Bộ Thông tin và Truyền thông

Trung tâm VNCERT

TĂNG CƯỜNG GIÁM SÁT AN TOÀN MẠNG TRONG PHÁT TRIỂN CHÍNH PHỦ ĐIỆN TỬ

Trình bày: Vũ Quốc Khánh

TP.HCM, 23-07-2015

Bài toán giám sát an toàn mạng (GSATM) và cảnh báo sớm

- Sự cố ATTT bao gồm cả các nguy cơ xác thực có thể xảy ra bất kỳ thời điểm nào.
- Bài toán GSATM = giám sát phát hiện và cảnh báo sự cố ATTT trên mạng, là các khâu đầu tiên trong quá trình đối phó với các nguy cơ mất an toàn thông tin trên mạng

- Các vấn đề lớn liên quan đến: Phát hiện sự cố, Báo cáo sự cố, Phát hiện các nguy cơ tinh vi (APT), Cung cấp thông tin xác thực chuẩn hóa.
- Giải pháp: Hệ thống giám sát an toàn mạng (HT GSATM).

Giám sát ATM là gì?

Giám sát ATM là gì?

- **GSATM =** hoạt động **kiểm soát, phân tích** các dấu hiệu tấn công mạng, các sự kiện ATTT nhằm phát hiện sớm các nguy cơ và sự cố đối với các hệ thống thông tin trên mạng.
- **GSATM** không phân tích **nội dung ngữ nghĩa** mà chỉ phân tích **nội dung kỹ thuật** luồng thông tin trong mạng.

Cơ sở pháp lý:

- **Nghị định 72/2013/NĐ-CP:** Điều 41 đặt nền tảng pháp lý cho dịch vụ GSATM
- **Quy hoạch Phát triển ATTT số quốc gia đến 2020** phê duyệt tại QĐ 63/QĐ-TTg ngày 13/01/2010 chỉ rõ nhiệm vụ theo dõi, phát hiện và cảnh báo sớm sự cố và nhiệm vụ đào tạo đội ngũ chuyên gia thực hiện việc này.
- **Dự thảo Luật An toàn thông tin** đang trình Quốc hội.
- **Dự thảo Thông tư** về giám sát an toàn mạng, hướng dẫn cho Nghị định 72/2013/NĐ-CP.
- **ISO/IEC 27002:2005**

Giám sát ATM để làm gì?

Mục đích cần đạt được:

- **Nhận biết sớm:**
  - **nguy cơ bị do thám, có hoạt động lạ, mã độc,**
  - **các quy trình, cơ chế tấn công mới (như APT),**
  - **khởi đầu cuộc tấn công và cường độ tấn công.**
- **Cảnh báo sớm:**
  - **các hoạt động tấn công ngầm,**
  - **nguy cơ và dấu hiệu tấn công.**

Khả năng hiện thực:

- **Công nghệ hiện đại, mức tự động hóa cao**
- **Có khả năng tích hợp, kết nối mở**
- **Xu hướng chuẩn hóa quốc tế về chia sẻ thông tin**

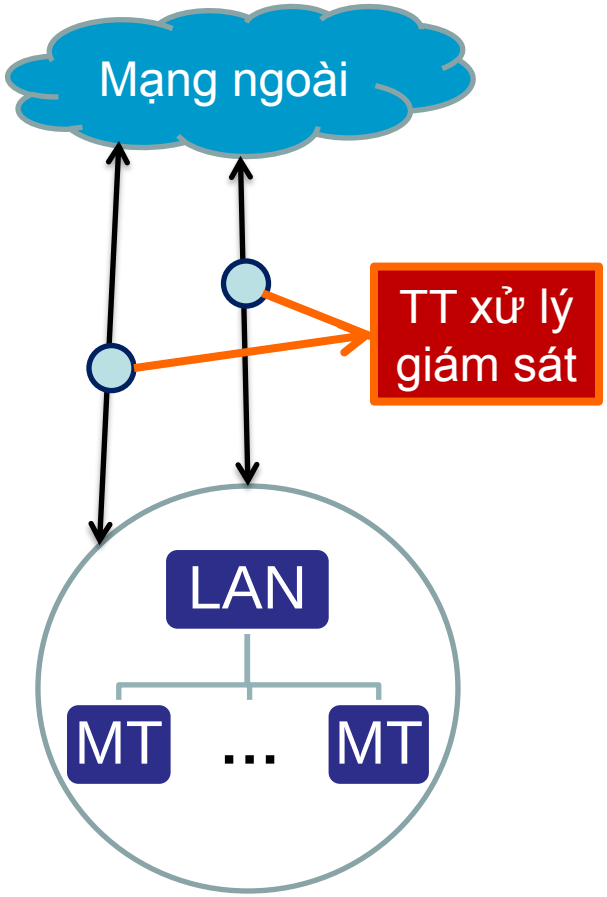
Khả năng giám sát ATM?

- **Giám sát các đối tượng:**
  - **Luồng tin**
    - **lưu lượng**
    - **nguồn, đích**
  - **Dịch vụ**
    - **cổng dịch vụ**
    - **giao thức**
  - **Hệ thống**
    - **CSDL, xử lý văn bản, QLĐH,**
    - **Thư điện tử,**
    - **Trang tin điện tử,**
    - **…**

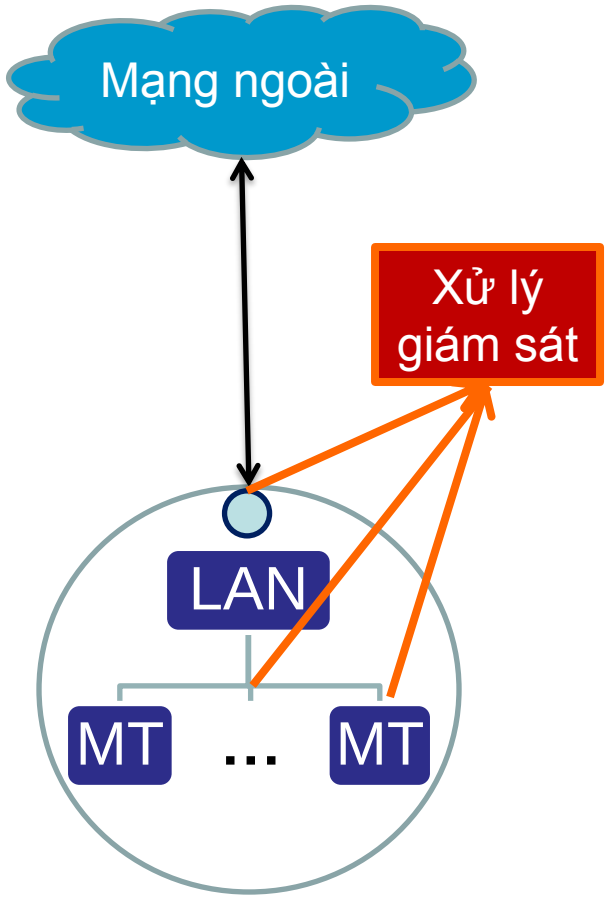
Giám sát như thế nào?

