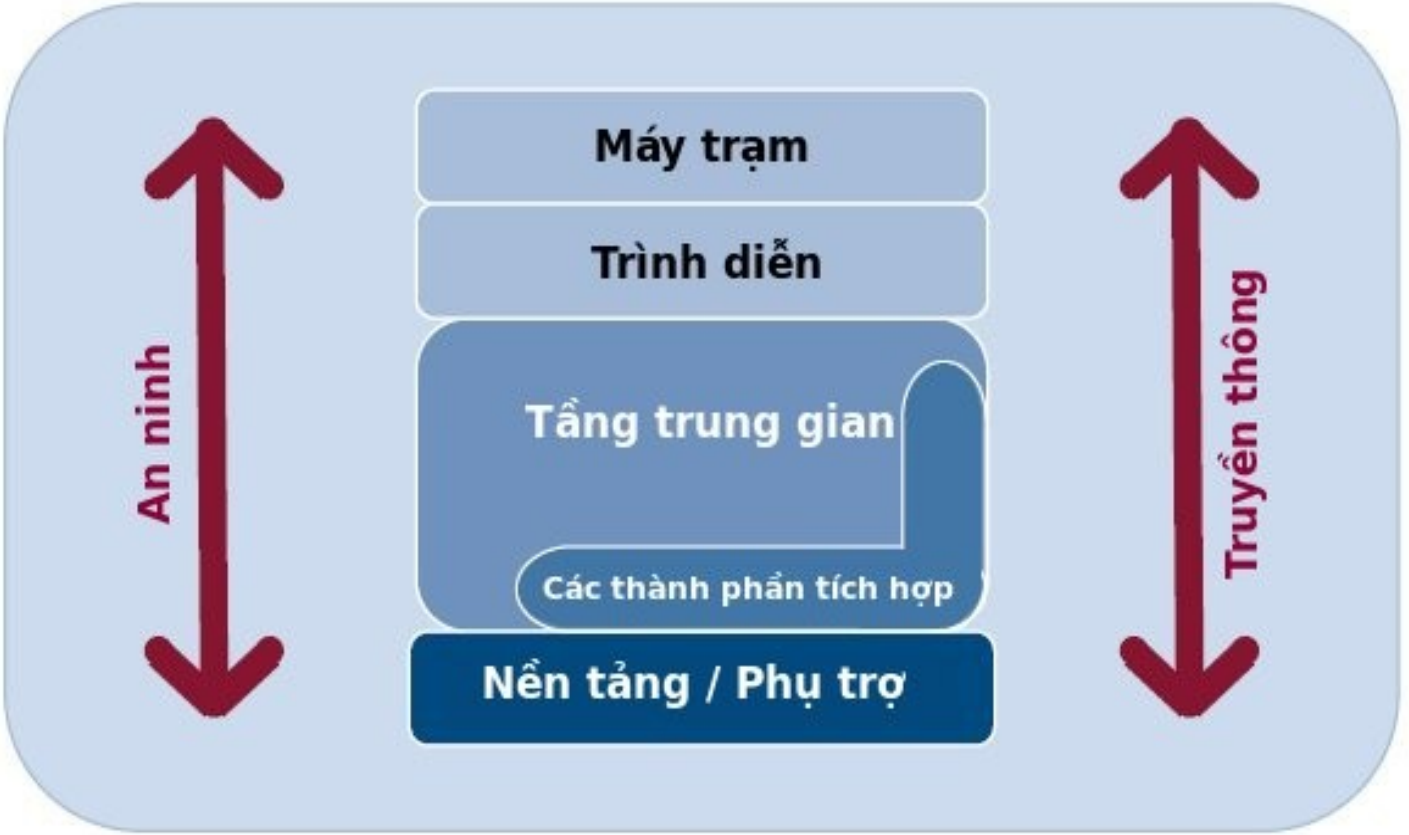


Kiến trúc hạ tầng hệ thống thông tin

An ninh hệ thống phụ thuộc:
1. Hạ tầng vật lý của hệ thống: phòng ốc, điện, điều hòa, chống sét, kiểm soát ra vào, sao lưu.
2. Phân vùng hệ thống
3. Giao tiếp giữa các vùng.
4. Mạng - là tầng kết nối hạ tầng với người sử dụng và các dịch vụ bên ngoài → mạng hành chính Chính phủ và Extranet là quan trọng từ quan điểm an ninh.



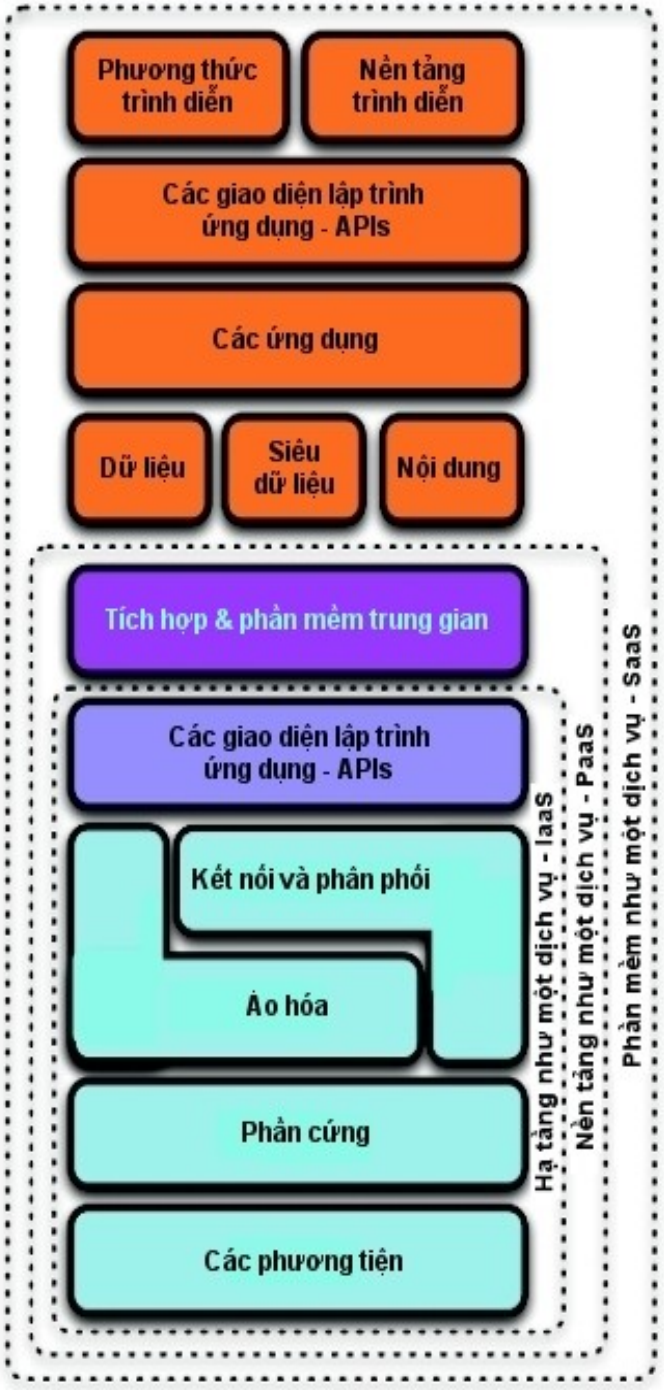
An ninh ứng dụng



- Kiến trúc phân tầng tách bạch giữa các tầng với nhau.
- Đảm bảo an ninh theo các tầng tương ứng.
- Chuẩn về an ninh ứng dụng ISO/IEC 27034 (dự thảo).

