BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU KHẨN CẤP MÁY TÍNH VIỆT NAM
VNCERT

CÁC NGUY CƠ VỀ AN TOÀN MẠNG & GIẢI PHÁP ĐẢM BẢO AN TOÀN HỆ THỐNG CNTT

LONG AN, 11-2016

Nội dung

- Các nguy cơ về an toàn mạng
- Đảm bảo an toàn cho các hệ thống CNTT
- Giới thiệu VNCERT

Tình hình
An toàn Thông tin
và
Các Xu hướng
Tấn Công Mạng hiện nay

Tình hình ATTT và Các xu hướng tấn công mạng

- Tấn công có mục tiêu:
  - Tấn công APT BlackEnergy vào lĩnh vực năng lượng của Ukraine cuối 2015-2016 (*),
  - Poseidon (Bồ Đào Nha, tấn công các máy PoS và mã độc được "may đo" riêng) (*),
  - Hacking Team (Ý) - tổ chức chuyên bán các công cụ do thám mạng cho các tổ chức / chính phủ bị hack và 400GB dữ liệu bị phát tán lên mạng qua chính tài khoản Twitter của công ty, (*)
  - BLOCKBASTER bởi Lazarus Group (Triều Tiên, tấn công Sony Pictures năm 2014),
  - 10 bệnh viện mạng MedStar bị mã độc mã hoá dữ liệu (chỉ duy nhất một bệnh viện ở California đã trả 17.000 USD để lấy khoá giải mã),
  - một loạt các tấn công vào ngành công nghiệp dầu hoả của Iran,
  - Xdedic - tấn công APT kiểu APT-as-a-Service
  - …

Tấn công có mục tiêu

Ban đầu sử dụng spearphishing với các macro trong các tập tin Excel, Word có trojan (https://securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/)

Các thành phần kỹ thuật sử dụng tấn công Ukraine

Tấn công có mục tiêu

Tấn công có mục tiêu

Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim

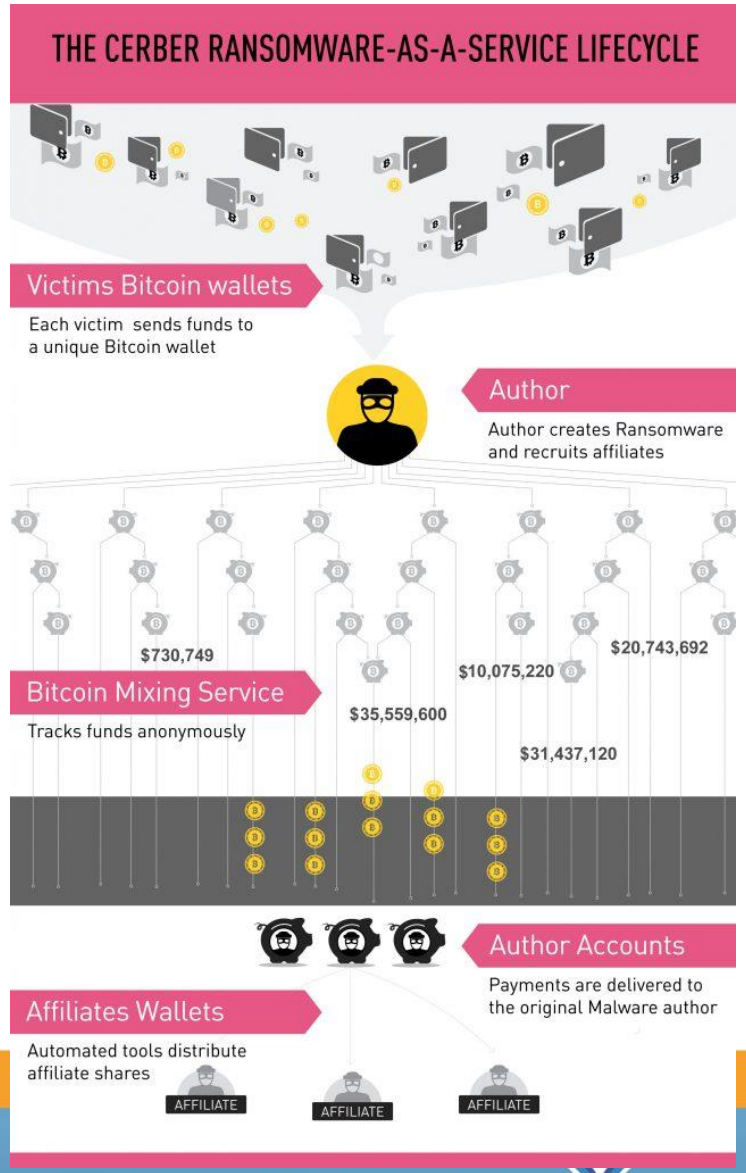
Cybersecurity firm has 400GB of what purport to be its own documents published via its Twitter feed after hack

Tình hình ATTT trên thế giới:

- Tội phạm mạng:
  - Adwind RAT (Remote Access Tool) hoạt động theo kiểu Malware-as-a-Service,
  - Ransomware-as-a-Service (RaaS) như Shark hoặc CerberRing RaaS ring (161 campaign và tăng mới 8 campaign mỗi ngày, nhiễm khoảng 150.000 người trên 201 quốc gia *(nguồn: CheckPoint, 08/2016)*) (*),
  - Các hiểm hoạ tấn công vào ngân hàng: 2 nhóm cướp ngân hàng kiểu APT là Metel & GCMAN sử dụng Carbanak 2.0 (2015, 29 tổ chức tại Nga bị nhiễm, trộm tiền ngân hàng với 4 kiểu phổ biến: online banking, e-payment, điều khiển các máy ATM, thay đổi số dư tài khoản) (*), Buhtrap giả mạo FinCERT tấn công vào ngân hàng trung ương Nga, tấn công vào ngân hàng trung ương Bangladesh và chuyển 20 triệu USD đến Sri Lanka, rút tiền đồng loạt 200 trạm ATM tại Nhật, lừa người
  - Xdedic - tấn công APT kiểu APT-as-a-Service
  - Bán đấu giá “vũ khí tấn công mạng” của Equation group (*) – một nhóm hacker được cho là cánh tay nối dài của NSA (National Security Agency – Hoa Kỳ)
  - …

Tội phạm mạng

(http://blog.checkpoint.com/2016/08/16/cerberring/)



Tội phạm mạng

Tội phạm mạng

Hacking group claims to offer cyber-weapons in online auction

Shadow (môi giới) đã nói rằng các công cụ bán đấu giá sẽ "tốt hơn Stuxnet"

(http://www.reuters.com/article/us-usa-cyber-auction-idUSKCN10Q29W)

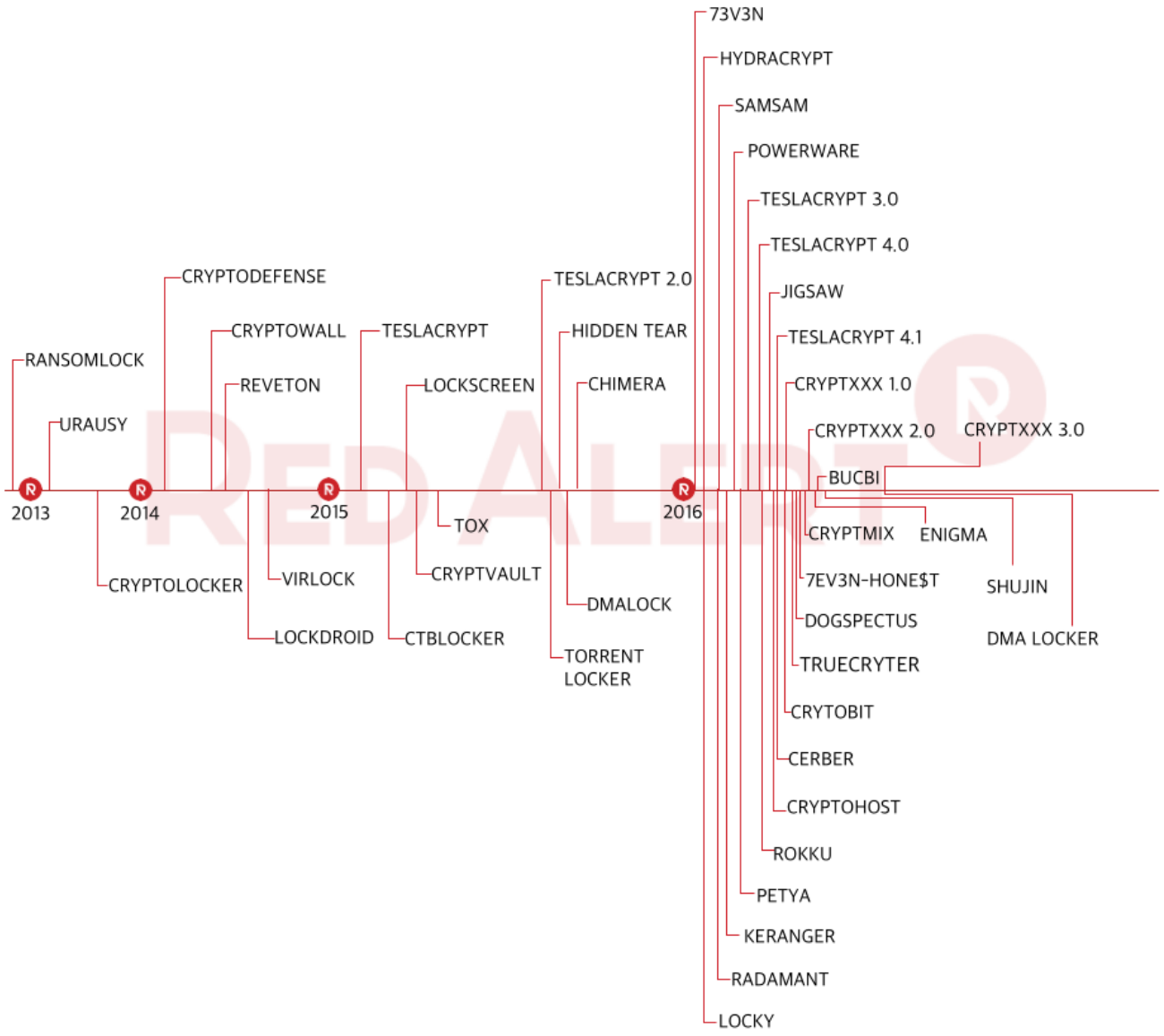
Tình hình ATTT trên thế giới:

- Hack: nở rộ trong thời gian gần đây. Các vụ việc mới nhất trong 2016:
  - 5/5/2016: công bố một vụ hack lớn nhất trong các năm gần đây nhưng không ai biết và cảnh báo
  - 31/5/2016: Hack MySpace và rao bán 427 triệu tài khoản kèm theo mật khẩu
  - 5/6/2016: 171 triệu tài khoản của VK.com bị trộm bởi hacker
  - 9/6/2016: Một hacker rao bán hàng triệu tài khoản Twitter
  - 13/6/2016: hacker rao bán trên dark web 51 triệu tài khoản chia sẻ file
  - 15/7/2016: diễn đàn của Ubuntu bị hack khoảng 2 triệu người dùng
  - 8/8/2016: Oracle điều tra trích xuất dữ liệu ở bộ phận point-of-sale của Micros
  - 18/8/2016: hàng triệu mã khoá của trò chơi Steam bị mất sau khi hacker trích xuất trang web
  - 22/8/2016: Diễn đàn của Epic bị hack lại một lần nữa, và bị trộm hàng ngàn tài khoản đăng nhập
  - 1/9/2016: Hacker trộm 43 triệu tài khoản của Last.fm
  - 6 tháng đầu 2016: 974 vụ và trộm khoảng 554 triệu record dữ liệu

Tình hình ATTT trên thế giới:

- Mã độc tống tiền Ransomware đang bùng phát trên trong năm 2016, tăng rất nhanh về số vụ và chủng loại. Các biến thể mới như Locky, Troldesh (Encoder.858), mã độc mã hoá toàn bộ đĩa Petya thay cho mã hoá file hiện nay, ransomware trên thiết bị di động, … Theo FBI, ước doanh thu tích luỹ trong 3 tháng đầu năm là hơn 209 triệu USD.