Giám sát một mục tiêu (hệ thống nhỏ)

Giám sát vòng ngoài



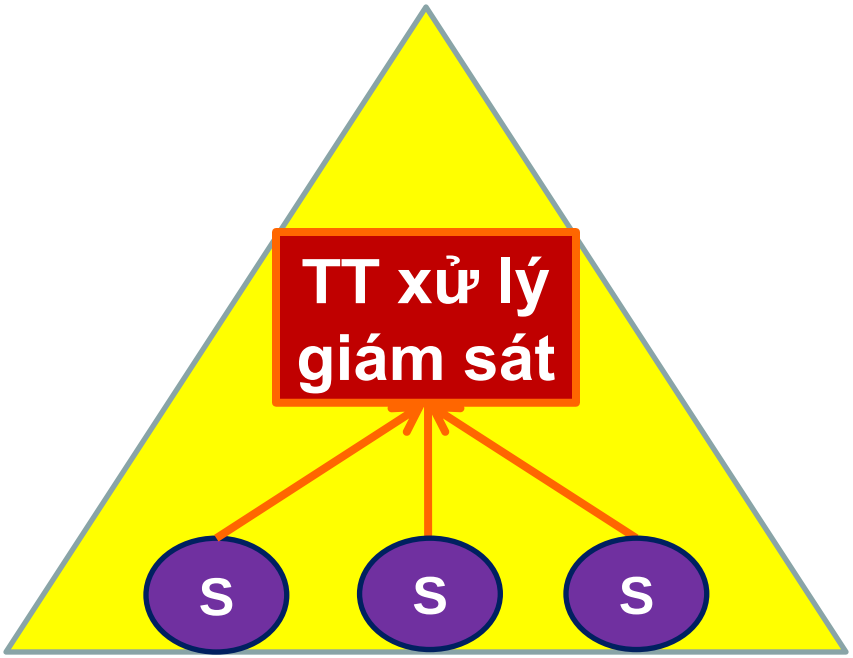
Giám sát trong HT



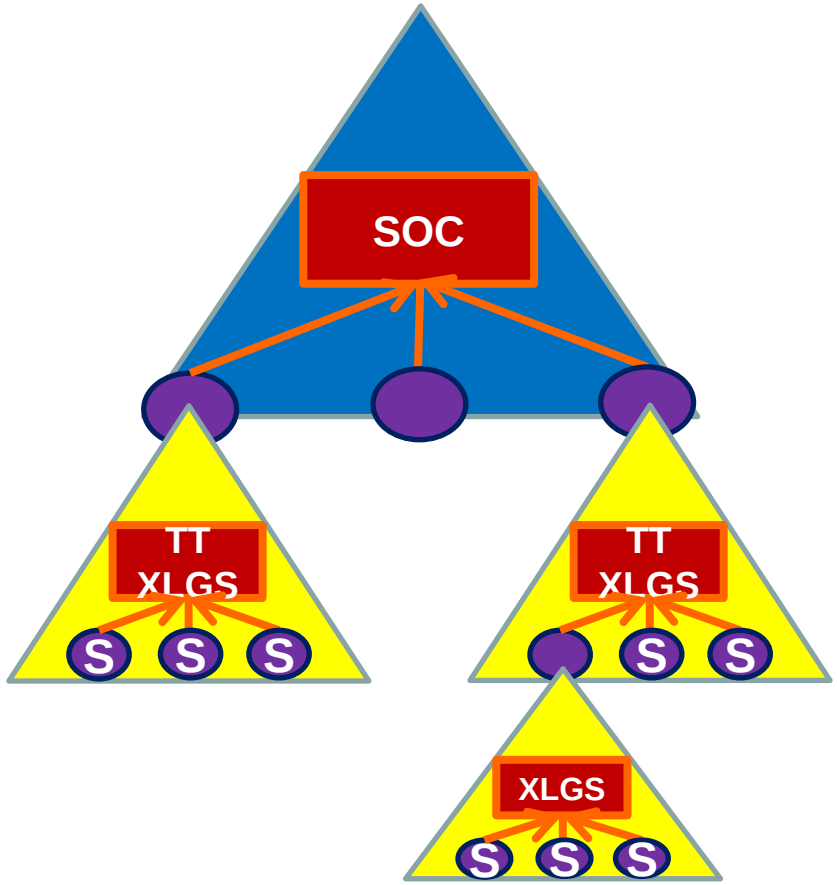
Giám sát như thế nào?

Giám sát nhiều mục tiêu (hệ thống lớn)