Kiến trúc hệ thống phần mềm thường thấy

Kiến trúc hệ thống điện toán đám mây



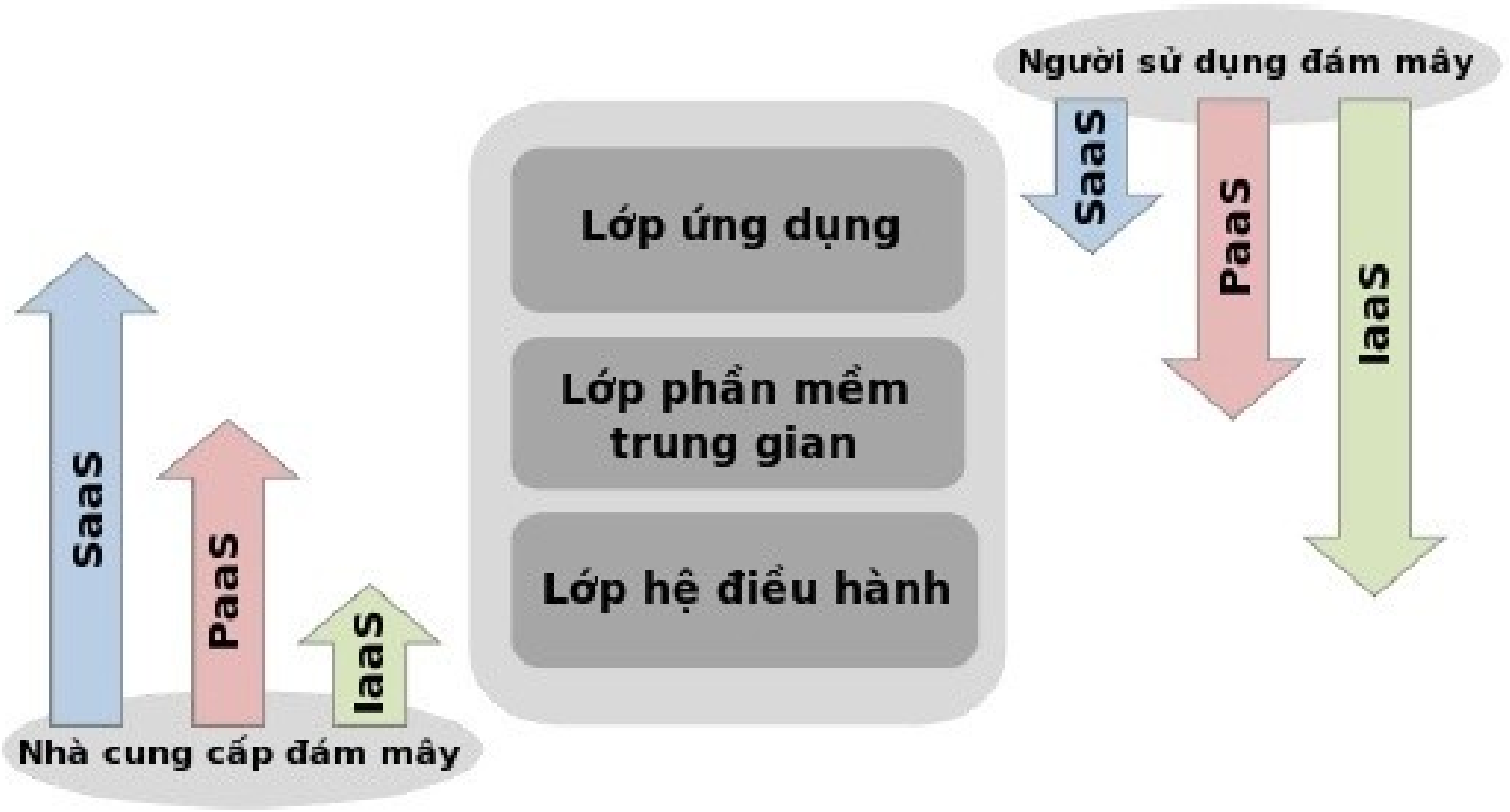
An ninh ĐTĐM = An ninh thông thường + An ninh đặc thù của đám mây.

An ninh ĐTĐT phụ thuộc vào kiến trúc của ĐTĐM và 12 (+1) lĩnh vực liên quan khác:

- 5 lĩnh vực quản lý: (1) Quản lý rủi ro; (2) Quản lý việc phơi lộ điện tử; (3) Quản lý tuân thủ và kiểm toán; (4) Quản lý vòng đời thông tin - dữ liệu khi xóa; (5) Tính khả chuyển và tính tương hợp → Chuẩn mở.
- 7 lĩnh vực vận hành & chỉ dẫn: (1) An ninh truyền thống; (2) Vận hành trung tâm; (3) Phản ứng, thông báo, xử lý tình huống; (4) An ninh ứng dụng; (5) Mã hóa và quản lý khóa; (6) Nhận dạng và quản lý truy cập; (7) Ảo hóa; (+1) [Sec. AaS] 2011.

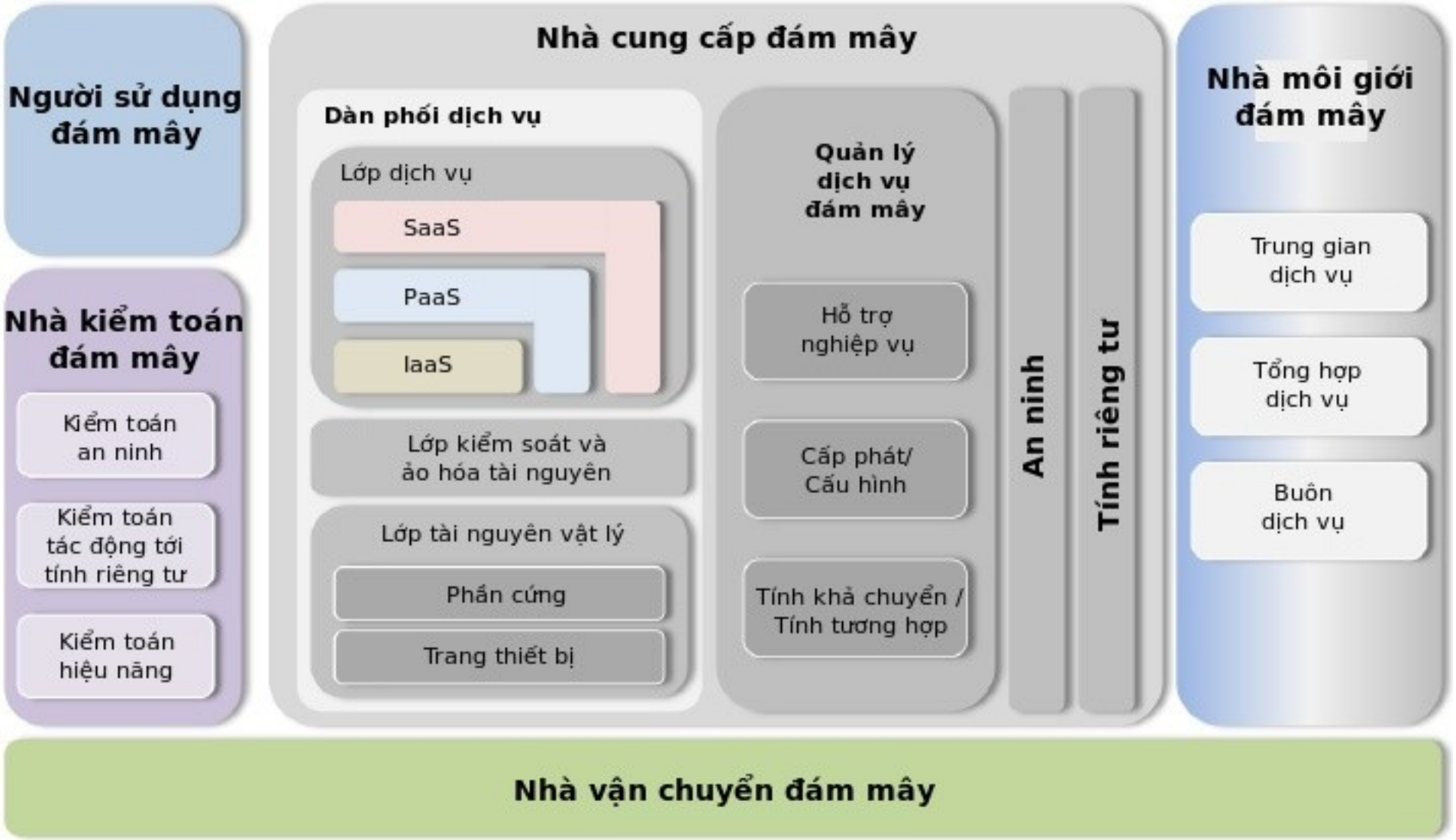
Tài liệu an ninh ĐTĐM của CSA, 12/2009.

Kiến trúc hệ thống điện toán đám mây



An ninh ĐTĐM là sự chia sẻ trách nhiệm giữa nhà cung cấp và người sử dụng, chứ không phải của chỉ một mình nhà cung cấp.

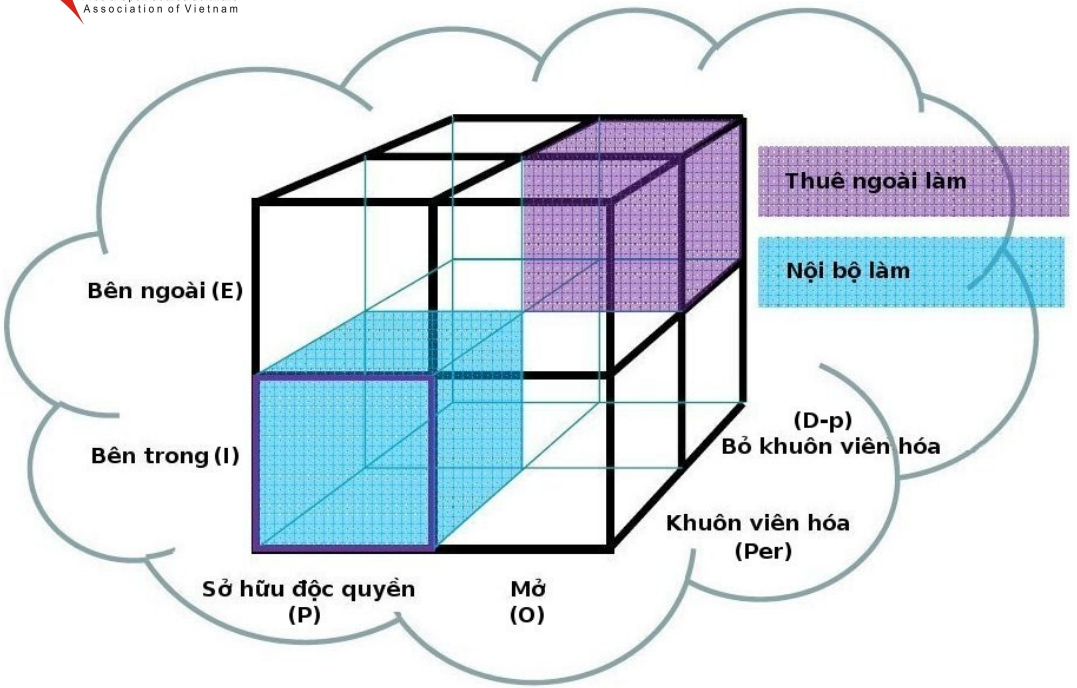
Kiến trúc hệ thống điện toán đám mây



Mô hình tham chiếu khái niệm kết hợp: tích hợp các thành phần hệ thống, tổ chức và qui trình trong ĐTĐM ► An ninh chuỗi cung ứng.