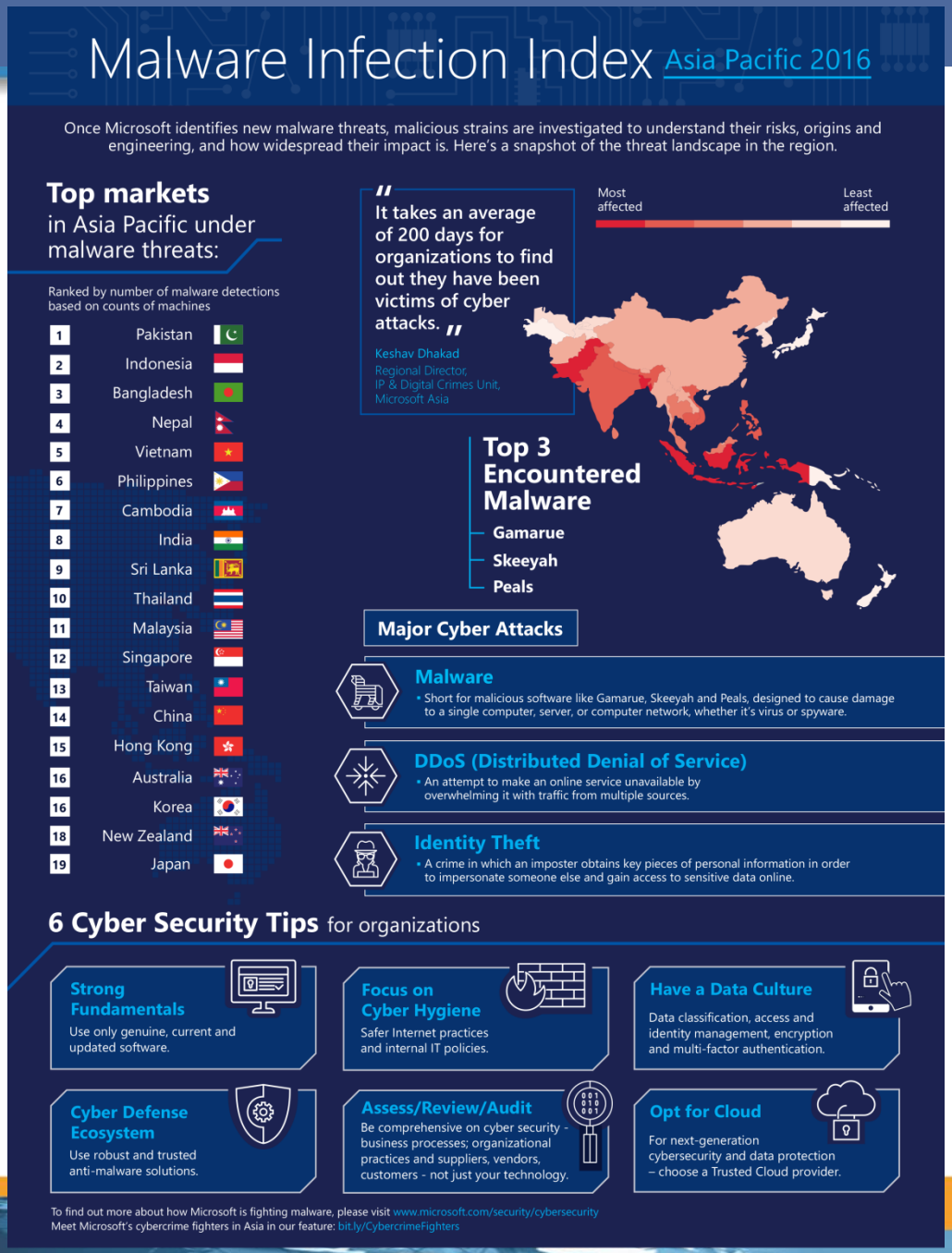
Mã độc tống tiền Ransomware



Các chủng loại ransomware & các biến thể theo các năm *(nguồn: Red Alert)*

Tình hình ATTT trên thế giới:

- Mã độc vẫn tiếp tục lan tràn, là công cụ tấn công APT, ransomware, phishing, … Châu Á - Thái Bình Dương là khu vực nguy cơ cao nhất với tại 5 nước Pakistan, Indonesia, Bangladesh, Nepal, Vietnam
  (nguồn: Malware Infection Index 2016, Microsoft)



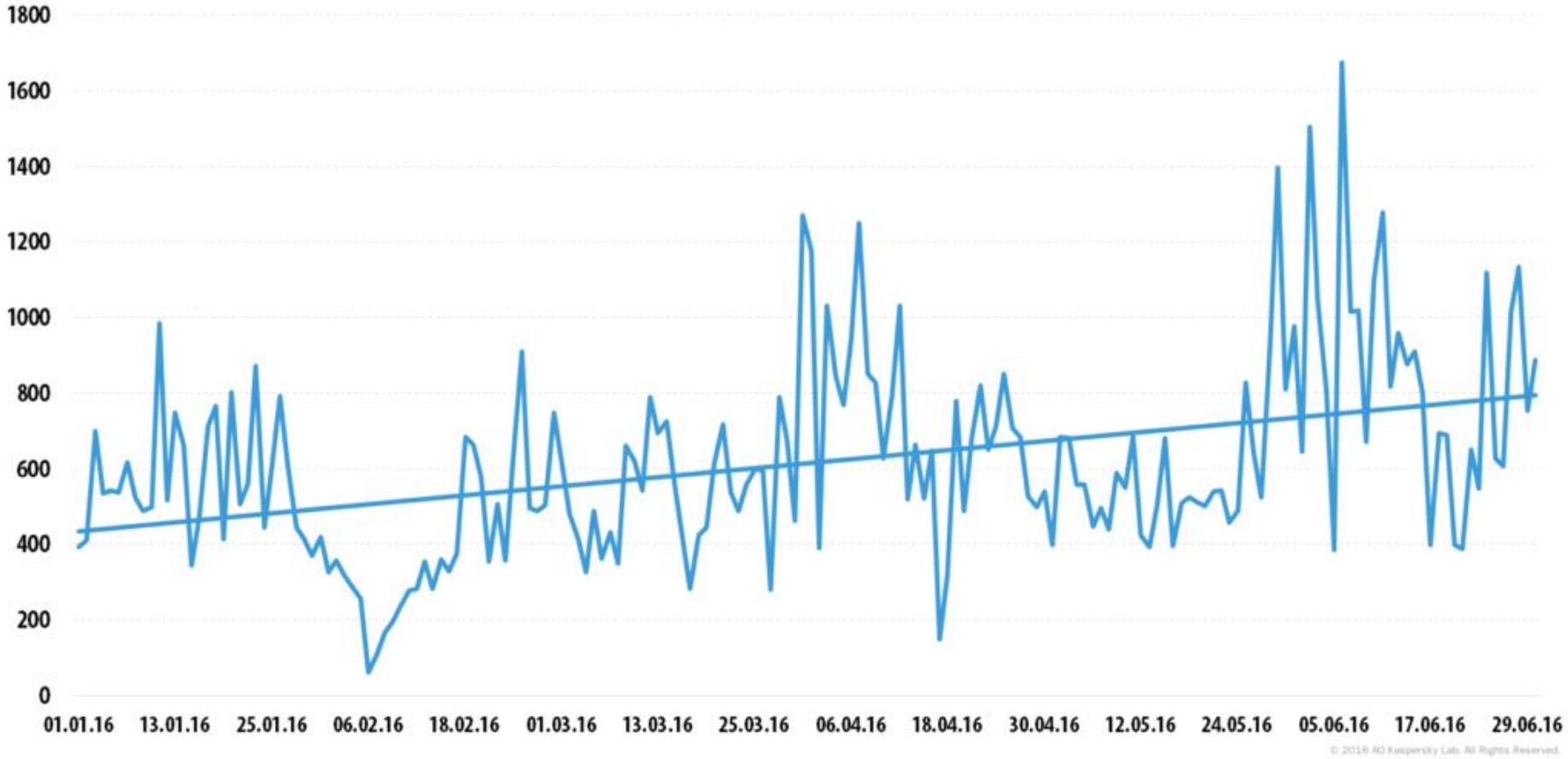
Nguồn:

Malware Infection Index 2016 highlights key threats undermining cybersecurity in Asia Pacific: Microsoft Report *(https://news.microsoft.com/apac/2016/06/07/malware-infection-index-2016-highlights-key-threats-undermining-cybersecurity-in-asia-pacific-microsoft-report/#sm.00074sxz219bse97ypp19jzoe1wle)*

Tình hình ATTT trên thế giới:

- Tấn công DDoS gia tăng:
  - Tấn công vào Akamai – nhà cung cấp hosting, sử dụng kiểu tấn công DDoS-as-a-service với lưu lượng đến **1100 Gbps** (23/9/2016);
  - Các kiểu tấn công mới: khai thác giao thức DNSSEC; dùng tính năng pingback của WordPress; sử dụng hỗ trợ của các botnet, sử dụng các thiết bị IoT; …
  - Thống kê của Kaspersky trong quý 2/2016:
    + 70 quốc gia có tấn công DDoS
    + 77,4% tài nguyên phục vụ tấn công được đặt tại Trung Quốc
    + Trung Quốc, Hàn Quốc, Hoa Kỳ dẫn đầu về số lượng và số mục tiêu tấn công
    + Cuộc tấn công dài nhất với thời gian lên đến 291 giờ (12,1 ngày)
    + 70,2% các tấn công phát hiện được được phát động bởi botnet Linux
    + Các kiểu tấn công phổ biến: SYN DDoS, TCP DDoS, HTTP DDoS
  - Mã nguồn sử dụng IoT để tấn công DDoS đã được phổ biến ra cộng đồng