Xử lý một cấp



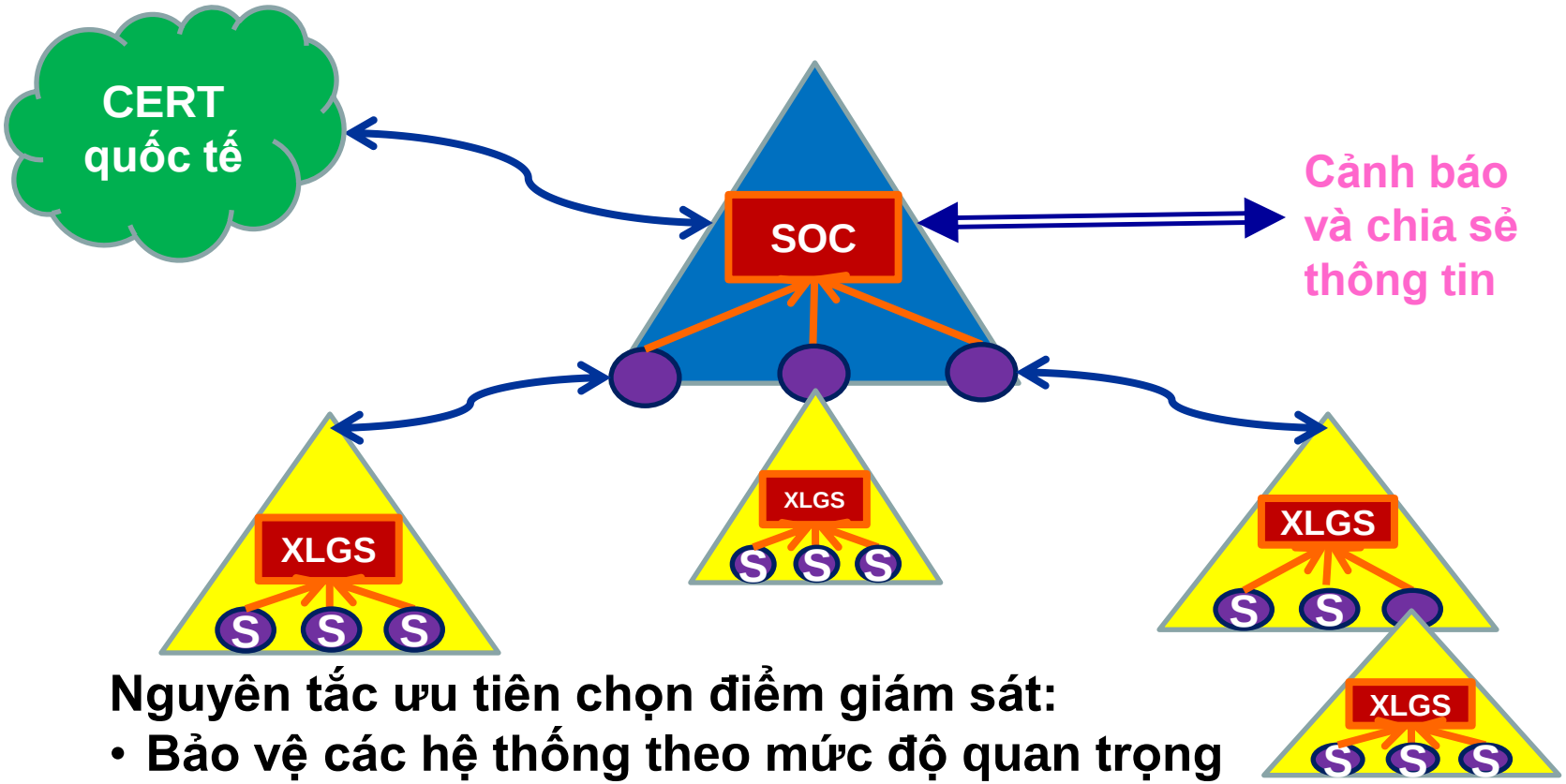
Xử lý đa cấp



Giám sát như thế nào?

Giám sát hệ thống mạng quốc gia

Hệ thống lớn, mở, phân tán, đa cấp, kết nối quốc tế



Nguyên tắc ưu tiên chọn điểm giám sát:

- **Bảo vệ các hệ thống theo mức độ quan trọng**
  - HT trọng yếu quốc gia, HT an ninh quốc gia
  - HT ảnh hưởng đến số đông, HT có giá trị kinh tế cao
- **Bảo vệ các điểm xung yếu trong hệ thống**

Công nghệ giám sát ATM?

1. **Thu thập sự kiện**
2. **Xử lý chuẩn hóa**
3. **Đánh giá độ rủi ro**
4. **Xử lý tương quan**
5. **Xác định sự cố**
6. **Phân tích sự cố**
7. **Thông tin, cảnh báo**

***Quan điểm hiện đại*: Một hệ thống phát hiện sự cố tốt là hệ thống cho phép **thu thập thông tin tự động,** hoạt động **phân tán** có chủ ý, **sử dụng tốt kết quả phát hiện của bên thứ ba** và **hỗ trợ chia sẻ thông tin dễ dàng**.**

- **Đảm bảo khả năng tương thích** cao nhất trên toàn quốc**.**
- **Cần có hệ thống hỗ trợ tiếp nhận các nguồn tin chia sẻ từ khắp thế giới, hệ thống hóa và cung cấp thông tin sự cố** (kiểu như Abuse Helper).
- **Báo cáo phải chuẩn hóa và hỗ trợ xử lý tự động (**Các chuẩn mô tả và trao đổi thông tin: chuẩn truyền thống **IODEF và IDMEF,** chuẩn mới được khuyến cáo **STIX và TAXII,** ngôn ngữ **CybOX,** khung **OpenIOC)**

CPĐT cần được giám sát ATM?

- **Hạ tầng CNTT cho CPĐT là HTTYQG,**
- **Lõi thông tin của Chính phủ là thông tin cần bảo mật cao,**
- **Dịch vụ công CPĐT phục vụ số đông**
- **Xã hội thông minh, Thành phố thông minh gắn liền với Chính quyền điện tử. Mạng máy tính là hệ thống thần kinh của CQĐT. Vai trò của ATM là cực kỳ quan trọng.**

⇨ ***Nhu cầu GSATM phục vụ CPĐT là tất yếu khách quan*.**

Ai thực hiện giám sát ATM?

- **Cơ quan/đơn vị chủ quản** (là người quản lý mạng) chịu trách nhiệm tổ chức GS mạng của mình.
- **Các cơ quan quản lý chuyên trách về đảm bảo ATTT mạng** chịu trách nhiệm hỗ trợ cung cấp dịch vụ GSATM và tổng hợp, cảnh báo thông tin trong ngành, địa bàn của mình, báo cáo lên trên trong mạng lưới điều phối quốc gia.
- **Các tổ chức và doanh nghiệp** hoạt động cung cấp dịch vụ GSATM.

Đảm bảo giám sát ATM?

- ***CQ chủ quản mạng/HT thông tin*:** phải chủ trì tổ chức GSATM, cho phép và hỗ trợ sử dụng dịch vụ GSATM.
- ***Các nhà mạng, đơn vị cung cấp hạ tầng mạng*:** đóng vai trò đặc biệt vừa là chủ quản mạng, vừa là người cung cấp dịch vụ mạng nên có trách nhiệm hỗ trợ khách hàng và hỗ trợ CQ/ĐV chuyên trách để thực hiện GSATM.
- ***CQ/TC cung cấp dịch vụ GSATM*:** triển khai hệ thống GS gồm các sensors và SOC, tương thích và chia sẻ thông tin với CQĐP QG (VNCERT).
- ***VNCERT*:** triển khai SOC QG và HT GSATM QG, tổng hợp và chia sẻ thông tin cảnh báo trên toàn quốc, tư vấn và hướng dẫn đảm bảo tính tương thích.

Hành lang pháp lý đang tiếp tục được khẩn trương hoàn thiện

Đầu tư giám sát ATM?