Tham khảo: Kiến trúc tham chiếu ĐTĐM của NIST, tháng 09/2011.

Kiến trúc hệ thống điện toán đám mây



Mô hình khối lập phương đám mây

8 dạng đội hình đám mây:
(1) Per(IP, IO, EP, EO) và
(2) D-p(IP, IO, EP, EO)

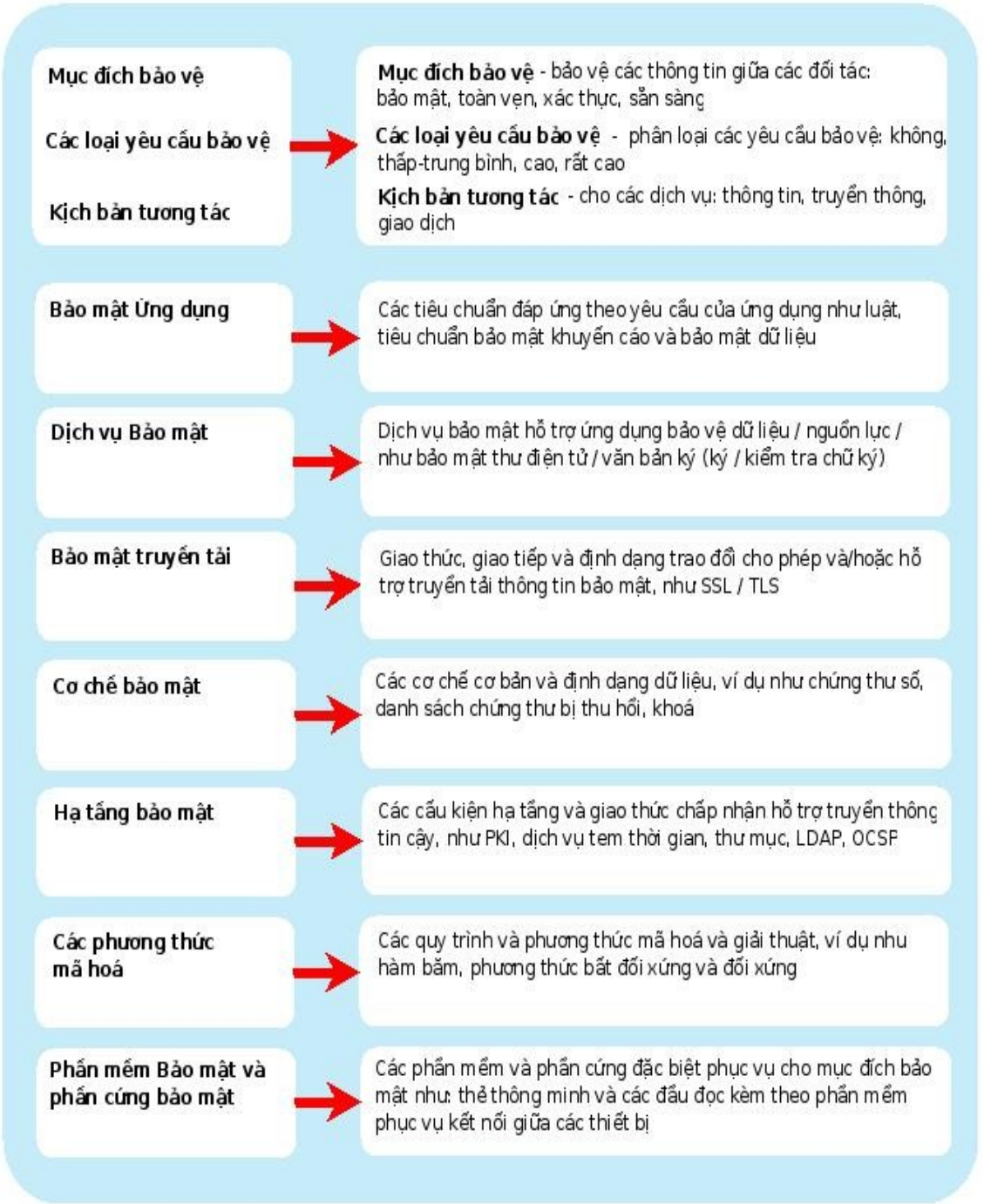
Đội hình đám mây E/O/D-p ở đỉnh bên phải có khả năng sẽ là "điểm đẹp" nơi mà tính mềm dẻo và sự cộng tác tối ưu có thể đạt được.

Tài liệu của Diễn đàn Jericho.

	Hạ tầng được quản lý bởi[1]	Hạ tầng được sở hữu bởi[2]	Hạ tầng được đặt ở[3]	Truy cập và sử dụng được bởi[4]
Công cộng	Nhà cung cấp là bên thứ 3	Nhà cung cấp là bên thứ 3	Bên ngoài	Không tin cậy
Riêng/ Cộng đồng	Hoặc: Tổ chức / Nhà cung cấp là bên thứ 3	Tổ chức / Nhà cung cấp là bên thứ 3	Bên trong / Bên ngoài	Tin cậy
Lai	Cả tổ chức & Nhà cung cấp là bên thứ 3	Cả tổ chức & Nhà cung cấp là bên thứ 3	Cả bên trong & Bên ngoài	Tin cậy & Không tin cậy

ĐTĐM có thể là còn quá mới và còn nhiều vấn đề cần phải được nghiên cứu để có thể triển khai tốt trong thực tế.

An ninh thông tin - dữ liệu



Tất cả việc đảm bảo an ninh nêu trên đều nhằm để đảm bảo an ninh cho thông tin - dữ liệu → các tiêu chuẩn an ninh thông tin - dữ liệu.

← Mô hình cho các tiêu chuẩn an ninh dữ liệu với các giải nghĩa và ví dụ.

C. Chuẩn hóa & an ninh hệ thống thông tin

1. Lớp nghiệp vụ: chuẩn hóa qui trình nghiệp vụ và thủ tục bằng công cụ tiêu chuẩn UML (Unified Modeling Language).
2. Lớp thông tin: Mô hình hóa bằng UML và chuẩn hóa dữ liệu
   - Mô hình dữ liệu chung & mô hình dữ liệu đặc thù
   - Chuẩn hóa dữ liệu bằng XML để đảm bảo tính tương hợp dù XML không đảm bảo được tính tương hợp về tổ chức.
3. Lớp hạ tầng: phân vùng và quản lý truy cập giữa các vùng.
4. Lớp ứng dụng: chuẩn hóa theo các nhóm tiêu chuẩn như trong các Khung tương hợp (GIF) hoặc theo Kiến trúc tổng thể quốc gia (NEA).
5. Lớp công nghệ: Chuẩn cho các loại công nghệ và tiêu chuẩn được chọn để sử dụng (kiến trúc thành phần, SOA, SaaS, ĐTĐM...) để đảm bảo tính tương hợp, sử dụng lại, tính mở, an ninh, tính riêng tư, mở rộng được về phạm vi... → đưa ra bộ tiêu chuẩn theo vòng đời và theo kiến trúc hệ thống.

Các tiêu chuẩn cần được phân loại theo vòng đời và được cập nhật liên tục trong môi trường mở!