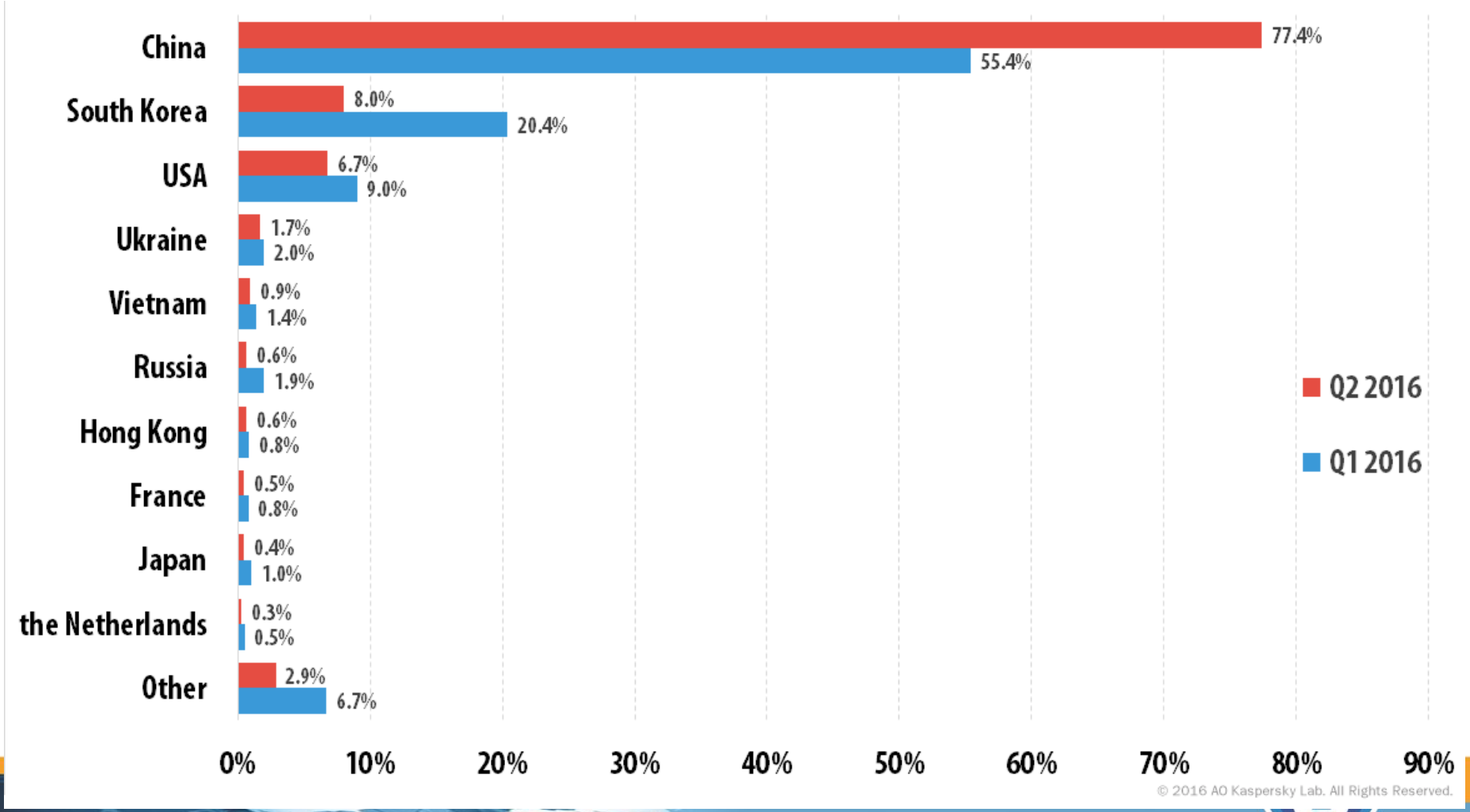
Tấn công DDoS



Số lượng các tấn công DDoS Q1-Q2/2016 *(nguồn: Kaspersky,)*

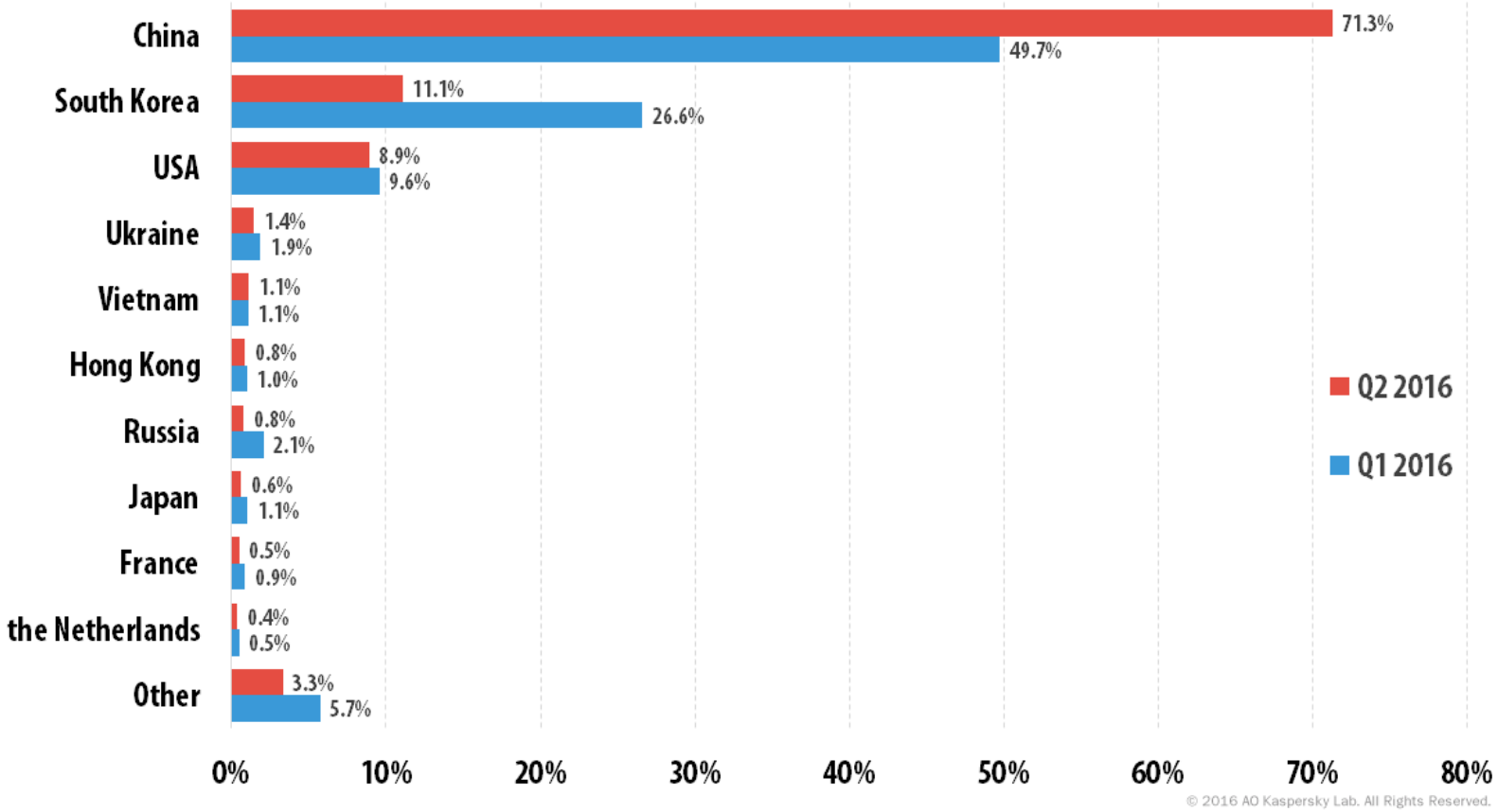
Tấn công DDoS

- 10 quốc gia bị tấn công DDoS cao (chiếm 97,3%)



Tấn công DDoS

- 10 quốc gia xuất phát tấn công DDoS cao (chiếm 94,3%)



Tình hình ATTT trên thế giới:

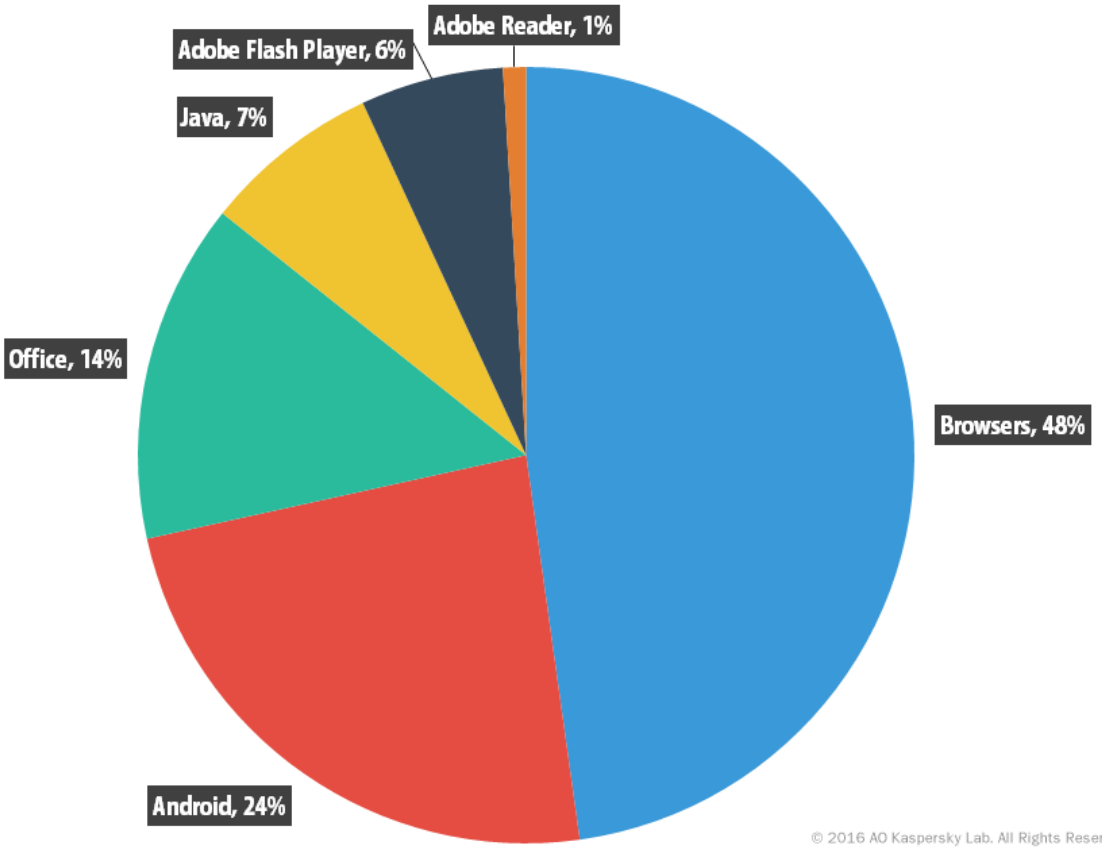
- Tấn công khai thác các lỗ hổng bảo mật đã công bố gia tăng: bình quân mỗi ngày có trên 1 triệu tấn công vào các trang web; gần 75% các trang web không vá lỗi kịp thời các lỗ hổng bảo mật mới; mỗi tuần phát hiện một lỗ hổng zero-day mới *(nguồn 2016 Internet Security Threat Report, Symantec),* trên 100 triệu xe ôtô của tập đoàn Volkswagen bị lỗ hổng có thể khai thác; trên 840.000 thiết bị Cisco có thể bị khai thác bởi công cụ của NSA; 5 lỗ hổng bảo mật được tìm thấy cùng lúc trong management console của EMC;

  + Tấn công tìm các lỗ hổng bảo mật để săn tiền thưởng của các hãng Cisco, Google, Facebook, …

Khai thác lỗ hổng bảo mật

Tỷ lệ khai thác lỗ hổng trên các ứng dụng để tấn công

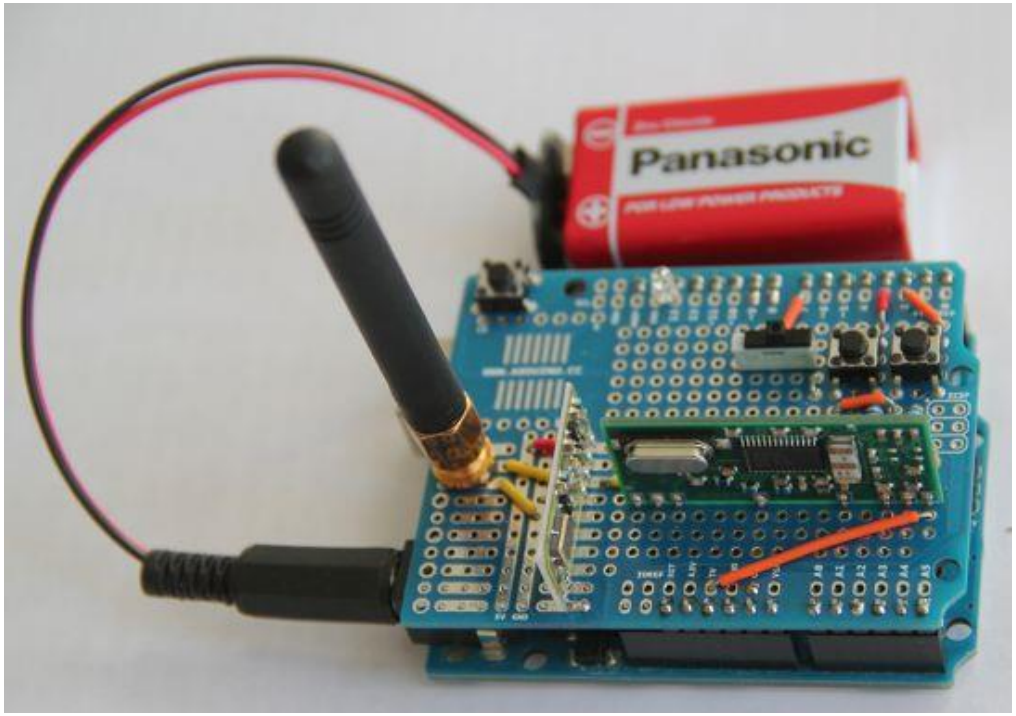
(nguồn: Kaspersky, Q2-2016)



Khai thác lỗ hổng bảo mật

Over 100 Million Volkswagen Group Cars Vulnerable to New Car Key Hack

Researchers recommend car owners to fall back on mechanical locks and thus leave the remote keys aside



Công cụ tấn công rất rẻ tiền và thực hiện qua xâm nhập qua kết nối vô tuyến đã mã hoá trong khoảng cách 90m (http://news.softpedia.com/news/over-100-million-volkswagen-group-cars-vulnerable-to-new-car-key-hack-507225.shtml)

A team of researchers from the University of Birmingham, the UK, have discovered two new vulnerabilities that allow an attacker to create copies of authentic car keys used by the Volkswagen Group.

Tình hình ATTT trên thế giới:

- Data Breach – Trộm dữ liệu: 81% tổ chức bị sự cố mất dữ liệu. Trong các dữ liệu gởi ra ngoài, 30% là dữ liệu về thẻ tín dụng (credit) và 25% là dữ liệu nhạy cảm của cá nhân *(nguồn: CheckPoint Security Report 2015)*. Một số sự cố gần đây:
  - 14/09/2016: Trang web của Donald Trump vô tình bị rò rỉ dữ liệu cá nhân của các thực tập sinh (http://motherboard.vice.com/read/donald-trump-website-leaked-interns-personal-data)
  - 13/09/2016: Hacker trộm mật khẩu trang EurekAlert!, rò rỉ tin tức cấm vận (http://motherboard.vice.com/read/hacker-steals-passwords-for-science-site-eurekalert-leaks-embargoed-news)
  - 07/09/2016: Trộm dữ liệu của Đại học Alaska làm lộ thông tin của sinh viên (http://www.scmagazine.com/university-of-alaska-breach-may-have-exposed-student-info/article/520975/)
  - 05/09/2016: Người khổng lồ Internet Rambler.ru của Nga bị hack, 98 triệu tài khoản bị trộm (http://www.zdnet.com/article/russian-portal-email-provider-rambler-hacked-98-million-accounts-leaked/)
  - 05/09/2016: Trung tâm Y tế Tư nhân Al Zahra ở UAE bị hack (https://www.databreaches.net/uae-al-zahra-private-medical-centre-hacked/)

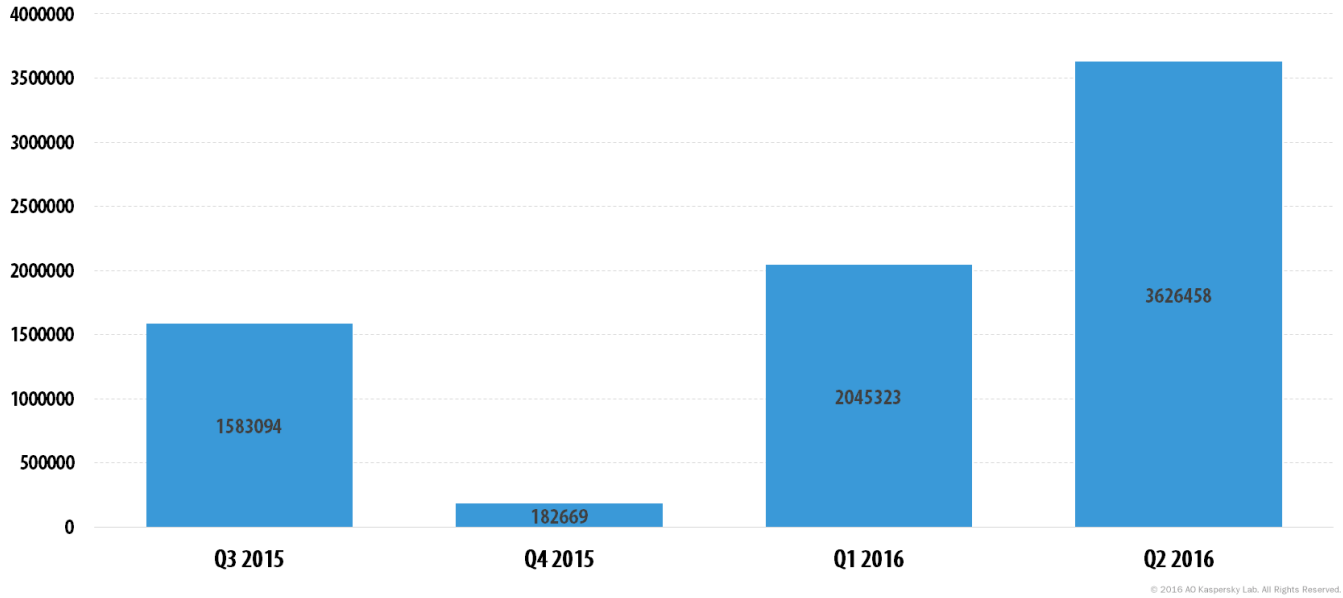
Tình hình ATTT trên thế giới:

+ Các sự cố Data Breach (tiếp):

- 19/09/2015: 324.000 thẻ thanh toán bị trộm và tung lên mạng từ 2 tháng nay (https://nakedsecurity.sophos.com/2016/09/19/324000-payment-cards-breached-cvvs-included-source-still-unknown/)
- 01/09/2016: hacker trộm trên 43 triệu tài khoản của Last.fm từ năm 2012 (http://www.zdnet.com/article/hackers-stole-43-million-last-fm-account-details-in-2012-breach/)
- 01/09/2016: Khách sạn Kimpton thông báo bị trộm dữ liệu (http://krebsonsecurity.com/2016/09/kimpton-hotels-acknowledges-data-breach/)
- 31/08/2016: Hacker trộm 68 triệu tài khoản gồm các địa chỉ email và mật khẩu đã hash của Dropbox (http://arstechnica.com/security/2016/08/dropbox-hackers-stole-email-addresses-hashed-passwords-68m-accounts/)
- 30/08/2016: Khách sạn SilverLand của Việt Nam để lộ thông tin thẻ tín dụng của khách hàng (https://www.databreaches.net/vietnamese-hotel-leaves-customers-credit-card-data-exposed-online/)
- 29/08/2016: 1,7 triệu người dùng Opera được yêu cầu đổi mật khẩu vì bị trộm (http://www.tripwire.com/state-of-security/latest-security-news/1-7m-opera-sync-users-encouraged-to-reset-all-passwords-following-breach/)
- 27/08/2016: Hacker trộm 2,9 triệu thẻ credit là con trai của một luật sư (http://arstechnica.com/security/2016/08/hacker-who-stole-2-9-million-credit-card-numbers-is-russian-lawmakers-son/)

Tình hình ATTT trên thế giới:

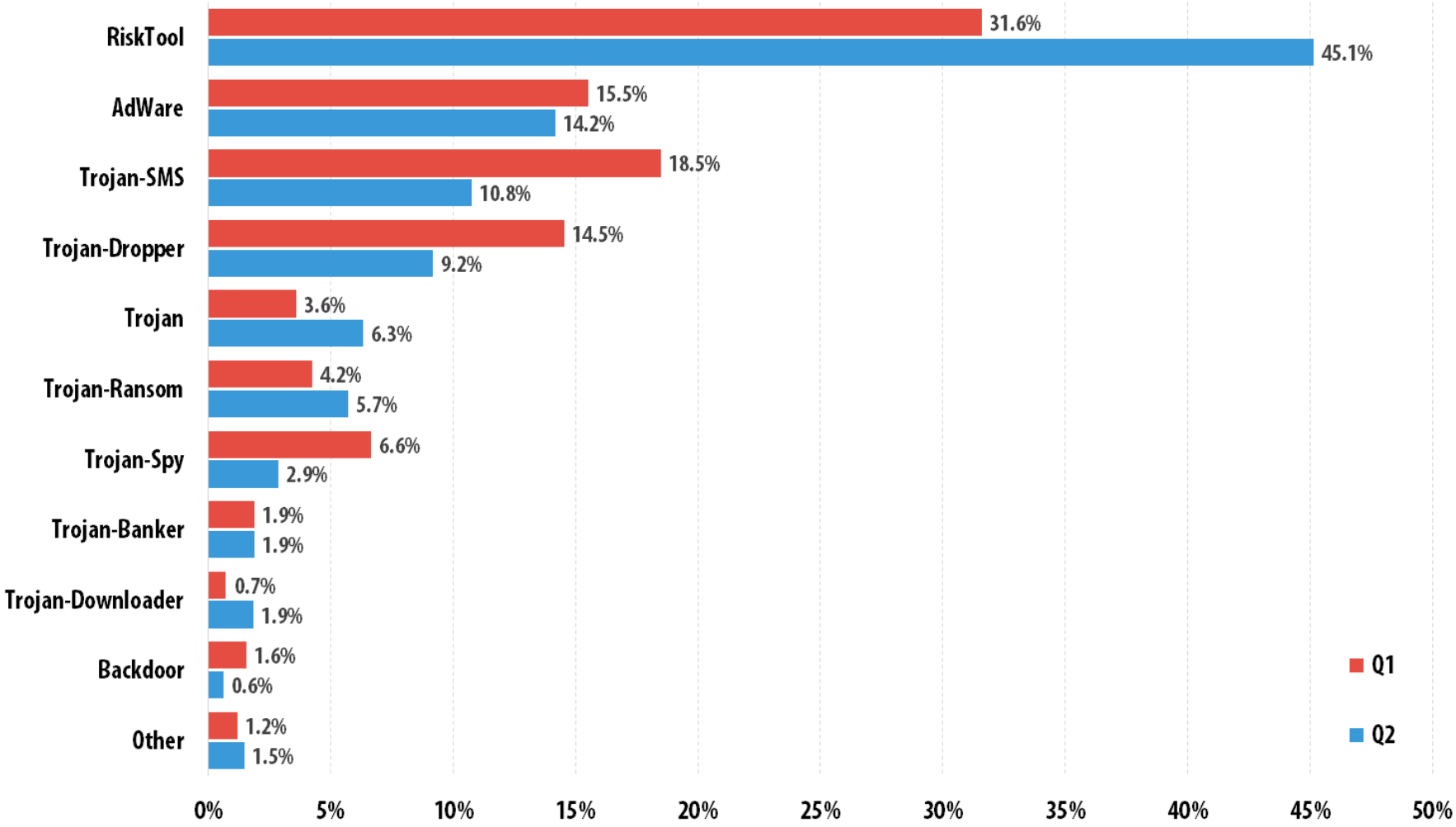
- Các hiểm hoạ trên di động gia tăng:
  + Mã độc viết cho di động
  + Trojan SMS (tấn công tài khoản ngân hàng của nạn nhân) như Trojan-Spy.AndroidOS.SmsThief.ay
  + Banker trojans (Trojan-Banker.AndroidOS.Binha.d
  + Ransomware trojan



Số các ứng dụng cài đặt có mã độc được phát hiện *(nguồn Kaspersky Q2 2016)*

Hiểm hoạ trên di động

Phân bố mã độc di động mới theo loại: *(nguồn Kaspersky Q2 2016)*



Hiểm hoạ trên di động

- 20 mã độc trên di động phổ biến nhất (nguồn: Kaspersky, Q2-2016)

	Name	% of attacked users*
1	DangerousObject.Multi.Generic	80.87
2	Trojan.AndroidOS.Iop.c	11.38
3	Trojan.AndroidOS.Agent.gm	7.71
4	Trojan-Ransom.AndroidOS.Fusob.h	6.59
5	Backdoor.AndroidOS.Ztorg.a	5.79
6	Backdoor.AndroidOS.Ztorg.c	4.84
7	Trojan-Ransom.AndroidOS.Fusob.pac	4.41
8	Trojan.AndroidOS.Iop.t	4.37
9	Trojan-Dropper.AndroidOS.Gorpo.b	4.3
10	Trojan.AndroidOS.Ztorg.a	4.3

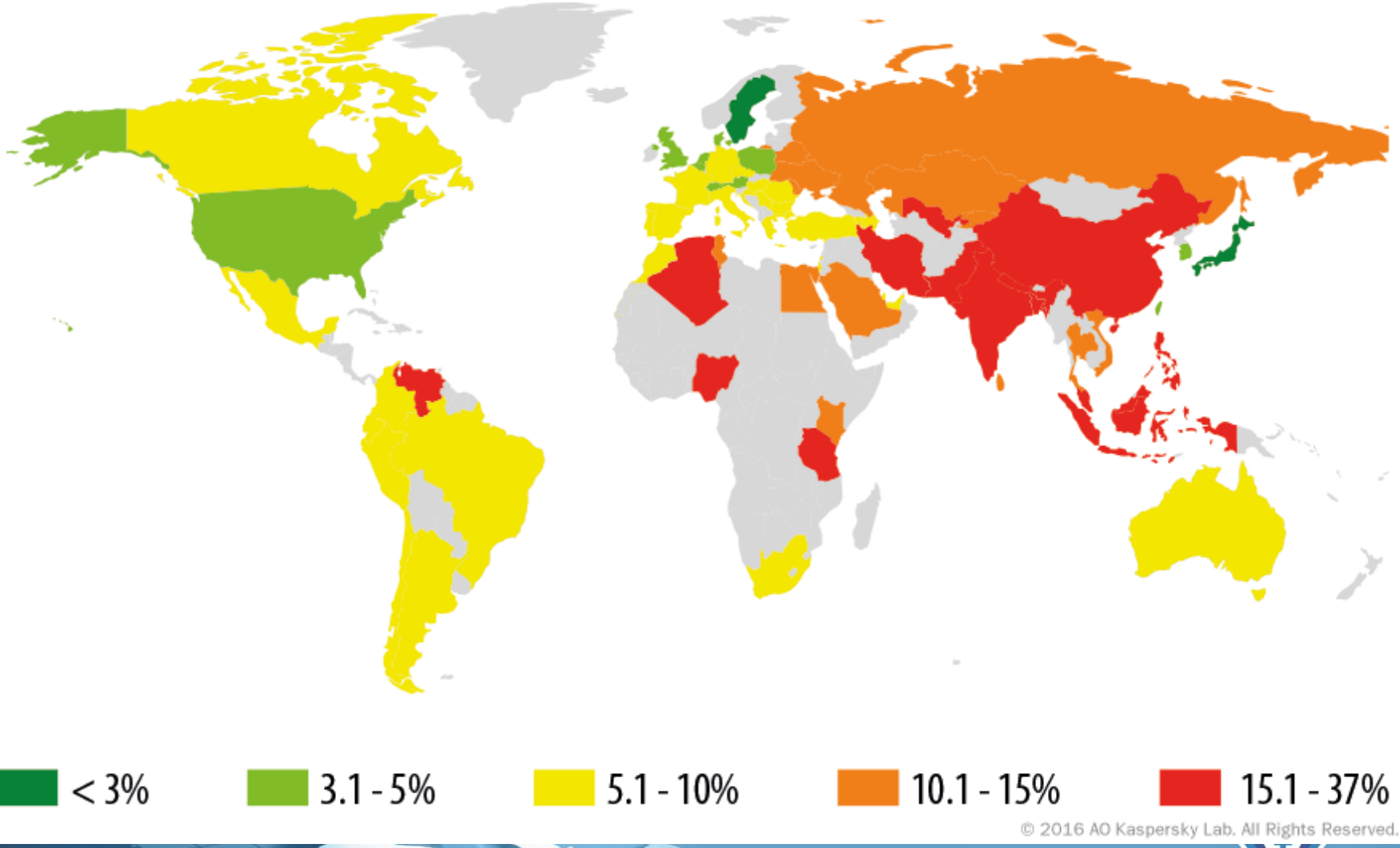
Hiểm hoạ trên di động

- 20 mã độc trên di động phổ biến nhất: *(tiếp)*

	Name	% of attacked users*
11	Trojan.AndroidOS.Ztorg.i	4.25
12	Trojan.AndroidOS.Iop.ag	4.00
13	Trojan-Dropper.AndroidOS.Triada.d	3.10
14	Trojan-Dropper.AndroidOS.Rootnik.f	3.07
15	Trojan.AndroidOS.Hiddad.v	3.03
16	Trojan-Dropper.AndroidOS.Rootnik.h	2.94
17	Trojan.AndroidOS.Iop.o	2.91
18	Trojan.AndroidOS.Rootnik.ab	2.91
19	Trojan.AndroidOS.Triada.e	2.85
20	Trojan-SMS.AndroidOS.Podec.a	2.83

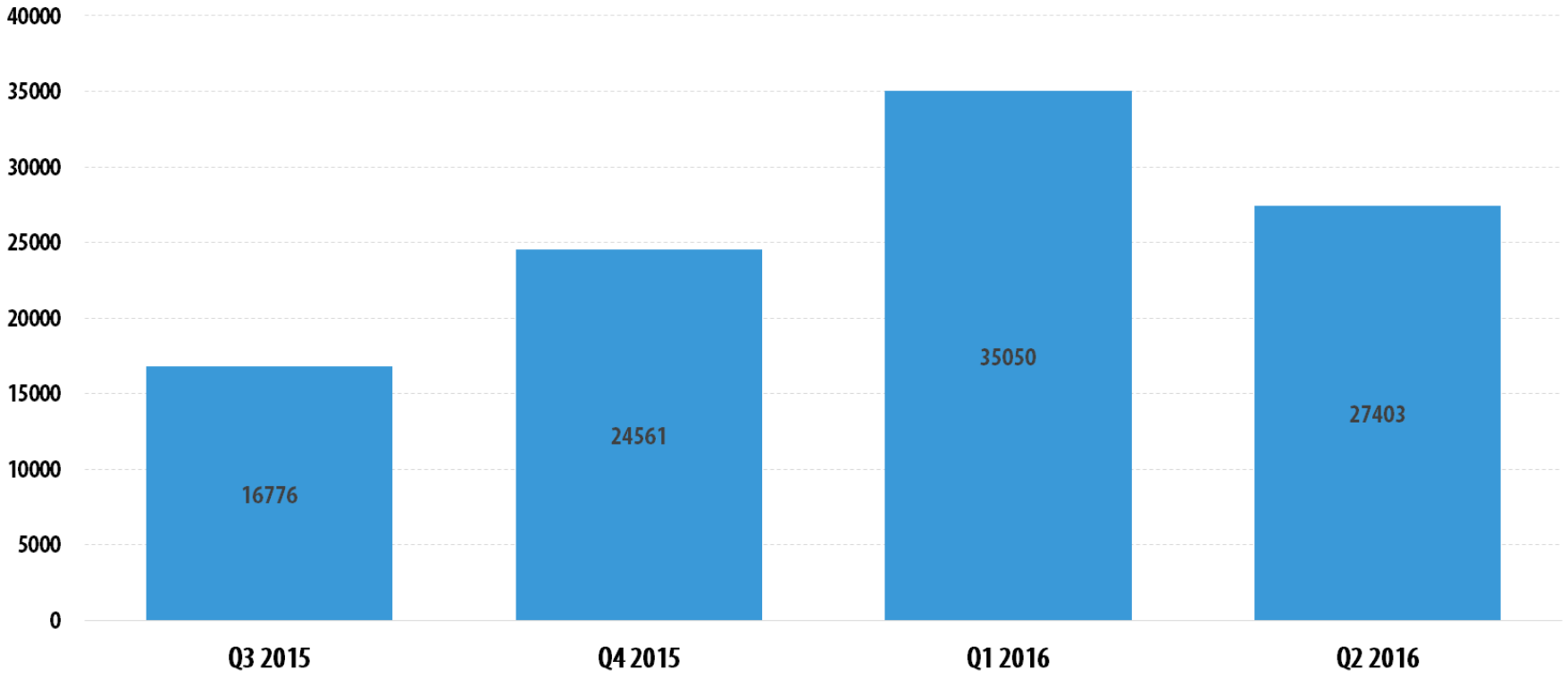
Hiểm hoạ trên di động:

Phân bố lây nhiễm mã độc di động: *(nguồn: Kaspersky, Q2-2016)*



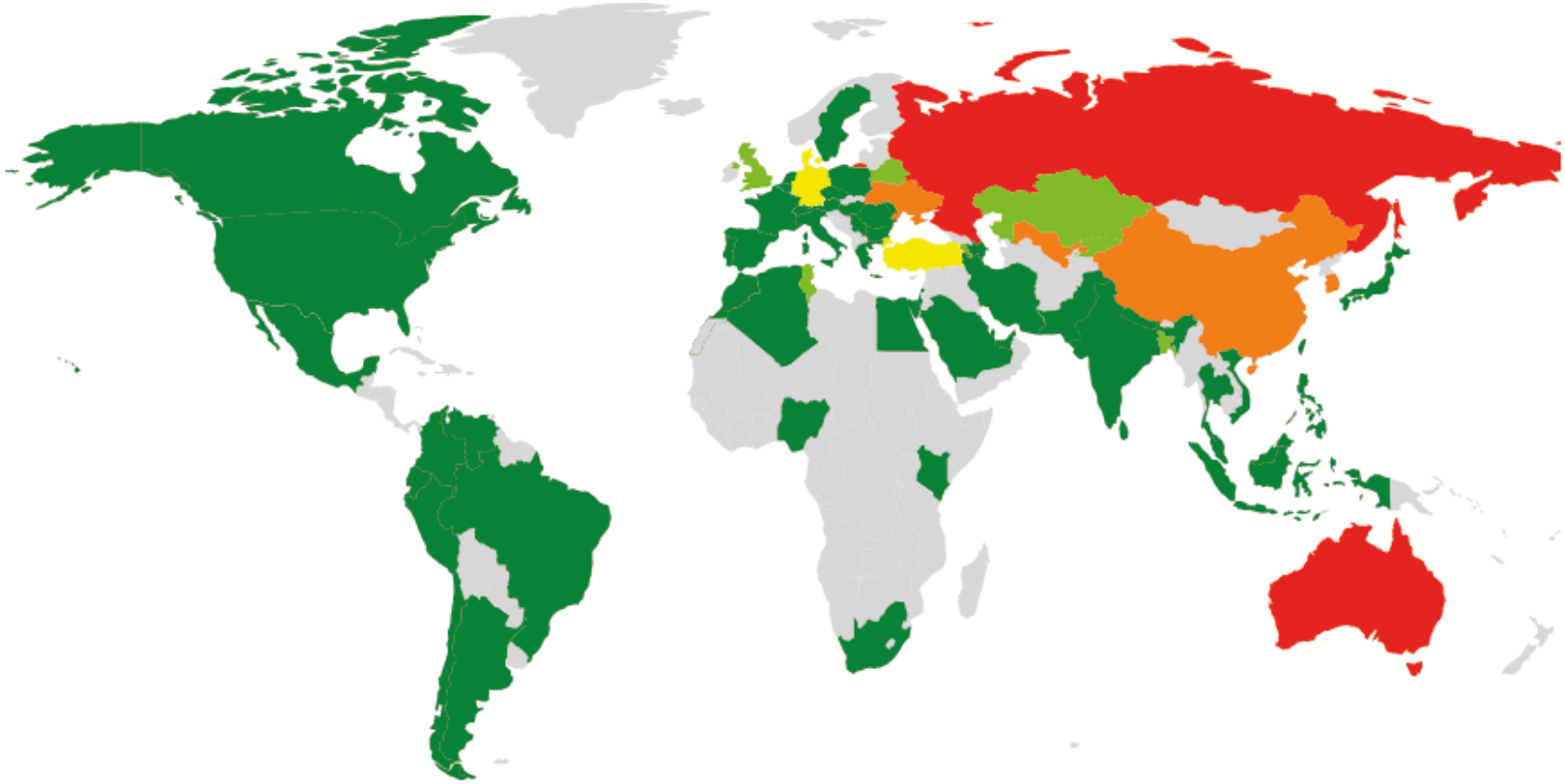
Hiểm hoạ trên di động

Số lượng Trojan mobile banking được phát hiện *(nguồn: Kaspersky)*



Hiểm hoạ trên di động

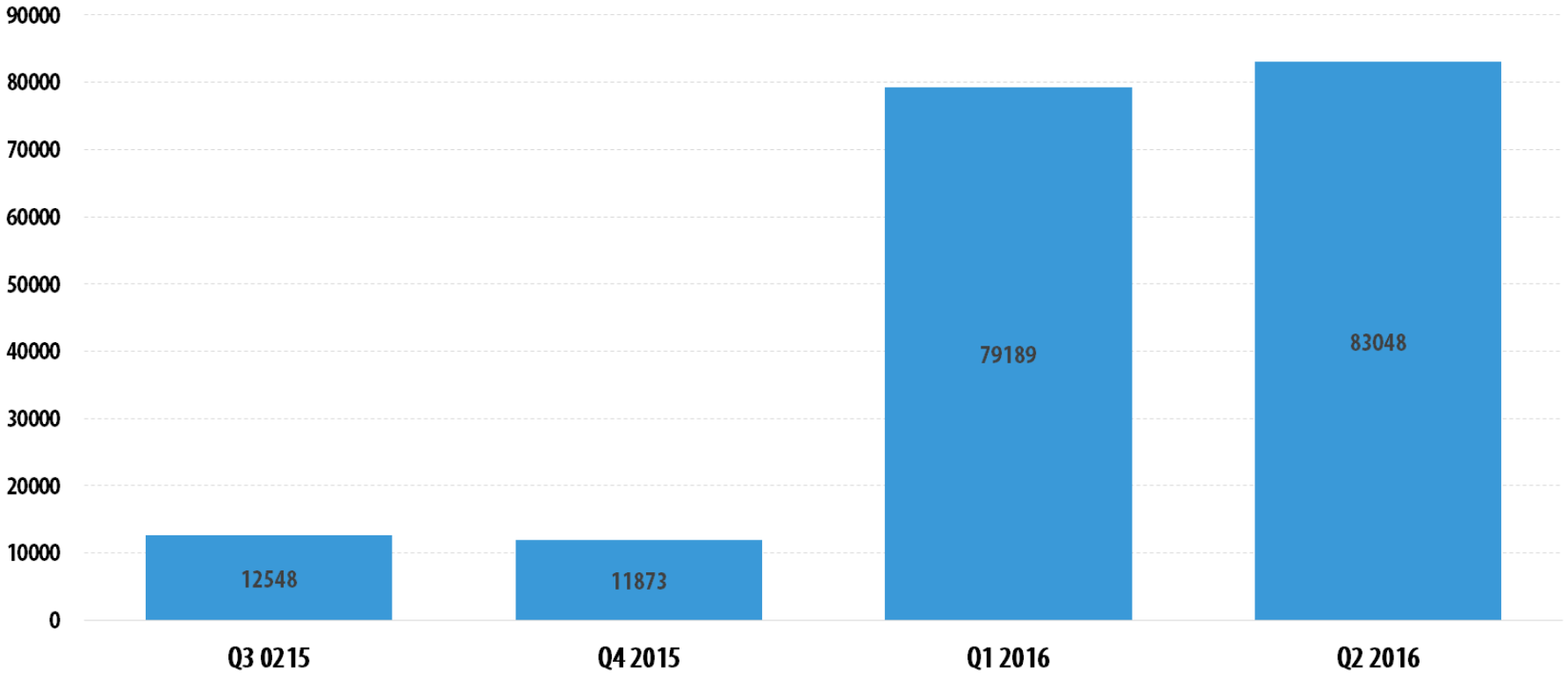
Phân bố số người dùng bị tấn công bởi mobile banking *(nguồn: Kaspersky, Q2-2016)*



Hiểm hoạ trên di động

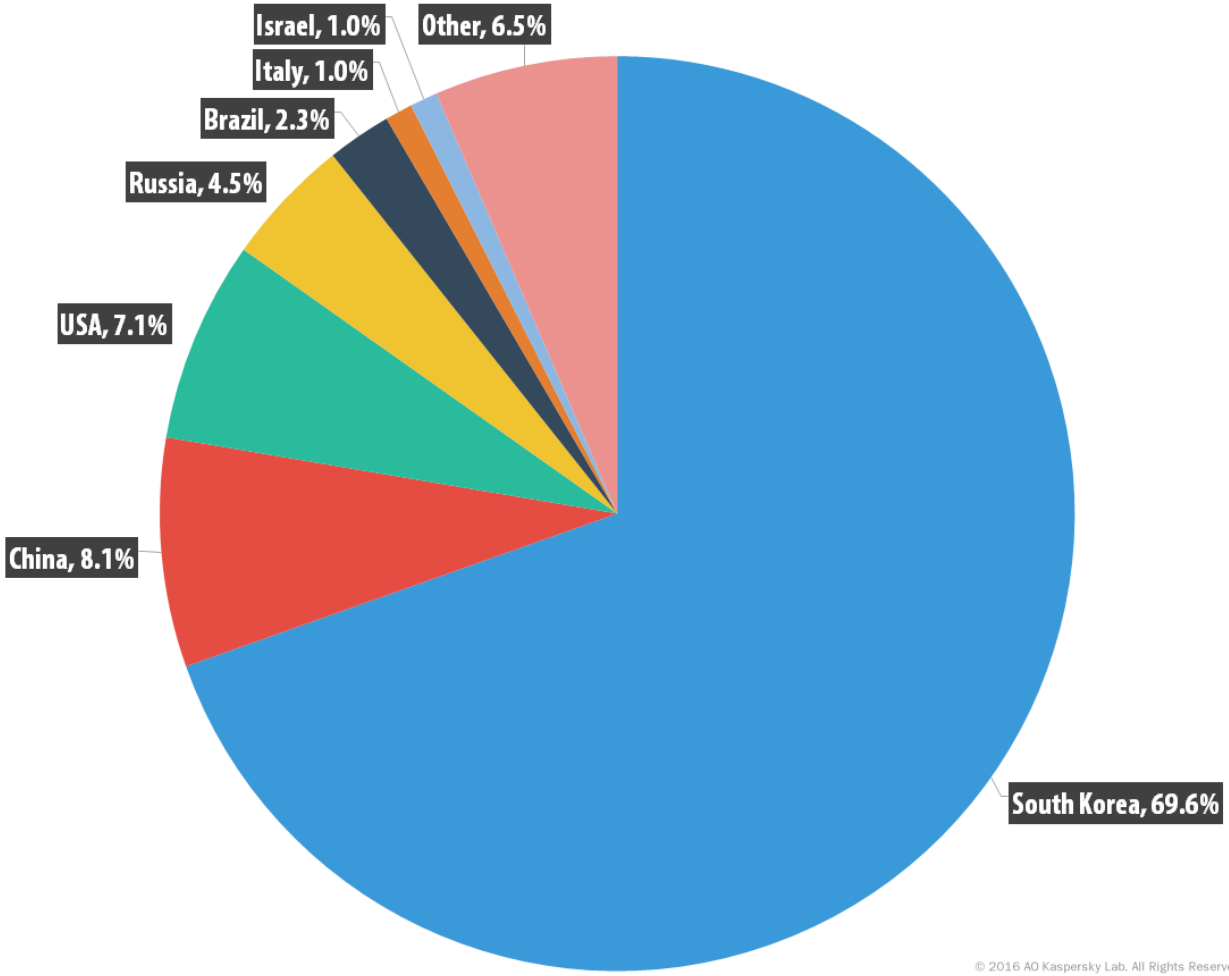
Số lượng phần mềm cài đặt cho di động có trojan-ransomware

(nguồn: Kaspersky, Q2-2016)