Bao gồm:

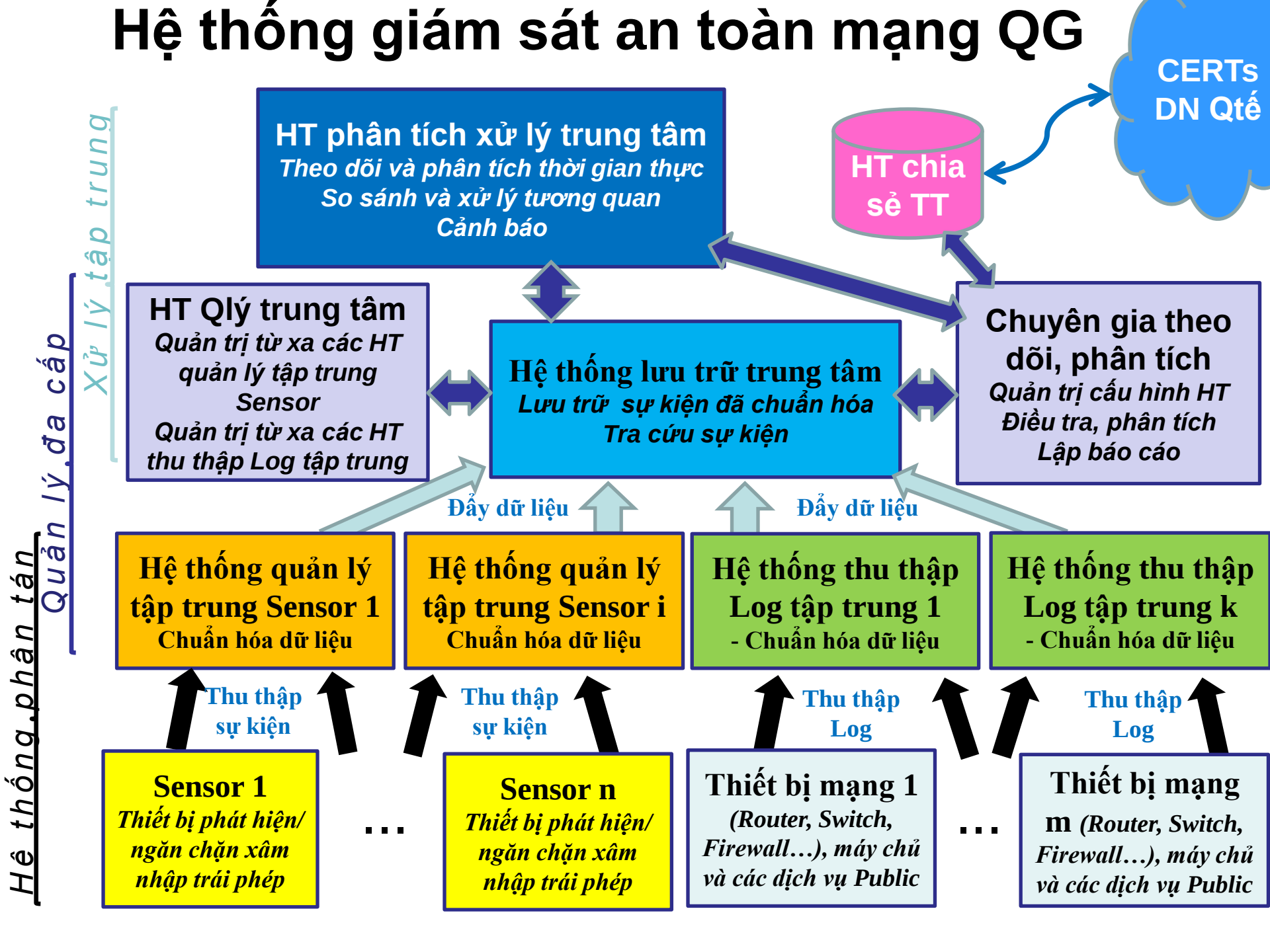
1. **Trang thiết bị và giải pháp phần mềm GSATM (một cấp hay nhiều cấp):**
   - **SOC + Lab + CSDL TT cảnh báo,**
   - **Mạng thu tin: sensors, thiết bị bảo vệ mạng, log-files,**
   - **Cần có các HT hỗ trợ như: HT xử lý tự động, HT nhận báo cáo, HT thu thập & phân tích thư rác, HT thu thập & phân tích mã độc, HT tạo chỉ số và tìm kiếm thông tin, HT quản lý và chia sẻ TT kỹ thuật chuẩn QT.**
2. **Đào tạo, duy trì đội ngũ chuyên gia giám sát, theo dõi, phát hiện, cảnh báo sớm và phản ứng với hiểm họa ATTT**

Hệ thống giám sát an toàn mạng Internet quốc gia

Trung tâm kỹ thuật an toàn mạng quốc gia

(VNCERT)

Hệ thống giám sát an toàn mạng QG



Hệ thống giám sát an toàn mạng Internet quốc gia

- **Nguyên lý:**
  - Không là công cụ do thám nội dung,
  - Hoạt động chủ động, xử lý số liệu lớn tự động hóa cao,
  - Cấu trúc mở, tích hợp theo chuẩn thông dụng,
  - Thu thập thông tin phân tán, quản lý đa cấp, xử lý tập trung,
  - Phối kết hợp thông tin quốc tế.
- **Phạm vi áp dụng:** Một số Bộ, ngành, tỉnh, thành và ISP
- **Khả năng hiện tại:**
  - Phát hiện nguy cơ APT, xâm nhập của Hacker,
  - Giám sát dịch vụ của hệ thống
  - Phát hiện hoạt động của mã độc, botnet
  - Phát hiện tấn công từ chối dịch vụ DoS/DDoS
  - Phát hiện các kỹ thuật của tin tặc sử dụng
  - Phát hiện các địa chỉ tấn công / bị tấn công
  - Tổng hợp toàn cảnh bức tranh ATTT

BÁO CÁO ĐỊNH KỲ ATTT

BÁO CÁO TỔNG HỢP KẾT QUẢ GIÁM SÁT

[redacted]

I. THÔNG TIN CHUNG

- **Thời gian:** 06/04/2015 đến 03/05/2015
- **Địa điểm:** [redacted]
- **Mục đích:** Giám sát các sự cố an toàn mạng cho một số dịch vụ cung cấp qua mạng của [redacted]
- **Thiết bị phát hiện:** Thiết bị phát hiện tấn công an toàn mạng chuyên dùng và hệ thống giám sát an toàn mạng quốc gia
- **Chế độ hoạt động:** Giám sát
- Tình hình an toàn thông tin: Nguy hiểm

II. TỔNG HỢP

- Thông qua kết quả giám sát từ 00:00 ngày 06/04/2015 đến 23:59 ngày 03/05/2015, Trung tâm VNCERT đã phát hiện và xử lý **53.127** sự kiện cảnh báo an toàn thông tin. Trong đó, đã phát hiện **8** hình thức tấn công điển hình và **188** kỹ thuật tấn công khác nhau.
- Hệ thống giám sát an toàn mạng Quốc gia tại VNCERT đã phát hiện ra dấu hiệu tấn công nguy hiểm của nhiều mã độc tấn công hệ thống. Bên cạnh đó, xuất hiện rất nhiều kiểu kỹ thuật tấn công nhằm vào dịch vụ Web có khả năng gây từ chối dịch vụ, thay đổi giao diện, đánh cắp thông tin… Đặc biệt là kiểu tấn công khai thác cài cắm shellcode lên hệ thống nhằm mục đích đánh cắp thông tin, chiếm quyền điều khiển,thay đổi giao diện của website [redacted]
- Hệ thống website [redacted] thường xuyên có các đợt dò quét từ các địa chỉ IP nước ngoài sử dụng các công cụ dò quét lỗ hổng phục vụ cho mục đích khai thác, tấn công gây nguy hại cho hệ thống.