Chuẩn mở là biện pháp đảm bảo an ninh TT -1

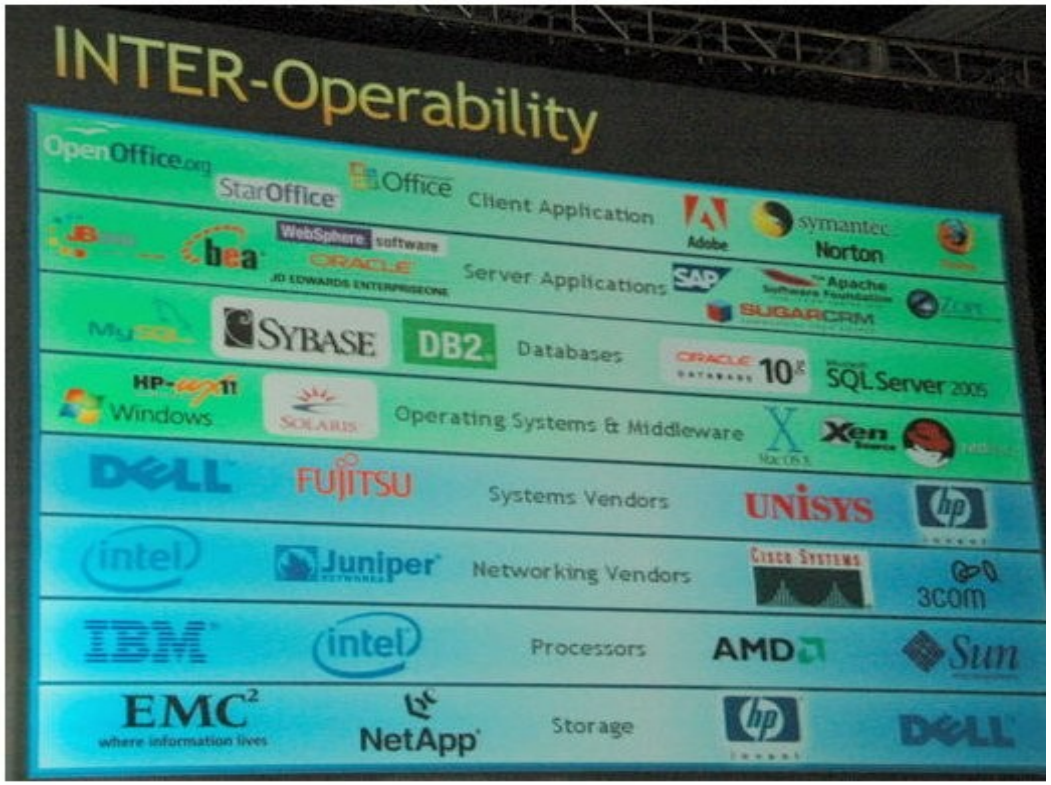
Định nghĩa tiêu chuẩn (TC) mở: có nhiều, một trong số đó là:
1. TC được áp dụng và do một tổ chức phi lợi nhuận duy trì, sự phát triển hiện hành của nó diễn ra theo một thủ tục ra quyết định mở, sẵn sàng cho tất cả các bên có quan tâm.
2. TC đã được xuất bản và tài liệu đặc tả là sẵn sàng hoặc tự do hoặc với phí tượng trưng. Tất cả mọi người phải được phép sao chép, phân phối và sử dụng nó không mất phí hoặc phí tượng trưng.
3. Sở hữu trí tuệ - nghĩa là, có thể có các bằng sáng chế đối với (các phần) tiêu chuẩn và được làm cho sẵn sàng không thể hủy bỏ được trên cơ sở không có phí bản quyền.
4. Không có bất kỳ ràng buộc nào trong sử dụng lại TC đó.

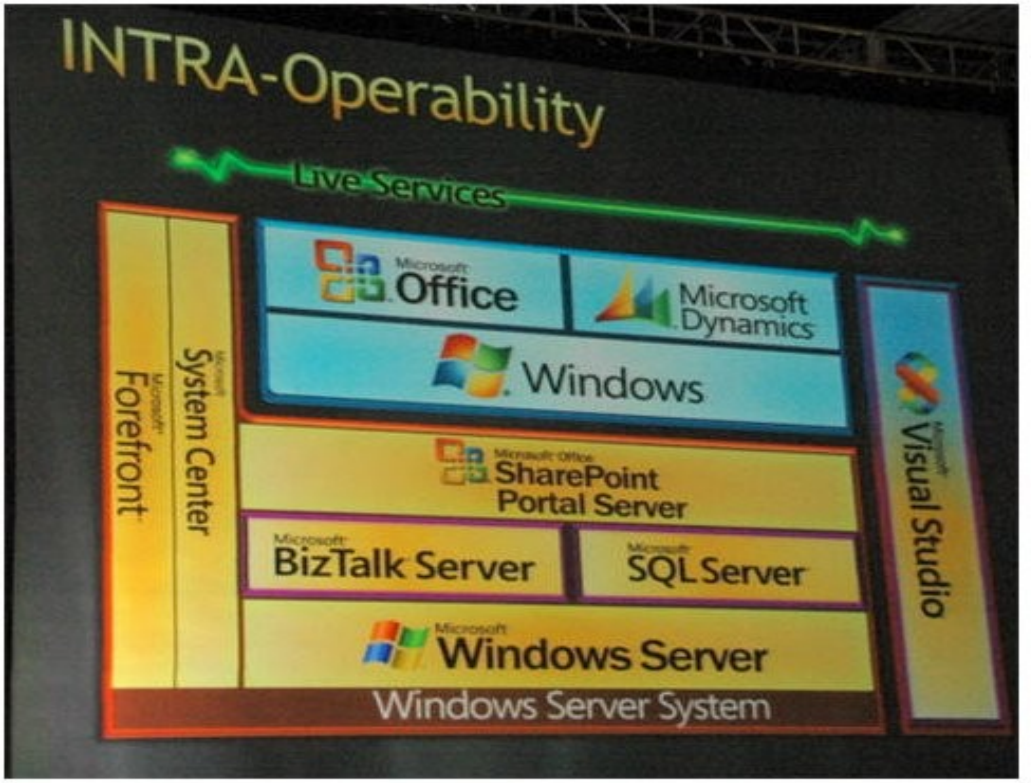
Với TC mở, an ninh được đảm bảo tốt hơn vì: (1) Không bị khóa trói vào nhà cung cấp; (2) Bảo toàn dữ liệu vĩnh cửu; (3) Đảm bảo tính tương hợp liên thông trong hệ thống; (4) Dễ chuyển dữ liệu từ hệ thống này sang hệ thống khác; (5) Khuyến khích đổi mới sáng tạo, cạnh tranh thị trường → hạ giá thành sản phẩm.

Nổi bật: Chính sách bắt buộc tiêu chuẩn mở của Anh, từ 01/11/2012.

Chuẩn mở là biện pháp đảm bảo an ninh TT -2

Tính tương hợp liên thông là yếu tố sống còn của hệ thống thông tin





NÊN THEO: SÂN CHƠI CHO MỌI NGƯỜI

KHÔNG NÊN THEO: BỊ KHÓA TRÓI

Ví dụ điển hình về chuẩn mở: Giao thức TCP/IP, có xuất xứ từ mạng ARPANET của Bộ Quốc phòng Mỹ.

Một số tiêu chuẩn về an ninh

1. Các tiêu chuẩn về hệ thống quản lý an ninh thông tin ISMS (Information Security Management System) ISO/IEC 27K
   - ISO/IEC 27001:2005, đặc tả ISMS → TCVN ISO/IEC 27001:2009.
   - Các chuẩn đã ban hành: từ 27002 tới 27012 đã được ban hành và về nhiều lĩnh vực khác nhau trong an ninh thông tin.
   - Các chuẩn sắp ban hành: từ 27013 tới 27043, trong đó có ANKGM, an ninh ĐTĐM, an ninh thuê ngoài, an ninh mạng, an ninh ƯD.
2. Các tiêu chuẩn an ninh trong ĐTĐM. Tài liệu của NIST, tháng 7/2011.
   - Tiêu chuẩn an ninh: xác thực ủy quyền (11), tính bí mật (7), tính toàn vẹn (4), quản lý nhận diện (5), an ninh (6), quản lý chính sách an ninh (1) và tính sẵn sàng (1).
   - Tiêu chuẩn về tính tương hợp (giao diện & chức năng của dịch vụ): tính tương hợp dịch vụ (4).
   - Tiêu chuẩn về tính khả chuyển (dữ liệu & tải công việc [mới]): tính khả chuyển về dữ liệu (1); tính khả chuyển về hệ thống (1).
3. Các tiêu chuẩn theo mô hình kiến trúc an ninh dữ liệu

   Triển khai khái niệm an ninh, phương pháp mã hóa không đối xứng và đối xứng, dữ liệu băm, quản lý khóa, thẻ thông minh tiếp xúc và không tiếp xúc.

D. Một số biện pháp và công cụ cho an ninh HTTT

Một vài vấn đề liên quan:

Các tác nhân:
(1) Những người vận hành Botnet; (2) Các nhóm tội phạm; (3) Các tin tặc; (4) Người bên trong; (5) Các quốc gia; (6) Người đánh fishing; (7) Người đánh spam; (8) Tác giả của PM độc hại/ PM gián điệp; (9) Những kẻ khủng bố.

Các mối đe dọa và lỗ hổng thường gặp:
(1) Tấn công từ chối dịch vụ; (2) Từ chối dịch vụ phân tán; (3) Bom logic; (4) Phishing; (5) Ngựa Trojan; (6) Vishing - dựa vào VoIP; (7) Thâm nhập qua không dây; (8) Sâu; (9) Khai thác các lỗi ngày số 0.