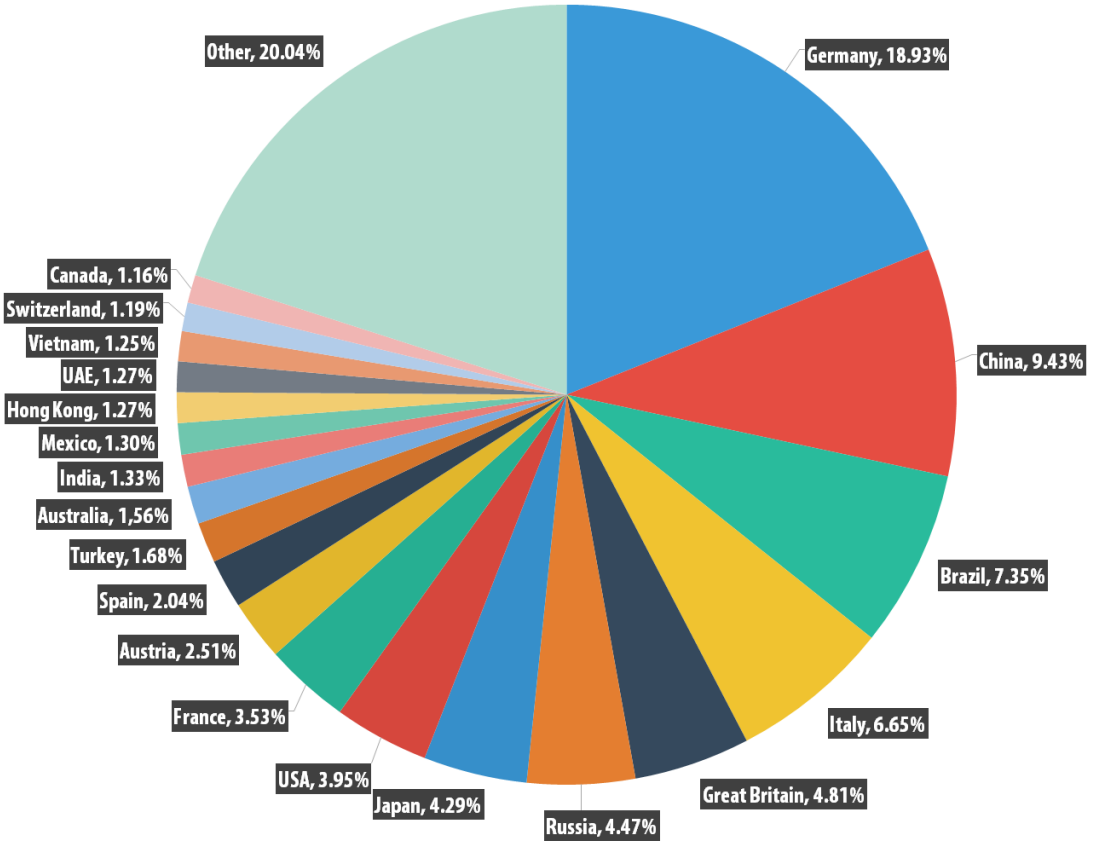
Tình hình ATTT trên thế giới:

- C&C Server & botnet: Hàn Quốc vẫn đứng đầu trong các nước có số lượng máy chủ C&C và sự vươn lên vị trí thứ 2 của Triung Quốc trong thờigian gần đây: *(nguồn: Kaspersky Q22016)*



Tình hình ATTT trên thế giới:

- Tấn công bằng email có đính kèm file/mã độc: vẫn là phương pháp tấn công chủ yếu với các kiểu fake e-mail, phishing email, …



Phân bố các quốc gia bị tấn công bởi email có mã độc

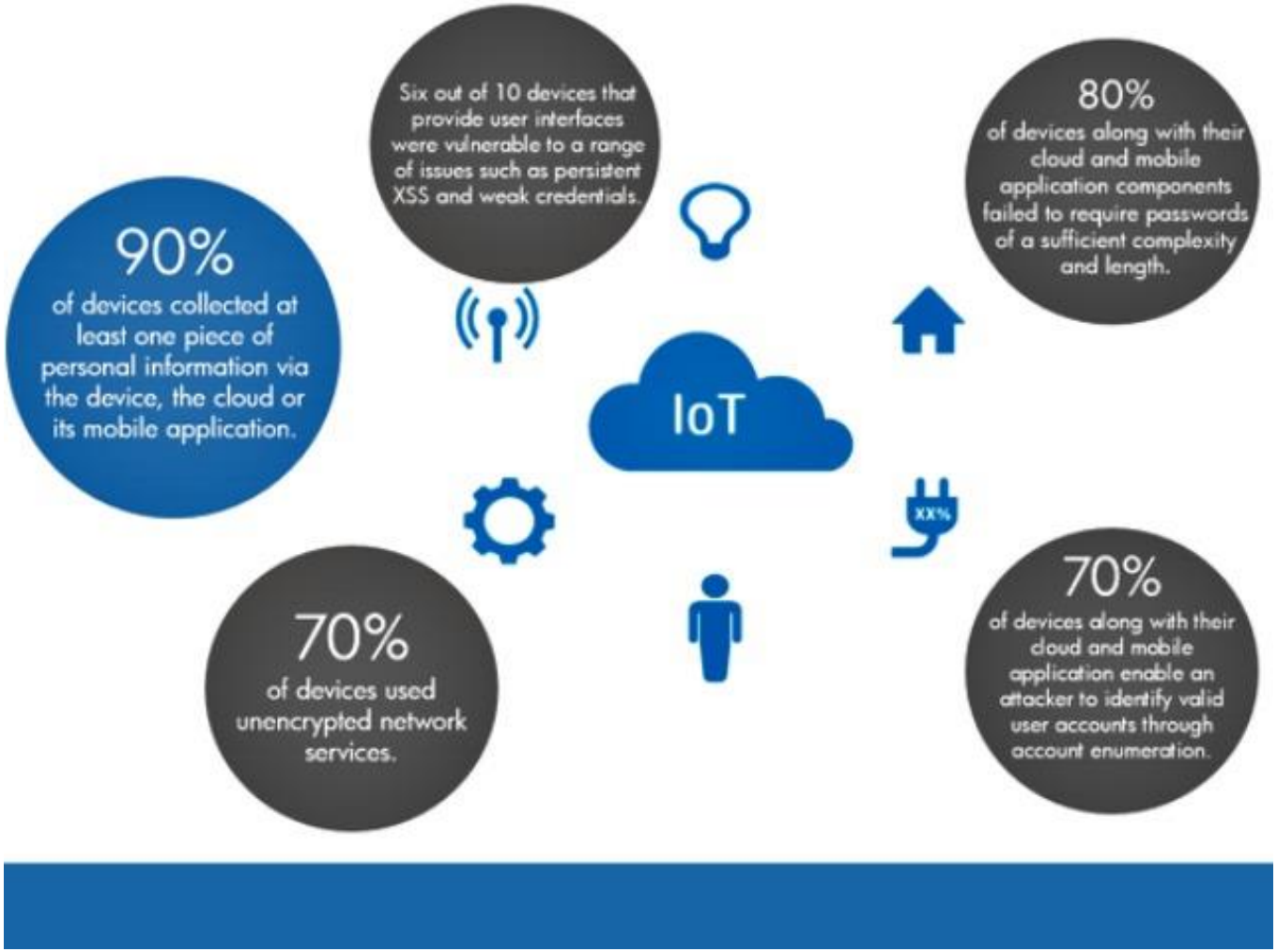
(nguồn Kaspersky, Q1 2016)

Tình hình ATTT trên thế giới:

- Xu hướng IoT – Internet của vạn vật sẽ phát triển nhanh chóng trong thời gian tới và kèm theo đó là khai thác các lỗ hổng trên các thiết bị IoT vốn khó nhận diện và kiểm soát hơn ở mức độ người dùng
  5 mối quan tâm về bảo mật cho IoT:
  - Sự riêng tư: 90% thiết bị thu thập ít nhất một thông tin về người dùng
  - Xác thực không đủ mạnh: 80% không yêu cầu mật khẩu đủ độ phức tạp
  - Mã hoá ở tầng vân chuyển: 70% thiết bị sử dụng các dịch vụ mạng không mã hoá
  - Giao diện web: 60% có vấn đề với giao diện người dùng như cross-site scripting thường trực, quản lý các session nghèo nàn, thông tin mặc định ban đầu yếu
  - Phần mềm không an toàn: 60% không sử dụng mã hoá khi tải các bản cập nhật về

  ➔ Đây là vấn đề lớn của tương lai gần

Tình hình ATTT trên thế giới:



IoT đang là mối nguy lớn về bảo mật, 70% thiết bị IoT thường dùng nhất có lỗ hổng như mật khẩu an toàn, vấn đề về mã hoá, thiếu các phân quyền chi tiết cho người dùng *(nguồn Fortify - HP Enterprise Security Products, http://www.cmswire.com/cms/internet-of-things/top-5-internet-of-things-security-concerns-026043.php)*

Tóm tắt tình hình ATTT trên thế giới:

- Xu hướng dịch vụ tội phạm mạng gia tăng với các kiểu APT/DDoS/ransomware/malware/crime-as-a-service;
- Các tấn công mạng không chỉ trong lĩnh vực kinh tế mà có mục tiêu chính trị của các quốc gia
- Các hãng bảo mật và các chính phủ có sự hợp tác.
  Dự án "No More Ransom" do Cảnh sát Hà Lan, cảnh sát Châu Âu (Europol), Intel Security và Kaspersky Lab tạo công cụ giải mã một số ransomware và hỗ trợ 2.500 người khôi phục lại dữ liệu của họ (17/10/2016, http://www.zdnet.com/article/these-free-ransomware-decryption-tools-have-rescued-data-from-2500-locked-devices/)
- Các thiết bị / ứng dụng không được kiểm soát hết và tiềm ẩn nhiều nguy cơ
- DarkNet / Deep– thế giới ngầm của tội phạm mạng

Tình hình ATTT tại Việt Nam:

- Xuất hiện nhiều cuộc tấn công có chủ đích, điển hình là tấn công vào Vietnam Airlines, tấn công các báo điện tử gần đây;
- Mã độc tống tiền (Ransomware) tiếp tục gia tăng và phát sinh nhiều biến thể mới, hầu hết là mã hoá dữ liệu không thể phá mã. Nhiều phần mềm chống virus không phát hiện được các mã độc dạng này
- Sự cố trộm cắp tiền từ tài khoản của khách hàng Vietcombank và sau đó là điểm yếu trong thiết kế của Smart OTP của Vietcombank
- Sự cố link ẩn trong website của các tổ chức, kể cả các cơ quan Nhà nước

Tình hình ATTT tại Việt Nam:

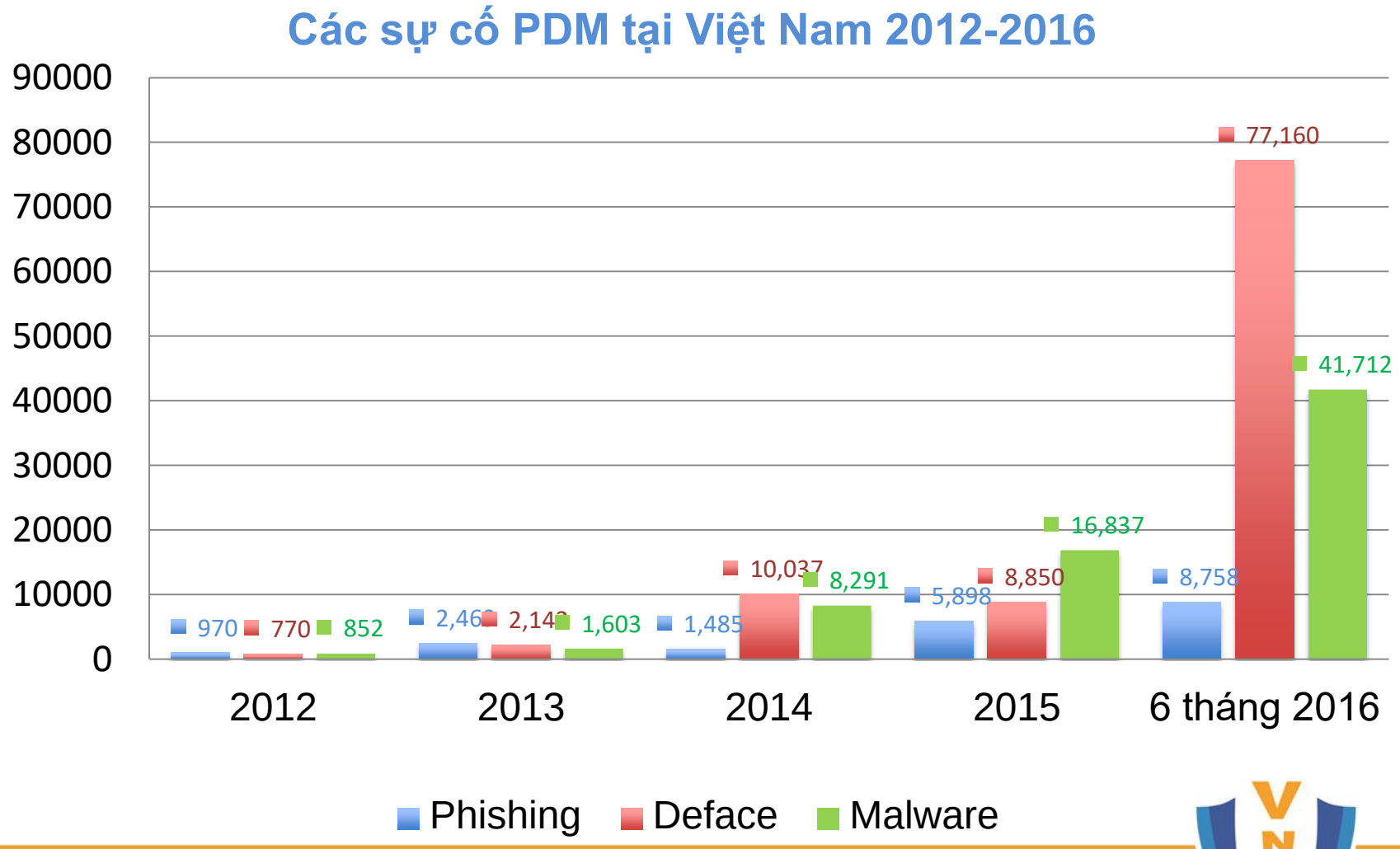
- Tấn công bằng các mạng bot tăng mạnh. Trong năm 2015, 1.451.997 lượt địa chỉ IP bị nhiễm mã độc botnet và bị điều khiển bởi các máy chủ C&C quốc tế
- Xu hướng sử dụng các mạng xã hội để phát tán mã độc, lừa đảo trúng thưởng, mạo danh, đánh cắp thông tin, … đang gia tăng
- Các ứng dụng độc hại trên di động chưa được kiểm soát, mối nguy cho người dùng Việt Nam vốn chưa quan tâm nhiều đến bảo mật
- Thư rác, tin nhắn rác tiếp tục tăng mạnh, chưa có biện pháp khắc phục hoặc hạn chế. Việt Nam là nước có tỷ lệ phát tán thư rác cao.
- Các tấn công vào các tổ chức/ cá nhân tại Việt Nam thường có liên quan đến các vấn đề chính trị;