Đề xuất và kiến nghị:

1

- Khẩn trương kiểm tra rà soát, kiểm tra đánh giá an toàn thông tin cho hệ thống máy chủ, rà soát các dịch vụ, phần mềm đã lỗi thời (sử dụng phiên bản cũ) và tiến hành cập nhật phần mềm ngay để đảm bảo an toàn.

III. CHI TIẾT

3.1 Tổng hợp các loại tấn công

a. Danh sách 5 kỹ thuật tấn công được phát hiện nhiều nhất

STT	Kỹ thuật tấn công	Số lượng cuộc tấn công
1	SERVER-APACHE Apache mod_rpaf x-forwarded-for header denial of service attempt	9683
2	PROTOCOL-DNS TCP inverse query overflow	199
3	SERVER-ORACLE database username buffer overflow	165
4	SERVER-WEBAPP redirect access	145
5	SERVER-WEBAPP content-disposition file upload attempt	121

b. Danh sách 5 cổng dịch vụ bị tấn công nhiều nhất

STT	Cổng dịch vụ	Số cuộc tấn công
1	80 (http)/tcp	19437 (7.91%)
3	53 (domain)/tcp	199 (0.08%)
2	3389/tcp	159 (0.06%)
4	445 (microsoft-ds)/tcp	148 (0.06%)
5	22233/tcp	68 (0.03%)

c. Danh sách một số hình thức tấn công điển hình

STT	Hình thức tấn công điển hình	Kiến nghị/ Đề xuất

2

3.2. Chi tiết các kỹ thuật tấn công điển hình

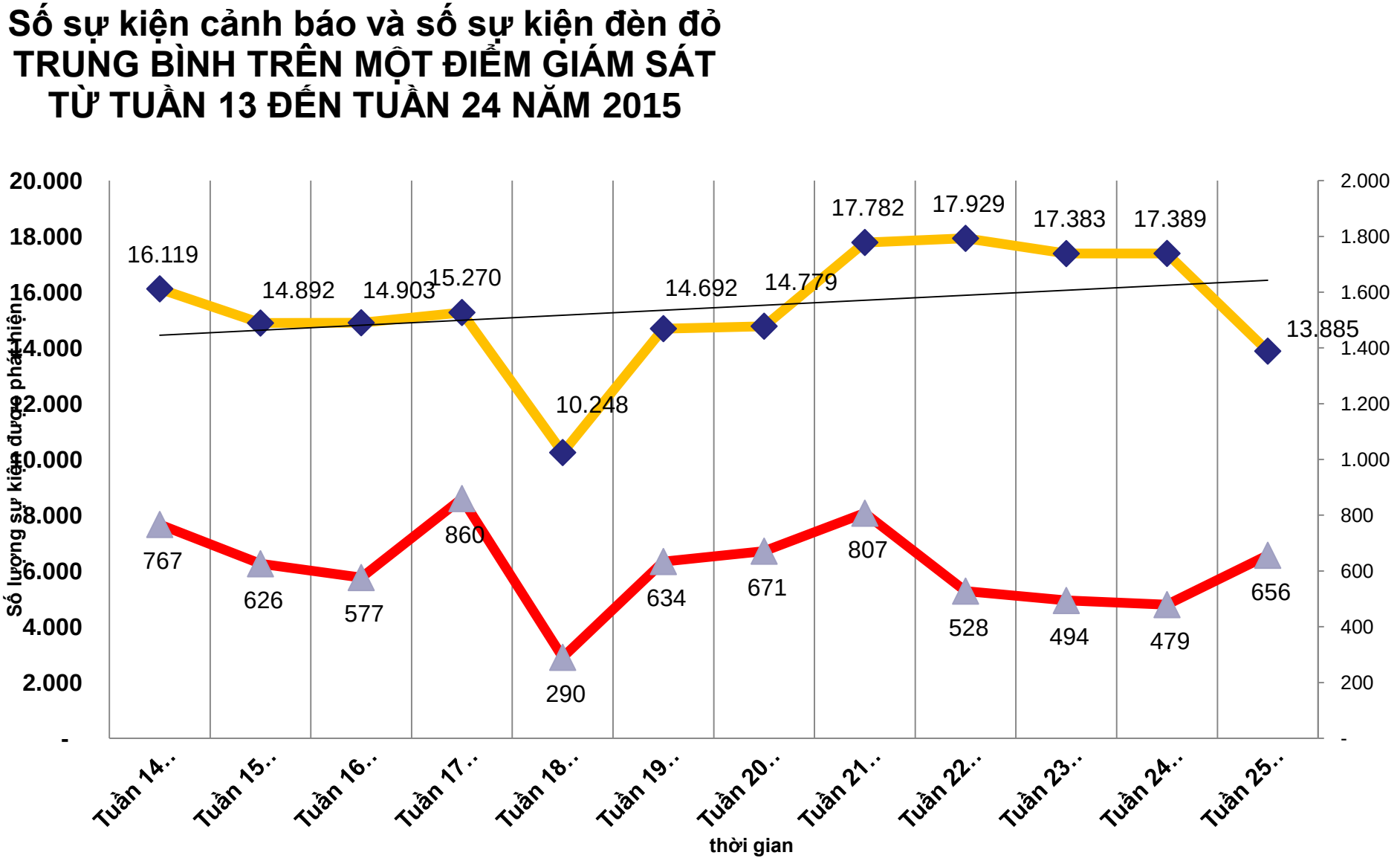
STT	Kỹ thuật tấn công	Thời gian phát hiện
1	**Tấn công ứng dụng Web (Web Application Attack)**	
1.1	SERVER-APACHE Apache mod_rpaf x-forwarded-for header denial of service attempt: Phát hiện dấu hiệu tin tặc khai thác lỗ hổng trong module "mod_rpaf x-forwarded-for" của Apache HTTP Server từ bên ngoài Internet. Nếu thành công, tin tặc có thể khởi tạo một cuộc tấn công DoS vào Website [redacted] Địa chỉ nguồn phát động tấn công: 66.249.82.146 66.249.82.155 141.0.8.140 82.145.216.239 168.235.194.60 37.228.108.15 82.145.211.61 216.163.188.222 223.25.196.254	2015-04-06 00:00:05