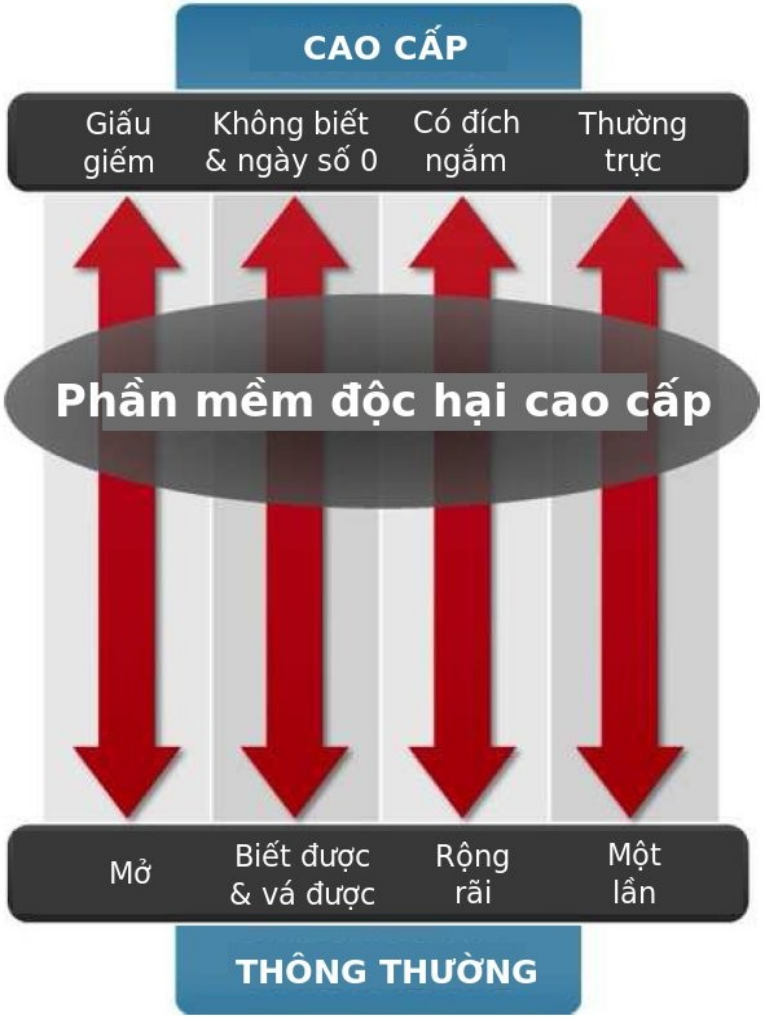
Những vấn đề liên quan khác đáng lưu ý:
1. Mất an ninh từ chuỗi cung ứng sản phẩm, cả cứng, mềm và các thiết bị viễn thông.
2. Luật Yêu nước của Mỹ: yêu cầu các công ty Mỹ phải (kể cả các chi nhánh) truyền tay gần như tất cả số liệu của người sử dụng theo yêu cầu của các cơ quan an ninh Mỹ như FBI mà không cần lệnh tòa án.

Mô hình độ chín ANKGM

Đánh giá khả năng sẵn sàng của một quốc gia đối với ANKGM.

Đặc điểm phần mềm độc hại hiện nay:

Mức độ giấu giếm: phần mềm (PM) được biết công khai → được giấu giếm và ngụy trang cao độ.
Mức độ nhận biết: nhằm vào những chỗ bị tổn thương có thể nhận biết được và chưa được vá → nhằm vào những chỗ bị tổn thương chưa biết & lỗi ngày số 0.
Mức độ rộng rãi: có mục đích chung rộng rãi, nạn nhân vô tình → mục đích cụ thể, nạn nhân đặc biệt, tới từng cá nhân.
Mức độ thường trực: gây hại 1 lần → được cập nhật liên tục để gây hại thường trực.



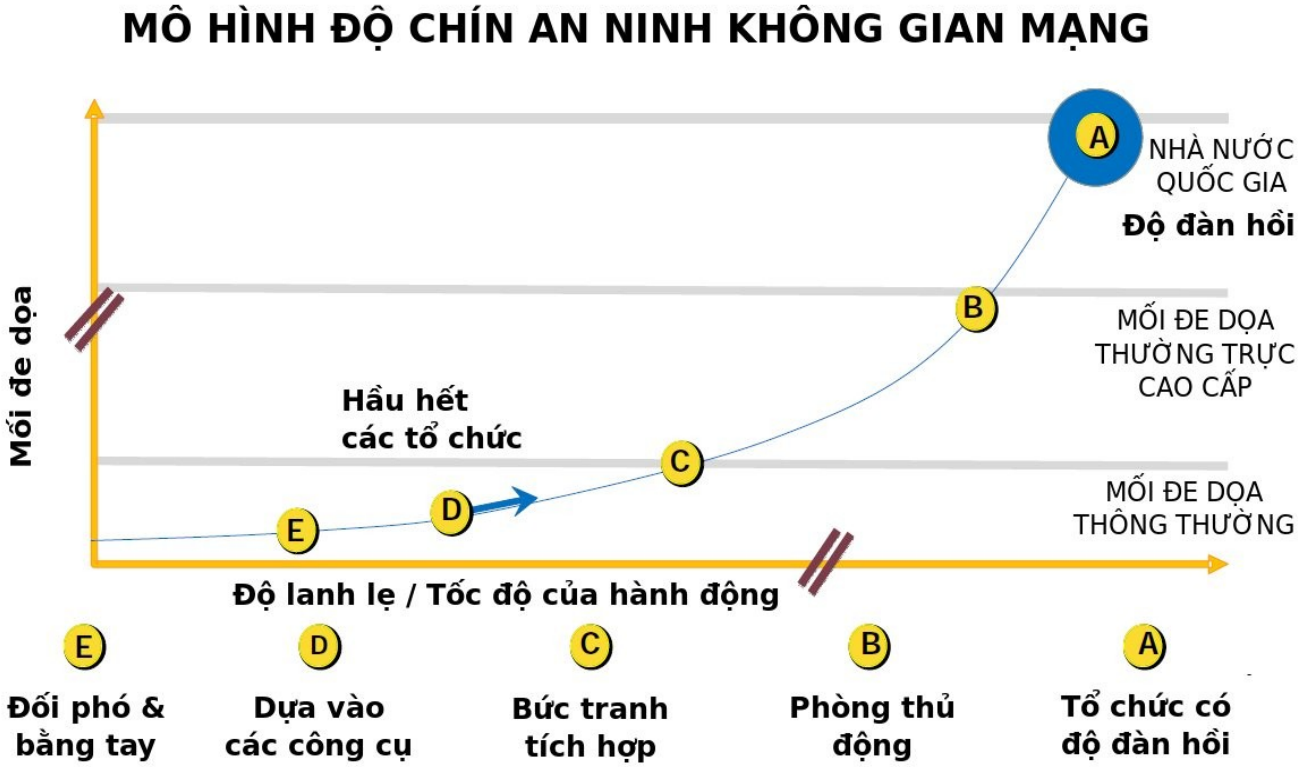
Stuxnet, Duqu, Flame, Gauss, Narilam...

Mô hình độ chín ANKGM

2. Mô hình:

5 giai đoạn hướng tới sự đàn hồi để chống lại các cuộc tấn công KGM.

Bảng xếp hạng một số quốc gia được khảo sát.



E. Tuân theo học thuyết để "dập tắt lửa" được tốt nhất.
D. Áp dụng từng phần công cụ & công nghệ để hỗ trợ đối phó nhanh hơn.
C. Hệ thống được tích hợp nhằm vào tính tương hợp và các tiêu chuẩn trao đổi dữ liệu về nhận thức bảo an thông tin.
B. Lanh lẹ, đoán trước được tình huống, ra chính sách nhanh, chuyên nghiệp, làm rõ sự việc, giúp người vận hành tìm, sửa và đối phó lại.
A. Dự đoạn trước được sự việc, cô lập và chịu đựng được thiệt hại nếu có, đảm bảo an ninh cho chuỗi cung ứng & bảo vệ được hạ tầng sống còn

Các công cụ an ninh

Nhiều công cụ an ninh, bao gồm cả các PMTDNM.
Danh sách 65 PMTDNM sử dụng trong an ninh thông tin:
1. Chống spam: ASSP, MailScanner, SpamAssassin, SpamBayes, Nixory.
2. Chống virus: ClamAV, ClamTK, ClamWin Free Antivirus, P3Scan.
3. Sao lưu: Amanda, Areca Backup, Bacula, Clonezilla, Partimage, Redo.
4. Trình duyệt: Chromium, Dooble, Tor.
5. Bổ sung cho trình duyệt: Web of Trust (WOT), PasswordMaker.
6. Xóa dữ liệu: BleachBit, Eraser, Wipe, Darik's Boot and Nuke.
7. Chống mất dữ liệu: OpenDLP, MyDLP
8. Mã hóa: AxCrypt, Gnu Privacy Guard, GPGTools, gpg4win, PeaZip, Crypt, NeoCrypt, LUKS/ cryptsetup, FreeOTFE, TrueCrypt.
9. Truyền tệp an ninh: WinSCP, FileZilla
10. Điều tra pháp lý: ODESSA, The Sleuth Kit/ Autopsy Browser
11. Gateway / Thiết bị quản lý các mối đe dọa thống nhất: Untangle Lite, ClearOS, Endian Firewall Community
12. Dò tìm thâm nhập trái phép: Open Source Tripwire, OSSEC, AFICK, Snort
13. Tường lửa mạng: IPCop, Devil-Linux, Turtle Firewall, Shorewall, Vuurmuur, m0n0wall, pfSense, Vyatta
14. Giám sát mạng: Wireshark, Tcpdump/ libpcap, WinDump
15. Phá mật khẩu: Ophcrack, John the Ripper,
16. Quản lý mật khẩu: KeePass Password Safe, KeePassX, Password Safe
17. Xác thực người sử dụng: WiKID
18. Lọc web: DansGuardian