Tình hình sự cố tại Việt Nam:

Số liệu sự cố ATTT các năm qua và 6 tháng 2016, số liệu của VNCERT:

Loại sự cố	*Năm 2010*	*Năm 2011*	*Năm 2012*	*Năm 2013*	*Năm 2014*	*Năm 2015*	*6 tháng 2016*
Phishing	233	385	970	2,469	1,458	5,898	8,758
Deface	19	340	770	1,603	8,291	8,850	77,160
Malware	8	13	852	2,142	10,037	16,837	41,712
Sự cố khác	11	17		165	8,400	1,451,997	
Tổng	**271**	**755**	**2,592**	**6,379**	**28,186**	**1,483,582**	**127,630**

Tình hình ATTT tại Việt Nam:



Đảm bảo an toàn cho các Hệ thống Công nghệ Thông tin

Đảm bảo an toàn cho các hệ thống CNTT

- Các cơ sở pháp lý đã được quan tâm xây dựng và ban hành trong thời gian qua:
  - Các luật: Luật An toàn thông tin mạng, Luật CNTT, Luật hình sự, …
  - Các quy định về quản lý cung cấp, sử dụng Internet và thông tin mạng, về chống thư rác;
  - Nghị quyết về xây dựng chính phủ điện tử và giám sát an toàn thông tin;
  - Quy định điều phối các hoạt động mạng lưới ứng cứu sự cố mạng
  - …

Đảm bảo an toàn cho các hệ thống CNTT

- Các cơ quan quản lý Nhà nước về An toàn Thông tin

1. Bộ Thông tin và Truyền Thông

- Cục An toàn Thông tin
- Trung tâm Ứng cứu Khẩn cấp Máy tính Việt Nam (VNCERT)
- Các Sở Thông tin và Truyền thông của 63 Tỉnh, Thành phố

2. Bộ Công An:

- Cục An Ninh Mạng
- Cục Phòng chống tội phạm Công nghệ cao C50

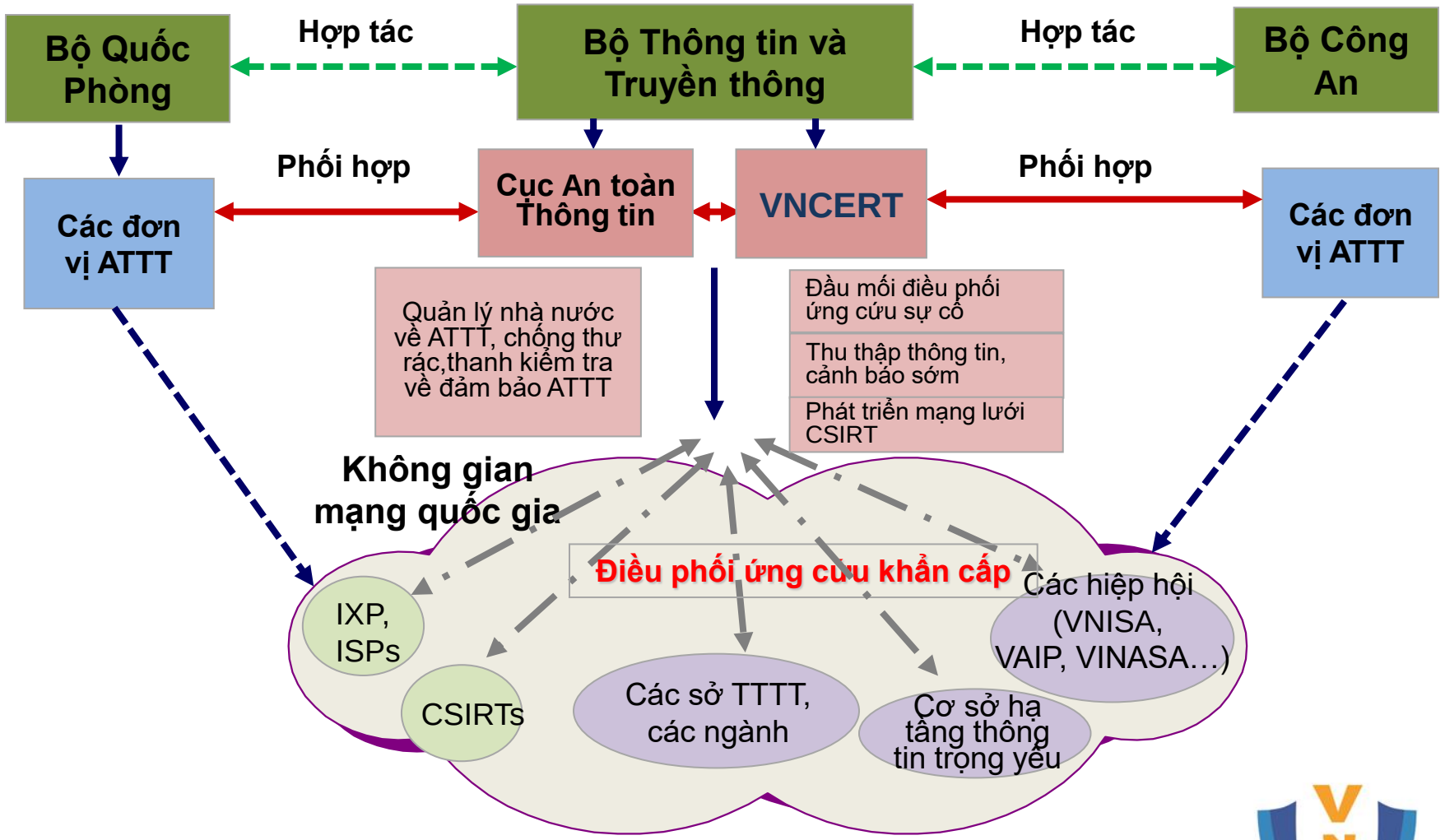
3. Bộ Quốc phòng:

- Cục Công nghệ thông tin – Bộ Tổng Tham mưu

4. Các cơ quan Trung ương, các Bộ - Ngành:

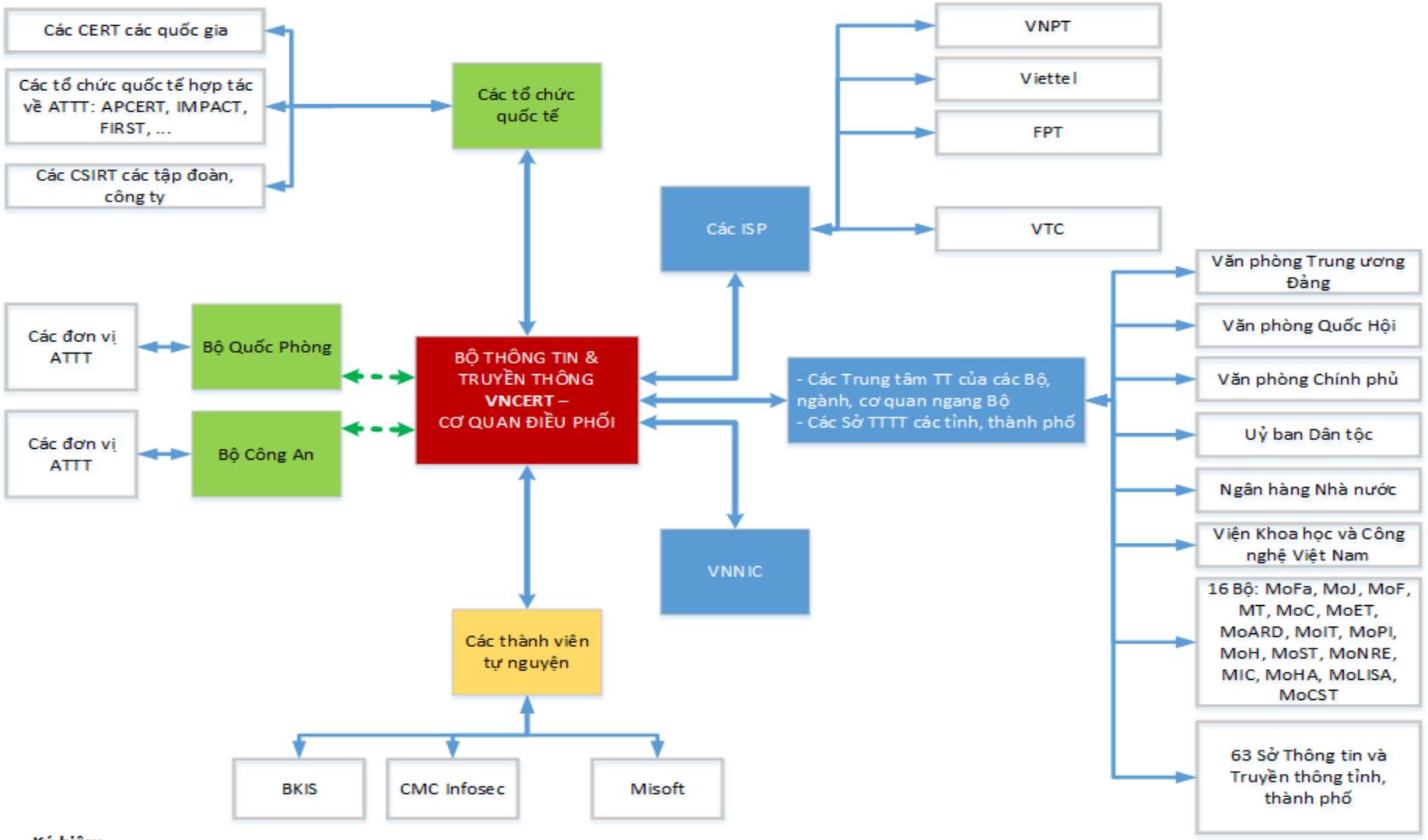
- Các Trung tâm Công nghệ thông tin

Mô hình quản lý nhà nước trong hoạt động ATTT & Điều phối - Ứng cứu

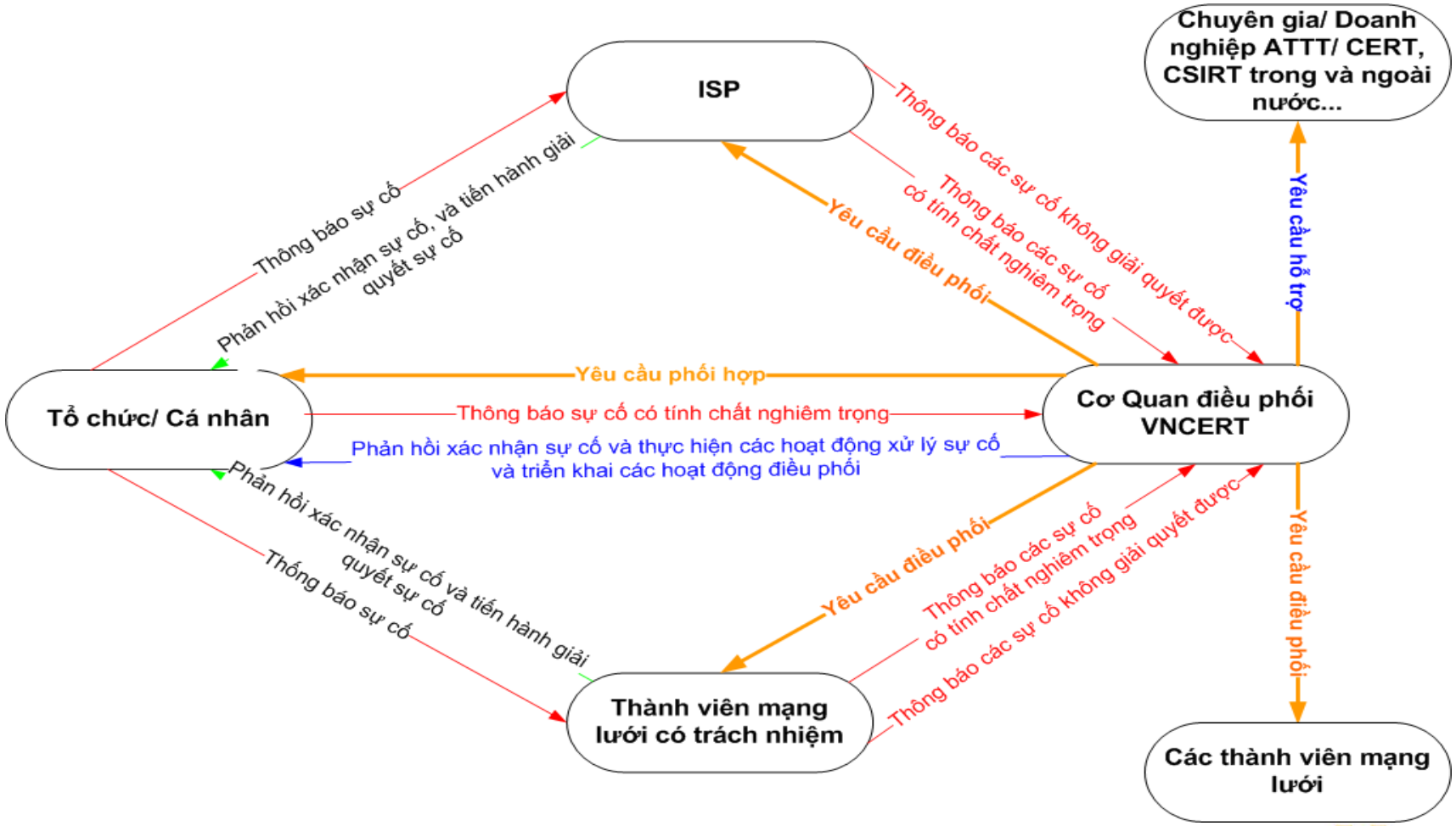


Mạng lưới Điều phối Sự cố ATM quốc gia

(124 thành viên tổ chức, 505 thành viên cá nhân)