8

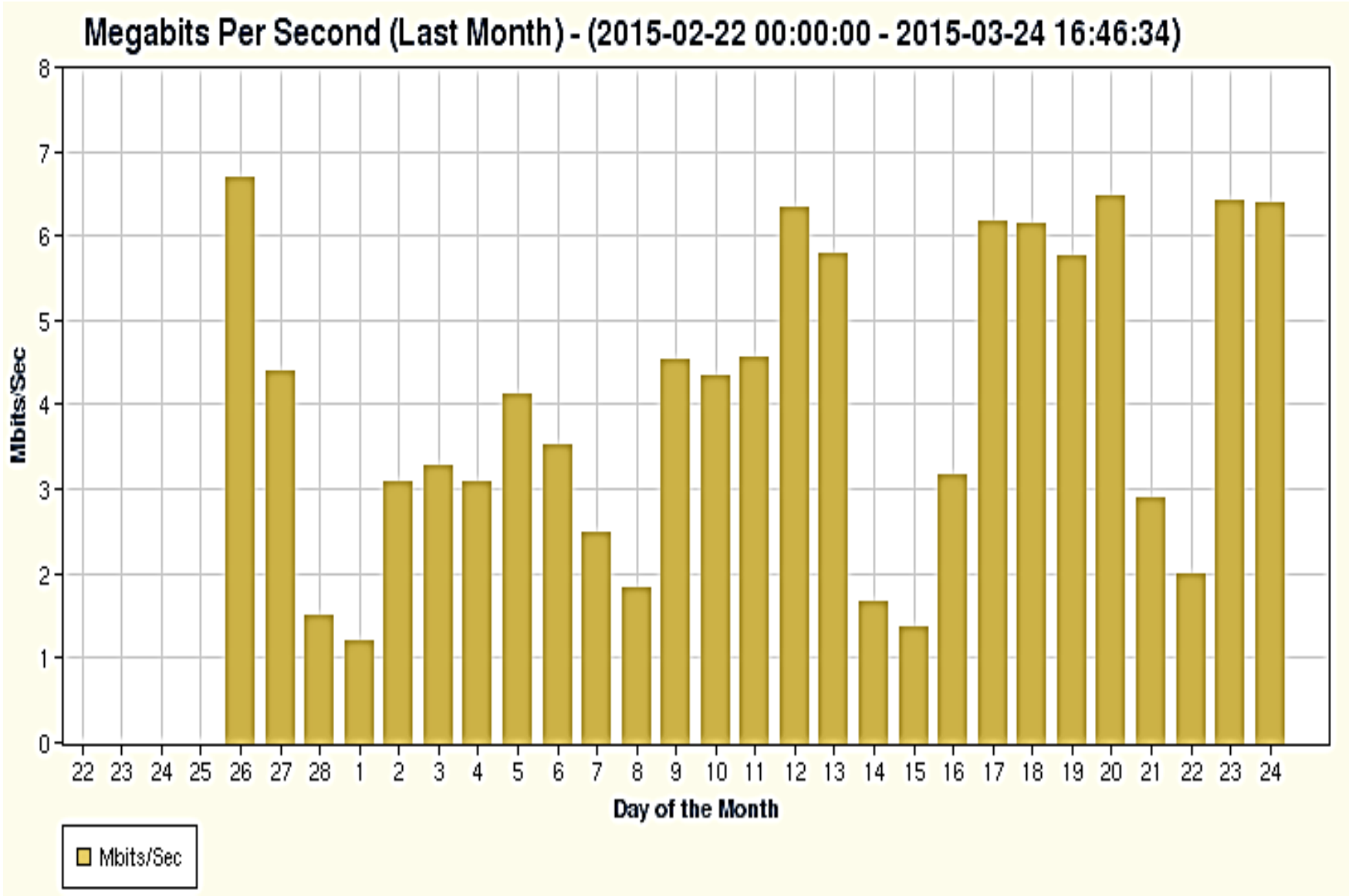
222.255.1.177
222.254.162.165
222.252.25.178
220.255.1.175
220.255.1.172
220.255.1.170
220.255.1.168
220.255.1.163
220.255.1.161
220.255.1.160
220.255.1.159
220.255.1.158
220.255.1.156
220.255.1.154
……

Địa chỉ đích bị tấn công:
10[redacted]23

Số sự kiện mức nguy hiểm cao (đèn đỏ)



Biểu đồ giám sát dịch vụ

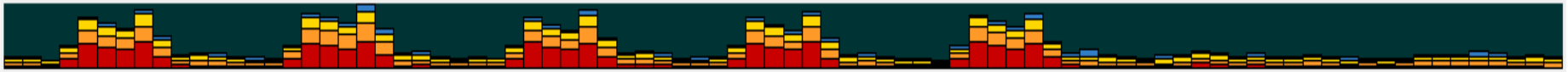


Giám sát phát hiện sự cố, nguy cơ APT

Start Time: 16 Mar 2015 00:00:00 ICT
End Time: 22 Mar 2015 23:59:00 ICT
Filter:
Inline Filter: No Filter
Verified Rules: No Rule