Các công cụ an ninh

Nhiều công cụ an ninh, bao gồm cả các PMTDNM.
Danh sách 12 PMTDNM khác sử dụng trong an ninh thông tin:
1. Xóa có an ninh, khôi phục dữ liệu, nhái lại, mã hóa: Darik's Boot and Nuke (DBAN)
2. Sửa và phục hồi tệp: TestDisk and PhotoRec
3. Cứu các ổ đĩa hỏng: GNU ddrescue
4. Nhái đĩa: Clonezilla
5. Mã hóa: TrueCrypt
6. An ninh di động: Master Password (iOS), Secure Chat, Rights Alert, Orbot, Dự án Guardian, Gibberbot, Droidwall

E. Nhu cầu giáo dục đào tạo về nguồn mở -1

Mô tả tình hình và các rủi ro tiềm ẩn

Windows XP SP3 and Office 2003 sẽ hết hạn hỗ trợ kể từ ngày **8 tháng Tư, 2014**.

Sau ngày này, Microsoft ***sẽ không*** cung cấp bất kỳ một sự hỗ trợ nào cho các sản phẩm này nữa, bao gồm các bản vá bảo mật (security patch), các bản sửa lỗi hoặc hỗ trợ xử lý sự cố.

Việc tiếp tục sử dụng Windows XP SP3 và Office 2003 trong hệ thống của Quý vị sau ngày này sẽ tạo ra các rủi ro tiềm ẩn, ví dụ như:

- **Các rủi ro về bảo mật & vi phạm các quy định.** Môi trường không được hỗ trợ và không có đủ các bản vá lỗi sẽ trở thành mục tiêu của các vụ tấn công về bảo mật. Điều đó sẽ dẫn đến việc tổ chức/ doanh nghiệp của Quý vị không kiểm soát được hệ thống, và điều này sẽ sớm được phát hiện bởi bộ phận kiểm toán (nội bộ hoặc bên ngoài), hệ quả là quá trình xin xét duyệt các chứng chỉ quốc gia/quốc tế sẽ bị chậm lại, cũng như tạo ra sự lo ngại của cộng đồng/khách hàng bên ngoài về việc tổ chức/doanh nghiệp của Quý vị không có khả năng kiểm soát hệ thống và bảo vệ dữ liệu cá nhân của công dân/khách hàng.
- **Không tiếp tục nhận được sự hỗ trợ của các hãng cung cấp phần mềm (ISV) cũng như các hãng sản xuất phần cứng (OEM).** Một báo cáo gần đây của hãng nghiên cứu Gartner đã chỉ ra "nhiều hãng cung cấp phần mềm (ISV) nhiều khả năng sẽ không hỗ trợ các phiên bản mới của ứng dụng trên Windows XP trong năm 2011, và trong năm 2012 điều này sẽ trở nên phổ biến." Một báo cáo tương tự của Gartner cho lĩnh vực phần cứng cũng nói rõ rằng trong năm 2012, đa số các hãng phần cứng (OEM) sản xuất PC sẽ ngừng hỗ trợ Windows XP trên đa số các kiểu máy PC mới của họ.

Các lựa chọn:

1. **Nâng cấp** – Lựa chọn này là hiệu quả nhất về mặt đầu tư thông qua việc hiện đại hóa PC bằng việc triển khai Windows 7 Enterprise và Office 2010. Không phụ thuộc vào quy mô triển khai to hay nhỏ, việc hiện đại hóa PC với Windows 7 Enterprise và Office 2010 sẽ giúp tổ chức/doanh nghiệp của Quý vị tăng năng suất làm việc cho cán bộ/nhân viên và tăng hiệu quả hoạt động thông qua việc bảo mật và quản lý PC được tăng cường.

   Để giúp đỡ khách hàng thực hiện quá trình chuyển đổi và triển khai thành công môi trường Windows 7 Enterprise và Office 2010, Microsoft và các đối tác tư vấn hiện đang cung cấp một số chương trình như Proof of Concept (PoC) và triển khai thử nghiệm (pilot), được thực hiện bởi các chuyên gia tư vấn của chính Microsoft hoặc các Đối tác Dịch vụ Cao cấp.

Microsoft
www.microsoft.com/vietnam

2. **Mua Hợp đồng Dịch vụ Hỗ trợ Đặc biệt thông qua nhóm Microsoft Premier Support để tiếp tục sử dụng các sản phẩm đã hết hạn hỗ trợ** - Nếu vì một lý do nào đó, Quý vị quyết định sẽ tiếp tục sử dụng Windows XP SP3 và Office 2003 sau khi đã hết hạn hỗ trợ, Quý vị cần phải ký một Hợp đồng Hỗ trợ Đặc biệt và chúng tôi sẽ yêu cầu Quý vị phải xây dựng một kế hoạch chuyển đổi. Chi phí của Hợp đồng Hỗ trợ Đặc biệt là sẽ cao hơn nhiều cho với Hỗ trợ Bình thường, và sẽ tăng dần theo năm tương ứng với chi phí hỗ trợ tăng dần cho sản phẩm đã hết hạn hỗ trợ.

3. **Không làm gì cả** - Microsoft khuyến nghị Quý vị không nên đi theo lựa chọn này để tránh gặp phải các rủi ro về bảo mật và vi phạm các quy định.

BỘ VĂN HOÁ, THỂ THAO VÀ DU LỊCH
CỤC BẢN QUYỀN TÁC GIẢ

Số: 15/BQTG-QTG
V/v khuyến cáo về việc sử dụng chương trình máy tính tại các doanh nghiệp Việt Nam xuất khẩu sản phẩm sang Hoa Kỳ

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 7 tháng 2 năm 2012

Kính gửi: Các doanh nghiệp,

Cục Bản quyền tác giả nhận được thông tin hai Bang Washington và Luoisiana của Hoa Kỳ đã ban hành Luật mới, yêu cầu các nhà sản xuất có sản phẩm bán tại các Bang này phải tuân thủ nghĩa vụ pháp lý đối với việc sử dụng công nghệ thông tin, liên quan đến bảo hộ chương trình máy tính theo Luật sở hữu trí tuệ, hoặc gánh chịu rủi ro theo Luật Cạnh tranh không lành mạnh. Luật này có hiệu lực kể từ ngày 22/7/2011, cho phép các nhà sản xuất hoặc chưởng lý tại các Bang tiến hành khởi kiện dân sự đối với các nhà sản xuất nước ngoài sử dụng công nghệ thông tin vi phạm để sản xuất, phân phối, tiếp thị hoặc bán sản phẩm, bộ phận sản phẩm trong hai Bang này.

Ngoài ra, 37 Bang và vùng lãnh thổ khác của Hoa kỳ cũng đã cam kết ban hành các điều luật tương tự. *(Xem thông tin chi tiết tại địa chỉ: http://law.ga.gov/00/press/detail/0,2668,87670814_167294941_178242145,00.html).*

Để tránh những thiệt hại không đáng có, Cục Bản quyền tác giả khuyến cáo các doanh nghiệp Việt Nam xuất khẩu sản phẩm, bộ phận sản phẩm vào thị trường các Bang và vùng lãnh thổ của Hoa Kỳ sớm kiểm tra và hợp pháp hóa việc sử dụng hệ thống công nghệ thông tin liên quan đến chương trình máy tính trong doanh nghiệp, để có được lợi thế khi xuất khẩu hàng hóa sang Hoa kỳ./.

Nơi nhận:
- Như trên;
- Lưu: VT, QTG (H).

CỤC TRƯỞNG

CỤC BẢN QUYỀN TÁC GIẢ

Vũ Mạnh Chu

◄ Hết hạn hỗ trợ Windows XP SP3 và Office 2003 từ ngày 08/04/2014.