Mô hình tiếp nhận và điều phối sự cố ATM



Hoạt động đảm bảo ATTT của VNCERT

- Chuỗi hoạt động đảm bảo ATTT mạng quốc gia :

- Các hoạt động đảm bảo ATTT của VNCERT:
  - Điều phối ứng cứu ứng cứu sự cố, tấn công mạng;
  - Giám sát, phát hiện, cảnh báo về sự cố, lỗ hổng, mã độc, botnet, APT và các tấn công mạng khác;
  - Kiểm tra, rà quét lỗ hổng, mã độc và đánh giá mức độ ATTT cho các hệ thống thông tin;
  - Phân tích, điều tra mã độc và hướng dẫn phòng chống, xử lý;
  - Tổ chức đào tạo, huấn luyện, diễn tập về an toàn thông tin mạng;
  - Tư vấn tổ chức hoạt động các đội ứng cứu sự cố mạng, tư vấn về giải pháp, chiến lược, kế hoạch, dự án bảo đảm ATTT mạng;
  - Hỗ trợ ngăn chặn, hạn chế thư rác, tin nhắn rác;
  - Cung cấp các dịch vụ về an toàn thông tin mạng.

Các hoạt động khác

Hợp tác quốc tế

- Thành viên chính thức của APCERT (Asia Pacific CERT) (từ 2008)
- Hợp tác với các CERT của các nước: thoả thuận hợp tác với JPCERT/CC (2009), KISA (Korea Information Security Acency) (2009), Bộ Viễn thông và Internet Lào (2010); phối hợp chặt chẽ với USCERT, TWCERT, CERT-Brazil, ….
- Phối hợp với các tổ chức KISDI (Korea Information Society Development Institute), Microsoft, Google, … và các hãng chuyên về bảo mật như IBM, HP, Fortinet, …

Các hoạt động khác

Tham dự thường xuyên các Diễn tập quốc tế hàng năm

Chương trình diễn tập	Thời gian	Thành phần tham gia
Diễn tập quốc tế APCERT	Tháng 3	- 20 quốc gia thuộc vùng lãnh thổ AP - VNCERT - Mạng lưới Ứng cứu sự cố quốc gia
Diễn tập quốc tế ASEAN – Nhật Bản	Tháng 5	- 11 quốc gia - VNCERT - Mạng lưới Ứng cứu sự cố quốc gia
Diễn tập quốc tế ACID	Tháng 9	- 10 quốc gia và các nước đối thoại - VNCERT - Mạng lưới Ứng cứu sự cố quốc gia

Các hoạt động khác

- **Kiểm tra, rà quét lỗ hổng, mã độc và đánh giá mức độ ATTT cho các cơ quan Nhà nước**:
  - Năm 2013: Đánh giá AT cho 82 trang Cổng/Trang thông tin điện tử
  - Năm 2014: Đánh giá AT cho 116 trang Cổng/Trang thông tin điện tử
  - Năm 2015: Đánh giá AT cho 116 trang Cổng/Trang thông tin điện tử
  - Năm 2016: Đánh giá AT 83 Cổng/Trang TTĐT (Đánh giá mức chuyên sâu: 30 Cổng/Trang, đánh giá mức cơ bản 53: Cổng/Trang)
- **Phân tích, điều tra mã độc và hướng dẫn phòng chống, xử lý**
- **Đào tạo, huấn luyện, diễn tập về an toàn thông tin mạng**
  + Đề án đào tạo phát triển nguồn nhân lực về ATTT (đề án 99)
  + Tổ chức diễn tập quốc gia hàng năm về ATTT
- **Đánh giá và chứng nhận sản phẩm an toàn thông tin**
- **Hỗ trợ ngăn chặn, hạn chế thư rác, tin nhắn rác**

Giải pháp Đảm bảo an toàn thông tin mạng

- Nâng cao nhận thức về an toàn thông tin cho toàn thể tổ chức, doanh nghiệp:
  - Thay đổi quan điểm của cấp lãnh đạo
  - Tập huấn, đào tạo nâng cao nhận thức an toàn bảo mật thông tin cho toàn bộ nhân viên và các cấp quản trị trong doanh nghiệp, trong tổ chức
  - Thử nghiệm, diễn tập các kiểu tấn công giả vào doanh nghiệp
- Ưu tiên ngân sách (budget) cho các hoạt động về ATTT:
  - Hoạt động đầu tư trang thiết bị, công cụ, dụng cụ, giải pháp
  - Chi phí cho các hoạt động thường xuyên về ATTT: lương cho chuyên gia và đội ngũ làm ATTT, các hoạt động đào tạo – vận hành,
  - Các hoạt động đánh giá, huấn luyện, diễn tập về ATTT
  - …

Giải pháp Đảm bảo an toàn thông tin mạng

- **Nhân sự về ATTT:**
  - Có đội ngũ chuyên về ATTT
  - Tạo điều kiện cho những người làm ATTT tham gia các khoá đào tạo chuyên môn và chuyên sâu, các hội thảo, diễn đàn chuyên môn
  - Thành lập Đội Ứng cứu Sự cố Bảo mật CSIRT (Computer Security Incident Response Team) riêng của doanh nghiệp, tổ chức
  - Có cơ chế thu hút, giữ chân người giỏi về ATTT
- Xây dựng, áp dụng các quy trình, quy định hoặc chuẩn quốc tế về ATTT:
  - Xây dựng hệ thống ISMS (Information Security Management System) và ISO 27001
  - Xây dựng các chính sách về ATTT, các quy trình vận hành – bảo vệ – phát hiện – ngăn ngừa tái diễn – phản ứng khi có sự cố
  - Xây dựng kế hoạch duy trì kinh doanh liên tục BCP (Business Continuity Plan) và khôi phục thảm hoạ (Disaster Recovery Plan)

Đảm bảo an toàn cho các hệ thống CNTT

Các DV Khắc phục Sự cố	Các DV Ngăn ngừa Sự cố	Các DV Tăng cường Chất lượng Bảo mật
• Xử lý Sự cố	• Cung cấp thông tin liên quan đến bảo mật	• Phân tích / đánh giá rủi ro
• Điều phối	• Xử lý thông tin lỗ hổng	• Chuẩn bị và sửa đổi các kế hoạch duy trì kinh doanh, khôi phục thảm hoạ
• Ứng cứu Sự cố tại chỗ	• Phát hiện Sự cố / Tình huống Bảo mật	• Tư vấn bảo mật
• Hỗ trợ ứng cứu sự cố	• Khảo sát xu hướng kỹ thuật	• Các hoạt động giáo dục / đào tạo / hướng dẫn về bảo mật
• Điều tra số máy tính	• Đánh giá / kiểm tra bảo mật	• Đánh giá / Chứng nhận sản phẩm bảo mật
• Xử lý nhân công	• Phát triển công cụ bảo mật	

Đảm bảo an toàn cho các hệ thống CNTT

- Đánh giá lại và bổ sung cho hệ thống bảo mật hiện tại:
  - Tự đánh giá hoặc mời các bên thứ 3 đánh giá khả năng bảo mật của hệ thống hiện tại
  - Tư duy mới: bảo mật / an toàn cho cả tiến trình thay vì chỉ đầu tư vào thiết bị / giải pháp công nghệ
  - Lưu ý các xu hướng tấn công hiện nay để tổ chức bảo vệ phù hợp:
    + xu hướng tấn công bằng các mã độc mới mà các phần mềm chống virus chưa nhận diện được: phát hiện mã độc dựa trên đặc điểm nhận dạng (signature) và hành vi (behaviour);
    + xu hướng tấn công bằng cách khai thác các lỗ hổng bảo mật: cập nhật các bản vá lỗi, giải pháp cảnh báo các lỗ hổng bảo mật mới công bố;
    + tấn công APT, tấn công qua người dùng cuối và các thiết bị BYOD, IoT, …
    ➔ các hệ thống bảo vệ đa chiều

Đảm bảo an toàn cho các hệ thống CNTT

- Đánh giá lại và bổ sung cho hệ thống bảo mật hiện tại: *(tiếp)*
  - Triển khai hoặc thuê các giải pháp giám sát bảo mật & cảnh báo thường xuyên, liên tục các thông tin về an toàn để ứng phó nhanh với các dấu hiệu của sự cố
  - Triển khai các hệ thống thu thập / phân tích và quản lý các log
  - Sử dụng các thiết bị trong whitelist và giám sát chặt chẽ việc đấu nối các thiết bị mới vào hệ thống, kể các các thiết bị di động
  - Có giải pháp bảo vệ dữ liệu chống rò rỉ/trộm cắp dữ liệu DLP
  - Đánh giá & hợp chuẩn các thiết bị bảo mật đang sử dụng, các thiết bị dự kiến sẽ đầu tư mới khi có quy định triển khai của CQNN.
  - Sử dụng hệ thống mail mã hoá và xác thực, khuyến nghị dùng PGP – miễn phí hoặc chữ ký số để xác nhận người gởi và bảo vệ nội dung, hạn chế nhận các thư không rõ nguồn gốc có kèm mã độc

Đảm bảo an toàn cho các hệ thống CNTT

- Phối hợp với các tổ chức bên ngoài để nâng cao năng lực và sự hỗ trợ:
  - Phối hợp với VNCERT khi có sự cố và để nhận sự hỗ trợ, điều phối khi gặp sự cố lớn mà không tự giải quyết được
  - Tham gia mạng lưới điều phối ứng cứu sự cố quốc gia như là thành viên tự nguyện
  - Tham gia các hoạt động chuyên môn về ATTT: các diễn tập ATTT quốc tế, quốc gia, các diễn đàn chuyên môn, …
  - Tham gia các hội nghề nghiệp về ATTT và trao đổi, chia sẻ thông tin về an toàn, nhất là thông tin các sự cố để có biện pháp và chủ động phòng tránh
  - Hợp tác với các đơn vị chuyên về an toàn thông tin bên ngoài để thực hiện các chức năng về ATTT mà công ty chưa tự thực hiện được: giám sát an toàn, phân tích các tập tin đáng ngờ, đào tạo nội bộ

Giới thiệu VNCERT

Giới thiệu VNCERT

- Trung tâm Ứng cứu Khẩn cấp Máy tính Việt nam – VNCERT (**V**iet**N**am **C**omputer **E**mergency **R**esponse **T**eam) được thành lập theo Quyết định số 339/2005/QĐ-TTg của Thủ tướng chính phủ ngày 20 tháng 12 năm 2005.
- Quyết định 1778/QĐ-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông ngày 26 tháng 10 năm 2015 quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam.
- **Chức năng chính:**
  - Giám sát an toàn thông tin đối với hệ thống, dịch vụ công nghệ thông tin, đặc biệt là Chính phủ điện tử;
  - Cảnh báo các vấn đề về an toàn mạng;
  - Điều phối các hoạt động ứng cứu sự cố;
  - Thúc đẩy hình thành các tổ chức CERT trong nước và là đầu mối hợp tác với các tổ chức CERT nước ngoài.

Giới thiệu VNCERT

MIC

VNCERT

- Phòng Hành chính Tổng hợp
- Phòng Kế hoạch Tài chính
- Phòng Điều phối và Ứng cứu an toàn mạng
- Phòng Kỹ thuật Hệ thống
- Phòng Nghiên cứu và Phát triển
- Phòng Tư vấn Đào tạo
- Chi nhánh Đà Nẵng
- Chi nhánh TP. Hồ Chi Minh

Giới thiệu VNCERT

Các hoạt động chính của VNCERT trong thời gian qua:

- Xây dựng văn bản QPPL về an toàn thông tin (ATTT)
- Cảnh báo tấn công và sự cố an toàn mạng
- Điều phối ứng cứu – xử lý sự cố an toàn mạng
- Giám sát an toàn mạng
- Đầu mối mạng ứng cứu sự cố (CSIRT) quốc gia
- Thúc đẩy và hỗ trợ thành lập các nhóm ứng cứu các tỉnh, địa phương
- CERT Việt Nam, làm việc và hợp các với các tổ chức CERT của các nước và hợp tác quốc tế trong lĩnh vực an toàn thông tin
- Kiểm tra, đánh giá an toàn mạng và hệ thống thông tin
- Quản lý, phòng và chống tin nhắn rác
- Xây dựng các tiêu chuẩn kỹ thuật về an toàn thông tin

Nguyễn Hữu Nguyên
Phụ trách Chi nhánh TP. HCM – VNCERT
Bộ Thông tin và Truyền thông
Email: nhnguyen@mic.gov.vn /
nhnguyen@vncert.vn