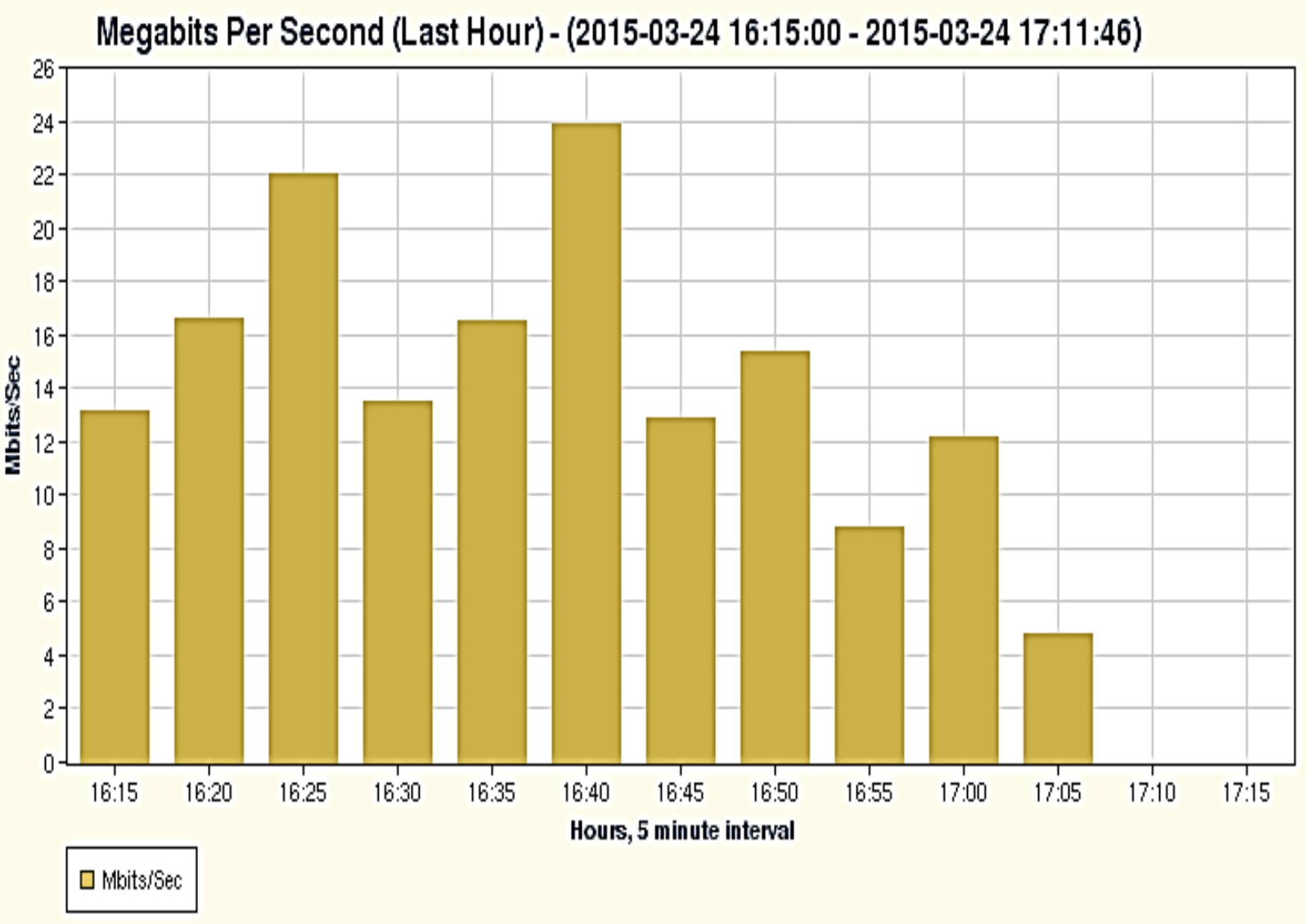
Very High: 308,532
High: 244,660
Medium: 205,368
Low: 104,937
Very Low: 0

Radar



End Time	Devi	Device	Name	Source Ad	Source Geo Country Nan	Source Po	Destinatio	Destination Geo Country	Destinatio	Priority
22 Mar 2015 23:56:49 ICT	12		SERVER-APACHE Apache mod_rpaf x-forwarded-for header denial of service attempt	168.63...	United States	30576	10.20....		80	9
22 Mar 2015 23:56:49 ICT	12		SERVER-APACHE Apache mod_rpaf x-forwarded-for header denial of service attempt	168.63...	United States	30576	103.22...		80	9
22 Mar 2015 23:56:46 ICT			Device Receipt Time from							5
22 Mar 2015 23:56:44 ICT	14		OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	192.16...		53215	103.24...		80	9
22 Mar 2015 23:56:40 ICT	7		HI_CLIENT_IIS_UNICODE	123.24...	Vietnam	20194	10.20....		80	4
22 Mar 2015 23:56:34 ICT	12		SERVER-MSSQL Microsoft SQL Server 2000 Server hello buffer overflow attempt	10.20....		51461	10.20....		1433	8
22 Mar 2015 23:56:34 ICT	12		SERVER-WEBAPP wrap access	116.98...	Vietnam	50327	10.20....		80	5
22 Mar 2015 23:56:33 ICT	14		BLACKLIST User-Agent known malicious user-agent string AutoIt	192.16...		2113	173.19...	United States	80	8
22 Mar 2015 23:56:31 ICT	21		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt	10.20....		53	123.30...	Vietnam	54397	7
22 Mar 2015 23:56:31 ICT	21		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt	10.20....		53	123.30...	Vietnam	3034	7
22 Mar 2015 23:56:29 ICT	12		APP-DETECT DNS request for potential malware SafeGuard to domain 360safe.com	103.22...		35451	8.8.8.8	United States	53	9
22 Mar 2015 23:56:28 ICT	12		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt	10.20....		53	10.140...		57602	8
22 Mar 2015 23:56:27 ICT	15		OS-WINDOWS Microsoft Windows UPnP malformed advertisement	192.16...		1025	239.25...		1900	6
22 Mar 2015 23:56:27 ICT	14		OS-WINDOWS Microsoft Windows UPnP malformed advertisement	192.16...		55819	239.25...		1900	6
22 Mar 2015 23:56:26 ICT	7		request to portal	123.30...	Vietnam	53891	10.20....		80	4
22 Mar 2015 23:56:25 ICT	11		OS-WINDOWS Microsoft Windows UPnP malformed advertisement	10.180...		1900	239.25...		1900	6
22 Mar 2015 23:56:19 ICT	20		OS-WINDOWS Microsoft Windows getbulk request attempt	134.14...	Germany	28360	103.28...	Vietnam	161	8
22 Mar 2015 23:56:17 ICT	7		SERVER-APACHE Apache mod_rpaf x-forwarded-for header denial of service attempt	82.145...	Iceland	45627	10.20....		80	7
22 Mar 2015 23:56:15 ICT	16		SERVER-WEBAPP calendar access	113.23...	Vietnam	18860	10.134...		80	5
22 Mar 2015 23:56:14 ICT	20		BLACKLIST DNS reverse lookup response to malicious domain .dataclub.biz - Win.Trojan...	8.8.8.8	United States	53	103.28...	Vietnam	50419	9
22 Mar 2015 23:56:14 ICT	12		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt	10.20....		53	10.140...		47013	8
22 Mar 2015 23:56:13 ICT	12		PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt	10.20....		53	10.140...		39941	8
22 Mar 2015 23:56:13 ICT	14		SERVER-APACHE Apache Struts wildcard matching OGNL remote code execution attempt	192.16...		53191	174.12...	United States	80	9

Biểu đồ giám sát lưu lượng phát hiện DoS/DDoS



Bức tranh tổng hợp Quý 1 -2015

- Trong quí I 2015 phát hiện 1.276.051 (IP) mã độc. Quý II có thêm trên 300.000 địa chỉ IP trong nước liên quan đến mạng mã độc, 783 địa chỉ IP của CQNN.