Nhu cầu giáo dục đào tạo về nguồn mở -2

Worldwide Mobile Device Sales to End Users by Operating System in 3Q12 (Thousands of Units)

Operating System	3Q12 Units	3Q12 Market Share (%)	3Q11 Units	3Q11 Market Share (%)
Android	122,480.0	72.4	60,490.4	52.5
iOS	23,550.3	13.9	17,295.3	15.0
Research In Motion	8,946.8	5.3	12,701.1	11.0
Bada	5,054.7	3.0	2,478.5	2.2
Symbian	4,404.9	2.6	19,500.1	16.9
Microsoft	4,058.2	2.4	1,701.9	1.5
Others	683.7	0.4	1,018.1	0.9
Total	**169,178.6**	**100.0**	**115,185.4**	**100.0**

Source: Gartner (November 2012)

▲ Gartner: Bán các thiết bị di động cho người sử dụng đầu cuối trên toàn cầu **tính theo hệ điều hành** vào Quý III/2012. **Android đứng số 1 với hơn 122 triệu chiếc, chiếm 72.4%**.

Worldwide Mobile Device Sales to End Users by Vendor in 3Q12 (Thousands of Units)

Company	3Q12 Units	3Q12 Market Share (%)	3Q11 Units	3Q11 Market Share (%)
Samsung	97,956.8	22.9	82,612.2	18.7
Nokia	82,300.6	19.2	105,353.5	23.9
Apple	23,550.3	5.5	17,295.3	3.9
ZTE	16,654.2	3.9	14,107.8	3.2
LG Electronics	13,968.8	3.3	21,014.6	4.8
Huawei Device	11,918.9	2.8	10,668.2	2.4
TCL Communication	9,326.7	2.2	9,004.7	2.0
Research in Motion	8,946.8	2.1	12,701.1	2.9
Motorola	8,562.7	2.0	11,182.7	2.5
HTC	8,428.6	2.0	12,099.9	2.7
Others	146,115.1	34.2	145,462.2	32.9
Total	**427,729.5**	**100.0**	**441,502.2**	**100.0**

Source: Gartner (November 2012)

▲ Gartner: Bán các thiết bị di động cho người sử dụng đầu cuối trên toàn cầu **tính theo nhà cung cấp** vào Quý III/2012.

Xuất xưởng máy tính cá nhân PC Quý III/2012 là 87.5 triệu chiếc

Chuyển đổi sang sử dụng các PMTDNM

Vì sao phải chuyển đổi:

1. Tiết kiệm chi phí mua sắm, duy trì, nâng cấp, cập nhật phần mềm
2. Đảm bảo được năng suất lao động
3. Đảm bảo sử dụng lại được các TT/DL đã có - có an ninh
4. Đảm bảo trao đổi dữ liệu bên trong & ngoài DN
5. Tôn trọng luật sở hữu trí tuệ - không bị dọa kiện, phá sản
6. Đảm bảo an ninh thông tin, dữ liệu cho lâu dài
7. Không bị khóa trói vào các nhà độc quyền
8. Ví dụ điển hình tại Việt Nam: Viettel.

Chuyển đổi trên các máy tính trạm cá nhân

1. Chuyển đổi một phần: Giữ nguyên hệ điều hành Windows, chuyển đổi một số ứng dụng: (1) bộ phần mềm văn phòng từ MS Office sang LibreOffice; (2) trình duyệt web IE sang Firefox; Chrome (3) trình thư điện tử máy trạm Outlook sang Thunderbird.

2. Chuyển đổi toàn phần: Chuyển nốt cả hệ điều hành Windows sang GNU/Linux, ví dụ Ubuntu, và chuyển đổi các ứng dụng nghiệp vụ.

GNU/Linux có hầu hết tất cả các ứng dụng thường có trên Windows và đều là tự do. Môi trường thực tế: môi trường hỗn hợp: Mở + Đóng.

Chuyển đổi sang sử dụng các PMTDNM

Chuyển đổi trên các máy chủ

1. Hệ điều hành: GNU/Linux Debian, Ubuntu, RedHat, ...
2. Dịch vụ chia sẻ máy chủ tệp & in ấn: SAMBA, OpenLDAP, CUPS
3. Các dịch vụ hệ thống: LDAP, DNS, DHCP, RAS, Web, FTP...
4. Máy chủ thư điện tử, các dịch vụ truyền thông: Zimbra
5. Máy chủ CSDL, các ứng dụng nghiệp vụ: MySQL, PostgreSQL
6. Máy chủ an ninh an toàn: tường lửa, ủy quyền, chống virus, chống truy cập trái phép...

Ở phía các máy chủ - vốn là thế mạnh của PMTDNM

Môi trường thực tế: môi trường hỗn hợp: Mở + Đóng.

Tìm kiếm sự trợ giúp trong và sau chuyển đổi

1. Trước hết từ cộng đồng nguồn mở Việt Nam (http://vfossa.vn/), cả cộng đồng chung và cộng đồng riêng của từng dự án.
2. Từ các công ty cung cấp các dịch vụ xung quanh các PMTDNM

Tham khảo các bài: (1) "Chuyển đổi các ứng dụng từ đóng sang mở".
(2) "Nguồn mở và sự hỗ trợ"
(3) "Hướng dẫn chuyển đổi..."

Chuyển đổi sang sử dụng các PMTDNM

Khó khăn thường gặp và cách khắc phục

1. Quyết tâm và sự tham gia trực tiếp của lãnh đạo cao nhất đơn vị trong việc chuyển đổi.
2. Tham vọng chuyển đổi lớn và nhanh ngay một lúc
3. Một số khác biệt trong thói quen sử dụng - chống đối
4. Các macro trong MS Office - phải viết lại cho LibreOffice
5. Xuất dữ liệu sang Excel - phải viết lại cho Cal
6. Các phần mềm nghiệp vụ chuyên dụng (kế toán) chỉ chạy trên Windows - đề nghị nhà sản xuất chuyển để chạy được trên GNU/Linux:
    a) Dùng các phần mềm mô phỏng như Wine
    b) Chuyển sang công nghệ Web để giải phóng máy trạm
    c) Dùng các máy ảo để chạy Windows trên GNU/Linux
    d) Giữ lại một số máy Windows không thể chuyển
7. Sử dụng hạ tầng khóa công khai (PKI) và chữ ký điện tử → Yêu cầu nhà cung cấp dịch vụ phải có giải pháp cho môi trường nguồn mở:
    a) Chạy được trong hệ điều hành GNU/Linux như Ubuntu, Fedora...
    b) Chạy được trong các trình duyệt web như Firefox, Chrome, …
    c) Chạy được trong bộ phần mềm văn phòng LibreOffice, OpenOffice..
    d) Chạy được cho các hệ quản trị CSDL: MySQL, PostgreSQL
    e) Chạy được trong các máy chủ thư điện tử: SendMail, Postfix, ...

Một số gợi ý khác

Chuyển sang các PMTDNM như được nêu:

1. Theo thông tư số 41/2009/TT-BTTTT ngày 30/12/2009
2. Các lựa chọn nguồn mở v1.0 của Chính phủ Anh, tháng 10/2011.

Khi sử dụng các dịch vụ điện toán đám mây

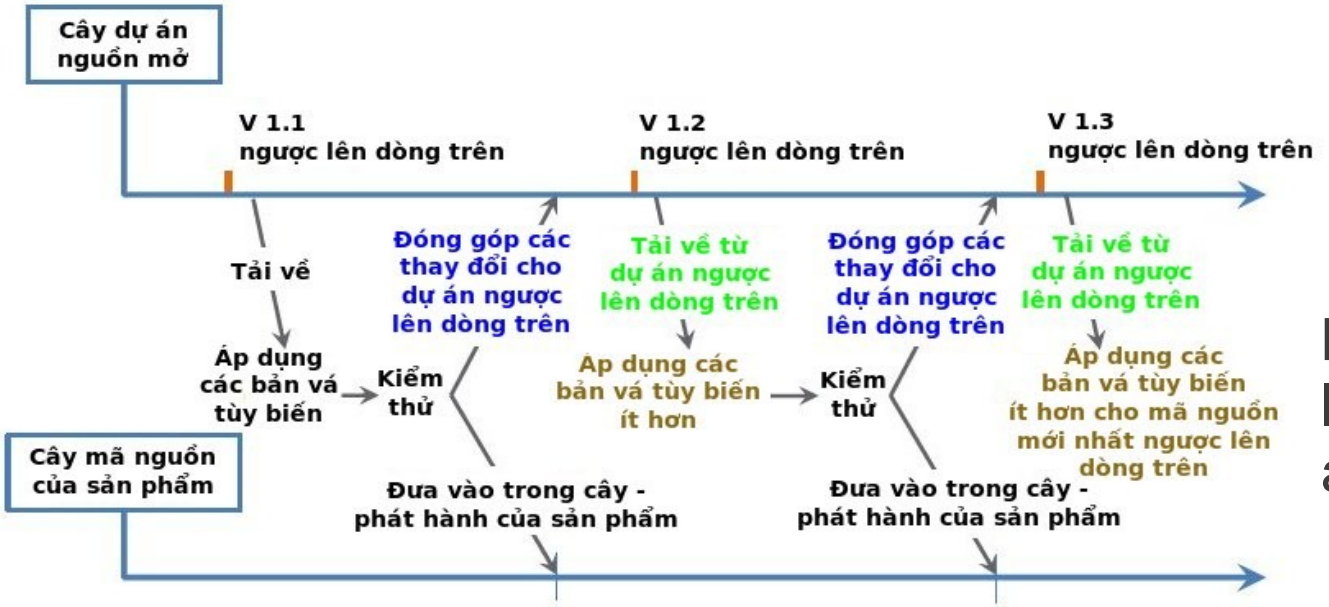
1. Chỉ nên sử dụng với các dữ liệu không thật sống còn với DN
2. Luôn có bản sao trong hệ thống của DN
3. Luôn đặt ra câu hỏi: **Nếu tôi lấy dữ liệu của tôi để chuyển sang một đám mây khác, với công nghệ khác thì có được không?**
4. Luôn ghi nhớ, trong mọi trường hợp, **nghĩa vụ đảm bảo an ninh thông tin là sự chia sẻ giữa nhà cung cấp và người sử dụng.**

Tham khảo các tài liệu về điện toán đám mây (ĐTĐM):

1. Chỉ dẫn về an ninh trong ĐTĐM v2.1, CSA, tháng 12/2009.
2. Lộ trình ĐTĐM của Chính phủ Mỹ, v1.0, NIST, tháng 11/2011.
3. Kiến trúc tham chiếu ĐTĐM, NIST, tháng 09/2011.
4. Lộ trình tiêu chuẩn ĐTĐM v1.0, NIST, tháng 07/2011.
5. Bản ghi nhớ cho các CIO về an ninh ĐTĐT, Văn phòng Điều hành Tổng thống Mỹ, ngày 08/12/2011.