- Top 5 kỹ thuật được tin tặc sử dụng nhiều nhất là:

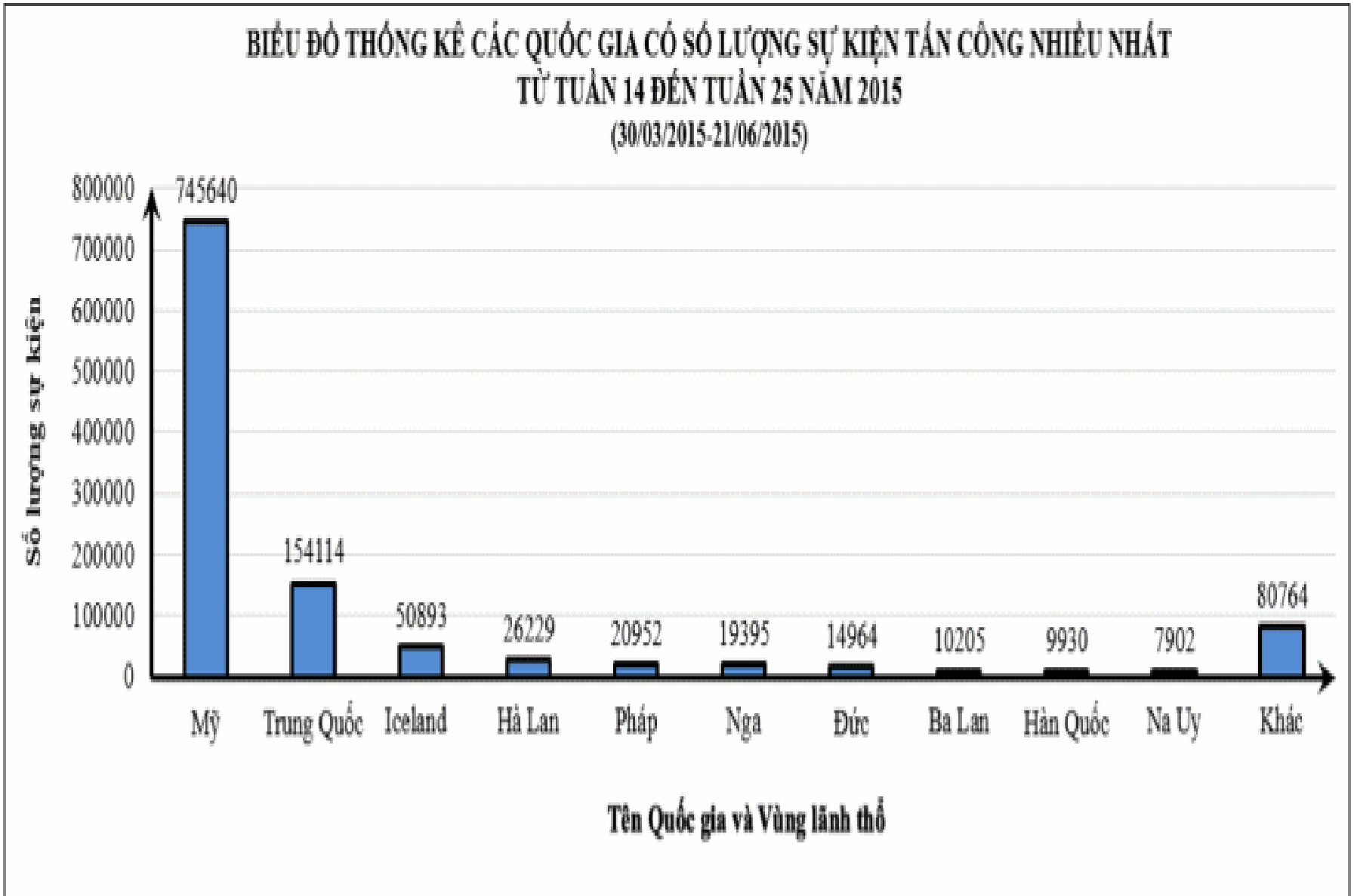
#	Tên kỹ thuật tấn công
1	OS-WINDOWS Microsoft Windows UPnP malformed advertisement
2	APP-DETECT failed FTP login attempt
3	PROTOCOL-DNS potential dns cache poisoning attempt - mismatched txid
4	INDICATOR-SCAN SSH brute force login attempt
5	SERVER-WEBAPP content-disposition file upload attempt

Bức tranh tổng hợp Quý 2 -2015 (2)

Danh sách 10 cổng dịch vụ bị tấn công nhiều nhất

STT	Cổng dịch vụ	Tỉ lệ (%)
1	80 (http)/tcp	21.55
2	53 (domain)/tcp	9.31
3	1900/udp	4.50
4	22 (ssh)/tcp	2.51
5	8080/tcp	1.57
6	443 (https)/tcp	1.53
7	21 (ftp)/tcp	1.12
8	1433 (ms-sql-s)/tcp	0.63
9	3389/tcp	0.43
10	25 (smtp)/tcp	0.35

Bức tranh tổng hợp Quý 1 -2015 (3)



Bức tranh tổng hợp Quý 1 -2015 (4)

Một số loại tình hình tấn công đặc biệt nguy hiểm điển hình trong quý II:

1. Tấn công thay đổi giao diện hệ thống website
2. Tấn công gây từ chối dịch vụ bằng cách sử dụng dịch vụ của Google cung cấp phục vụ cho việc tìm kiếm thông tin.
3. Tấn công vét cạn để phát hiện mật khẩu các dịch vụ điều khiển và chia sẻ tệp tin từ xa SSH và FTP
4. Tấn công nhằm tải trái phép các tệp tin điều khiển nguy hiểm (Shell) lên máy chủ Web
5. Mạng mã độc có máy chủ điều khiển sử dụng tên miền do các nước sau đây quản lý: Hoa Kỳ, Trung Quốc, Cộng hòa Ai-xơ-len, Hà Lan, Pháp và Nga.

Tấn công gây từ chối dịch vụ phân giải tên miền (DNS) được phát hiện có số lượng lớn và tăng nhanh trong hai tuần cuối tháng 6/2015, nhưng chưa gây tác hại lớn.

Hoàn thiện HT thống giám sát an toàn mạng Internet quốc gia (giai đoạn 2)

- Tăng cường năng lực xử lý trung tâm,
- Bổ sung năng lực phân tích mã độc, thư rác,
- Mở rộng khả năng tích hợp với các hệ thống giám sát của các tổ chức nhà nước, doanh nghiệp,
- Thiết lập hệ thống tiếp nhận báo cáo tự động theo chuẩn mới (STIX, TAXII,…),
- Xây dựng hệ thống tiếp nhận và chia sẻ thông tin tự động,
- Phối hợp với VNISA và các DN cùng đẩy mạnh phát triển và áp dụng công nghệ nội địa (dựa trên mã nguồn mở, tự phát triển) trong lĩnh vực giám sát và chia sẻ thông tin sự cố an toàn mạng.

Xin trân trọng cảm ơn

Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam,
Bộ Thông tin và Truyền thông
18 Nguyễn Du, Hà Nội, Việt Nam

Tel: (84) 90 343 4470

Fax: (84) 43 640 4425

Email: vqkhanh@vncert.vn