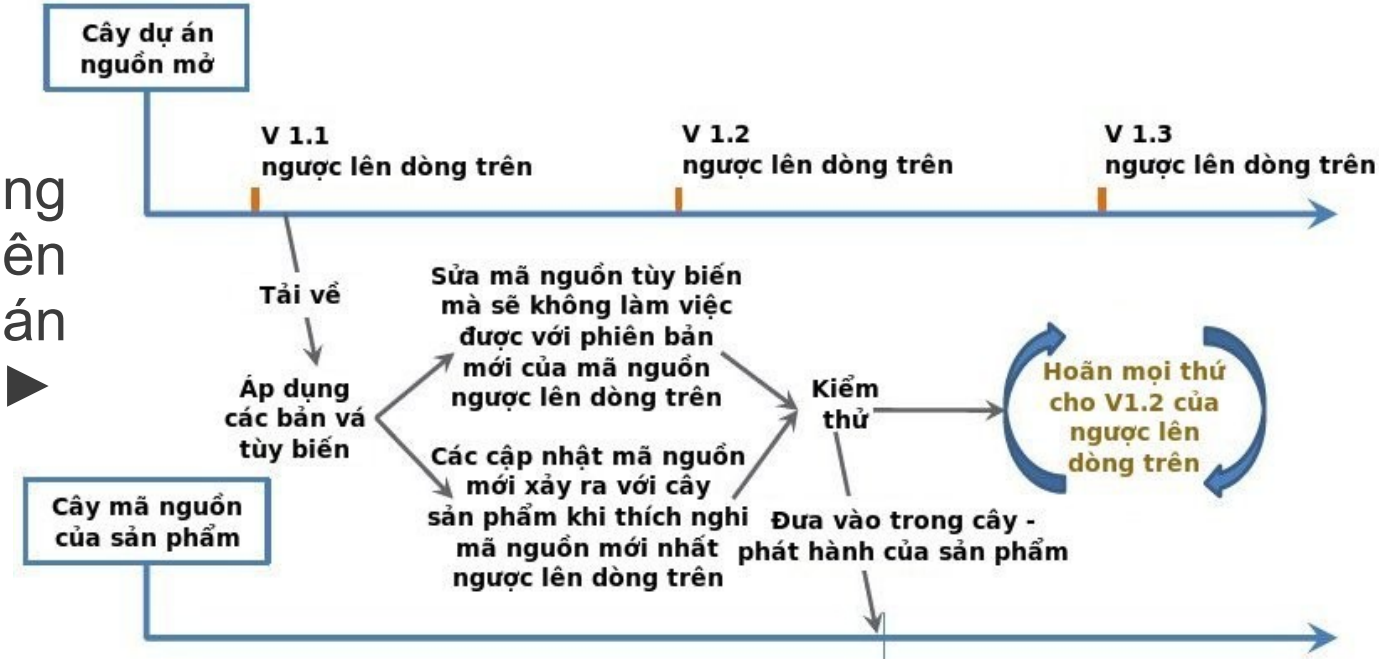
Tuân thủ mô hình phát triển PMTDNM

Phải tuân thủ mô hình phát triển PMTDNM, không đóng mã nguồn → tạo rẽ nhánh không cần thiết, gây hại cho cơ quan phát triển và các đơn vị sử dụng.

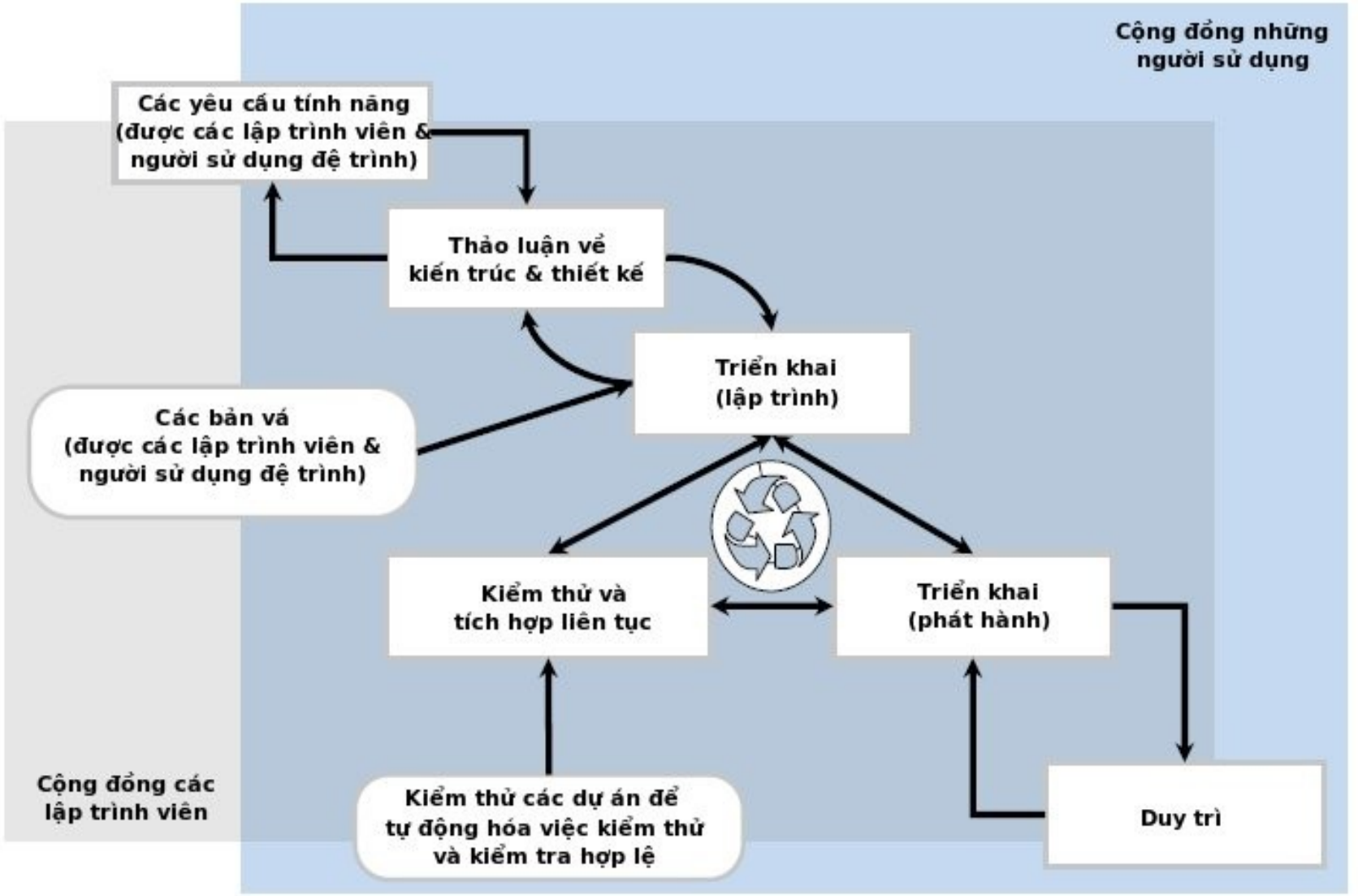


◄ Phát triển đúng mô hình, có đóng góp ngược lên dòng trên cho cây dự án nguồn mở gốc ban đầu.

Phát triển rẽ nhánh, không có đóng góp ngược lên dòng trên cho cây dự án nguồn mở gốc ban đầu. ►



Tuân thủ mô hình phát triển PMTDNM



Cộng đồng những người sử dụng tham gia vào tiến trình phát triển PMTDNM → Đưa ra các yêu cầu tính năng, báo cáo lỗi...

FOSSA
Free & Open Source Software
Association of Vietnam

Cảm ơn!

Hỏi đáp